



**पंडित रविशंकर शुक्ल विश्वविद्यालय, रायपुर छत्तीसगढ़ भारत**  
**Pt. Ravishankar Shukla University, Raipur Chhattisgarh, India**  
Estd-1964 – recognized by UGC U/s 2(f) and 12 (B)  
**NAAC “A” Grade**

### **CRITERION-III**

#### **EVIDENCE(S), AS PER SOP**

<b>METRIC No. 3.4.5</b>	Number of research papers published per teacher in the Journals as notified on UGC website during the year
<ul style="list-style-type: none"><li>• Link landing to the paper/article</li><li>• Link to the journal website</li><li>• Screenshots of research articles clearly showing the title of the article, affiliation, name of the journal, year and authors name if the links and DOI number are not available</li></ul>	

**FACTORS OF MODERN SOCIAL STRATIFICATION: AN ANTHRO-SOCIOLOGICAL PERSPECTIVE**

**Dr. Shailendra Kumar** Assistant Professor, School of Studies in Anthropology, Pt. Ravishanker Shukla University, Raipur-492010 (Chhattisgarh), E-mail and Mobile: [shailverma48@gmail.com](mailto:shailverma48@gmail.com)

**Abstract :**

Indian societies and their structure have varieties on the basis of various social phenomena. Social stratification is one of them. Social stratification based on various criteria. In Indian society primary criteria of social stratification were Varna system, caste system and after that economic system. In the present context, Indian society has different criteria of stratification or in other word, we can say the whole world has criteria of symbol or image works as criteria of social stratification. How a family or individual live? How they eat? How they are arranging ceremonies? How they wear? These kinds of criteria explore their situation of an individual or family is society. In social theory, some post-modernism tried to explore how an image impact positivity and negatively in human society. Present research paper tried to explain new criteria's of social criteria, especially in the Indian context. Present research conduct from 142 respondents of 04 districts of Chhattisgarh state of India. Current research paper based on triangulation method include quantitative and qualitative research methods. Present research paper tried to show the relationship between various factors of social stratification and variable like age, education, economic status, social category, etc. Results of presents papers show old criteria or factors of social stratification are changed with modern life style and their symbol. And present results also show criteria of dominant caste are also working as present criteria for social stratification like economic status, education level, etc. Social stratification is a major subject area of social anthropology and sociology. Social stratification is indirect and sometime direct base of social category and social category is a direct base of reservation policy that why we want to know above changes of social stratification.

**Key word:** Indian society, Social stratification, Criteria of Social Stratification.

**I. INTRODUCTION**

Every society has social stratification in various levels. Generally, we know or define social stratification is a kind of social differentiation where by a group of members of society are grouped into social-economic strata. In modern western societies, social stratification is typically defined is term of social classes, social level and sometime that is defined as lower, middle and upper culture also. The origin of social stratification is based on the Varna system in Indian context. The Indian fan system is divided into four types that named *brahman*, *chatriya*, *vashya* and *sudra*. According to the Varna system every bonus are people have separated work like Brahmins works is worship, the chatriya is warrior etc.

Social Stratification is also related to the natural behavior of human society as a part of the competition. John Gowdy (2006) writes, "Assumptions about human behavior that members of market societies believe to be universal, that humans are naturally competitive and acquisitive, and that social stratification is natural, do not apply to many hunter-gatherer peoples." 'Gowdy (2006)'

Another concept, which is called "Concept of Dominant Caste" given by M. N. Shrinivas is also directing related with factors of dominant caste. The concept of 'dominant caste' was propounded by M.N. Srinivas. It was for the first time appeared in his essay on the social system of a Mysore village. According to M.N. Shrinivas "A caste may be said to be "dominant" when it preponderates numerically over the other castes, and when it also weilds preponderant economic and political power.,. A large and powerful caste group and be more easily dominant if its position in the local caste hierarchy is not too low." 'Srinivas (1995: 18)'

Dominant caste is a mixed concept which is related to caste, social hierarchy, process of sanskritization etc. It was in 1962 that M.N. Srinivas specified the following three characteristics of a dominant caste:

1. A caste dominates when it weilds economic and political power.

2. It has a high rank in caste hierarchy.
3. Numerical strength.

All above three factors is related to dominant caste. But in present era there are some other criteria are also include in above factors like education status, field of job and nature of job etc. like a family have not mJOR number of there member, they have low economic status and also have not any political power but if one family member have higher class degree or government job in his/her area than they known dominant caste

One other concept is post-modernism concept. According to one famous post-modernist Jean Baudrillard said present society is society of image and symbol. In present era a person knew what he or she wears? What he, she or they eat? Etc. All above criteria are criteria of social stratification also.

## II. RESEARCH AREA, METHODS AND TECHNIQUE

Data was collected in the present research by schedule, interview, case study etc. from 142 respondents. After receiving respondent's response, data were tabulated and analysis from SPSS-16. Some case studies were also collected from respondents. Present data collected from 142 respondents of 04 districts (Durg, Raipur, Rajnandganv and Balod) of Chhattisgarh state of India. Respondents are selected in current research work by purposive sampling.

## III. RESULT AND DISCUSSION

Society as a concept which is known as non- visible concept and their elements like social structure, social status, social stratification etc. all are non-visible but they are still present in our society. Human made above concept for sustaining their life and all above concept are totally psychologically. So naturally these are changeable with the and phenomena. The present study is also studying on social stratification and there factors which are made by human psychology is also changed by some factors like education status, economic status, residence, gender, marital status, age etc. Result and discussion part of the present research paper also tried to explore the relationship between modern or changeable factors of social stratification with various variables like age, education status, residence etc.

**Table No.1 Relationship between thinking about criteria of social stratification and age of respondents**

S. No.	Age (In Year)	Criteria of Social Stratification									
		Varna/Caste		Economic		Education		Living style/symbol		Total	
		N	%	N	%	N	%	N	%	N	%
1.	18-25	08	19.0	12	28.6	07	16.7	15	35.7	42	100
2.	26-35	11	26.8	02	4.9	15	36.6	13	31.7	41	100
3.	36-45	17	51.1	08	24.2	04	12.1	04	12.1	33	100
4.	45+	11	3.4	02	6.7	03	10.3	13	44.8	29	100
Total		47	32.4	24	16.6	29	20	45	31.0	145	100

**Figure No.1 Relationship between thinking about criteria of social stratification and age of respondents**

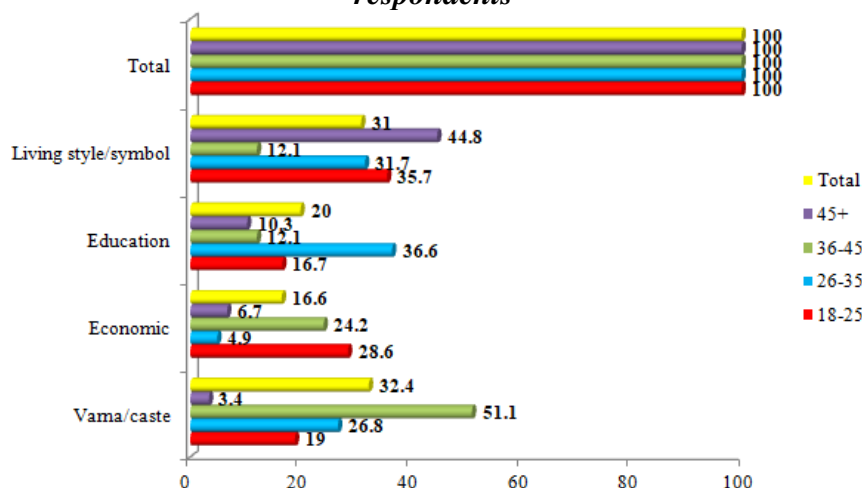


Table and figure no.1 Shows relationship between thinking about criteria of social stratification and age of respondents. Maximum 35.7 percent respondents which represent 18 to 25 year age group thought living style and modern symbol are major criteria of social stratification, 28.6 present respondents think economic status is a major criteria for social stratification. In 26 to 35 year age group, maximum 36.6 percent respondents response for education as a major part for social stratification. In 36 to 45 year age group, maximum 51.1 percent respondent's response Varna/caste is a bigger criterion in discussion of social stratification and respondents who are represent 45 years plus age group maximum 44.8 percent respondents are think living style and modern symbol are major criteria of social stratification in present era. According to the table, we can say all age group respondents thinking is same for modern criteria of social stratification.

**Table No.2 Relationship between thinking about criteria of social stratification and gender of respondents**

S. No.	Gender	Criteria of Social Stratification									
		Varna/caste		Economic		Education		Living style/symbol		Total	
		n	%	n	%	N	%	n	%	N	%
1.	Male	30	36.6	12	14.6	16	19.5	24	29.3	82	100
2.	Female	17	27.9	12	19.7	12	19.7	20	32.8	61	100
3.	Transgender	00	00	00	00	01	50	01	50	02	100
Total		47	32.4	24	16.6	29	20	45	31.0	145	100

**Figure No.2 Relationship between thinking about criteria of social stratification and gender of respondents**

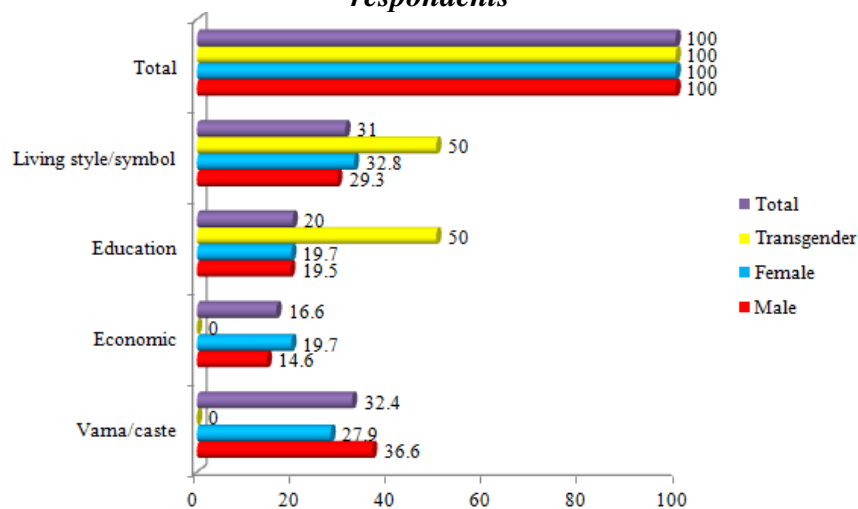


Table and figure no. 2 Shows relationship between thinking about criteria of social stratification and gender of respondents. According to the table maximum (36.6 %) male respondents think Varna/caste system is a major criteria of social stratification and other side maximum (32.8%) female respondents think living style is major criteria of social stratification in present era. In transgender, there thinking are divided in two parts, one for education and secondly present modern life style. So, we can say almost male and female, both informants think Varna/caste and modern life style both are major criteria for social stratification.

**Table No.3 Relationship between thinking about criteria of social stratification and social categories of respondents**

S. No.	Social Categories	Criteria of Social Stratification									
		Varna/Caste		Economic		Education		Living style/symbol		Total	
		N	%	n	%	n	%	N	%	N	%
1.	General	11	21.6	09	17.6	11	21.6	20	39.2	51	100
2.	Other Backward Caste	13	32.5	07	17.5	08	20	12	30	40	100
3.	Schedule Caste	12	40	06	20	04	13.3	08	26.7	30	100
4.	Schedule Tribe	11	45.8	02	8.3	06	25	05	20.8	24	100
Total		47	32.4	24	16.6	29	20	45	31.0	145	100

Figure No.3 Relationship between thinking about criteria of social stratification and social categories of respondents

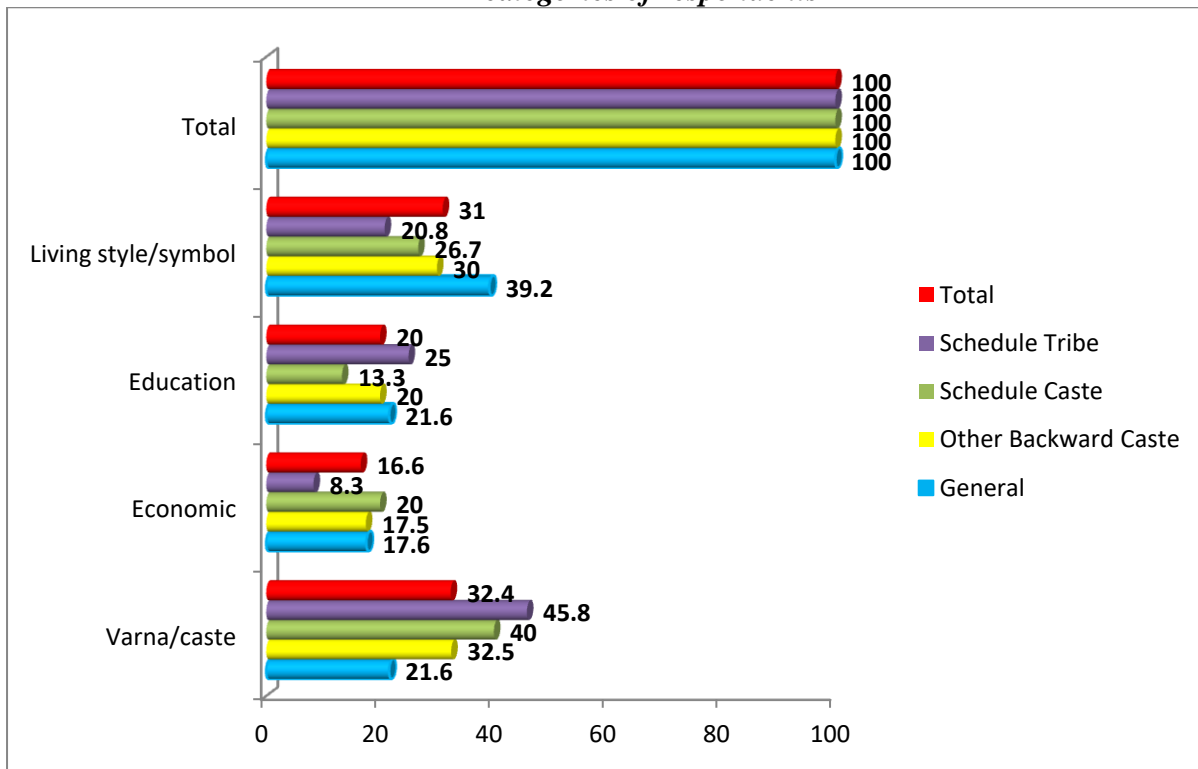


Table and figure no. 3 Shows relationship between thinking about criteria of social stratification and social categories of respondents. According to the table maximum (39.2 %) general, respondents think living style/symbol system is a major criteria of social stratification in present era. In other backward class, maximum (32.5%) other backward class respondents think Varna/caste is a major criteria of social stratification in present era. Maximum 40 percent, schedule caste also thinks Varna/caste is criteria of social stratification and 45.8 percent, schedule tribe are thought Varna/caste is a major criteria of social stratification and its change to living style/symbol system from Varna/Caste. So, we can say all social categories thoughts for major criteria of social stratification is mixed with living style/symbol system and Varna/caste.

Table No.4 Relationship between thinking about criteria of social stratification and education level of respondents

S. No.	Education Level	Criteria of Social Stratification									
		Varna/caste		Economic		Education		Living style/symbol		Total	
		n	%	n	%	N	%	n	%	n	%
1.	Illiterate	19	59.4	6	18.8	3	9.4	4	12.5	32	100
2.	Literate	12	50	5	20.8	2	8.3	5	20.8	24	100
3.	Primary	5	38.5	2	15.4	3	23.1	3	23.1	13	100
4.	Middle	3	27.3	1	9.1	4	36.4	3	27.3	11	100
5.	High and Higher	2	15.4	3	23.1	5	38.5	3	23.1	13	100
6.	Graduate	3	14.3	2	9.5	4	19.0	12	57.1	21	100
7.	Post Graduate	3	9.7	5	16.1	8	25.8	15	48.4	31	100
Total		47	32.4	24	16.6	29	20	45	31.0	145	100

Figure No.4 Relationship between thinking about criteria of social stratification and education level of respondents

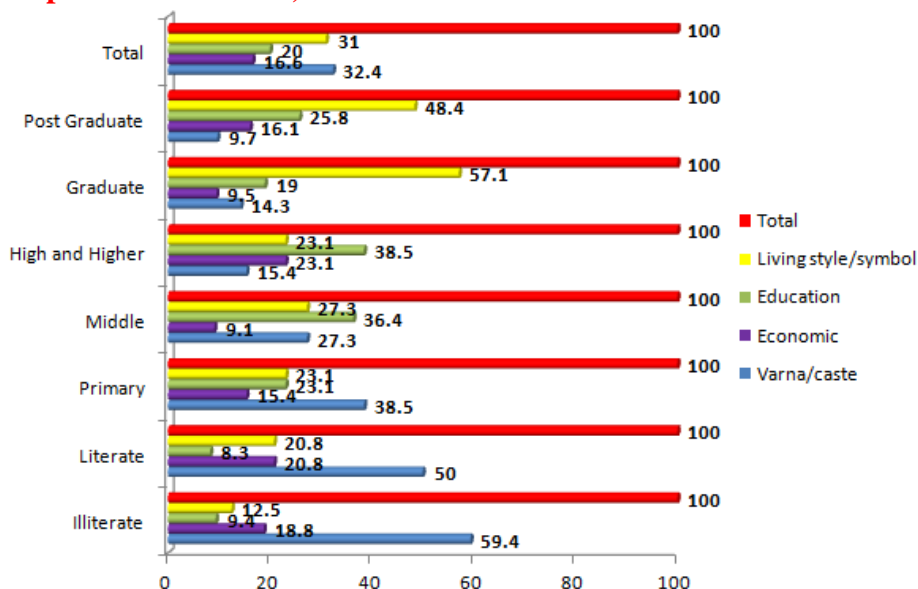


Table and figure no. 4 Shows relationship between thinking about criteria of social stratification and education level of respondents. According to the table maximum (59.4%) primary level education person think Varna/Caste system is a major criteria of social stratification and other side maximum (48.4%) postgraduate respondents think, living style is major criteria of social stratification in present era. So, we can say educated person think traditional thinking about a social stratification switch into Varna to life style. According to the table, we can say higher education is a factor for change mentality of peoples like traditional factors of social stratification are changed.

**Table No.5 Relationship between thinking about criteria of social stratification and residence of respondents**

S. No.	Residence	Criteria of Social Stratification									
		Varna/caste		Economic		Education		Living style/symbol		Total	
		N	%	N	%	N	%	N	%	N	%
1.	Rural	20	32.3	10	16.1	12	19.4	20	32.3	62	100
2.	Urban	27	32.5	14	16.9	17	20.5	25	30.1	83	100
	Total	47	32.4	24	16.6	29	20	45	31.0	145	100

**Figure No.5 Relationship between thinking about criteria of social stratification and residence of respondents**

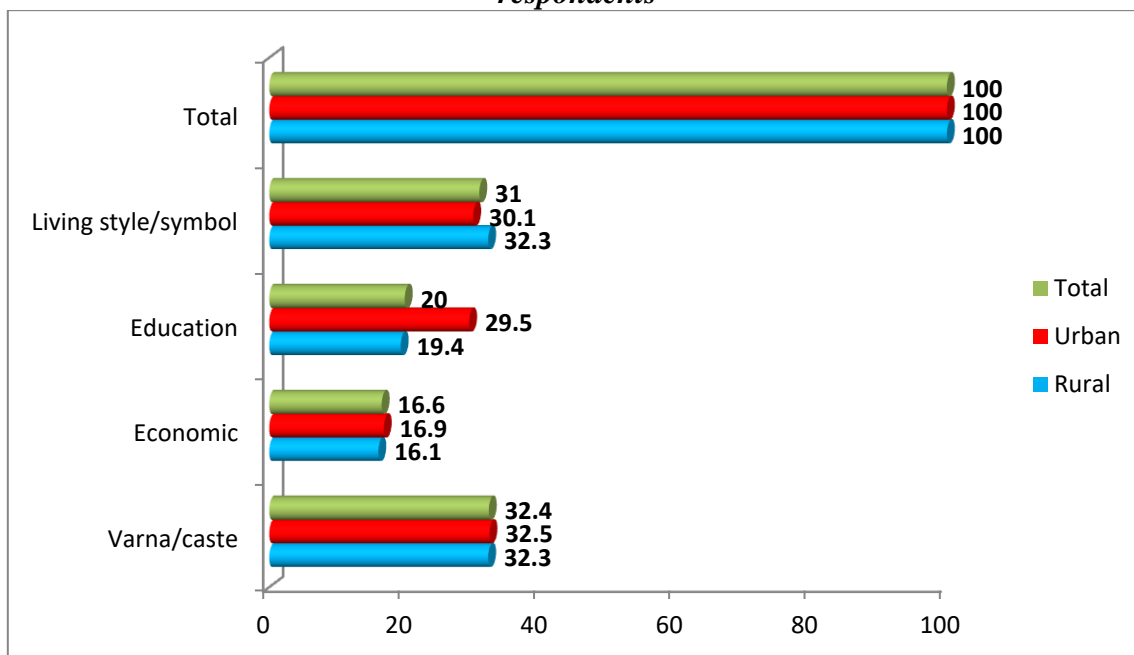


Table and figure no. 5 Shows relationship between thinking about criteria of social stratification and residence of respondents. Maximum 32.3 percent rural respondents thought living style and modern

symbol are major criteria of social stratification and same 32.3 percent respondent's response for Varna/Caste. In urban area almost same 32.5 percent urban respondents also thought Varna/Caste is a major criteria of social stratification and 30.1 percent rural respondent's thought living style and modern symbol are major criteria of social stratification. According to the table, we can say rural and urban respondents thinking is same for modern criteria of social stratification.

**Table No.6 Relationship between thinking about criteria of social stratification and economic status of respondents**

S. No.	Economic Status	Criteria of Social Stratification									
		Varna/Caste		Economic		Education		Living style/symbol		Total	
		N	%	N	%	n	%	N	%	N	%
1.	5000-10000	08	34.8	02	8.7	04	17.4	09	39.1	23	100
2.	10001-20000	07	38.9	02	7.1	06	21.4	13	46.4	28	100
3.	20001-30000	04	22.2	07	38.9	03	16.7	04	22.2	18	100
4.	30001-40000	11	33.3	08	24.2	06	18.2	08	24.2	33	100
5.	40001-50000	14	45.2	03	9.7	06	18.2	08	25.8	31	100
6.	50000+	03	25	02	16.7	04	33.3	03	25	12	100
Total		47	32.4	24	16.6	29	20	45	31.0	145	100

**Figure No.6 Relationship between thinking about criteria of social stratification and economic status of respondents**

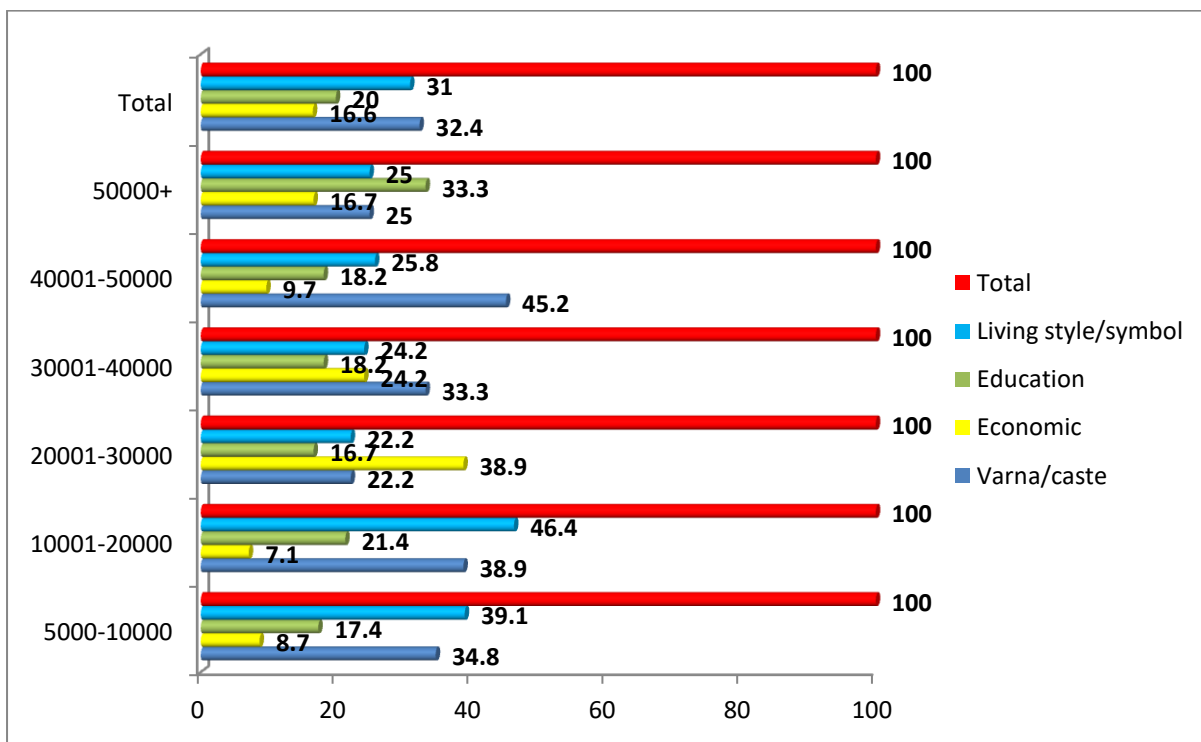


Table and figure no. 6 Shows relationship between thinking about criteria of social stratification and economic status of respondents. Maximum 39.1 percent respondents which represents 5000-10000 INR/month income group thought living style and modern symbol are major criteria of social stratification, 17.4 percent respondents think education status is a major criteria for social stratification. In 10001-20000 INR/month income group respondents, maximum 46.4 percent respondent's response for living style and modern symbol are major criteria as a major part of social stratification. In 20001-30000 INR/month income group respondents, maximum 38.9 percent respondent's response education level is a bigger criterion in discussions of social stratification and respondents who are represented in 30001-40000 INR/month income group maximum 33.3 percent respondents think Varna/Caste is a major criteria of social stratification in present era. Maximum 45.2 percent respondents which represents 40001-50000 INR/month income group thought Varna/Caste are major criteria of social stratification, 25.8 percent respondents think living style and modern symbol

are major criteria for social stratification. In 50000 INR/month income group respondents, maximum 33.3 percent respondent's response the living, education are major criteria as a major part of social stratification.

According to the table, we can say all income group respondents thinking are mix for which one is/are modern criteria of social stratification in present era, but according to responses we can say all respondents think Varna/Caste is not only single criteria as a factor for create social stratification.

#### **IV. CONCLUSION**

Social stratification known as a universal concept. Factors and causes of social stratification are differences in various societies, but it is universal. In historical perspective, about Indian Society, factors of social stratification are related to religious, caste and Varna system. At the present time all above factors are changing. Generally, these criteria are changing slowly but that is happening. Present research paper shows peoples of all regions, different education status, different social categories thought old criteria of social stratification like Varna and caste are changed or replace with life style and some modern images of lifestyle. Like Weber developed a multidimensional approach to social stratification that reflects the interplay among wealth, prestige and power. Results of the present research paper also show the concept of dominant caste and post-modernism is applicable in the present thought about social stratification. So we can say society is changeable and their elements are changeable and it's changing. We want to generate new concepts about society and their elements with the help of ole classical theories and concept.

#### **V. REFERENCES :**

- Gowdy, John (2006), "Hunter-gatherers and the mythology of the market", in Lee, Richard B. and Richard H. Daly (ed.). The Cambridge Encyclopedia of Hunters and Gatherers. Cambridge University Press, Cambridge pp. 391–393.
- Holborn, M. & Langley, P. (2004) "AS & A level Student Handbook", accompanies the Sixth Edition: Haralambos & Holborn, Sociology: Themes and perspectives, London: Collins Educational, London.
- Mondol, Pooja, (), "Dominant Caste: Characteristics and Criticism of Dominant Caste" available at <https://www.yourarticlelibrary.com/sociology/rural-sociology/dominant-caste-characteristics-and-criticism-of-dominant-caste/31940> site accessed on 01 August 2020.
- Macionis, Gerber, John, Linda (2010), Sociology, Ontario: Pearson Canada Inc., Toronto p. 243.
- Oommen, T.K. (1970), The Concept of Dominant Caste: Some Queries", available at *Contributions to Indian Sociology*, <https://doi.org/10.1177/006996677000400105>, site accessed on 7<sup>th</sup> September, 2020.
- Pradhan, A.K., Kumar, S. (2017), "Universalization to Localization: Sapnadev", International Journal of Research in Social Sciences, Vol.7, No.10, pp.1-6.
- Srinivas, M.N. (1995), The Dominant Caste and Other Essays, Oxford India Paperbacks, India.
- Verma, S. (2014), "Audhikikaran Ka Gramin Jeevan Shaili per Prabhav (In Hindi)". Scholarly Research Journal for Interdiscipli-nary Studies, Vol.II, No.XIV, pp.2058-2068.





# Assessment of culture medium without commercial ammonium nitrate for in vitro culture of industrially important plant species

Vikram Singh<sup>1</sup> · Ravishankar Chauhan<sup>2,3</sup> · Inderpal Kaur<sup>3</sup> · Afaque Quraishi<sup>2,3</sup>

Received: 18 June 2021 / Accepted: 1 September 2021  
© The Author(s), under exclusive licence to Springer Nature B.V. 2021

## Abstract

Ammonium nitrate (AN) is one of the major nitrogen sources of Murashige and Skoog (MS) medium. It is prohibited in various countries, including India because it is used in explosive manufacturing. Since MS is the most successful medium used for in vitro culture of many plant species, an attempt was made to achieve the composition of MS medium using ammonium hydroxide and nitric acid as an alternative to AN. This acid–base neutralization product AN, was further characterized by ATR-FTIR spectroscopy. Micropropagation of *Musa acuminata* cv ‘Grand Naine’ was tested using the alternate MS medium (AMS) and good mean shoot number was achieved. Shoot proliferation of *M. acuminata* cv ‘Grand Naine’ on AMS was significantly better than on normal MS medium. A 1-year production cycle of *M. acuminata* cv ‘Grand Naine’ was successfully accomplished with seven successive subcultures and rooting on AMS medium followed by satisfactory acclimation. To check broad cross-species utility of AMS for shoot proliferation, a range of species including *Chlorophytum borivilianum*, *Dalbergia sissoo*, *Dregea volubilis* and *Plumbago zeylanica* were tested. The in vitro shoot multiplication rate of these species on AMS was statistically not different from MS medium. These results indicate that AN can be replaced with ammonia hydroxide and nitric acid in preparing MS-based medium, without negatively affecting shoot proliferation/ rooting and it would be cost-effective too for micropropagation operations in comparison to commercially available MS medium.

## Key message

Commercial  $\text{NH}_4\text{NO}_3$  could be replaced with  $\text{HNO}_3$  and  $\text{NH}_4\text{OH}$  in tissue culture medium to follow the explosive regulations and was efficient for in vitro culture of various plant species.

**Keywords** Banana · FTIR · Micropropagation · Murashige and Skoog medium · Nitrogen source · Tissue culture

## Abbreviations

AN Ammonium nitrate  
BA 6-Benzyleadenine  
IAA Indole-3-acetic acid  
IBA Indole-3-butyric acid  
NAA Naphthalene acetic acid

AMS Alternate MS medium  
MS Murashige and Skoog medium

## Introduction

If a plant is recognized as a target of research for commercialization, conservation or for both purposes, understanding its growth requirements is of supreme importance (Moyo et al. 2011). The chemical composition of a plant tissue culture medium plays a significant role in the success of in vitro propagation (Phillips and Garda 2019). Plants fulfil their nitrogen requirements primarily in the form of nitrate ( $\text{NO}_3^-$ ) and ammonium ( $\text{NH}_4^+$ ) (Zhang et al. 2019). The sub-optimal nutrient medium may cause disorders or death of cultures (Nas and Read 2000; Iovinella et al. 2020). Nowadays, micropropagation technology is extensively applied in the production

Communicated by Ranjith Pathirana.

✉ Afaque Quraishi  
drafaque13@gmail.com

- <sup>1</sup> School of Studies in Life Sciences, Pt. Ravishankar Shukla University, Raipur 492010, India
- <sup>2</sup> National Center for Natural Resources, Pt. Ravishankar Shukla University, Raipur 492010, India
- <sup>3</sup> School of Studies in Biotechnology, Pt. Ravishankar Shukla University, Raipur 492010, India



# Contribution of strigolactone in plant physiology, hormonal interaction and abiotic stresses

Anita Bhoi<sup>1</sup> · Bhumika Yadu<sup>1,2</sup> · Jipsi Chandra<sup>1</sup> · S. Keshavkant<sup>1,3</sup> 

Received: 28 March 2021 / Accepted: 30 June 2021

© The Author(s), under exclusive licence to Springer-Verlag GmbH Germany, part of Springer Nature 2021

## Abstract

Strigolactones (SLs) are carotenoid-derived molecules, which regulate various developmental and adaptation processes in plants. These are engaged in different aspects of growth such as development of root, leaf senescence, shoot branching, etc. Plants grown under nutrient-deficient conditions enhance SL production that facilitates root architecture and symbiosis of arbuscular mycorrhizal fungi, as a result increases nutrient uptake. The crosstalk of SLs with other phytohormones such as auxin, abscisic acid, cytokinin and gibberellins, in response to abiotic stresses indicates that SLs actively contribute to the regulatory systems of plant stress adaptation. In response to different environmental circumstances such as salinity, drought, heat, cold, heavy metals and nutrient deprivation, these SLs get accumulated in plant tissues. Strigolactones regulate multiple hormonal responsive pathways, which aids plants to surmount stressful environmental constraints as well as reduce negative impact on overall productivity of crops. The external application of SL analog GR24 for its higher bioaccumulation can be one of the possible approaches for establishing various abiotic stress tolerances in plants.

**Keywords** Abiotic stress · Arbuscular mycorrhizal fungi · Crosstalk · GR24 · Phytohormones · Strigolactones

## Highlights

- SLs promote AMF symbiosis that fulfills nutrient requirement of plants.
- SLs interact with other phytohormones and affect the physiology of plant.
- SLs counteract the ill effects of abiotic stresses.
- SLs-related mutant plant possesses a number of impaired developmental processes.

## Introduction

Plants encounter multiple environmental stresses, time-to-time, in their entire lifecycle. These environmental stresses (such as biotic and abiotic) are culpable for crop deterioration and have become a hazard for sustainable farming (Abouqamar et al. 2017). To shield crops from various biotic stresses (such as diseases, pests, weeds, etc.), chemical solutions are known to be a well-established segment, while, only limited measures are available to counteract abiotic stresses (like drought, salt, heavy metal, nutrient deficiency, temperature, etc.) at various stages of growth and development. Plants have evolved various responses as a survival stratagem towards unfavorable circumstances by eliciting a series of signals for reprogramming of metabolic and genetic pathways (Banerjee et al. 2017). Phytohormones are inherent signaling molecules which harmonize with various stresses and boost-up the growth as well as development of plants by producing complex responses under such environmental circumstances (Choudhary et al. 2012). They act centrally and govern stress reactions even at minute concentrations such as  $10^{-5}$ – $10^{-6}$  mol L<sup>-1</sup> (Banerjee and Roychoudhury 2018). The standard plant growth regulators (PGRs) are composed mainly of abscisic

---

Communicated by Gerhard Leubner.

✉ S. Keshavkant  
skeshavkant@gmail.com; skeshavkant@prsu.nic.in

<sup>1</sup> School of Studies in Biotechnology, Pt. Ravishankar Shukla University, Raipur 492 010, India

<sup>2</sup> School of Life and Allied Sciences, ITM University, Raipur 492 002, India

<sup>3</sup> National Center for Natural Resources, Pt. Ravishankar Shukla University, Raipur 492 010, India



## Ethnobotanical Survey of Medicinal Plant Species used by Tribal Communities Around Katghora Tehsil of Korba District

Shriram Kunjam, G.S. Thakur and S.K. Jadhav\*

Department of Botany, Govt. V.Y.T. PG Autonomous College, Durg (Chhattisgarh)-491001 India  
Email - [shriramkunjam07@gmail.com](mailto:shriramkunjam07@gmail.com)

\*School of Studies in Biotechnology, Pt. Ravishankar Shukla University, Raipur (Chhattisgarh) - 492010 India  
Email - [jadhav9862@gmail.com](mailto:jadhav9862@gmail.com)

The traditional knowledge about plants and their uses in India is disappearing in recent years because the new generations of villagers migrate to cities for better life and jobs. Katghora tehsil is located at 22.50 N 82.550 E and has an average elevation of 293 meters above the sea levels in Korba district of Chhattisgarh State, India. The ethnobotanical information was obtained through interviews using semi-structured questionnaires of 32 traditional healers of 14 villages. Details of plant species, part(s) used and remedy formulations were also collected for the treatment of different health problems.

A total 52 species in 35 families and 51 genera were reported in the treatment of various health conditions. Family Fabaceae was dominant of the plant species documented. Roots (38%) were the most frequently used parts in preparing herbal remedies. Decoction and oral administration were commonly used method of herbal medicine preparation. 26 health conditions were treated using medicinal plants.

This study highlighted the closed relationship between people of the area and plant species especially when faced with frequent diseases. Many plant species are used as remedies for multiple ailments. However, most of the species used were collected in the surrounding of the villages.

**Keywords :** Ethnobotany, Tribal community, Katghora, Medicinal plants.

### INTRODUCTION

be used therapeutically, or can be used as raw material for chemical /pharmaceutical synthesis\* is classified as drugs.

## In Silico Approaches to Reveal Structural Insights, Stability and Catalysis of *Bacillus*-Derived $\alpha$ -Amylases Prior to Advance Lab Experiments

Nisha Gupta, Jai Shankar Paul\* and S. K. Jadhav

School of Studies in Biotechnology, Pt. Ravishankar Shukla University,  
Raipur 492010 (CG), India

\*Corresponding author. E-mail: [jaishankar\\_paul@yahoo.com](mailto:jaishankar_paul@yahoo.com)

**ABSTRACT:**  $\alpha$ -amylase is the most widely used Glycoside Hydrolase (GH) in industries for decades. It randomly cleaves the  $\alpha$ -D-(1, 4) glucosidic bonds of  $\alpha$ -polysaccharides (starch and glycogen) to release glucose and short-chain oligosaccharides. Substantial advances have taken place in research related to  $\alpha$ -amylases. However, bioinformatics study needs a little more exploration before conducting wet-lab experiments. We aimed to perform a comparative structure-function relationship study of 10 different *Bacillus*-derived  $\alpha$ -amylases using several computational biology tools. After aligning all the  $\alpha$ -amylases, 3D structures were made using the SWISS-MODEL. The accuracy and stability of the predicted models were validated via different web servers like Verify-3D, ERRAT, RMSD and ProSA. MolProbity and PROCHECK were used for mapping the residues in the most favored region of the Ramachandran plot. The Ramachandran plot reveals that >90% of the amino acid residues of the selected  $\alpha$ -amylase genes lie within the favored region. Our findings suggest that all the  $\alpha$ -amylases were stable as per the validation results we got. The study has revealed clear and concise structural related aspects. This paper will encourage the researchers to include and prioritize *in silico* work of  $\alpha$ -amylase genes to obtain more accurate outcomes. As the output obtained in this study via *in silico* tools reveals the structural peculiarity and more about the catalytic domain impression, it highly recommends incorporating such studies for better results. This approach will save efforts, costs and time for researchers.

**KEYWORDS:**  $\alpha$ -amylase gene; bioinformatics; computational biology; *in silico*; molecular modeling; structural insights.

### 1. INTRODUCTION

Amylases, notably  $\alpha$ -amylase, are one of the most crucial enzymes offering several industrial applications.  $\alpha$ -amylase (EC 3.2.1.1, 1,4- $\alpha$ -glucan-glucanohydrolase) is an endo-acting GH that catalyzes the breakdown of  $\alpha$ -D-(1, 4) glycosidic bonds present in starch, glycogen and other related polysaccharides to yield  $\alpha$ -anomeric hydrolytic products like glucose, maltose and limit dextrin.<sup>1–4</sup>  $\alpha$ -amylase belongs to GH13 which is the largest glycoside hydrolase (GH) family of clan H (group of GH13, GH70 and GH77 sharing common catalytic machinery) having 122,203 protein sequences followed by GH57 (3919 sequences), GH119 (38 sequences), and GH126 (1289 sequences) (<http://www.cazy.org/>, accessed on October 15th, 2021). Microorganisms serve as a precious source for producing extremely useful  $\alpha$ -amylases. *Bacillus* sp. (*Bacillus subtilis*, *Bacillus licheniformis*, *Bacillus cereus*, *Bacillus*

*amyloliquefaciens*, etc.) are readily used for large-scale enzyme production.<sup>4–8</sup> After proteases, significant contribution in the enzyme market is shared by  $\alpha$ -amylase by about  $\sim 30\%$ .<sup>9–11</sup> As  $\alpha$ -amylases have become an essential part of several industries (Fig. 1), it is very mandatory to focus on the qualitative aspects rather than just paying attention to quantitative production.

Computational biology or bioinformatics is considered as a boon for the scientific field. It has enabled various researchers in enzymology to predict the structural and catalytic peculiarities of novel  $\alpha$ -amylases after comparing them with the existing  $\alpha$ -amylases. It has provided several opportunities to obtain

Received: 1 September 2021

Accepted: 20 October 2021

Published: 26 November 2021

REVIEW

Open Access



# A comprehensive review on oleaginous bacteria: an alternative source for biodiesel production

Deepali Koreti, Anjali Kosre, Shailesh Kumar Jadhav and Nagendra Kumar Chandrawanshi\*

## Abstract

Due to continuously increasing population, industrialization, and environmental pollution, lead to generating high energy demand which suitable for our environment. Biodiesel is an alternative renewable fuel source. According to the feedstock of production, biodiesel has been categorized into four generations. The main disadvantage of the first and second generation is the raw material processing cost that the challenge for its industrial-level production. Oleaginous bacteria that contain more than 20% lipid of their cellular biomass can be a good alternative and sustainable feedstock. Oleaginous bacteria used as feedstock have numerous advantages, such as their high growth rate, being easy to cultivate, utilizing various substrates for growth, genetic or metabolic modifications possible. In addition, some species of bacteria are capable of carbon dioxide sequestration. Therefore, oleaginous bacteria can be a significant resource for the upcoming generation's biodiesel production. This review discusses the biochemistry of lipid accumulation, screening techniques, and lipid accumulation factors of oleaginous bacteria, in addition to the overall general biodiesel production process. This review also highlights the biotechnological approach for oleaginous bacteria strain improvement that can be future used for biodiesel production and the advantages of using general biodiesel in place of conventional fuel, along with the discussion about global policies and the prospect that promotes biodiesel production from oleaginous bacteria.

## Highlights

- Biodiesel from oleaginous bacteria and its importance are summarized.
- Biochemical pathways for fatty acid synthesis are described.
- Critical biotechnological approaches for bacterial strain improvement have been discussed.
- Sustainable biodiesel production, challenges, and future possibilities have been discussed.

**Keywords:** Biodiesel, Bio-harvesting, Feedstock, Oleaginous microbes, Transesterification

\*Correspondence: [chandrawanshi11@gmail.com](mailto:chandrawanshi11@gmail.com)  
School of Studies in Biotechnology, Pt. Ravishankar Shukla University,  
Raipur, Chhattisgarh, India



# A mini-review on electrotherapeutic strategy for the plant viral elimination

Smriti Adil<sup>1</sup> · Vikram Singh<sup>1</sup> · Afreen Anjum<sup>1</sup> · Afaque Quraishi<sup>1</sup>

Received: 19 December 2021 / Accepted: 23 February 2022  
© The Author(s), under exclusive licence to Springer Nature B.V. 2022

## Abstract

Plants have electrophysiological phenomena and are influenced by external electrical fields too. Plants have been studied for this property since the early 17th century. Stimulation in the physiological processes of plants in response to the electric field was observed in several studies. The use of electric current for phytosanitation purposes was known since the 19th century. This approach gained much attention only during the late 90s when electrotherapy applied to viral-stressed plants showed viral elimination possibilities. Concerning viruses, electrotherapy has shown an elimination rate greater than 50% over a varied range of voltage, time duration, and the plant part subjected to electro-exposure. Until now, the understanding of this mechanism is obscure, and assumptions included an increase in cell temperature causing denaturation of virus particles or its movement protein. Thus, a brief bibliographic research review would give directions for improving virus eradication from infected crops and producing virus-free plant stock material using an inexpensive and rapid electrotherapy technique in the future. Alongside, comprehensive studies are needed for a better understanding of the underlying mechanisms behind electrotherapy. Viral eliminations in plants via electro-exposure blended with other therapies such as thermotherapy, cryotherapy or chemotherapy are also discussed. The studies revealed that in some cases, electrotherapy alone is a more reliable method for producing virus-free plants, whereas, in others, the therapy combined with other virus-elimination techniques exhibited a higher virus-elimination efficiency rate.

**Keywords** Electrotherapy · Electric field · Phytosanitation · Therapy · Virus-free plants

## Electric fields and electrical phenomena in plants

In the past 180 years, much has been written on the relationship between life and electricity. Some animals and plants have been found to possess electric fields associated with them and are also influenced by electric fields applied from the outside (Briggs et al. 1926; Burr and Northrop 1939; Lund 1947a, b; Blinks 1949; Rosene and Lund 1953; Osterhout 1957; Schrank 1959). Unsurprisingly, living cells remain separated from one another through aqueous phases as well as from the external medium through lining membranes and maintain contrasting ionic composition from the

environment and from the other cells, too. The passage of merely a few ions in solutions could generate an electric field (Scott 1967). These electric fields can influence the physiology of plants. Therefore, since the 18th century, researchers have been attracted to the electrical phenomena in plants.

Over 130 years ago, both Burdon-Sanderson (1873) and Darwin (1875) demonstrated the existence of electrical signals in insectivorous ('motorized') plants. Next, Darwin and Darwin (1880), who worked chiefly on circumnutation, provided evidence for chemical signals in plants. Due to such compelling reasons, plant electrical activity was forgotten soon, focusing exclusively on chemical signals. However, research studies by Bose (1924) and later Pickard (1973) have gathered substantial evidence for the existence of electrical signals (action potentials (AP)) in a wide array of plants, apart from insectivorous or other 'motorized' plants. Despondently, the hope was very short-lived, and for many years, the phenomena surrounding electrical signalling in plants were forgotten. However, about 20 years later, a breakthrough in the field

---

Communicated by Ranjith Pathirana.

✉ Afaque Quraishi  
drafaque13@gmail.com

<sup>1</sup> School of Studies in Biotechnology, Pt. Ravishankar Shukla University, Raipur 492010, India



# A Review on Role of Nanomaterials in Bioconversion of Sustainable Fuel Bioethanol

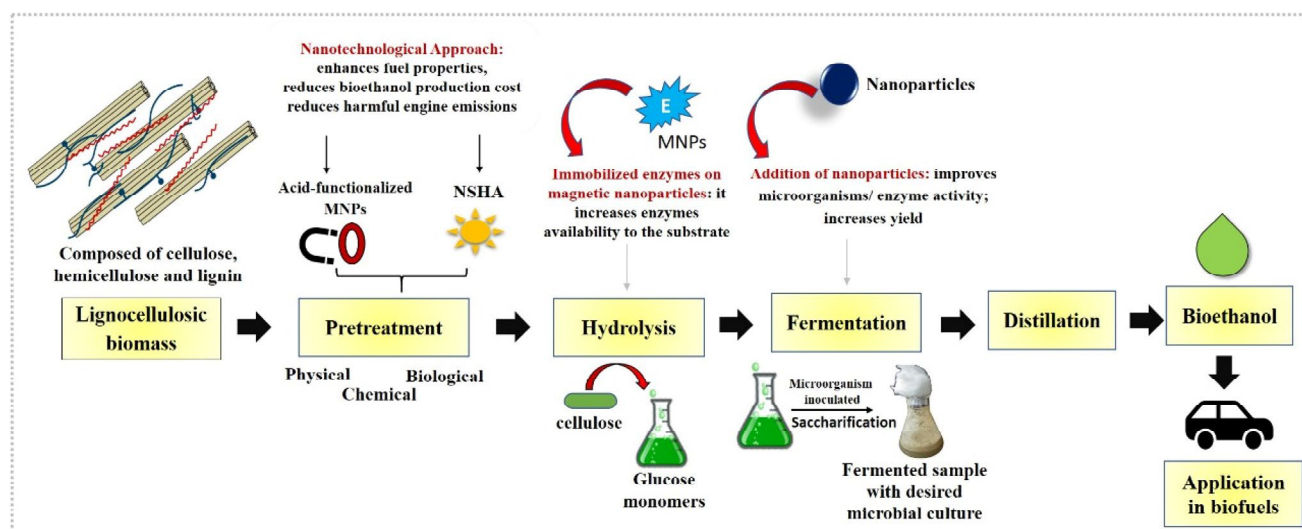
Dristi Verma<sup>1</sup> · Jai Shankar Paul<sup>1</sup> · Shubhra Tiwari<sup>1</sup> · S. K. Jadhav<sup>1</sup>

Received: 3 March 2022 / Accepted: 14 June 2022  
© The Author(s), under exclusive licence to Springer Nature B.V. 2022

## Abstract

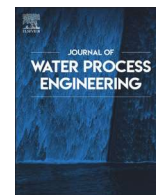
The growing consumption of fossil fuels like coal, petroleum, and diesel releases greenhouse gases that ultimately deteriorate the air quality. Moreover, fossil fuels pose serious threats like global warming, ocean acidification, unusual climate change and ecosystem fluctuation to the environment and human health. Biofuel is a feasible and sustainable alternative to overcome the limitations of fossil fuels. Among all the biofuels, bioethanol is currently in trend. The industrial-scale bioethanol production is a time-consuming process due to the non-availability of potential techniques and instrumentation. The pretreatment of rigid and recalcitrant lignocellulosic biomass to release fermentable sugars is crucial in the bioethanol production process. Conventionally it was done through physical, chemical and biological methods that demand high energy input, temperature, pressure, efficient organisms, expensive chemicals and solvents to loosen the compact structure of the raw materials. All these methods are sophisticated and expensive which results in the formation of harmful and inhibitory compounds and may also cause equipment corrosion. In this context, the introduction of nanotechnology in bioethanol production has shown improvement on a large scale. The small size, sturdiness and high surface to volume ratio of nanoparticles make them suitable for application in bioethanol production. Thus, the current review provides an insight into the role of nanotechnology in the various steps of the bioethanol production process. The paper will focus on the application of various nanomaterials and nanobiocatalyst in boosting the conversion of rigid lignocellulosic feedstock into fermentable sugar and facilitating the extent of reaction during fermentation for higher bioethanol yield.

## Graphical Abstract



**Keywords** Bioethanol · Fermentation · Immobilization · Lignocellulosic · Nanobiocatalyst · Nanoparticles

Extended author information available on the last page of the article



# Electrogenic potential of *Enterococcus faecalis* DWW1 isolated from the anodic biofilm of a dairy wastewater fed dual chambered microbial fuel cell

P.S. Parihar, S. Keshavkant<sup>\*</sup>, S.K. Jadhav<sup>\*</sup>

School of Studies in Biotechnology, Pt. Ravishankar Shukla University, Raipur 492 010, India

## ARTICLE INFO

### Keywords:

Microbial fuel cell  
Dairy wastewater  
*Enterococcus faecalis*  
DREAM assay  
Bioelectricity

## ABSTRACT

In this investigation, a novel electrochemically active Gram positive bacterium was isolated from the biofilm of a dual chambered microbial fuel cell (MFC) flooded with dairy wastewater (DWW), and was annotated as *Enterococcus faecalis* DWW1 following the 16 s rRNA sequencing. The dye-reduction based electron-transfer activity (DREAM) assay was used as a simple criterion for evaluation of electrochemical activity (0.43) in the candidate microbe. The electrochemical activity of the strain DWW1 was characterized using cyclic voltammetry (CV). CV studies revealed that the redox compound present in the DWW was exploited by the strain DWW1 for extracellular electron transfer towards anode. Current generation and chemical oxygen demand (COD) removal efficiencies of the strain DWW1 was examined following an optimum COD concentration of 1.440–1.665 kg COD/m<sup>3</sup> and anolyte pH of 8 (maximum current density 258 mA/m<sup>2</sup>; power density 144 mW/m<sup>2</sup>, 220 Ω; COD removal efficiency 53.5%; coulombic efficiency 10.89%). Such observations revealed the potential of *E. faecalis* DWW1 towards DWW remediation and energy generation.

## 1. Introduction

India is one among the larger producers of milk and dairy products. According to an estimate, annual milk production in India has now increased multi-fold, from 17 million tonnes (MTs, 1950–51) to 176.4 MTs (2017–18). Besides, being major power consumers, the Indian dairy industry, as a whole discharges approximately 300 MTs of wastewater, annually [1–3]. Dairy wastewater (DWW) produces a very persistent unpleasant foul smell apart from having higher organic load (complex carbohydrates, proteins, vitamins and lipids) and elevated concentrations of fermentable substrates [4]. Its improper disposal imposes severe ill impact on terrestrial and aquatic environments [3]. This voluminous discharge of DWW can be used for the production of energy (electrical), exploiting its organic load, for onsite usage, with simultaneous treatment of it.

Microbial fuel cell (MFC), an attractive renewable and sustainable green energy technology, can spontaneously convert the organic biomass into the electricity by exploiting microorganisms as natural biocatalysts [2]. The anode is one of the most important components of the MFC. Production of power in the MFC depends on the exoelectrogenic microorganisms that adhere on the surface of anode and catalyses the oxidation of organic matter into carbon dioxide, water and electrons

[4]. Carbon based various anode materials have been employed as conventional electrodes in the MFCs [5–8] but were suffered from a severe drawback of having lower galvanic potential [9]. On the other hand, nanostructured carbonaceous anodes and fine structured metal anodes require substantially complicated procedures for their preparation. Hence, these were classified as relatively unsuitable for large scale applications such as wastewater treatment. Therefore, greater attention has now been paid over electrodes that are actual current collectors. In this regard, metals are considered as suitable anode materials for the MFCs [10]. Various metal electrodes such as Cu(II), Ag(I), Mo(VI), Zn (II), etc., has been reported as a suitable surfaces for growth of microbial films [9–12].

Wastewaters are known to harbour rich diversity of microorganism that can be used as an inoculum for the MFC. Analyses of the anodic biofilms of the MFCs revealed a great bacterial diversity, however; did not divulged any specific trend in dominant members of anodophilic communities [13]. A large number of non-exoelectrogens are directly competing with exoelectrogens by propagating simultaneously with them, thus, decreasing the power output [4]. Several researchers have evaluated the performances of the MFCs using microbial consortium [1,14,15] but were failed to identify the roles of individual microorganisms, and mechanisms involved in power production. In order to

<sup>\*</sup> Corresponding authors.

E-mail addresses: [skeshavkant@gmail.com](mailto:skeshavkant@gmail.com) (S. Keshavkant), [jadhav9862@gmail.com](mailto:jadhav9862@gmail.com) (S.K. Jadhav).





# Elimination of BBTV via a systemic in vitro electrotherapy approach

Vikram Singh<sup>a</sup>, Smriti Adil<sup>b</sup>, Afaque Quraishi<sup>b,\*</sup>

<sup>a</sup> School of Studies in Life Sciences, Pt. Ravishankar Shukla University, Raipur, Chhattisgarh, India

<sup>b</sup> School of Studies in Biotechnology, Pt. Ravishankar Shukla University, Raipur, Chhattisgarh, India

## ARTICLE INFO

### Keywords:

Banana bunchy top virus  
Electrotherapy  
ISSR  
Indexing  
*Musa acuminata*  
Physio-biochemical

## ABSTRACT

Banana bunchy top virus (BBTV) is the most destructive etiological agent limiting banana cultivation areas globally. This study attempted BBTV elimination by traditional shoot-tip culture (control) and alternative shoot-tip + electrotherapy (treated) techniques. Shoot-tip culture from *Musa acuminata* cv. 'Grand Naine' infected sources were exposed to 100 mA electric current for different time intervals (20–60 min). Virus indexing (via PCR) and genetic fidelity (by ISSR assay) from the cultures were tested, alongside the physio-biochemical parameters. Exposure of electric current for less than 50 min was ineffective for BBTV elimination. Still, a rise in the duration from 50 min or more led to eradicating the virus from some explants. Elimination of BBTV was complete from 100 % of explants exposed to 100 mA for 60 min, as confirmed by lack of BBTV detection even at six months after acclimatization. In the control treatment, the maximum efficiency of BBTV elimination was 28 % after eight subcultures. On the other hand, improved survival % was observed in the treated culture. Moreover, homogenous ISSR patterns were there between the treated and the mother plant and similar physio-biochemical activities were seen in electro-exposed cultures and healthy ones. Thus, the study reports complete BBTV-elimination from banana with international compliances, for the first time, via electrotherapy while maintaining genomic template and biochemical stability.

## 1. Introduction

Banana (*Musa* spp.), belonging to the *Musaceae* family, is one of the most common crops in tropical and subtropical regions (Teycheney et al., 2005). Banana occupies fourth place, alongside rice, wheat and maize, in gross production value. More than 130 countries of Asia, America, Africa, Oceania, and the Pacific cultivate it (Pei et al., 2007; FAOSTAT, 2014). Banana production occupied approximately 5.6 million hectares of land globally (FAOSTAT, 2017). Banana bunchy top virus (BBTV) caused banana bunchy top disease (BBTD) is the most economically destructive of banana viral diseases as it can contribute up to 100 % yield reductions (Qazi, 2016).

BBTV comes under the genus *Babuvirus*, which belongs to the family *Nanoviridae* (King et al., 2011). The genome is comprised of at least six circular ssDNA segments (DNA 1–6) of approximately 1 kb each, singly encapsidated in isometric virions of 18–20 nm diameter, which are composed of a single coat protein of 20,000 Mr (Harding et al., 1991; Dietzgen and Thomas, 1991). BBTV is restricted to the phloem tissue

(Magee, 1940). The typical bunchy top symptoms include chlorosis of the leaf margin, narrowing and bunching of successive leaves with a 'Morse code' pattern, J-hook markings along the midrib of the leaves, and dark green streaking petioles (Dale, 1987). *Pentalonia nigronervosa* Coquerel (Hemiptera: Aphididae) transmits BBTV through a circulative and non-propagative mechanism in banana (*Musa* spp.) (Magee, 1927). *P. caladii* is also recognized as a competent BBTV vector (Bressan and Watanabe, 2011). Traditionally, bananas propagate vegetatively through suckers are shoots growing from a lateral bud on the parental rhizome (Ali et al., 2011). A series of non-professional cultivation practices, abiotic and biotic stresses significantly reduce the yield of vegetatively propagated bananas and plantains (Helliot et al., 2002; Matsumoto and Silva Neto, 2003). This process is not profitable commercially, as the multiplication rate of suckers is slow (15–20 per plant per year). Its success depends on clone selection, environmental conditions and cultural practices (Ali et al., 2011). Moreover, as explained by Lassois et al. (2012), the virus transmission is particularly an issue in the vegetatively propagated crops, like banana, because of

**Abbreviations:** CAT, catalase; POX, peroxidase; SOD, superoxide dismutase; ROS, reactive oxygen species; TEM, transmission electron microscope; MDA, malondialdehyde; BA, 6-benzyladenine; IAA, indole-3-acetic acid; IBA, indole-3-butyric acid; TAE, tris-acetate-EDTA; CTAB, cetyl trimethyl ammonium bromide; GTS, genomic template stability; ISSR, inter simple sequence repeat; LPX, lipid peroxidation.

\* Corresponding author.

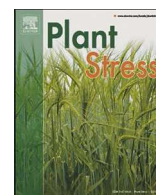
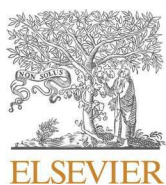
E-mail addresses: [vickys.singh11@gmail.com](mailto:vickys.singh11@gmail.com) (V. Singh), [15oct.sadil@gmail.com](mailto:15oct.sadil@gmail.com) (S. Adil), [drafaque13@gmail.com](mailto:drafaque13@gmail.com) (A. Quraishi).

<https://doi.org/10.1016/j.jviromet.2021.114367>

Received 9 April 2020; Received in revised form 20 September 2021; Accepted 18 November 2021

Available online 22 November 2021

0166-0934/© 2021 Published by Elsevier B.V.



## Review

# Gamma radiation: A potential tool for abiotic stress mitigation and management of agroecosystem

Priya Katiyar<sup>a</sup>, Neha Pandey<sup>a,b</sup>, S. Keshavkant<sup>a,\*</sup>

<sup>a</sup> School of Studies in Biotechnology, Pt. Ravishankar Shukla University, Raipur 492 010, India

<sup>b</sup> Kristu Jayanti College (Autonomous), Bengaluru, India

## ARTICLE INFO

**Keywords:**

Gamma rays  
Abiotic stress  
Reactive oxygen species  
Antioxidants  
Mutation

## ABSTRACT

**Context:** Being sessile, it is impossible for the plants to evade from the unfavourable environmental conditions prevailing due to various abiotic stresses like heat, salinity, drought, flood, heavy metals, and high radiance amongst many others. These abiotic stresses disrupt plant growth and limit crop productivity to a large extent globally. Crop plants need to acclimatize themselves in these unsuitable environmental and edaphic conditions utilizing their inherent biological mechanisms. Massive amount of pertinent researches have been done in the last few decades regarding utilization of gamma rays for improvement in traits, and management of agroecosystem by developing superior quality crops/ germplasms. It has been well established that the gamma rays promotes abiotic stress tolerance in plants at low doses (50–100 Gy). Gamma rays are also being widely used as mutation techniques in an attempt to raise abiotic stress tolerance and, disease resistant crop varieties. Furthermore, a better understanding of tolerance mechanisms induced by gamma rays will help in improving crop productivity under stress conditions. However, the potential mechanisms involved in this are still indefinable. This review illustrates general information about gamma ray, its dose dependant responses; beneficial effects and lethality, and also the potential mechanism(s) underlying the tolerance induction and performance enhancement of plants growing under various abiotic stress conditions.

**Objective:** To elucidate the role of gamma rays as a potential tool for stress mitigation and management of agroecosystem.

**Methods:** Gamma rays have been used quite differently by various researchers for alleviation of abiotic stress imposed responses in plants.

**Results and conclusions:** Application of gamma radiation has popularly been noticed to enhance nutrient uptake, modulate biosyntheses of numerous secondary key metabolites and osmolytes, and regulate various metabolic activities to engender tolerance against environmental stresses.

**Significance:** In most of the developing and under developed nations, owing to limited development in agro-management systems, abiotic stresses are seen to cause potential threats to growth and productivity of crops. Therefore, it is essentially to explore novel cost effective possibilities like use of low dose of gamma rays in crop plants for improvement in their performance during these rapidly changing climatic conditions.

## 1. Introduction

Crop plants encounter various abiotic stresses in their life span owing to global warming and climatic abnormalities which majorly limits their growth and productivity. Drought, temperature extremes, salinity and acidity of soil, light intensity, submergence, and anaerobiosis are dominant abiotic stresses amongst others, and are hostile to farming and the ecosystem (Wania et al., 2016). Crop plants of approximately 90% of

cultivable area are facing one or several of the above stresses (dos Reis et al., 2012), which results in approximately 70% losses in the yield of major food grains viz.; *Oryza sativa*, *Triticum aestivum* and *Zea mays*, and hence affecting food security (Tigchelaar et al., 2018). As per the report of FAO (2007), merely 3.5% land area has left untouched by any of the environmental constrain.

Amongst the enlisted abiotic stresses, salinity becomes the most stubborn one by escalating the salt concentration in the arable land

*Abbreviations:* Reactive Oxygen Species, ROS.

\* Corresponding author.

*E-mail address:* [skeshavkant@gmail.com](mailto:skeshavkant@gmail.com) (S. Keshavkant).

<https://doi.org/10.1016/j.stress.2022.100089>

Received 29 December 2021; Received in revised form 13 April 2022; Accepted 14 April 2022

Available online 16 April 2022

2667-064X/© 2022 The Author(s). Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

## Review Paper:

# Interaction between Nitric Oxide and Hydrogen Sulfide in Abiotic Stress Challenged Plants

Chandrakar Vibhuti<sup>1</sup>, Kumar Meetul<sup>2</sup> and Keshavkant S.<sup>1\*</sup>

1. School of Studies in Biotechnology, Pt. Ravishankar Shukla University, Raipur, INDIA

2. Directorate of International Cooperation, Defense Research and Development Organization, New Delhi, INDIA

\*skeshavkant@gmail.com

## Abstract

Nitric oxide (NO) and hydrogen sulfide (H<sub>2</sub>S) are two versatile gaseous molecules which play myriad roles in the growth and development of plants. They play an important role in signal transduction process in plants exposed to various environmental stresses. Signal transduction and various antioxidant strategies are vital for the management of abiotic stress imposed alterations in plants. These two secondary messengers neutralize the cell perturbations caused by stress-triggered over produced reactive oxygen species. Study of crosstalk between NO and H<sub>2</sub>S reveals the functional importance of proteins regulated during S-nitrosylation and S-sulphydration respectively, the two major signal-dependent post-translational protein modifications.

Also, NO and H<sub>2</sub>S decrease the toxic impacts of reactive species by triggering the signal transduction process, enhancing antioxidant enzymes, stimulating other signaling molecules and regulating the transcript levels of different stress-responsive genes. This review mainly emphasizes on the roles of NO and H<sub>2</sub>S in responses of plants to abiotic stresses and reveals the crosstalk involving NO and H<sub>2</sub>S in stress tolerance mechanisms.

**Keywords:** Hydrogen Sulfide, Nitric Oxide, Oxidative stress, Reactive oxygen species, Signal transduction, Signaling molecules, Stress tolerance.

## Introduction

Abiotic stresses such as heat, cold, salinity, drought, metal/loid, ultraviolet (UV) radiation etc. adversely affect the rate of germination, development and yield of economically essential crop plants and more than 50% yield losses are direct result of these stresses<sup>23,26</sup>. One of the most common phenomena taking place during the plant responses to these abiotic stresses is the oxidative explosion illustrated by the uncontrolled production of reactive oxygen species (ROS) such as singlet oxygen (<sup>1</sup>O<sub>2</sub>), hydroxyl radical (<sup>•</sup>OH), hydrogen peroxide (H<sub>2</sub>O<sub>2</sub>) and superoxide (O<sub>2</sub><sup>•-</sup>)<sup>41</sup>.

These elevated levels of ROS are severely injurious to plant cells as they directly oxidize the lipids, proteins and amino acids, inactivate enzymes and damage pigments and nucleic acids<sup>6,17</sup>. Condition of oxidative stress triggers a series of

detrimental impacts in plants including reduced germination score, biomass, root and shoot length, reduction in the number of leaves and leaf area, curling, wilting and necrosis of leaf blades, disturbed cellular osmotic balance, alteration in flow of energy, interference with minerals and ions uptake, losses in the mineral contents, inhibition in the rate of photosynthesis, chlorophyll biosynthesis, enzyme activities and cellular metabolism<sup>4,37</sup>. These damaging effects of oxidative stress hamper / hinder the growth and development and ultimately lead to death of plants.

The effectual control and rapid removal of ROS is essential for the proper functioning and survival of the plants. Thus, to counterbalance the environmental stresses, plants store multiple groups of compatible solutes such as proline, glycinebetaine, sugars etc. together with defensive enzymes and non-enzymatic components<sup>36</sup>. Enzymatic components include superoxide dismutase (SOD), catalase (CAT), peroxidases such as ascorbate peroxidase (APX), guaiacol peroxidase (POD) and glutathione peroxidase whereas flavonoids, glutathione (GSH), ascorbate (AsA) and  $\alpha$ -tocopherol constitute non-enzymatic components which protect the plants against ROS-induced oxidative damage<sup>28,35</sup>. Thus, understanding the mode of action of some of the molecules applied exogenously that can improve the defensive system of plants, could help in the mitigation of detrimental effects of abiotic stress-induced oxidative burst.

The two important gaseous molecules viz. nitric oxide (NO) and hydrogen sulfide (H<sub>2</sub>S) have crucial roles in several developmental processes of the plants and are also involved in their protection against various abiotic stresses<sup>29</sup>. In plants, both of these molecules are key signal messengers involved in various developmental processes such as seed germination and root organogenesis. Also, these signaling molecules elicit the antioxidant defensive mechanisms of plants to reciprocate the oxidative damage to cellular structures<sup>33</sup>. The interactions of NO and H<sub>2</sub>S have also been used in awarding plant tolerance to various stresses such as aluminum, arsenic (As), cadmium (Cd), salinity and heat in plants<sup>11,16,23,32,33</sup>.

Being a ubiquitous, gaseous bioactive molecule and a secondary messenger, NO has gained an increasing attention of scientific research in plant cells. It is well known that NO has significant role in the management of plant growth, development, interaction with other signaling molecules and in the adaptive responses to the abiotic stresses<sup>15</sup>. In addition, its role is evident in seed germination, root formation and elongation, fruit yield, photomorphogenesis,



# Lead induced-toxicity in vegetables, its mitigation strategies, and potential health risk assessment: a review

S. K. Kumbhakar<sup>1</sup> · R. Chauhan<sup>1,2</sup> · S. K. Jadhav<sup>1</sup> · A. Quraishi<sup>1</sup>

Received: 30 November 2021 / Revised: 25 January 2022 / Accepted: 8 February 2022

© The Author(s) under exclusive licence to Iranian Society of Environmentalists (IRSEN) and Science and Research Branch, Islamic Azad University 2022

## Abstract

In developing countries, rapid urbanization and industrialization cause heavy metal contamination, including lead (Pb). India is one of the most developing countries where anthropogenic sources are the chief generators of Pb contaminants. Mining, smelting Pb containing paints, papers, gasoline, and municipal sewage sludge enriched with Pb come in contact with a natural drain subsequently used for irrigation and cultivation of food crops and vegetables. Wastewater irrigated crops tend to cause contamination with Pb and thus pose a threat to the environment and human beings. The present review explored the anthropogenic sources of Pb and its bioaccumulation in vegetables and further consequences on human health. It also focused on reducing the phyto-bioavailability and accumulation of Pb in vegetables by using various improved strategies. Approaches like biochar application, microbes and their combination with biochar, co-remediation, co-cropping, nanoparticle-based method, biofilters, and fertilizers might hinder the subsequent transfer of Pb and other heavy metals in the food chain system and reduce the health risk.

**Keywords** Bioaccumulation · Contamination · Industrialization · Lead toxicity · Phyto-bioavailability

## Introduction

Globally, over 20 million hectares of land are considering soil-polluted sites where hazardous heavy metals and metalloids pollution are responsible for > 50% of lands contamination (Kumar et al. 2019). Now, soil and vegetable contaminations due to the accumulation of heavy metals is a prime environmental concern (Aslam et al. 2021). Lead (Pb) is one of the toxic heavy metals existing in many forms in the world. Apart from its nitrate, chlorate, and chloride salts, other inorganic salts are poorly soluble in water (WHO 2001). Various anthropogenic activities such as mining, metallurgy, industrial waste, pesticides transportation, construction, manufacturing, fossil-fuel combustion, incinerator emissions, and urban activities are responsible for elevating

Pb in soils (Yongpisanphop et al. 2017). Generally, Pb is stable, highly persistent, and has less solubility in soil solutions (Zhang et al. 2014; Kaur et al. 2018b). Therefore, it can be absorbed by vegetables through rhizosphere mediated solubility. Soils derived Pb contamination from various leaded-house paint, leaded-gasoline, some pressure-treated wood, and lead-arsenate pesticide (Schooley et al. 2008). Despite the phases out of leaded-gasoline and paint, beginning in the 1970s, historical Pb contaminations are persisted in urban, industrial, and high-traffic areas (McBride et al. 2013). Currently, due to low maintenance of vehicles resulting high emission has also significantly increased the production and consequent dry sediment deposition of Pb content (Guo et al. 2008). The by-products of municipal solid waste in urban areas of developing and developed countries are the biggest concern. Incineration is a method of disposing of municipal garbage, produces airborne metals that bind to particles or volatile metal components in the atmosphere (Sahu and Basti 2021). In the peri-urban ecosystem, industrial or municipal wastewater is mostly used for the irrigation of vegetables and other crops due to its easy availability, disposal problems, and the inadequacy of freshwater (Muchuweti et al. 2006). Water shortage is already a recurring issue in certain European nations (EEA, 2018), resulting in environmental

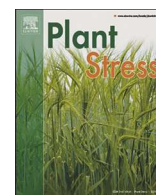
Editorial responsibility: Maryam Shabani.

✉ A. Quraishi  
drafaque13@gmail.com

<sup>1</sup> School of Studies in Biotechnology, Pt. Ravishankar Shukla University, Raipur 492 010, India

<sup>2</sup> National Center for Natural Resources, Pt. Ravishankar Shukla University, Raipur 492 010, India





# Mutagenesis: A coherent technique to develop biotic stress resistant plants

Anita Bhoi<sup>a</sup>, Bhumika Yadu<sup>b</sup>, Jipsi Chandra<sup>a</sup>, S. Keshavkant<sup>a,c,\*</sup>

<sup>a</sup> School of Studies in Biotechnology, Pt. Ravishankar Shukla University, Raipur 492 010, India

<sup>b</sup> School of Life and Allied Sciences, ITM University, Raipur, 492 002, India

<sup>c</sup> National Center for Natural Resources, Pt. Ravishankar Shukla University, Raipur 492 010, India

## ARTICLE INFO

### Keywords:

Biotic stresses  
Crispr/cas9  
Gene editing  
Physical and chemical mutagens  
Phytohormones  
Plant defense

## ABSTRACT

Modernization leads to frequent and remarkable alterations in the environmental factors which consequently affect the global agricultural productivity. Environmental factors can be broadly categorized into biotic and abiotic components. Biotic factors, which are represented by pests, bacteria, viruses, fungi, nematodes, etc., pose a severe threat to plants growth and development, thereby adversely impact the productivity. Taking this into consideration, crop improvement may prove to be a leading approach to ensure the sustainability of food and plant products. Modern agricultural practices rely upon agrochemicals and formulations for disease control that are responsible for causing environmental pollution and have detrimental effect on human health. Thus, development of stress resistance crop varieties must be a better approach in the current agriculture system. An array of genetic, biochemical and metabolic variations is required to produce such desirable alleles for appropriate crop improvement. Moreover, increasing genetic variation beyond natural variation is a crucial aspect of plant breeding programs. In connection, mutagenesis is one of the most prevalent tools to control plant stresses. To induce mutagenesis, techniques such as physical (gamma radiation, ultra-violet rays, etc.), chemical (ethyl methane sulfonate, methyl methane sulfonate, sodium azide, etc.) and gene editing (ZFN, TALEN, and CRISPR) are highly preferred by plant breeders. This review aims to provide an insight into mutation breeding techniques that facilitate the variable spectrum of agronomic and economic characters which is a prerequisite for successful crop improvement programs.

## 1. Introduction

A wide range of environmental factors are known to constantly affect plant's life. These factors are known to disturb growth, development, reproduction and overall productivity of crops. Environmental factors are broadly categorized into two groups: biotic and abiotic. Biotic factor comprises all the pathogens and plant parasites like fungi, bacteria, viruses, nematodes, and phytophagous insects and pests, while abiotic agent includes environmental cues, viz. cold, drought, heat, salinity, heavy metals, ultra-violet (UV) radiation, flood, etc., (Meena et al., 2017). Stresses occurring due to deterioration/damage by biotic components are considered as a serious threat to global food safety, as they cause pre- and post-harvest losses of crops. These are also known to trigger deprivation in the nutrient content which leads to death of plants. In general, surrounding environmental conditions dictate the type of biotic stress that may affect the plants (Gull and Kausar, 2019). For example, *Phytophthora infestans*, an Oomycete causes potato late

blight, which is one of the peak emerging biotic stresses for *Solanum tuberosum* (Coca-Morante and Tolin-Tordoya, 2013), while *Magnaporthe oryzae* has been reported to induce rice blast disease in *Oryza sativa* and reduces 10–35% of the yield (Li et al., 2019).

Plants possess intricate mechanisms to sense external signals and enable optimal responses to survive under such stress-inducing conditions. They establish a hierarchy of defense mechanisms to counter the effect of these stresses. Plants also possess damage repair mechanisms for stress neutralization, usually followed by removal of damaged tissues and restoration of tissue growth. One of the most common and effective defense mechanisms in plants is the hypersensitivity response (HR). Hypersensitive response causes rapid and localized cell death at precise site of pathogen infection (Wu et al., 2008). Endogenous low molecular weight phytohormones like ethylene (ET), abscisic acid (ABA), jasmonic acid (JA), along with salicylic acid (SA) predominantly regulate plant's protective response to various biotic stresses. Additionally, these hormones play a dominant role during pathogen infection (Fujita et al.,

\* Corresponding author at: School of Studies in Biotechnology, Pt. Ravishankar Shukla University Raipur 492010, India, Phone: 91 771 2263022, Fax: 91 771 2262583.

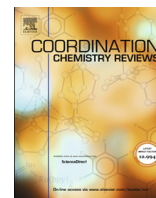
E-mail address: [skeshavkant@gmail.com](mailto:skeshavkant@gmail.com) (S. Keshavkant).

<https://doi.org/10.1016/j.stress.2021.100053>

Received 31 July 2021; Received in revised form 9 December 2021; Accepted 25 December 2021

Available online 26 December 2021

2667-064X/© 2021 The Author(s). Published by Elsevier B.V. This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>).



## Review

Nanoarmoured  $\alpha$ -amylase: A route leading to exceptional stability, catalysis and reusability for industrial applicationsNisha Gupta<sup>a</sup>, Esmil Beliya<sup>a,b</sup>, Jai Shankar Paul<sup>a,\*</sup>, S.K. Jadhav<sup>a</sup><sup>a</sup> School of Studies in Biotechnology, Pt. Ravishankar Shukla University, Raipur 492010, CG, India<sup>b</sup> Department of Botany, Govt. College, Bichhua, Chhindwara 480111, MP, India

## ARTICLE INFO

## Article history:

Received 13 August 2021

Accepted 1 April 2022

## Keywords:

$\alpha$ -Amylase  
Immobilization  
Nanobiocatalyst  
Nano-support  
Nanotechnology  
Reusability

## ABSTRACT

Enzymes are tremendous bio-product for nature whose absence can make a remarkable difference in the 21st century. Amylases have attracted a lot of industries due to their several applications.  $\alpha$ -Amylase (EC 3.2.1.1, *endo*-1,4- $\alpha$ -D-glucan glucanohydrolases) is a crucial enzyme for various industries. It selectively hydrolyzes the  $\alpha$ -1–4 glucosidic bonds of  $\alpha$ -polysaccharides to generate glucose, maltose and short-chain oligosaccharides. The only limitation associated with the applicability of enzymes is their non-reusability and instability in extreme conditions. Immobilization is a technique to offer easier recovery and several additional benefits to the enzyme by using appropriate support or carrier. Nanotechnology is the rapidly growing area of research dealing with the various biological disciplines at the molecular level. A duet of nanotechnology and immobilization can generate robust nanobiocatalyst explicating potential benefits. The most exciting properties of NMs is their high surface to volume ratio, easier fabrication and good dispersibility attracting the scientific community to utilize them for producing sturdy nanobiocatalysts. The present review evaluates the recent research and development undergoing in the field of nanoarmoured  $\alpha$ -amylase. It deals with the various NMs like metallic nanoparticles, nanostructured metal oxide, nanofibers, nanotube and graphene-based nanocomposites used as excellent support for  $\alpha$ -amylase immobilization along with its bottlenecks. Our study potentially delivers the measures for immobilizing  $\alpha$ -amylase on a nanosupport without compromising with its catalytic performance. There are prospective strategies highlighted in the review dealing with the obstacles hampering the  $\alpha$ -amylase immobilization procedure with several illustrations for easier understanding.

© 2022 Elsevier B.V. All rights reserved.

## Contents

1. Introduction	2
2. Types of immobilization	2
3. Nanotechnology: A modern era of biotechnology	3
4. Types of nanomaterials (NMs) used for immobilizing $\alpha$ -amylase	3
4.1. Metallic nanoparticles	8
4.1.1. Magnetic nanoparticles	8
4.1.2. Polymer coated magnetic nanoparticles	8
4.1.3. Non-Magnetic metallic nanoparticles	9
4.2. Nanostructured metal oxides (NMOs)	10
4.3. Nanocomposites	10
4.3.1. Graphene oxide nanosheets-flexible support for $\alpha$ -amylase immobilization	10
4.4. Nanotube-porous support for $\alpha$ -amylase immobilization	10
4.5. Nanofibers	10
4.6. Dendrimers	11
5. Functionalization of nanoparticles (NPs)	11

\* Corresponding author.

E-mail address: [jaishankar\\_paul@yahoo.com](mailto:jaishankar_paul@yahoo.com) (J.S. Paul).



# Production and Assessment of Stick-Shaped Spawns of Oyster Mushroom from Banana Leaf-Midribs

Priyanka Chouhan<sup>1</sup> · Deepali Koreti<sup>1</sup> · Anjali Kosre<sup>1</sup> · Ravishankar Chauhan<sup>1,2</sup> · S. K. Jadhav<sup>1</sup> · Nagendra Kumar Chandrawanshi<sup>1</sup>

Received: 25 June 2021 / Revised: 30 September 2021 / Accepted: 16 November 2021 / Published online: 15 April 2022  
© The National Academy of Sciences, India 2022

**Abstract** *Pleurotus ostreatus* is generally known as oyster mushroom that comprised in the category of edible mushroom. Various grain spawns were chiefly utilized for its commercial production. However, these spawns have several limitations such as high production cost and more contamination rate. Henceforth, the current study dealt with the development of stick-shaped spawns as an alternative to solid spawn. In the present study, banana leaf-midrib sticks were submerged in the liquid mycelium culture of *P. ostreatus* for the production of spawn. The efficiency of developed spawns were examined by the cultivation process and compared with the wheat spawn or mixture of wheat and cocopeat spawn. In term of mycelium accumulation stick spawn and wheat spawn show higher accumulation efficiency. The stick-shaped spawn exhibited significant mushroom production; its biological efficiency was 30.83% and 34.57% for both 1st and 2nd harvesting, respectively, when the stick-shaped spawn was used while it was comparably lowest for mixed spawns. Similarly nutritional content was also higher in stick and wheat spawn. Besides, it was cost-effective along with easier maintenance and handling. Thus, the banana leaf-midrib stick-shaped spawn developed in the present investigation

was comparable to wheat spawn with a promising alternative in industrial application and is reported the first time for mushroom cultivation.

**Keywords** Cost-effective · Lignocellulosic waste · Liquid submerged culture · Oyster mushroom · Stick spawn

## Introduction

The demand for mushrooms has increased due to its nutritional, medicinal, and pharmacological properties [1]. *Pleurotus ostreatus* is commonly known as oyster mushroom, which is one of the widely cultivated mushrooms worldwide followed by *Agaricus bisporus* [2]. It requires cheap and easy artificial conditions for its cultivation [3]. *P. ostreatus* well documented for lignocellulosic biodegradation potential and utilization as agro-waste management [4]. Biologically active molecules reported in this mushroom are different, such as exopolysaccharides,  $\beta$ -D Glucan, Lectin, Lovastatin, Ubiquitin-like protein, hydrophobin like proteins and Proteoglycans. This bioactive compounds exhibited various biological activity like; anticancer agent, antioxidant, antibacterial, anti-hypercholesterolic, antiviral, and anti-arthritic [5–7]. *P. ostreatus* can be cultivated in various lignocellulosic materials and agro-wastes such as banana leaves waste [8], eucalyptus waste [9], rice/wheat straw [10], date-palm leaves [11], and sugarcane bagasse [12]. Spawns are the viable material used for mushroom cultivation, and they are commonly known as mushrooms seeds [13]. The quality and production of mushrooms is directly influenced by the spawn used for its cultivation [14]. For the commercial cultivation of mushroom both solid and liquid spawns are frequently used [13]. Solid spawns are made via various grains such as

**Significance statement** Stick-shaped spawn produced by using submerged liquid mycelium culture. It unveiled high productivity, cost effective and easier to handle and is first report of using banana leaf-midrib for preparing stick-shaped spawns.

✉ Nagendra Kumar Chandrawanshi  
chandrawanshi11@gmail.com

<sup>1</sup> School of Studies in Biotechnology, Pt. Ravishankar Shukla University, Raipur 492 010, India

<sup>2</sup> National Center for Natural Resources, Pt. Ravishankar Shukla University, Raipur 492 010, India



# Rice Husk: A Potent Lignocellulosic Biomass for Second Generation Bioethanol Production from *Klebsiella oxytoca* ATCC 13182

Shubhra Tiwari<sup>1</sup> · Esmil Beliya<sup>1,2</sup> · Monika Vaswani<sup>1</sup> · Khushbu Khawase<sup>3,4</sup> · Dristi Verma<sup>1</sup> · Nisha Gupta<sup>1</sup> · Jai Shankar Paul<sup>1</sup> · Shailesh Kumar Jadhav<sup>1</sup>

Received: 8 July 2021 / Accepted: 3 January 2022 / Published online: 17 January 2022  
© The Author(s), under exclusive licence to Springer Nature B.V. 2022

## Abstract

The demand for an alternative source of energy is an imperative requirement of the current time. Second-generation biofuel (bioethanol) is capable of overcoming the problem of energy crises soon. Bioethanol production from agricultural by-products is an effective and sustainable approach. Bioethanol from agro-waste residues fulfil the energy demand and also reduce the pollution load of the environment. The present study was based on bioethanol production from cheap lignocellulosic agro-waste ‘rice husk’ by using *Klebsiella oxytoca* ATCC 13182 and standardization of production parameters and determining proficient pretreatment strategies. The present investigation reveals that bioethanol production can be enhanced significantly up to  $32.61 \pm 0.45$  g/L at pH 7, 36 °C after 48–72 h of incubation. The nitrogen supplementation like ammonium chloride, peptone, and beef extract increased bioethanol production up to  $38.95 \pm 0.65$  g/L,  $42.29 \pm 0.01$  g/L,  $43.23 \pm 0.71$  g/L respectively. Among the trace metals and ions analyzed, the highest bioethanol production ( $44.60 \pm 0.11$  g/L) and ( $35.13 \pm 0.01$  g/L) was obtained in  $Zn^{2+}$  and  $MgCl_2$  supplementation respectively. Out of all the pretreatment approaches analyzed, the acid and biological pretreatment (particularly with *Aspergillus niger*) had enhanced the bioethanol production ( $47.98 \pm 1.25$  g/L) up to 1.47 fold. Therefore, the current study will provide complete standardized parameters with an effective pretreatment strategy for utilizing lignocellulosic agro-wastes as an efficient and economical substrate for bioethanol production.

---

Shubhra Tiwari and Esmil Beliya contributed equally as first author.

---

✉ Jai Shankar Paul  
jaishankar\_paul@yahoo.com

<sup>1</sup> School of Studies in Biotechnology, Pt. Ravishankar Shukla University, Raipur, CG 492010, India

<sup>2</sup> Department of Botany, Govt. College, Bichhua, Chhindwara, Bichhua, MP 480111, India

<sup>3</sup> School of Sciences, MATS University, Raipur, CG 492002, India

<sup>4</sup> Department of Microbiology, AIIMS Raipur, Raipur, CG 492099, India





(Home.aspx)

# Journal of Ravishankar University

Pt. Ravishankar Shukla University, Raipur, Chhattisgarh

(Home.aspx)

PART-B

(SCIENCE)

ISSN: 0970-5910

HOME (HOME.ASPX)

EDITORIAL BOARD (EDITORIALBOARD.ASPX)

PAST ISSUES (PASTISSUES.ASPX)

FOR AUTHORS (FORAUTHORS.ASPX)

Submit Article (SubmitArticle.aspx)

search

## Article In HTML

# Screening Some Extracellular Enzymes of Wild Mushrooms from Pt. Ravishankar Shukla University Campus (AbstractView.aspx?PID=2022-35-1-6)

**R** Author(s): Srishti Verma (search.aspx?key=Srishti Verma), Visheshta Valvi (search.aspx?key=Visheshta Valvi), Kamlesh Kumar Shukla (search.aspx?key=Kamlesh Kumar Shukla)

Email(s): kshukla26@yahoo.co.in (mailto:kshukla26@yahoo.co.in)

Address: School of Studies in Biotechnology, Pt. Ravi Shankar Shukla University, Raipur (C.G.)

School of Studies in Biotechnology, Pt. Ravi Shankar Shukla University, Raipur (C.G.)

School of Studies in Biotechnology, Pt. Ravi Shankar Shukla University, Raipur (C.G.)

\*Corresponding author E-mail: kshukla26@yahoo.co.in

Published In: Volume - 35, Issue - 1, Year - 2022 (Issues.aspx?VID=35&IID=1)

Keywords: Amylase () Cellulase () Enzyme () Screening () Wild Mushroom ()



Cite this article:

Verma, Valvi and Shukla (2022). Screening Some Extracellular Enzymes of Wild Mushrooms from Pt. Ravishankar Shukla University Campus. *Journal of Ravishankar University (Part-B: Science)*, 35(1), pp. 42-52.



## Screening Some Extracellular Enzymes of Wild Mushrooms from Pt. Ravishankar Shukla University Campus

Srishti Verma<sup>1</sup>, Visheshta Valvi<sup>2</sup>, Kamlesh Kumar Shukla \*

<sup>1, 2, \*</sup> School of Studies in Biotechnology, Pt. Ravi Shankar Shukla University, Raipur (C.G.)

\*Corresponding author E-mail: kshukla26@yahoo.co.in (mailto:kshukla26@yahoo.co.in)

### Abstract:

Wild mushrooms are well known to produce wide range of bioactive metabolites and different types of enzymes. In this study 5 wild mushroom samples were collected which belongs to different groups. Samples were isolated and observed the culture characteristics, during the growth of mycelia many biochemical changes are known to occur, as a result of which enzymes are secreted extracellularly to degrade the insoluble materials into the substrates. Primary screening of extracellular amylase and cellulose were carried out by plate culture method in the GYP media with soluble starch to test the amylase activity and for cellulase, CMC (Carboxymethyl cellulose) plate assay was used. All the mushroom cultures differ in context of extracellular enzymatic activity. The activity of amylase enzyme was substantially higher in all the mushroom cultures. In the screening of cellulase enzyme two cultures were observed as positive. Present study suggests the capacity of these wild mushrooms in the production of biotechnologically useful enzymes with great industrial importance.

**Keywords:** Amylase, Cellulase, Enzyme, Screening, Wild Mushroom

### List of Abbreviations:

A-	:	After
AV	:	Average
B-	:	Before
CMC	:	Carboxymethylcellulose
DS	:	Dietary Supplement
E.E	:	Extracellular Enzyme
Gxm	:	Glucoonoxylomanan <sup>+1</sup> Variant
GYP	:	Glucose Yeast Peptone media
HEPA	:	High Efficiency Particulate Air
LAF	:	Laminar Air Flow
MM	:	Medicinal Mushroom
MW	:	MiliQ Water
PDA	:	Potato Dextrose Agar
pH	:	potential of Hydrogen
psi	:	Pounds per Square Inch
SD	:	Standard Deviation

### 1. Introduction

[ABOUT JOURNAL \(ABOUTJOURNAL.ASPX\)](#)[CONTACT US \(CONTACTUS.ASPX\)](#)[JRU \(PART-A\) \(HTTPS://JRU-A.COM/\)](#)[f](#) [G+](#)[\(HT](#)[GOOGLE.CO.IN/SCHOLAR?HL=EN&AS\\_SDT=0%2C5&JRNAL+OF+RAVISHANKAR+UNIVERSITY'&BTNG=\)](https://www.google.co.in/scholar?hl=en&as_sdt=0%2C5&jrnal+of+ravishankar+university&btng=)[\(Home.aspx\)](#)

# Journal of Ravishankar University

Pt. Ravishankar Shukla University, Raipur, Chhattisgarh

[\(Home.aspx\)](#)

**PART-B**

**(SCIENCE)**

ISSN: 0970-5910

[HOME ▾ \(HOME.ASPX\)](#)[EDITORIAL BOARD \(EDITORIALBOARD.ASPX\)](#)[PAST ISSUES \(PASTISSUES.ASPX\)](#)[FOR AUTHORS ▾](#)[Submit Article \(SubmitArticle.aspx\)](#)[MORE NEWS \(NEWS.ASPX\)](#)

## Article In HTML

# Species of Termitomyces (Agaricales) Occurring in Achanakmar Biosphere Reserve, Chhattisgarh (AbstractView.aspx?PID=2022-35-1-8)

Author(s): Srishti Verma ([search.aspx?key=Srishti Verma](search.aspx?key=Srishti+Verma)), Mahesh Tiwari ([search.aspx?key=Mahesh Tiwari](search.aspx?key=Mahesh+Tiwari)), R.V. Shukla ([search.aspx?key=R.V. Shukla](search.aspx?key=R.V.+Shukla)), Kamlesh Shukla ([search.aspx?key=Kamlesh Shukla](search.aspx?key=Kamlesh+Shukla))

Email(s): [kshukla26@yahoo.co.in](mailto:kshukla26@yahoo.co.in) (<mailto:kshukla26@yahoo.co.in>)

Address: School of Studies in Biotechnology, Pt. Ravi Shankar Shukla University, Raipur (C.G.)

Department of Botany C. M. D. College Bilaspur (C.G.)

\*Corresponding author E-mail: [kshukla26@yahoo.co.in](mailto:kshukla26@yahoo.co.in)

Published In: Volume - 35, Issue - 1, Year - 2022 (<Issues.aspx?VID=35&IID=1>)

Keywords: Agarics () Chhattisgarh () Diversity () Termites () Termitomyces ()



Cite this article:

Verma, Tiwari, Shukla and Shukla (2022). Species of Termitomyces (Agaricales) Occurring in Achanakmar Biosphere Reserve, Chhattisgarh. Journal of Ravishankar University (Part-B: Science), 35(1), pp.87-100.



View PDF

## Species of Termitomyces (Agaricales) Occurring in Achanakmar Biosphere Reserve, Chhattisgarh

Srishti Verma<sup>1</sup>, Mahesh Tiwari<sup>2</sup>, R.V. Shukla<sup>3</sup>, Kamlesh Shukla<sup>1\*</sup>

<sup>1</sup> \*School of Studies in Biotechnology, Pt. Ravi Shankar Shukla University, Raipur (C.G.)

<sup>2, 3</sup> Department of Botany C. M. D. College Bilaspur (C.G.)

\*Corresponding author E-mail: kshukla26@yahoo.co.in (mailto:kshukla26@yahoo.co.in)

### Abstract:

The Agarics as a group, occurs in a varieties of habitat. Some species exist in areas that are geographically separated, while some are known only from restricted areas and many species do seem to show preference for a certain type of natural habitats as well as for a particular substrate. An extensive exploration of wild mushrooms carried out from 2019 to 2021 at different forest ranges of Achanakmar Biosphere Reserve, Chhattisgarh India. Seven different species of *Termitomyces* namely *Termitomyces clypeatus*, *T. microcarpus*, *T. rabuorii*, *T. streatus*, *T. radicans*, *Termitomyces sp. -1*, *Termitomyces sp -2*, were found in edible form. So far members of the group which are found in soil, dung, plant debris, independently or in association with particular plant species has minimal documentation and germ-plasm collection from Chhattisgarh state, which is known for the largest forest land and the tribal population.

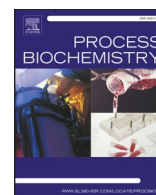
**Key Words:** Agarics, Chhattisgarh, Diversity, Termites, *Termitomyces*.

### 1. Introduction

Recent studies have diversified the existence of *Termitomyces* species in Tanzania, Uganda, of Africa and South - east and west India. The species of *Termitomyces* grow in association with termites were found to originate from tropical forests (Mosseboet al., 2017; Nobre and Aanen, 2010) like ancient Sal forests of Central – India. The genus is absolutely dependent on the possible symbiont relative termites. The number of fungus-farming Termites' species is reported approximately 165 in Africa, that belong to 11 genera (Kambhampati and Eggleton, 2000), which are underestimated considering on the novel termite species that has been already discovered (Makonde et al., 2013). There are about more than 30 *Termitomyces* species have been globally recorded (Tang et al., 2020; Sathiyi et al., 2020).

The Achanakmar Biosphere Reserve (ABR) accounts for the occurrence and distribution of many unexplored novel varieties of *Termitomyces* and Termites due to the richness of variety of tree species. Because the large tree canopies and huge amount of litter fall in ground surface provide suitable home to various species of both the biological agents. The Sal tree provides shelter for many more species of Termites to build their nests between ridges and furrow at various heights of tree trunks. Nevertheless, the Sal and many other native tree species return back substantial amount of leaf litter that protects soil by water run-off conserving soil moisture under which Termites and microorganisms feed upon and regulate the process of biodegradation, decomposition to humification.

In fact, the species of *Termitomyces* are linked with the economic importance of the termites as not a single species of *Termitomyces* could be grown independently (Kuja et al., 2014) so far. This is an indication of mutualistic relationship of *Termitomyces species* with an animal group to place the genus in advance position rather than primitive ectomycorrhizal



# Valorization of rice milled by-products (rice husk and de-oiled rice bran) into $\alpha$ -amylase with its process optimization, partial purification and kinetic study

Ankita Rathi<sup>a,1</sup>, Nisha Gupta<sup>a,1</sup>, Vani Dhruw<sup>a</sup>, Esmil Beliya<sup>a,b</sup>, Shubhra Tiwari<sup>a</sup>, Jai Shankar Paul<sup>a,\*</sup>, S.K. Jadhav<sup>a</sup>

<sup>a</sup> School of Studies in Biotechnology, Pt. Ravishankar Shukla University, Raipur, CG 492 010, India

<sup>b</sup> Department of Botany, Govt. College, Bichhua, Chhindwara, MP 480111, India

## ARTICLE INFO

### Keywords:

$\alpha$ -Amylase  
Agro-waste  
Rice bran  
Rice milled by-products  
Valorization  
Solid waste management

## ABSTRACT

A massive amount of waste is generated globally from agriculture sector annually that offers potential feedstock for biorefineries. Undoubtedly  $\alpha$ -amylase has become the backbone of starch-based industries. It is a crucial amylolytic enzyme possessing versatile applications. An expensive synthetic substrate that is non-eco-friendly and toxic is not sustainable enough for large scale enzyme production. The agricultural residues should be employed as they are the low-budget production medium with high yield and are eco-friendly. Thus, current study deals with the valorization of agricultural by-products for  $\alpha$ -amylase production. Two divergent rice-milled by-products (de-oiled rice bran and rice husk) were investigated to ascertain the best economical medium for  $\alpha$ -amylase production. The study deals with production, partial purification and kinetics analysis of  $\alpha$ -amylase from rice milled by-products by two bacteria (*Staphylococcus aureus* MTCC 3160 and *Bacillus subtilis* MB6). Out of all combinations, the best production ( $161.45 \pm 2.60$  U/mL) was obtained in DORB *S. aureus*. The  $K_m$  and  $V_{max}$  values of DORB *S. aureus* were 1.468 mg/mL and 34.722 mg/mL/min respectively. The study provides a roadmap for significant consumption of agricultural by-products. The study highly recommends researchers to explore some more agricultural residues as an eco-friendly and inexpensive medium to synthesize various bio-products under green technology.

## 1. Introduction

$\alpha$ -Amylase (1,4- $\alpha$ -D-glucan glucanohydrolase, EC 3.2.1.1) is a hydrolytic endoenzyme that preferentially cleaves the  $\alpha$ -1,4 linkages of the  $\alpha$ -polysaccharides resulting in the formation of short-chain oligosaccharides including maltose, maltotriose and limit dextrin [1].  $\alpha$ -amylase belongs to the family 13 of Glycoside Hydrolase (GH) which has a total of 131896 members (<http://www.cazy.org/GH13.html> as of May 11<sup>th</sup>, 2022). The microorganism sources are the most preferred for large scale  $\alpha$ -amylase production due to their easy and faster cultivation, simple nutritional requirement and ease of manipulation.  $\alpha$ -Amylase poses applications in several industrial sectors such as food, textile, laundry, pharmaceutical and paper [2–4]. The research related to  $\alpha$ -amylase production has widened in several aspects mainly focusing on cheaper and sustainable production. Agro-waste represents the potent feedstock

for manufacturing different value-added products such as hydrolytic enzymes. The foremost benefit of using these agro-residues is their cost-effectiveness, biodegradable nature, and relatively more native to the microorganism than synthetic media. Every year an enormous amount of agricultural by-products is generated. For their management, they are served as animal feed or sometimes dumped in a landfill or burned. The burning of these valuable feedstock releases various poisonous gases that raise serious environmental concerns. Therefore, instead of burning the leftover residue of agricultural fields can be utilized for industrial-scale bio-product formation. This approach is economical and sustainable.

Rice (*Oryza sativa* L.) is the staple food crop in many Asian countries. In India, it is grown in more than one-fifth of the total gross area of cropping and therefore contributes about one-fourth of total calorie intake [5]. India with a total production of 145,777MT in 2020 is the

\* Corresponding author.

E-mail address: [jaishankar\\_paul@yahoo.com](mailto:jaishankar_paul@yahoo.com) (J.S. Paul).

<sup>1</sup> These authors contributed equally as first author.



# The Indian Economic Journal

JOURNAL OF THE INDIAN ECONOMIC ASSOCIATION

Volume - 2

Special Issue, January 2022

## Accelerating Economic Growth : Trends and Way Forward

- ▶ Infrastructure Development
- ▶ Health Issues and Economic Growth
- ▶ Revival of Agriculture and Rural Area Development



## Indian Economy Moving from K and W to V: Post COVID – 19

Pragati Krishnan\*  
Ravindra Brahme\*\*

### ABSTRACT

The beginning of the year 2020 brought new challenges prior to the world economy because of the abrupt emergence of the Coronavirus pandemic. After the great depression of the 1930's, this COVID-19 pandemic indubitably gave the world economy the greatest set back ever before. Around 60% of the world's population is either under extreme lockdown or partial lockdown without providing a medical cure to the coronavirus disease, and also the economic growth has either slowed down or decelerated drastically across the countries to take away millions of livelihoods. According to the International Monetary Fund, the global economy is expected to contract rapidly by -4.9 percent in 2020 as a consequence of the pandemic, which was even worse than the financial crisis of 2008-2009. However, the Indian economy is not exceptional. It faced anomalous shock due to the outburst of the Covid-19 pandemic. The parlous state of the economy was as well witnessed even before the outbreak of the covid-19 all around the globe. With the diligent lockdown across the nation followed by global economic decline resulting in gradual disruption of demand and supply chains, the economy was facing a prolonged slowdown over the period of time. Thus there were a lot of lessons to be learnt from the Post COVID-19. The present paper is divided into 5 sections: Introduction, followed by Pre COVID-19 Growth, then the K and W factors and Recession. The fourth section discusses about Post COVID-19: A "V" Shaped Sustainable Recovery Path and lastly the conclusions.

**Keywords:** COVID-19, Indian Economy, Sustainable recovery

### 1. INTRODUCTION

The beginning of the year 2020 brought new challenges prior to the world economy because of the abrupt emergence of the Coronavirus pandemic (Tiwari,2020). After the great depression of the 1930's, this COVID-19 pandemic indubitably gave the world economy the greatest set back. Around 60% of the world's population is either under extreme lockdown or partial lockdown without providing a medical cure to the coronavirus diseases, and also the economic growth has either slowed down or decelerated drastically across the countries to take away millions of livelihoods (Sahoo and Aashwani,2020).

---

\*Research Scholar, SoS in Economics, Pandit Ravishankar Shukla University, Raipur,  
\*\*Professor, SoS in Economics, Pandit Ravishankar Shukla University, Raipur Chhattisgarh.



# The Indian Economic Journal

JOURNAL OF THE INDIAN ECONOMIC ASSOCIATION

Volume - 2

Special Issue, January 2022

## Accelerating Economic Growth : Trends and Way Forward

- ▶ Infrastructure Development
- ▶ Health Issues and Economic Growth
- ▶ Revival of Agriculture and Rural Area Development





## The Covid-19 and Reverse Migration in Rural Chhattisgarh

Pragati Krishnan\*  
Ravindra Brahme\*\*  
Hanumant Yadav\*\*\*

### ABSTRACT

In India in 2017-18 the total employment is 465.1 millions and informal employment is 421.9 million. With respect to Chhattisgarh the percentage share of informal workers in non-agriculture sector is 49.0 percent. Chhattisgarh stood in fourth place with Rajasthan being the first, followed by Punjab and Andhra Pradesh. The worldwide spread of Coronavirus has influenced the lives of millions around the globe. To constrain its effect, India executed a series of lockdown began from 25 March, 2020. Because of Covid-19 and its consequences Informal sectors are affected the most. Moreover, the informal workers face challenges on the most basic level of survival, owing to the economic lockdown which has left them stranded with no income and little savings. Thus, the sustainable development goal 08 which is related to decent work and economic growth and SDG 10 related to reduced inequalities deals in some or the other way to enhance the conditions of these migrants and to bring back their life on track. In this regard the purpose of the present work is to study how the COVID -19 has influenced the life of the migrant workers engaged in informal sectors in Chhattisgarh. For this, the study has been carried out keeping in mind the broad objectives of the socio demographic status of the reverse migrants in rural Chhattisgarh. Further the study tries to explore the occupational structure of the reverse migrants in their original source and also analyses the association of Covid-19 among gender reverse migrants and districts of rural Chhattisgarh. The results of the Chi- square test shows that there is a district wise significant association of Covid-19 pandemic in rural Chhattisgarh but with respect to gender reverse migrants there is so such significant association is found. Thus, the study came with the conclusion that Sustainable development strategies are incorporated in order to bring back the lives of the reverse migrant labors into a new normal, so that they were no longer be suffer from the problem of identity crisis.

**Keywords:** Covid-19, Reverse Migration, Rural Chhattisgarh, Sustainable development goals.

---

Research Scholar, SoS in Economics, Pandit Ravishankar Shukla University, Raipur, Chhattisgarh.

\*\*Professor, SoS in Economics, Pandit Ravishankar Shukla University, Raipur Chhattisgarh.

\*\*\* Professor, SoS in Economics, Pandit Ravishankar Shukla University, Raipur Chhattisgarh.



# The Indian Economic Journal

JOURNAL OF THE INDIAN ECONOMIC ASSOCIATION

Volume - 1

Special Issue, January 2022

## Accelerating Economic Growth : Trends and Way Forward

- ▶ Covid - 19, Global Developments and Their Impact on India
- ▶ Domestic Economic Situation in the Last few Years
- ▶ Policies for Exports and Trade
- ▶ Monetary Policy for Inflation and Growth
- ▶ Fiscal Policy for Growth



## Impact of Foreign Direct Investment on Manufacturing Industry after Make in India

Ram Pd. Chandra  
Ravindra Brahme  
Suresh K. Patel

### ABSTRACT

This paper focused on Impact of Foreign direct investment(FDI)on manufacturing industry after make in India program. "Make in India" is one of the multidimensional missions of India after globalization. Make in India mission is one such long term initiative which will help to realize the dream of transforming India into a manufacturing hub. FDI is regarded as a factor that drives economic growth. FDI has increased its importance by transferring technologies and establishing marketing and procuring networks for efficient production and sales internationally. An analysis of FDI inflow and impact on manufacturing sector components the data used for last eight year (during 2011-12 to 2018-19) based on economic survey 2018-19 indicate that there is positive correlation 0.724 exist between two variable. SPSS 'version 20' has been used for processing of the data; linier regression analysis, ANOVA Model and Durbin-Watson test (DWT) has been performed to test the relationship. The Calculated F-value 6.623 and p-value  $0.042 < 0.050$ , 5% level of significant and 1df, Study result shows that there is high correlation between manufacturing sector and FDI inflows. It means that there is significant change in effect of FDI on manufacturing industries from greater technology transfer and increased productive capacity. DWT value are  $0.617 < 2$ ; shows that positive relation between manufacturing sector and FDI. It is clear that, foreign direct investment is very essential in the development of manufacturing sector.

**Keyword:** Manufacturing Industries; Foreign Direct Investment; Manufacturing Industry; MCEGW; Regression Equation; ANOVA

**JEL Classification:** C12, C22, E01, E22, E23

### 1. INTRODUCTION

"Make in India" is one of the multidimensional missions of India after globalization. Make in India mission is one such long term initiative (Srivastava V., 2015) which will help to realize the dream of transforming India into a major source of job creation and manufacturing hub (Vijayaragavan T., 2015). "Make in India" campaign launched by prime minister (PM Narendra Modi) on 25<sup>th</sup> September 2014 at Vigyan Bhavan, New Delhi. Its symbol is a big lion equipped with a lot of wheels.

---

Asstt. Professor, Department of Economics, Govt. MLS PG College Seepat, Bilaspur (CG), India  
Professor, School of Studies in Economics, Pt. RSS University Raipur (CG), India  
Asstt. Professor, Department of Economics, L. S. Govt. College Tapkara, Jashpur (CG), India

Peer Reviewed Journal for M.Phil. , Ph.D. & Appointment of Teacher in Universities & College

ISSN : 2454-4655

VOLUME - 8 No. : 4, May - 2022

# International Journal of Social Science & Management Studies

Peer Reviewed & Refereed Journal

Indexing & Impact Factor 5.2



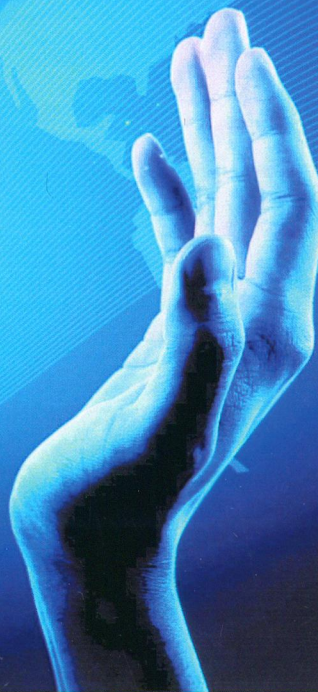
Radiant Group of Institutions, Jabalpur (M.P.), India  
Indian Economic Association  
& Social Science & Management Welfare Association



2 Days International Conference on  
Multidisciplinary Research in

**Education, Employment & Entrepreneurship Development**

Date : 1-2 May 2022, Venue : Jabalpur (M.P.), INDIA



**International Journal of  
Social Science & Management Studies**

## A Study on Women Empowerment in Rural Chhattisgarh

Prof. Ravindra Brahme

Professor (SoS in Economics) and Dean (Social Science)  
Pandit Ravishankar Shukla University, Raipur, Chhattisgarh

Pragati Krishnan

Research Scholar, SoS in Economics, Pandit Ravishankar Shukla University, Raipur, Chhattisgarh

**Abstract :-** Empowerment may be described as a process which helps to assert their control over the factors which affect their lives. Empowerment of woman means developing them as more aware individuals, who are politically active, economically productive and independent and are able to make intelligent discussion in matters that affect them. Women empowerment as a concept was introduced at the **International women Conference in 1985 at Nairobi**, which defined it as redistribution of social power and control of resources in favour of women. Women's empowerment is "a process whereby women become able to organize themselves to increase their own self-reliance, to assert their independent right to make choices and to control resources which will assist in challenging and eliminating their own subordination" (Keller and Mbwewe, 1991). Although empowering women is one of the most crucial concerns of the Millennium Development Goals of the United Nations. With this aim the broad objectives of the present study are to know the participation of rural women of Chhattisgarh in decision-making, to find out the extent of women empowerment in rural Chhattisgarh and to recommend measures for future implications. The results of the study shows that the total empowerment index for Mahasamund district, from all the four empowerment indices is 0.96. It shows that women in Mahasamund are empowered and their empowerment index indicates high empowerment. Similarly, the total empowerment index for the Uttar Bastar Kanker is 0.76. Again, it shows that women in the tribal district of Uttar Bastar Kanker are empowered and their empowerment index depicts a medium empowerment. The study concludes with the

suggestions that awareness generation programmes regarding the importance of empowering women should be implemented in the rural areas, so that the rural women could acquire knowledge about the economic, social, psychological and political aspects of empowerment. Also, it is the need of the hour to empower women so that they could participate in the decision-making aspects of the family. Rural women should be motivated to become independent and face challenges of their own. In this way we could reach the Sustainable development goal 5 focusing on gender equality by 2030.

**Keywords :-** Millennium development goals, Rural Chhattisgarh, Sustainable development goals, Women Empowerment

**Acknowledgement :-** The present paper is a part of the Ph.D. work and the authors would like to thank the Indian Council of Social Science Research (ICSSR), New Delhi for providing financial assistance in the form of Short-term doctoral fellowship.

**1. Introduction :-** Empowerment may be described as a process which helps to assert their control over the factors which affect their lives. Empowerment of woman means developing them as more aware individuals, who are politically active, economically productive and independent and are able to make intelligent discussion in matters that affect them.

Women empowerment as a concept was introduced at the **International women Conference in 1985 at Nairobi**, which defined it as redistribution of social power and control of



# The Indian Economic Journal

JOURNAL OF THE INDIAN ECONOMIC ASSOCIATION

Special Issue, December 2019

**ECONOMY OF  
CHHATTISGARH**



## Energy Disparity in Chhattisgarh: A District Level Analysis

Pragati Krishnan & Ravindra Brahme

### INTRODUCTION

There is a strong interconnection between energy and well-being of women in rural and informal sectors which has yet to be studied in the required depth. Women's energy needs go beyond the general uninformed concept that by and large they will be well served if cooking energy needs are addressed. While it is true that cooking energy needs are an important need, women also work as street vendors, construction workers, agricultural workers, small shopkeepers, and also work from home. As such, they need consistent electricity supply during the day, electricity for storing perishable goods, operating basic irrigation pumps, basic lighting of small shops, etc. Apart from energy requirements for functional needs, energy requirements for aspirational needs of women also have to be addressed if we are to build a society oriented towards gender parity.

Clean energy is presently being seen as a result of the means forward for reliable energy provide to thousands of people with investment and capability enhancements set to continue for coming few years. The commitment underneath Cop 21 provides a thrust to countries globally for increasing renewable capability to mitigate the impact of climate change. Despite the impressive program, one must remember that over 1 billion people, 14% of the population do not have access to electricity. Sanguinity in the renewable sector is accompanied by skepticism on whether the momentum can be maintained for the next two decades. Equitable and affordable access to and control over sustainable energy services for women and men is a key requisite right to development. Therefore providing clean and affordable energy to women and impoverished sections of society is a matter of great concern around the globe (Bhattacharya, 2005). Thus many international business, civil societies, NGOs, multilateral organizations and banks and other programmes and agencies of the United Nations are drawing high attention to the agendas of energy issues (The energy challenge for Achieving the Millennium Development Goals, 2005). Thus, achieving all of the MDGs will require much greater energy inputs and access to energy services (Modi Vijay, 2006). One of the hindrances arising in achieving the progress of the MDGs is due to the shortage of energy and most particularly the availability and accessibility to modern cooking fuels and electricity (Energy and Millennium Development goals). Thus



**RESEARCH ARTICLE**

**भारतीय कृषि का वैश्वीकरण**

अर्चना सेठी, बी. एल सोनेकर

\*सहायक प्राध्यापक, अर्थशास्त्र अध्ययन शाला, पं रविशंकर शुक्ल विश्वविद्यालय रायपुर  
\*सह प्राध्यापक, अर्थशास्त्र अध्ययन शाला, पं रविशंकर शुक्ल विश्वविद्यालय रायपुर

\*Corresponding Author E-mail: archanasethi96@gmail.com

**ABSTRACT:**

जब भी सरकार विदेशी कंपनियों को भारत के किसी भी क्षेत्र में पूंजी लगाने की अनुमति देती है तो पहले यह सुनिश्चित कर ले कि विदेशी कंपनी निवेश से जो लाभ कमाती है उसका भारत के विकास में भी एक निश्चित योगदान हो यदि ऐसा नहीं होता तो सरकार को यह अनुमति नहीं देनी चाहिए।

**KEYWORDS:** वैश्वीकरण, बहुराष्ट्रीय निगम, कृषि उत्पाद।

**प्रस्तावना**

वैश्वीकरण के अंतर्गत भारत सरकार ने दो प्रमुख प्रक्रियाओं को प्रोत्साहित किया है: 1. भारतीय अर्थव्यवस्था के विभिन्न क्षेत्रों में विदेशी पूंजी का निवेश 2. भारत के विदेशी ब्यपार को विश्व ब्यापार संगठन के अनुसार नियमित करना। इस अध्ययन में हम भारतीय कृषि के विकास में विदेशी पूंजी की भूमिका का अध्ययन करेंगे जो प्रायः बहुराष्ट्रीय निगमों द्वारा लगायी जाती है:

**अध्ययन का उद्देश्य :**

1. भारतीय कृषि पर वैश्वीकरण के प्रभाव का अध्ययन करना।
2. कृषि में विदेशी पूंजी के निवेश का अध्ययन करना।

**भारतीय कृषि और विश्व ब्यापार संगठन**

ब्रेटनवुडस समझौते के परिणामस्वरूप अंतर्राष्ट्रीय मुद्राकोश, विश्वबैंक और कुछ समय बाद सीमाशुल्क और और ब्यापार पर सामान्य समझौते के अंतर्गत ब्यापार और अंतर्राष्ट्रीय मुद्रा प्रणाली को नियंत्रित करने के लिए एक प्रणाली की स्थापना की गई। 15 अप्रैल 1994 को मोरक्को के मारकेश में 124 देश एकत्र हुए और सीमा शुल्क और ब्यापार पर सामान्य समझौते पर हस्ताक्षर किये। इस समझौते का मुख्य उद्देश्य सीमा शुल्क घटाना, कोटा कम करना, बहुपक्षीय विश्व ब्यापार को बढ़ावा देना था। विश्व ब्यापार संगठन या WTO<sup>1</sup> अप्रैल 1995 से प्रचलन में है। विश्व ब्यापार संगठन की प्रस्तावना के अनुसार विकासशील देश विशेषकर पिछड़े देश अंतर्राष्ट्रीय ब्यापार की वृद्धि में वह भाग प्राप्त कर सकें जो उनकी आर्थिक विकास संबंधी आवश्यकताओं के अनुरूप हो। GATT का स्थान WTO ने ले लिया है। WTO विश्व ब्यापार को बढ़ावा देगा। यह विश्व के



JUNI KHYAT

II

# जूनी ख्यात

(सामाजिक विज्ञान; कला एवं संस्कृति की शोध पत्रिका)

A Peer-Reviewed and Listed in UGC CARE List  
ISSN 2278-4632

संपादक  
डॉ. बी. एल. भादानी  
प्रोफेसर

प्रबंध संपादक  
श्याम महर्षि



मरुभूमि शोध संस्थान  
संस्कृति भवन

एन.एच. 11, श्रीडूंगरगढ़ (बीकानेर) राजस्थान

**“छत्तीसगढ़ के असंगठित क्षेत्र में कार्यरत महिला उद्यमियों की रोजगार एवं आय का अध्ययन”  
(दुर्ग जिला के धमधा एवं दुर्ग जनपद पंचायत के विशेष संदर्भ में)**

शंकर लाल पटेल शोधछात्र पं. रविशंकर शुक्ल विश्वविद्यालय, रायपुर (छ.ग.)  
डॉ.अर्चना सेठी सहायक प्राध्यापक पं. रविशंकर शुक्ल विश्वविद्यालय, रायपुर (छ.ग.)

**सारांश :-**असंगठित क्षेत्र में कार्यरत महिला उद्यमियों के सर्वेक्षित क्षेत्र में कुल न्यादर्श 80 लिया गया है जिसमें ग्रामीण क्षेत्र से 20 तथा शहरी क्षेत्र से 60 है जिसके अध्ययन से यह सारांश प्राप्त होता है कि दुर्ग जिला के धमधा तथा दुर्ग विकास खण्ड मैदानी क्षेत्र तथा उद्यम के लिए अनुकूल वातावरण, शिक्षा के स्तर आर्थिक संपन्नता होने से उद्यम के क्षेत्र बहुत अधिक विकास किया है। असंगठित क्षेत्र में उद्यम प्रारंभ कर अपना ही नहीं बल्कि अपने साथ अन्य लोगों को भी उद्यम में सर्वाधिक 0-2 व्यक्तियों को रोजगार देने वाली महिला उद्यमियों का प्रतिषत 76.25 है। आय प्राप्त कर वह स्वयं तो संपन्न हो रही है साथ ही साथ अन्य लोगों को भी संपन्न बना रही है। उद्यम में सर्वाधिक आय 1000-3000 रूपय मासिक प्राप्त करने वालों का प्रतिषत 68.57 है। हालांकि यह असंगठित क्षेत्र में उद्यम चलाने में शहरी क्षेत्र की महिला उद्यमी ग्रामीण क्षेत्र की महिला उद्यमियों से आगे है शहर की महिलाएं अधिक जागरूक, शिक्षित तथा अधिक स्वतंत्र महसूस कर रही है। ग्रामीण क्षेत्र की महिलाएं रूढ़ीवादी तथा सामाजिक संबंध के कारण से कम ही या एक-दो ही महिलाएं असंगठित क्षेत्र में उद्यम का संचालन कर पा रही है, परन्तु समस्याएं कितनी भी हो असंगठित क्षेत्र में कार्य करने वाली महिला उद्यमी विकास के लक्ष्य को प्राप्त करने के लिए हर समस्या को पार कर आधुनिक समाज की मुख्यधारा से जुड़ती जा रही है।

**संकेत शब्द :-** महिला उद्यमी, उद्यम, समस्याएं, सामाजिक, आर्थिक, संतुष्ट, असंतुष्ट, कार्य, रोजगार,

**प्रस्तावना :-** भारत देश 135 करोड़ की आबादी वाला दुनिया की द्वितीय बड़ा देश है जहां की 27 प्रतिषत आबादी युवा शक्ति है जिसे रोजगार दे पाना भारत सरकार के लिए चुनौती से कम नहीं है। यहां शिक्षा का स्तर 73 प्रतिषत है, जिसे अपनी जीवन यापन हेतु रोजगार की तलाश है ऐसे में हमारे देश के युवाओं को रोजगार की लिए सरकार की ओर नजर गड़ाने से अच्छा है कि वह स्वरोजगार प्रारंभ कर अपने ही नहीं अपने साथ अन्य लोगों को भी रोजगार प्रदान कर सके।

आधुनिक भारतीय समाज में महिलाएं पुरुषों से कम नहीं वह पुरुषों से कदम से कदम मिलाकर चल रही है। किसी भी क्षेत्र की बात हो वह हर एक क्षेत्र में पुरुषों से कम नहीं है चाहे वह रोजगार हो राजनीति हो, समाज या उद्यम की क्षेत्र क्यों न हो। आज असंगठित क्षेत्र में देखा जाये तो भारत की ग्रामीण तथा शहरी दोनों क्षेत्र में महिलाओं की भागीदारी बढ़ती जा रही है। वह उद्यम के हर क्षेत्र में अपनी पांव पसार रही है। असंगठित क्षेत्र के प्रमुख उद्यम जैसे फल दुकान, किराना दुकान, सब्जी दुकान, ब्यूटि पार्लर, फैंसी स्टोर, दोना पत्तल, सिलाई-कढ़ाई, कपड़ा दुकान, जैविक खाद, डेयरी, मुर्गी पालन आदि व्यवसाय को महिलाएं ही संचालित कर रही है।

समय के इस चक्र में व्यक्तियों के दृष्टिकोण बदल रहा है। आज कल स्त्रियां उद्योग-धन्धों का तीव्रगति से विकास कर रही है। विभिन्न अध्ययनों से यह बात भी सिद्ध हो चुका है कि वर्तमान समय के आर्थिक विभाजन में महिलाओं की भूमिका तथा परिस्थिति में अत्यधिक परिवर्तन आयी है। आर्थिक विकास की इस स्वरूप में महिलाओं में सोचने, समझने तथा निर्णय करने की क्षमता में आमूल चूल परिवर्तन आया है। इसी परिवर्तन का परिणाम कहा जा सकता है कि समाज कृषि आधारित व्यवसाय से आगे आधुनिक औद्योगिक व्यवस्था की ओर अग्रसर हुआ तथा अब वह घर से बाहर भी विभिन्न प्रकार से उद्यमी कार्य कर अर्थतंत्र में अपनी महत्वपूर्ण भूमिका निभा रही है।

महिला उद्यमी से आषय

सामान्य रूप से यदि कहा जाये तो भी महिलायें किसी भी प्रकार की वस्तुओं और सेवाओं का उत्पादन कर रही है महिला उद्यमी कही जायेगी। इस प्रकार से वह महिला अपने उद्योग की स्थापना से लेकर वितरण व्यवस्था तक की सम्पूर्ण जवाबदारी लेती है अर्थात् वह उद्योग स्थापित करती है उसमें लगने वाली पूंजी की व्यवस्था करती है। उद्योग का सुनिश्चित ढंग से संचालन करती है। उसमें लगने वाले कच्चे माल की व्यवस्था करती है। उत्पादन प्राप्त कर उसकी बिक्री के लिए बाजार की खोज, वितरण की व्यवस्था तथा उस उद्योग से प्राप्त होने वाले लाभ-हानि की भागीदारी होती है उन्हें महिला उद्यमी कहा जाता है। इस प्रकार हम कह सकते हैं कि महिला उद्यमी जनसंख्या के उस भाग से है जो कि अपने स्वयं के

Peer Reviewed Journal for M.Phil. , Ph.D. & Appointment of Teacher in Universities & College

ISSN : 2454-4655

VOLUME - 8 No. : 4, May - 2022

# International Journal of Social Science & Management Studies

Peer Reviewed & Refereed Journal

Indexing & Impact Factor 5.2



Radiant Group of Institutions, Jabalpur (M.P.), India  
Indian Economic Association  
& Social Science & Management Welfare Association  
2 Days International Conference on  
Multidisciplinary Research in



**Education, Employment & Entrepreneurship Development**

Date : 1-2 May 2022, Venue : Jabalpur (M.P.), INDIA



**International Journal of**  
Social Science & Management Studies

## स्व-सहायता समूह में कार्यरत महिलाओं की सामाजिक-आर्थिक स्थिति का विश्लेषण (दुर्ग जिला के विशेष संदर्भ में)

पूजा यादव

पोष छात्रा

डॉ. अर्चना रोटी

सहायक प्राध्यापक (अर्थशास्त्र) पं. रविपंकर पुवल विपविद्यालय, रायपुर (छ.ग.)

**सारांश :-** स्व-सहायता समूह में कार्यरत महिलाओं की सामाजिक-आर्थिक अध्ययन के लिए न्यादर्ष में कुल 20 स्व-सहायता समूहों से 60 सदस्यों का चयन किया गया है, जिसमें से समूह में कार्यरत 24 महिला सदस्य दुर्ग विकासखण्ड से तथा 36 महिला सदस्य धमधा विकासखण्ड से लिया गया है। उक्त अध्ययन से यह सारांश प्राप्त होता है कि स्व-सहायता समूह में कार्यरत महिलाएं अपने आपको सामाजिक-आर्थिक दृष्टिकोण से मजबूत करना चाहती हैं। समूह में कार्यरत महिलाओं का सर्वाधिक 46.67 प्रतिशत महिला सदस्य अन्य पिछड़ा वर्ग का पाया गया, तथा महिला अपने सामाजिक-आर्थिक स्थिति में मजबूत करने के लिए अधिकतर महिला सदस्यों एकल परिवार में रहना पसंद करते हैं। वैवाहिक दृष्टिकोण से देखा जाय तो समूह में सबसे अधिक 46.67 प्रतिशत महिला सदस्य हैं। समूह में कार्यरत महिलाओं 83.33 प्रतिशत महिला सदस्य शिक्षित हैं तथा 3000-6000 रुपये तक मासिक आय प्राप्त करने वाले समूह में कार्यरत महिलाओं का सर्वाधिक (43.33) प्रतिशत है। समूह में कार्यरत अधिकांश महिलाएं रोजगार के लिए कृषि में संलग्न हैं, जिसके कारण उसकी बचत करने की प्रवृत्ति अनिश्चित होती। समूह में कार्यरत महिलाओं का सर्वाधिक 50.00 प्रतिशत महिलाएं अपनी बचत को बैंक में रखते हैं। स्व-सहायता समूह में कार्यरत महिलाओं का 78.33 प्रतिशत महिला सदस्य समूह में सदस्यता से संतुष्ट है। इस प्रकार महिलाएं अपने आय का कुछ भाग का बचत करते हैं, जिससे अपने रोजगार के अवसर को बढ़ा कर और अधिक आय प्राप्त करके अपने सामाजिक-आर्थिक स्थिति सुदृढ़ कर सकें।

**संकेत शब्द :-** कार्यरत महिला, सामाजिक-आर्थिक स्थिति, बचत, आय, रोजगार।

**प्रस्तावना :-** किसी भी देश में स्त्रियां समाज का एक महत्वपूर्ण घटक हैं और समाज में महिलाओं की सम्मानजनक स्थिति के अभाव में समग्र विकास की कल्पना करना निरर्थक है। क्योंकि महिलाओं की स्थिति समाज में जितनी सुदृढ़ होती है, समाज उतनी ही समृद्ध व मजबूत होता है। समाज तथा सभ्यता के

विकास में महिलाओं का योगदान सर्वोपरी रही है। इतिहास इस बात की साक्ष्य है कि जब-जब कभी पुरुष प्रधान सभ्यता ने नारी जाति की अवहेलना की तब-तब समाज का विकास अवरुद्ध हुआ है। महिलाएं सम्पूर्ण विषय की लगभग आधी आवादी का प्रतिनिधित्व करती हैं फिर भी आप्चर्य की बात यह है कि समाज में आज भी उन्हें सामाजिक-आर्थिक रूप से पुरुषों की तुलना में कमजोर, असहाय एवं काफी पिछड़े हुए माना गया है। भारतीय समाज विविधता से युक्त समाज है और यह समाज भी अन्य समाजों की भाँती पितृसत्तात्मक है, जहाँ स्त्रियों को पारस्त्रीय एवं धार्मिक आधार पर तो पूजनीय अव्यय माना जाता है, किन्तु वास्तविक जगत में उसकी स्थिति दयनीय है। प्राचीन समय महिलाओं के लिए स्वर्ण काल था। उस समय पुरुषों की सहभागी होने के साथ-साथ महिलाओं को सामाजिक-आर्थिक कार्यों में भाग लेने का पूर्ण अधिकार था, परन्तु प्राचीन समय इतनी अच्छी होने के बाद भी समय और विचारधारा में परिवर्तन से समाज में महिलाओं के प्रति यह विचार पनपने लगा कि बौद्धिक दृष्टि से तो महिलाएं पुरुषों की तुलना में निम्न हैं। सती प्रथा, बाल विवाह, विधवा विवाह, पर्दा प्रथा जैसे दिन-हीन सामाजिक कुरूपतियों ने महिलाओं की स्थिति को और दयनीय बना दिया, जो न केवल उनकी शिक्षा तथा स्वतंत्रता को बाधित किया, बल्कि सम्पूर्ण नारी जाति को घर की चारदीवारी में कैद रहने को मजबूर कर दिया। जबकि भारतीय संस्कृति महिला-पुरुष की समानता पर बल देती है। जहाँ पुरुषों महिलाओं को पुरुषों के समान समाज में आगे बढ़ने की पूरी स्वतंत्रता थी, स्त्री को षक्ति का स्वरूप माना गया है।

इसी प्रकार हमारे भारतीय संविधान में भी महिलाओं पूरी स्वतंत्रता दे रखी है। कानूनी अधिकारों में सुधार किया है, फिर भी हमारे समाज में स्त्रियों का मूल्य और स्थान सामाजिक-आर्थिक दृष्टि से उस स्तर तक नहीं उठ पाया जितना उठना चाहिए था। भारतीय समाज सुधारक आन्दोलन के प्रवर्तकों ने स्त्रियों की सुरक्षा के लिए कानून बनाकर उनके कल्याण के लिए अनेक प्रयास किये गये, जिसके

# International Journal of Social Science & Management Studies

Peer Reviewed & Refereed Journal

Indexing & Impact Factor 5.2



Radiant Group of Institutions, Jabalpur (M.P.), India  
Indian Economic Association  
& Social Science & Management Welfare Association  
2 Days International Conference on  
Multidisciplinary Research in



**Education, Employment & Entrepreneurship Development**

Date : 1-2 May 2022, Venue : Jabalpur (M.P.), INDIA



**International Journal of**  
Social Science & Management Studies

## असंगठित क्षेत्र के उद्यम में सशक्त होती महिला उद्यमियों का एक अध्ययन (दुर्ग जिला के घमघा एवं दुर्ग विकासखण्ड के विशेष संदर्भ में)

शंकर लाल पटेल

षोडश छात्र

डॉ. अर्चना सेठी

सहायक प्राध्यापक अर्थशास्त्र, पं. रविशंकर पुवल विश्वविद्यालय, रायपुर (छ.ग.)

**सारांश :-** अध्ययन से यह स्पष्ट होता है कि महिला उद्यमी को असंगठित क्षेत्र के उद्यम में संलग्न है। उनमें अधिकांश का सामाजिक-आर्थिक कार्य के प्रति लगाव के कारण संप्रतिकरण में एक निष्चित उम्र का विशेष प्रभाव पड़ता है। जिसमें 40-50 आयु वर्ग के महिला उद्यमी अपनी उद्यम के प्रति संलग्न दिखाई दिये, जिनका सर्वाधिक 34 प्रतिशत है। असंगठित क्षेत्र में अधिष्ठित या कम पढी लिखी महिलाओं द्वारा उद्यम संचालन अधिक किया जा रहा है, जिसका सर्वाधिक 54 प्रतिशत है। उद्यम से महिलाओं में निर्णय क्षमता का विकास हुआ है। रोजगार प्रदान करने की क्षमता बढी। वह स्वयं तो उद्यम से रोजगार प्राप्त कर रही हैं साथ ही अन्य लोगों को भी अपने उद्यम में रोजगार दे रही हैं। अध्ययन से यह स्पष्ट हो गया कि असंगठित क्षेत्र के उद्यम में महिला उद्यमी सशक्त हो रही हैं तथा अपने समाज को भी सशक्त कर रही हैं।

**शब्द संकेत :** संप्रतिकरण, महिला उद्यमी, उद्यम, सामाजिक स्थिति, आर्थिक स्थिति, कार्य, असंगठित क्षेत्र।

“नारी सृष्टि की अनमोल रचना हैं, जो कोमल होते हुए भी विषाल मन, अद्वितीय तप व मन सहनशीलता की प्रतिमूर्ति हैं। अपनी मधुर मुस्कान से जीवन के हर पल की कटुता व खुषी को जीती वह न केवल स्वयंका जीवन व्यतीत करती हैं, बल्कि परिवार की हर खुष व दुख को आंचल में समेटे हर दायित्व के लिए कुवानियां देती हैं।”

**प्रस्तावना :-** किसी भी देश का आर्थिक विकास वहां उपलब्ध मानव शक्ति की व्यवस्था एवं उसके विकास पर निर्भर करता है। निःसंदेह प्राकृतिक संसाधन, पूँजी निर्माण, तकनीकी एवं नवाचार, विदेशी सहायता, सामाजिक, आर्थिक, धार्मिक एवं राजनीतिक संस्थायें तथा अन्तर्राष्ट्रीय व्यापार आर्थिक विकास में अपनी भूमिका निभाते हैं, परन्तु इसमें सबसे महत्वपूर्ण मानव है। मानव आर्थिक विकास के प्रत्येक घटक से जुड़ा हुआ है। हमारे देश में कृषि, उद्योग, यातायात, रंचार,

शिक्षा, स्वास्थ्य आदि सभी क्षेत्रों में काफी तीव्र गति से विकास हुआ है, जिसमें महिलाओं के योगदान को प्रत्यक्ष और अप्रत्यक्ष रूप से नकारा नहीं जा सकता। आज महिलायें पुरुषों के साथ सरकारी तथा निजी क्षेत्र में कन्धे से कन्धे मिलाकर कार्य कर रही हैं। महिलाओं ने अनेक अवसरों पर अपनी शक्ति संपन्नता का एहसास कराया है। आर्थिक भागीदारी की दृष्टि से अर्थव्यवस्था के प्रत्येक क्षेत्र में महिलाओं के योगदान के अनुपात में बहुत सीमा तक वृद्धि हुई है। महिलाओं की आर्थिक क्रियाओं से संबंधित नये आयाम उभकर सामने आये हैं।

इस प्रकार घर की चारदीवारी से बाहर निकल कर महिलाएं मोर्चे भी संभाल रही हैं। इस तरह धन की उपलब्धता, व्यवसाय की संभावना और निरन्तर मिलती सफलता ने आसमान को छुने लगी है। जो महिलाएं घर के चार दिवारी से बाहर नहीं आना चाहती थी, अब वे महिलाएं भी रोजगार के क्षेत्र में लगातार अपनी संख्या में वृद्धि कर रही हैं तथा उनमें भविष्य के व्यवसाय के प्रति जागरूकता में भी वृद्धि होने लगी है। इस प्रकार महिलाएं जीवन के विभिन्न क्षेत्र में सामाजिक, सांस्कृतिक, आर्थिक मूल्यों में बदलाव आये। वर्तमान युग की महिलाएं समाज में अपनी महत्व को बहुत अच्छे एवं प्रभावी ढंग से स्थापित किये हैं। अब समाज में कोई भी महिला होने पर बोझ नहीं कहे जायेंगे। समाज में महिला को अवला से संबोधित नहीं करेंगे, क्योंकि सभी महिलाओं में जागरूकता, कार्य के प्रति रुझान, आत्मविश्वास, निर्भरता तथा योग्यताएं हैं।

एक जमाने में महिला और पुरुष के काम में बंटवारा होता था, परन्तु नारी ने पुरुष और महिला के मध्य खिंची लक्ष्मण रेखा को अपने बलवृते पर मिटा दिया है। पुरुष वर्चस्व वाला ऐसा कोई क्षेत्र नहीं है, जिसे महिला नहीं कर सकती हो। महिलाओं ने चौखट से लेकर चाँद तक का सफर बड़ी सहजता से तय किया है। अब महिला को अपनी पहचान बनाने के लिए पिता अथवा पति का नाम बताने की आवश्यकता नहीं पड़ती है।

## छत्तीसगढ़ में स्व-सहायता समूह के माध्यम से महिलाओं के सामाजिक एवं आर्थिक सशक्तिकरण का अध्ययन (दुर्ग एवं राजनांदगांव जिला के विशेष संदर्भ में)

डॉ अर्चना सेठी\* ओमप्रकाश वर्मा\*\*

सहायक प्राध्यापक, अर्थशास्त्र अध्ययनशाला, पं रविशंकर शुक्ल विश्वविद्यालय, रायपुर, छत्तीसगढ़,

ई. मेल – [archanasethi96@gmail.com](mailto:archanasethi96@gmail.com)

शोध सहायक, अर्थशास्त्र अध्ययनशाला, पं. रविशंकर शुक्ल विश्वविद्यालय, रायपुर, छत्तीसगढ़

### सारांश –

वर्तमान भारतीय परिप्रेक्ष्य में विशेषकर ग्रामीण क्षेत्र में महिलाओं ने अपने मेहनत और लगन के बल पर यह साबित कर दिया कि स्व सहायता समूह के साथ जुड़कर एक नया मुकाम हासिल किया जा सकता है। प्रस्तुत अध्ययन में छत्तीसगढ़ के दुर्ग एवं राजनांदगांव जिले के स्व-सहायता समूह का महिलाओं के सामाजिक एवं आर्थिक सशक्तिकरण पर प्रभाव एवं संतुष्टि का अध्ययन किया गया है। दुर्ग जिले में स्व-सहायता समूह की सदस्यता से पूर्व 37.3 प्रतिशत महिलाएं सशक्त थीं एवं स्व-सहायता समूह की सदस्यता के पश्चात 41.6 प्रतिशत महिलाएं सशक्त हो गईं। राजनांदगांव जिले में स्व-सहायता समूह की सदस्यता से पूर्व 38.5 प्रतिशत महिलाएं सशक्त थीं एवं स्व-सहायता समूह की सदस्यता के पश्चात 46.8 प्रतिशत महिलाएं सशक्त हो गईं अर्थात् हमारी प्रथम शून्य परिकल्पना महिला स्व-सहायता समूह से सदस्यों के सामाजिक आर्थिक सशक्तिकरण में कोई सार्थक प्रभाव नहीं पड़ा है, अस्वीकार की जाती है। स्व-सहायता समूह की सदस्यता से क्रमशः दोनों जिलों में 4.3 एवं 8.3 प्रतिशत अतिरिक्त महिलाएं सशक्त हुईं एवं दुर्ग जिले में महिला सशक्तिकरण सूचकांक स्व-सहायता समूह की सदस्यता से पूर्व 0.64 था जो स्व-सहायता समूह की सदस्यता के पश्चात 0.75 हो गया। राजनांदगांव जिला में महिला सशक्तिकरण सूचकांक स्व-सहायता समूह की सदस्यता से पूर्व 0.65 था जो स्व-सहायता समूह की सदस्यता के पश्चात 0.78 हो गया। संतुष्टि का अध्ययन करने हेतु कोई स्क्वेयर परीक्षण किया गया है। परिगणित मूल्य 7.36 तालिका मूल्य 11.00 से छोटा है। अतः शून्य परिकल्पना अस्वीकार की जाती है कि स्व-सहायता समूहों के माध्यम से महिलाओं के संतुष्टि में कोई सार्थक प्रभाव नहीं पड़ा है अर्थात् स्व-सहायता समूहों के माध्यम से महिलाओं के संतुष्टि में सार्थक प्रभाव पड़ा है। स्व-सहायता समूह के आय को प्रभावित करने वाले तत्वों का अध्ययन करने के लिए बहुगुणी प्रतिपगमन गुणांक का प्रयोग किया गया है। स्व-सहायता समूह का कार्य, स्व-सहायता समूह का निर्माण अवधि, स्व-सहायता समूह का आकार या सदस्यों की संख्या, सदस्यों की शिक्षा, समूह द्वारा दिए गए ऋण का आकार, समूह द्वारा दिये गये ऋण का ब्याज दर, बचत आदि आय को धनात्मक रूप से प्रभावित कर रहे हैं।

**आभार:** राज्य योजना आयोग से अनुदान प्राप्त।

**शब्द कूजी:** स्व-सहायता समूह, महिला सशक्तिकरण, पंचसूत्र।

### प्रस्तावना –

भारत में कुल जनसंख्या में से आधी अबादी महिलाओं की है और यहां के अधिकांश जनसंख्या ग्रामीण प्रधान है जिसमें से लगभग 77 प्रतिशत जनसंख्या गांवों में बसती है और अर्थव्यवस्था मूल रूप से कृषि पर आधारित है। अभी भी अधिकांश महिलाएं सामाजिक व आर्थिक दृष्टिकोण से पिछड़ी हुई हैं। ऐसी स्थिति में महिलाओं को सशक्त सबल करने, उनके अधिकारों की रक्षा करने, स्वावलंबी बनाने तथा उसकी सामाजिक, आर्थिक व राजनीतिक दशा सुधारने में स्व सहायता समूह अपनी महत्वपूर्ण भूमिका निभा रही है। महिला स्व-सहायता समूह महिलाओं को संगठित कर उनकी सामाजिक, आर्थिक व राजनीतिक सशक्तिकरण का एक सशक्त माध्यम बन चुकी है। (थानामनी, एस. एवं मुदुसेलवी, एस.)

भारतीय समाज में नारी का स्थान पूजनीय रहा है। समाज तथा सभ्यता के विकास में महिलाओं का योगदान सर्वोपरि रही है। महिलाएं प्रत्येक समाज का एक महत्वपूर्ण अंग हैं जिसका संख्या लगभग पुरुषों के समान ही होती है। अतः महिलाओं का विकास करके ही सार्वभौमिक विकास की कल्पना को साकार करना सम्भव है। पं. जवाहरलाल नेहरू ने भी इसी तथ्य को पुष्ट करते हुए कहा है कि "यदि आपको विकास करना है तो महिलाओं का उत्थान करना होगा, महिलाओं का विकास होने पर समाज का विकास स्वतः हो जाएगा।" यह विभिन्न सामाजिक आर्थिक घटकों पर महिलाओं के जीवन शैली को बेहतर बनाने का एक स्वैच्छिक संगठन है। जिसके माध्यम से महिलाओं के विकास में महिला सशक्तिकरण अपनी महत्वपूर्ण भूमिका निभा रही है। (कप्पाकौडल)

SHODH SAMAGAM

RNI : CHHIBIL/2018/77892

ISSN : 2582-1792 (P)

2581-6918 (E)



# SHODH SAMAGAM

**January to March 2021**  
**Year- 02, Volume - 02, Issue - 03**

A Double - blind, Peer-reviewed, Quarterly,  
Multidisciplinary and Bilingual Research Journal

**Part - 1**

Editor in Chief

**Dr. (Smt.) Shobha Agrawal**

M.Com., M.Phil., Ph.D.

Assistant Professor & Head of Management Department

Agrasen Mahavidyalaya, Raipur (C.G.)

मुद्रक, प्रकाशक एवं स्वामी अजय कुमार अग्रवाल द्वारा अदिति पब्लिकेशन के लिये, बर्फ कारखाना के पास शक्ति साउण्ड गली, कुशालपुर, रायपुर तहसील व जिला रायपुर छत्तीसगढ़ से प्रकाशित तथा यश ऑफसेट लिलि चौक, पुरानी बस्ती, रायपुर, तहसील व जिला रायपुर छत्तीसगढ़ से मुद्रित किया गया है, संपादिका डॉ. (श्रीमती) शोभा अग्रवाल, मो 9425210308





## महिला मजदुरों की कृषि में भूमिका एवं उनके आर्थिक जीवन पर पड़ने वाले प्रभाव का अध्ययन (विशेष : दुर्ग जिले के धमधा विकासखण्ड के संदर्भ में)

शंकर लाल पटेल, शोधार्थी, अर्थशास्त्र विभाग  
अर्चना सेठी, (Ph.D.), अर्थशास्त्र विभाग  
पंडित रविशंकर, विश्वविद्यालय, रायपुर, छत्तीसगढ़, भारत

### ORIGINAL ARTICLE



#### Corresponding Authors

शंकर लाल पटेल, शोधार्थी, अर्थशास्त्र विभाग  
अर्चना सेठी, (Ph.D.),  
पंडित रवि शंकर, विश्वविद्यालय,  
रायपुर, छत्तीसगढ़, भारत

shodhsamagam1@gmail.com

Received on : 22/01/2021

Revised on : ----

Accepted on : 01/02/2021

Plagiarism : 00% on 22/01/2021



#### Plagiarism Checker X Originality Report

Similarity Found: 0%

Date: Friday, January 22, 2021

Statistics: 9 words Plagiarized / 2676 Total words

Remarks: No Plagiarism Detected - Your Document is Healthy.

efgyk strqjtsa dh —fk esa hkoqfedk .oa muds vk/fkZd thou ij iM+us okys ghkko dk v;u  
l;to'ks'k nqzZ l;ys dh /ke/kk fodk [c-M ds lan-ikZ esa %B jka'k & efgyksksa dk —fk  
esa egr gh eghoq.kZ hkoqfedk jgh gSa i; dgk tk lanrk gSa bl v'kZOr;fkk ih xsm+h  
ds pykus okys —fk efgyk strqj gSa) jh efgyksksa dk —fk laa/kh Lokfero ugksus ds  
dkj

### शोध सार

महिलाओं का कृषि में बहुत ही महत्वपूर्ण भूमिका हैं। यह कहा जा सकता है कि इस अर्थव्यवस्था रूपी गाड़ी को चलाने वाले कृषि महिला मजदुर हैं। यद्यपि महिलाओं का कृषि संबंधी स्वामित्व न होने के कारण महिलाओं के कार्य को न के बराबर समझा जाता है। 2011 के अनुसार कुल महिला कामगारों में से 65 प्रतिशत महिलाएँ कृषि कार्य करती हैं। देश में कुल किसानों का 118.7 करोड़ में से 30.3 करोड़ महिलाओं का है जिसमें महिला कृषि श्रमिकों का भागीदारी 55.21 प्रतिशत है। यह अध्ययन दुर्ग जिले के धमधा विकास खण्ड के संदर्भ में है। इस शोध का प्रमुख उद्देश्य महिला मजदुर की कृषि कार्य करने वाली परिवार का अध्ययन, आर्थिक, महिला मजदुरों की कृषि में भागीदारी तथा जीवन का रोजगार का अध्ययन किया गया है। इस अध्ययन में यह पाया गया कि महिलाएँ, पुरुषों की अपेक्षा अधिक योगदान दे रही हैं। अतः खिलोराकला और कन्हारपुरी और करेली के महिलाओं का योगदान अद्वितीय है। वहाँ महिलाएँ निंदाई, मिंजाई, कटाई तथा बीजरोपण एवं सब्जी उत्पादन में बहुत महत्वपूर्ण भूमिका निभा रही हैं। इन कृषि कार्य करने वाली मजदुर महिलाओं के परिवार के आय में वृद्धि के साथ-साथ आर्थिक स्थिति में सुधार हुई है, जिसके कारण महिलाओं में अपने आत्मसम्मान, परिवार तथा बच्चों की शिक्षा की स्थिति में सुधार हुई है। इस प्रकार अध्ययन क्षेत्र में कृषि महिला मजदुरों की आर्थिक, सामाजिक स्थिति सुदृढ़ हुई है।

### मुख्य शब्द

महिला मजदुर, सामाजिक, आर्थिक स्थिति, कृषि, शैक्षणिक स्थिति।

## IMPACT OF ONLINE PURCHASING UPON TRADITIONAL RETAIL BUSINESS ON CELL PHONE IN RAIPUR CITY OF CHHATTISGARH

**Sunil Kumar Kumeti**

Assistant Professor, School of Studies in Economics, Pt. Ravishankar Shukla University, Raipur,  
(C.G.) India. Email – [sunilkumeti.eco@gmail.com](mailto:sunilkumeti.eco@gmail.com)

**Neelima Singh Thakur**

Research Scholar, School of Studies in Economics, Pt. Ravishankar Shukla University, Raipur, (C.G.)  
India.

### **Abstract**

In the outshine of globalised world with easy accessibility of network connectivity, internet and advancement of technology the online business is growing up promptly whether it is B2B, B2C, C2C, C2B, B2A or C2A. The online market is now reachable beyond their domestic territories, thus seller from online market can easily connect customer to a greater extent through various online business platforms. The emerging online market affects the local traditional retail market; they started facing lots of fluctuation in their business turnover yearly. The main objective of this research is to analyse and know the influence of online market upon biggest and largest traditional retail cell phone market of Raipur city of Chhattisgarh. The study is based on primary data collection by directly interviewing the owner of traditional cell phone stores through interview schedule. Sample size of 120 from universe has been selected by random sampling technique. The data collected has been studied and interpreted based on 16 key indicators which shows the impact on traditional cell phone market due to arisen of online market. The chi-square test has been performed in the data collected, reveals and concluded that there is significant impact of online purchasing on traditional cell phone retailers, the business pattern and profit margin has been significantly affected because of growing online market. This empirical analysis finds that many traditional stores were unable to gain super profits after deducting the expenses. The major effect of online market on traditional business is the discount offered by online stores to catch the attention of more customers. Online business also decreased the annual turnover and number of units sold of traditional businessmen. This study suggests comprehensive list of practical customer-winning ideas, tips and techniques to set business apart and to compete with online market, like traditional retailer should, analyze and understand the market forces that affect the consumer's attitude, provide additional services like product segmentation, special Offers, lower prices, better service, wider selection, good location, or convenient hours, new offers, new items, new prices, special announcements, stronger ads and better headlines.

**Key words:** Traditional retail market, online market, domestic territory, annual turnover, market forces, numbers of units sold, consumers' attitude.

---

### **1. Introduction**

In the emerging globalized market with rapid growth of internet and technology, the competition has been continuously increasing between traditional retail stores and online stores. The reaches of online stores are beyond domestic territories which penetrate the domestic market of traditional retail stores. Online purchasing of product is emerging very fast in rapid way in last two decades. Millions of people shop online daily from various online stores. Online shopping allows consumer to directly buy goods and services according to their need anytime and anywhere in the world from online stores, due to which

ISSN 2347-5145 (Print)  
2454-2687 (Online)

Available online at  
[www.anvpublication.org](http://www.anvpublication.org)

Vol. 10 | Issue-02|  
April – June | 2022

*International Journal of  
Reviews and Research in Social Sciences*



## **RESEARCH ARTICLE**

# दुर्ग जिला के पाटन विकासखण्ड में कृषकों के आर्थिक विकास में कृषि उपज मण्डी की भूमिका

सुनील कुमार कुमेटी<sup>1</sup>, बी. एल. सोनेकर<sup>2</sup>, भारती सिंह कुमेटी<sup>3</sup>

<sup>1</sup>सहायक प्राध्यापक, अर्थशास्त्र अध्ययनशाला, पं. रविशंकर शुक्ल विश्वविद्यालय रायपुर (छ.ग.)

<sup>2</sup>एसोसिएट प्राफेसर, अर्थशास्त्र अध्ययनशाला, पं. रविशंकर शुक्ल विश्वविद्यालय रायपुर (छ.ग.)

<sup>3</sup>सहायक प्राध्यापक अतिथि, अर्थशास्त्र विभाग, शासकीय दू. ब. महिला स्नातकोत्तर महाविद्यालय रायपुर (छ.ग.)

\*Corresponding Author E-mail: [sunilkumeti.eco@gmail.com](mailto:sunilkumeti.eco@gmail.com)

### **ABSTRACT:**

आज कृषि जीवन व्यापन का साधन मात्र ही नहीं बल्कि कृषकों के आर्थिक विकास का प्रमुख स्रोत भी है। कृषि राज्य का विषय है और अधिकांश राज्य सरकारों ने पारदर्शिता और व्यापारियों के विवेकाधिकार को समाप्त करने के लिए 1950 के बाद कृषि उपज विपणन समिति अधिनियम लागू किया। जिसके अंतर्गत कृषि उपज विपणन मण्डियों की स्थापना की गई। यह समग्र रूप से सरकारी नीतियों का विस्तार है, जो खाद्य सुरक्षा, किसानों को लाभकारी मूल्य और उपभोक्ताओं के उचित मूल्य को निर्देशित करता है। कृषि उपज विपणन मण्डी के अन्तर्गत उपजों को एकत्रित करना, उनका श्रेणीकरण व प्रमाणीकरण करना, भण्डारण, परिवहन, वितरण प्रणालियां आदि क्रियाओं को किया जाता है। प्राचीन काल से ही कृषि उत्पादों की क्रय-विक्रय में बिचौलियों का बोलबाला रहा है जिससे किसानों को उसके उत्पादों की लागत भी नहीं मिल पाती थी। आजादी के पश्चात् हमारे देश के नीति निर्माताओं ने कृषि एवं कृषकों के महत्व को ध्यान में रखते हुए योजनाएं बनाई। जिससे भारत ने 19 वीं सदी के छठवें दशक के उत्तरार्ध में अनाज और कृषि उत्पादों के मामले में लगभग पूर्णतः आत्मनिर्भर हो गया था। भारत सरकार के कृषि मंत्रालय के अंतर्गत ग्रामीण विकास विभाग की कृषि-विपणन शाखा द्वारा कृषि उपज की विपणन के लिए अनेक प्रयास किए गए हैं। लेकिन देश में लगभग 86 प्रतिशत कृषि योग्य भूमि का स्वामित्व छोटे एवं सीमांत कृषकों के पास है। इन किसानों के लिए विपणन योग्य अधिशेष सीमित होने के कारण मंडियों तक की परिवहन लागत को वहन करना संभव नहीं होता है। परिवहन लागत से बचने के लिए कृषकों को अपनी उपज स्थानीय व्यापारियों को ही बेचनी पड़ती है, भले ही कम कीमत पर क्यों न बेचनी पड़े। मण्डियों के व्यापक तंत्र के अभाव में छोटे व सीमांत किसानों को अपनी उपज की बिक्री के लिए स्थानीय व्यापारियों पर ही निर्भर रहना होगा।

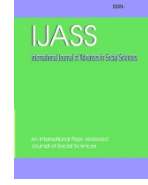
**KEYWORDS:** कृषि विकास, कृषि विपणन व्यवस्था, कृषकों का आर्थिक विकास।

### **प्रस्तावना :-**

भारत एक कृषि प्रधान देश है। हमारे देश की खुशहाली का रास्ता खेतों-खलिहानों और गांवों से होकर गुजरता है। आज हमारे देश की दो तिहाई जनसंख्या अपनी आजीविका के लिए कृषि पर निर्भर है। कृषि

ISSN 2347-5153 (Print)  
2454-2679 (Online)

Available online at  
www.anvpublication.org



Vol. 10| Issue-02|  
April - June| 2022

International Journal of Advances in  
Social Sciences

## RESEARCH ARTICLE

# छत्तीसगढ़ में खनिज संसाधनों का सकल राज्य घरेलू उत्पाद में योगदान

भारती सिंह कुमेटी<sup>1</sup>, सुनील कुमार कुमेटी<sup>2</sup>

<sup>1</sup>सहायक प्राध्यापक (अतिथि), अर्थशास्त्र विभाग, शासकीय दू. ब. महिला स्नातकोत्तर महाविद्यालय रायपुर (छ.ग.)

<sup>2</sup>सहायक प्राध्यापक, अर्थशास्त्र अध्ययनशाला, पं. रविशंकर शुक्ल विश्वविद्यालय रायपुर (छ.ग.)

\*Corresponding Author E-mail: [bharti9229@gmail.com](mailto:bharti9229@gmail.com)

### **ABSTRACT:**

खनिज पदार्थ किसी भी देश की वह प्रकृति प्रदत्त संचित निधि है जो उद्योग धन्धों, यातायात के साधनों एवं अन्य विकास कार्यों की आधारशीला निर्मित करती हैं। दुनियाभर में आधुनिक शहरीकरण, औद्योगीकरण, परिवहन और संचार प्रणाली का विकास स्थायी खनिज संसाधन और विभिन्न क्षेत्रों में उनके उचित उपयोग की उपलब्धियां हैं। सतत् खनिज संसाधनों ने आधुनिक सभ्य औद्योगिक विश्व को आकार देने में महत्वपूर्ण भूमिका निभाई है और अब भी निभा रही है। इसका मतलब यह है कि किसी भी देश का सतत् सामाजिक-आर्थिक मुलभूत संरचना प्राकृतिक संसाधनों में इसकी समृद्धि, इसकी तकनीकी जानकारी, खनिज संसाधनों का पता लगाने और दोहन करने की क्षमता और अंत में राष्ट्र की विकास गतिविधियों में उन संसाधनों का उचित उपयोग करने में उनकी समझदारी का संकेत है। विकास गतिविधियों में विकासशील देश आमतौर पर विकसित देशों की तुलना में बहुत पीछे हैं। यह मुख्य रूप से प्राकृतिक संसाधनों की कमी, समुचित शिक्षित मानव संसाधनों और सुदृढ़ सामाजिक-आर्थिक स्थितियों के अभाव के कारण है। एक स्थायी और मजबूत समाज की दिशा में प्रगति के लिए छत्तीसगढ़ जैसे प्रदेश को अपने मौजूदा खनिज संसाधनों के विकास को प्राथमिकता देनी चाहिए, जो प्रदेश के सामाजिक-आर्थिक बुनियादी ढांचे को आकार देने में प्रमुख भूमिका निभा सकती है।

**KEYWORDS:** छत्तीसगढ़, खनिज संसाधन, सकल घरेलू उत्पाद, आर्थिक विकास।

### **प्रस्तावना:**

भारत के संदर्भ में यह कहा जाता है कि प्रकृति ने उदारतापूर्वक भारत को प्राकृतिक संसाधन दिये हैं, किन्तु भारतवासी उनसे समुचित लाभ उठाने में असमर्थ रहे हैं। यही स्थिति छत्तीसगढ़ प्रदेश की भी है। प्रदेश में भी प्राकृतिक संसाधनों की बहुलता है। इन सबके बावजूद छत्तीसगढ़ आर्थिक विकास की दौड़ में अन्य प्रदेशों की तुलना में पीछे है। प्रदेश में प्राकृतिक संसाधनों में सबसे प्रमुख यहां के खनिज संसाधन हैं। यहां लगभग 28 प्रकार के खनिज ज्ञात हैं। किन्तु यहां 20 प्रकार के खनिजों का खनन एवं विपणन का कार्य किया जाता है। यहां लौह अयस्क, कोयला, मैंगनीज़, डोलोमाइट, ग्रेनाईट, चूना पत्थर, बॉक्साइड, क्लोराईट, सीसा, तांबा, टिन, क्वार्टजाईट, केओलिन इत्यादि के प्रचुर भण्डार उपलब्ध हैं। इसके अतिरिक्त यहां पर स्थानीय स्तर पर अनेक बहुमूल्य खनिज विद्यमान हैं। इन खनिजों संसाधनों के विदोहन से तीव्र आर्थिक विकास की दर को

# **Epileptic Seizure Detection Using Deep Learning Based Long Short-Term Memory Networks and Time-Frequency Analysis: a Comparative Investigation in Machine Learning Paradigm**

[Sunandan Mandal](#) [Bikesh Kumar Singh](#) [Kavita Thakur](#)

[ABOUT THE AUTHORS](#)

» Abstract

## Abstract

Epilepsy is a noncontagious brain abnormality, which causes electrical distraction and strains the neural system. Generally, epilepsy is treated and diagnosed through continuous examination and interpretation of the electroencephalography (EEG) signals. This is a very time-consuming and tedious job. Further, it is subjected to observational errors and observer variability. Hence, the development of an efficient automatic alarm system to recognize epileptic seizure signals is of important concern. The objectives of the present study are to investigate deep learning based long short term memory (LSTM) networks for the classification of epileptic EEG signals using time-frequency analysis. Additionally, a comparative investigation is carried out to evaluate the various state-of-the-art feature selection and classification models for automatic classification of EEG signals for Epilepsy detection. Features based on statistics, entropy, and fractal were extracted from both the time domain and frequency domain. The extracted features were supplied to LSTM networks and traditional machine learning models for epileptic EEG classification. High classification accuracy of 100% (under hold out and 10 fold protocol) and



View PDF

Access through another institution

Search ScienceDirect



## Article preview

Abstract

Introduction

Section snippets

References (191)

Cited by (21)

Recommended articles (6)



## Solar Energy

Volume 224, August 2021, Pages 1369-1395



# Progress in ambient air-processed perovskite solar cells: Insights into processing techniques and stability assessment

B.Gopal Krishna <sup>a</sup> , Dhriti Sundar Ghosh <sup>b</sup> , Sanjay Tiwari <sup>a</sup>

Show more

+ Add to Mendeley Share Cite

<https://doi.org/10.1016/j.solener.2021.07.002>

Get rights and content

Get citation



View PDF

Access through another institution

Search ScienceDirect



Outline

Highlights

Abstract

Keywords

1. Introduction

2. Methodology

3. Results and discussion

4. Conclusion

CRediT authorship contribution statement

Declaration of competing interest

Acknowledgements

References

Show full text

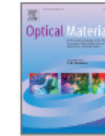
Cited By (5)



ELSEVIER

# Optical Materials

Volume 119, September 2021, 111357



Research Article

## Optical properties of CsPbBr<sub>3</sub> perovskite nanocrystals with silver nanoparticles using a room-temperature synthesis process

B. Gopal Krishna , Sanjay Tiwari

Show more

+ Add to Mendeley Share Cite

<https://doi.org/10.1016/j.optmat.2021.111357>

Get rights and content

### Recommended articles

Zinc ions doped cesium lead bromide perov...

Journal of Alloys and Compounds, Volume 866, 20...

View details

Effect of combination of etching modes on t...

Optical Materials, Volume 119, 2021, Article 111358

View details

Rapid synthesis of highly stable all-inorgani...

Journal of Alloys and Compounds, Volume 872, 20...

View details

1 2 Next

Published: 25 November 2021

# Tuning optical properties of CsPbBr<sub>3</sub> perovskite nanocrystals through silver doping


B. Gopal Krishna , Dhriti Sundar Ghosh & Sanjay Tiwari

*Journal of Materials Science: Materials in Electronics* **33**, 1324–1336 (2022) | [Cite this article](#)

869 Accesses | 3 Citations | [Metrics](#)

## Abstract

All-inorganic perovskite nanocrystals have emerged as an alternative for hybrid organic–inorganic perovskite for optoelectronic applications because of their unique optical, electrical properties and higher chemical stability. Doping of metal or metal nanoparticles into all-inorganic perovskite nanocrystals can modify or tune optical properties. In this paper, Ag-CsPbBr<sub>3</sub> nanocrystals were synthesized by the hot injection method. The influence of doped silver on the optical properties of CsPbBr<sub>3</sub> nanocrystals is analyzed by ultraviolet spectroscopy, PL spectroscopy, and Raman spectroscopy. There is an enhancement in the PL

Download PDF 



### Working on a manuscript?

Avoid the most common mistakes and prepare your manuscript for journal editors.

[Learn more](#) →

Sections

Figures

References

[Abstract](#)

[Introduction](#)

[Methodology](#)

[Results and discussion](#)

[Conclusion](#)

[References](#)



# Device Simulation of Perovskite/Silicon Tandem Solar Cell with Antireflective Coating

Gopal Krishna Burra (✉ [krishna\\_burra85@yahoo.com](mailto:krishna_burra85@yahoo.com))

Pandit Ravishankar Shukla University <https://orcid.org/0000-0002-7781-231X>

Dhriti Sundar Ghosh

Indian Institute of Technology Bhilai

Sanjay Tiwari

Pandit Ravishankar Shukla University

---

## Research Article

**Keywords:** Perovskite, Tandem Solar Cell, Single-diode Model, Matlab, Anti-reflective Coating, Efficiency

**Posted Date:** August 13th, 2021

**DOI:** <https://doi.org/10.21203/rs.3.rs-790945/v1>

**License:** © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

---

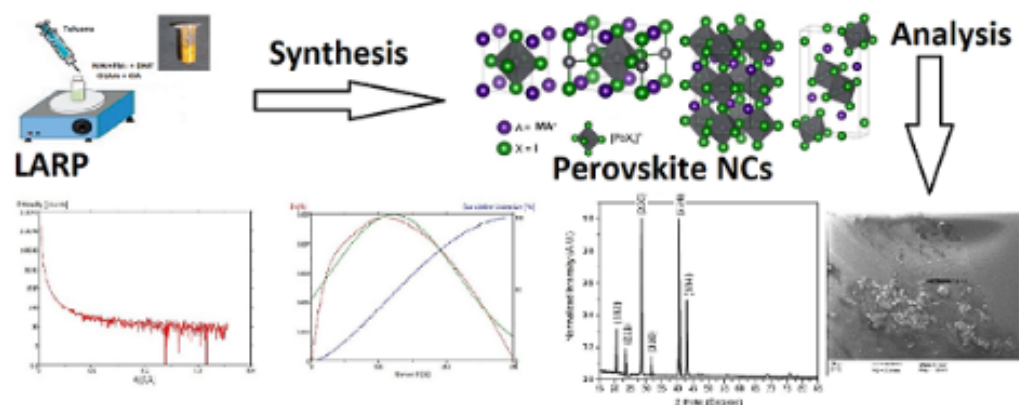
Search [Advance Search](#)

Everything ▼ Å

Browse By: [Author](#) [Issue](#) [Title](#) [Other Journals](#)

- [Home](#) [About](#) [Login](#) [Register](#) [Search](#) [Current](#) [Archives](#) [Submission](#) [Editorial Board](#)

Home > Vol 8, No 1 (2021) > Burra



## X-ray and Raman Study of $\text{CH}_3\text{NH}_3\text{PbI}_3$ Perovskite Nanocrystals

Gopal Krishna Burra, Dhriti Sundar Ghosh, Sanjay Tiwari

### Abstract

Organic-inorganic hybrid perovskite nanocrystals have gained a considerable attention for optoelectronics applications due to their unique properties like high light absorption coefficient, band gap tunability and larger diffusion length. In this research, ligand-assisted reprecipitation method (LARP) was employed to synthesize  $\text{CH}_3\text{NH}_3\text{PbI}_3$  nanocrystals (NCs). The optical and structural properties of nanocrystals depend on their size. X-ray diffraction (XRD) and small angle X-ray scattering (SAXS) techniques were used to determine the crystal structure, particle size distribution and surface to volume ratio of  $\text{CH}_3\text{NH}_3\text{PbI}_3$  nanocrystals. The organic-inorganic interactions of  $\text{CH}_3\text{NH}_3\text{PbI}_3$  nanocrystals were studied by Raman spectra at room temperature. This study will provide the basis to interpret the morphological properties of perovskite nanocrystals for their full exploitation in different optoelectronics applications.

### SUBSCRIPTION

Login to verify subscription

[Give a gift subscription](#)

### Article Tools

- [Print this article](#)
- [Indexing metadata](#)
- [How to cite item](#)
- [Email this article \(Login required\)](#)
- [Email the author \(Login required\)](#)

### 2021 Vol 8

[Iss 1 Pg 1-50](#)    [Iss 2 Pg 51-on](#)

### 2020 Vol 7

[Iss 1 Pg 1-35](#)    [Iss 2 Pg 36-92](#)

### 2019 Vol 6

[Iss 1 Pg 1-37](#)    [Iss 2 Pg 38-81](#)

### 2018 Vol 5

[Iss 1 Pg 01-28](#)    [Iss 1 Pg 29-60](#)

### 2017 Vol 4

[Iss 1 Pg 01-12](#)    [Iss 1 Pg 13-24](#)

### 2016 Vol 3

[Iss 1 Pg 1-19](#)    [Iss 2 Pg 22-56](#)

### 2015 Vol 2

[Iss 1 Pg 01-14](#)    [Iss 1 Pg 15-26](#)



View PDF

Download full issue

Search ScienceDirect

Outline

Highlights

Abstract

Graphical abstract

Keywords

1. Introduction

2. Methodology

3. Results and discussion

4. Conclusions

Declaration of Competing Interest

Acknowledgement

References

Share this article

Get citation

Cited By (11)



### Results in Optics

Volume 4, August 2021, 100083



# An investigation on the influence of temperature variation on the performance of tin (Sn) based perovskite solar cells using various transport layers and absorber layers

Priyanka Roy <sup>a</sup>, Sanjay Tiwari <sup>b</sup>, Ayush Khare <sup>a</sup>

Show more

+ Add to Mendeley Share Cite

<https://doi.org/10.1016/j.rio.2021.100083>

Under a Creative Commons license

Get rights and content

Open access

### Recommended articles

An investigation on the impact of temperatu...  
Materials Today: Proceedings, Volume 39, Part 5, 2...  
View details

Simulation of narrow-bandgap mixed Pb-S...  
Optical Materials, Volume 112, 2021, Article 110751  
View details

Performance analysis of MAPbI<sub>3</sub> based pero...  
Solar Energy, Volume 193, 2019, pp. 948-955  
View details

1 2 Next

# **Use of E – Resources by Post Graduate College Students of Science of Dhamatari Distric, Chhattisgarh: A Study**

**Dr. Santu Ram Kashyap<sup>1</sup>; Deepa Sahu<sup>2</sup>**

Sr. Assistant Professor, SoS in Library & Information Science, PT. Ravishankar Shukla  
University, Raipur (C.G.) – 492010, India<sup>1</sup>; Research Scholar, SoS in Library & Information  
Science, PT. Ravishankar Shukla University, Raipur (C.G.) – 492010, India<sup>2</sup>

sr\_kashyap1976@rediffmail.com

## **ABSTRACT**

*This study attempt to know the use of e – resources by post graduate college students of science of dhamatari district, Chhattisgarh. The main purpose of the study is to know the use of e- resources by the PG Students. The study was based on survey method. The study found that the most of the respondents use the internet daily with 1 – 2 hours. Where majority 278(78.97%) of the respondents use e-books, 343 (94.44%) respondents use e-resources for their study, highest 75 (21.31%) respondents spent 2 - 3 hours on the e-resources. and the maximum 229 (65.06%) respondents faced the slow downloading problem when they use electronic resources, and highest 260 (73.86%) respondents are highly satisfied with e-resources, 69 (19.60%) are satisfied, 13 (3.69%) are not satisfied and 10 (2.84%) respondents fairly satisfied with using e-resources.*

**KEYWORDS:** E-Resources, P.G. Students, Science, Govt. College Dhamtari, Chhattisgarh.

## **INTRODUCTION**

E- Resource is a special type of e –document which is also known as supplementary document of print document. it is available in the electronic/soft format. The major characteristics of e- resources is they provide abstracting and full text information in the online & offline mode which can be Accessed any time from any place through computer and mobile technology. The major types of e – resources are e – books, e – journal, e- database, e- institutional repository, web resources, e-magazine, e- online archives, e – reference book and e- pg pathashala etc. In this context it is boon for college students. We know that presently college students are studying in the digital/ electronic environment. In this context digital/electronic collection of college libraries is very useful for college students because they provide his/her subject related relevant study materials for the study.

Volume No- 1, October 2021

# Journal of The lisforum\_orissa

**Theme- Future of Indian Librarianship:  
Progressive, Regressive or Compulsive?**



[www.lisforumorissa.com](http://www.lisforumorissa.com)

9	Indian Librarianship at the Crossroads <i>Satpathy, Kishor Chandra</i>	61-62
10	Indian Library Professionals Current Scenario <i>Behera, Mukesh</i>	63-63
11	Librarianship in India: A Progressive approach <i>Sahu, Srikanta Kumar</i>	64-65
12	Librarianship: The Confused Profession <i>Mishra, Manoj</i>	66-67
13	Relevance of Indian Academic Library in the Digital Age <i>Sa, Manoj Kumar</i>	68-69
14	Role of LIS schools in future librarianship <i>Maharana, Bibhuti Bhusan</i>	70-71
15	The Future of Indian Librarianship: as Librarians What We Can Do? <i>Behera, Sanat Kumar</i>	72-73
16	The Metamorphosis of Librarianship <i>Maharana, Bulu</i>	74-74

#### Articles in Hindi

1	Granthapal ka Samajik Sarokar <i>Choudhury, BR</i>	75-77
2	Bharatiya Granthalitya: Dasha aur Disha <i>Soni, Neelam</i>	78-81
3	Bhartiya Pustakalayadhakhyata: Bhutkal Bartaman abam Bhabisya <i>Khute, VK and Kashyap, SR</i>	82-86
4	Granthalyitv aur Takniki Gyan ka Vikas <i>Tamrakar, N</i>	87-88
5	Bharatiya Pustakalay Peshewaron ka Bhabishya <i>Sahu, Rekharaj</i>	89-90
6	Bharatiya Pustakalay Peshewaron ka Bhabishya: Pragatishil, Pratigami aur Badhyakari <i>Yadav, Shrawan</i>	91-92
7	Bharatiya Pustakalay Peshewaron ka Bhabishya: Pragatishil, Pratigami aur Badhyakari <i>Pradhan, Suryakant</i>	93-94

भारतीय पुस्तकालयाध्यक्षता: भूतकाल, वर्तमान और भविष्य



**Mr. Vinod Kumar Khunte**

Ph.D (course work)

Sos in Library & Information Science

Pt. Ravishankar Shukla University, Raipur C.G.

E-mail- [Vinodkhunte107@gmail.com](mailto:Vinodkhunte107@gmail.com)



**Dr. Santu Ram Kashyap**

Sr. Assistant Professor

Sos in Library & Information Science

Pt. Ravishankar Shukla University, Raipur C.G.

E-Mail- [sr\\_kashyap1976@rediffmail.com](mailto:sr_kashyap1976@rediffmail.com)

**प्रस्तावना:-**

किसी भी पुस्तकालय का प्रबंधन, व्यवस्थापन, तथा संचालन करने की कला को पुस्तकालयाध्यक्ष कहते हैं। किसी पुस्तकालय का कुशल रूप से व्यवस्थापन तथा उसका संचालन उस पुस्तकालय के पुस्तकालयाध्यक्ष पर निर्भर करता है, वह उसका मुख्य संचालक अधिकारी होता है। ऐसा कहा गया है कि पुस्तकालयाध्यक्ष जितना कुशल और विवकेशील होगा उसका पुस्तकालय उतना ही व्यवस्थित और सफल होगा। सर्वसुविधायुक्त पुस्तकालय और पुस्तकों का पर्याप्त संकलन होने के बावजूद भी अगर पुस्तकालयाध्यक्ष न हो तो ऐसी स्थिति में पुस्तकालय में उपलब्ध सूचना संसाधन तथा ज्ञान प्रदान करने वाली पाठ्य सामग्रियों पाठकों के लिए बहुत ही कम लाभदायक सिद्ध होगी। पुस्तकालय में पाठक रूपी उपयोगकर्ताओं को दी जाने वाली सेवाओं और पुस्तकालय के व्यवस्थापन तथा संचालन से संबंधित अनेक कार्यों को निष्पादित करने हेतु एक भलिभॉति शीक्षित एवं प्रशिक्षित, कुशल, एवं



# Use of E- Resources by College Students of Arts, Social Science and Science Stream of Raipur city: A Comparative Study

**Dr. Santu Ram Kashyap**

Sr. Assistant Professor

SoS in Library & Information Science

PT. Ravishankar Shukla University, Raipur (C.G.) – 492010, India.

\*Corresponding author: [sr\\_kashyap1976@rediffmail.com](mailto:sr_kashyap1976@rediffmail.com)

**Abstract.** The major objective of this study to compare the use of e -resources by students from Arts, Social Science and Science stream and compare preferences of the Use of e - resources by students of Arts, Social Science and Science stream of Raipur city. The study was based on survey method. Among various techniques of Survey Method, Questionnaire Technique was used for the study. Accordingly a Self structured questionnaire was designed to collect data from the regular UG and P G students of various college of Raipur city. The major findings of the study shows that The calculated value is  $\chi^2 (df=2) = 5.32$  and Table value is 5.991 so Ho Hypothesis is Accepted and Ha Hypothesis is rejected it means there are no Significant difference in Use of e - journals between Students of Arts, social Science and Science Stream. and e -book was found to be the most preferred e-resource by students of Arts, Social Science and Science students of Raipur city.

**Keywords:** E -resource, Arts, Social Science and Science students, College, Raipur, Chhattisgarh.

## INTRODUCTION

Normally any kind of material which fulfills our needs is called resources. In the library, books are such kinds of resources that fulfill our information needs. we know that reading is the foremost part of the students. In this context E – resources are the very important and helpful reading materials in pandemic situation for college students because this supports their reading, learning, seminar presentation, preparation of project work and research activities etc. This means that present e - resources are boon for students and it gives a boost to them. e - Resources are such kinds of resources which are available online and offline in the electronic form such as e -Book, e - journal, e - News clipping, e -research report and online database. etc. The Characteristic of e - resources are that it is available on web in E- form which can be accessed anywhere from any places in the world.

## OBJECTIVES OF THE STUDY

1. To Know the Types of e – resources used by College students of Arts, Social Science and Science stream of Raipur city.
2. To identify most important e – resources usually used by college students of Arts, Social Science and Science stream of Raipur city.
3. To compare use of e-resources by students from Arts, Social Science and Science stream of Raipur city.
4. To Know & compare preferences of Use of e- resources by students of Arts, Social Science and Science stream of Raipur city.





## Research Trends in Library and Information Science of Pt. Ravishankar Shukla University Raipur, Chhattisgarh: A Study

Dr. Santu Ram Kashyap

SoS in Library & Information Science, PT. Ravishankar Shukla University, Raipur (C.G.), India  
[sr\\_kashyap1976@rediffmail.com](mailto:sr_kashyap1976@rediffmail.com)

\*Corresponding Author: [sr\\_kashyap1976@rediffmail.com](mailto:sr_kashyap1976@rediffmail.com)

**Abstract:** The present study is an attempt to find out the research trends in the field of Library and Information Science of Pt. Ravishankar Shukla University, Raipur Chhattisgarh. The study was based on the Ph.D. thesis awarded in the field of Library and Information Science between 1991 to 2020. This study was conducted to achieve following objectives like most working area of research in this field, highest no. of thesis done under supervisor and highest research productivity between the year 2016 to 2020. In this context, result found that out of 24 thesis majority of thesis i.e. 07 – 07 were awarded in the area of Bibliometric study and Information seeking behavior. Highest 10 doctoral thesis awarded under the supervision of Prof. A.K. Verma. followed by Prof. Maya Verma with 09 Thesis, Dr. Superna Sengupta with 03 thesis and Dr. Md Imtiaz Ahmed with 02 thesis respectively. The highest research productivity was produced between the year 2016 to 2020. This study will be beneficial for the future researcher to conduct their research.

**Keywords :** Research Trends, Ph – D. Thesis, Library and Information Science, Pt. Ravishankar Shukla University Raipur, Chhattisgarh.

### Introduction

Library and Educational Institute are the two faces of a coin. They cannot survive without each other. It provides opportunities for people to use their leisure time to increase and upgrade their knowledge. Library is a very important institution because it is useful to teachers and researchers for research.

Research plays an important role in the expansion of knowledge and discoveries. It is a scientific program that tells us the relationship between cause and effect. In other words, Research is a systematic investigation to discover new facts and reach the conclusion. It demands accurate investigation and description. According to Francis Rummel “Research is a careful inquiry or examination to discover new information or relationships and to expand and to verify existing knowledge (Verma and Verma). Clifford Woody defines Research as comprises defining and redefining the problem, formulating hypothesis or suggested solutions; collecting, organizing and evaluating data; making deductions and research conclusions; and at last, carefully testing the conclusion to determine whether fits the formulating hypothesis (Kothari).

Pt. Ravishankar Shukla University is one of the renowned and largest higher education institution which was founded in the year 1964. Presently there are 29 teaching departments running under this university. In which School of Studies Library & Information Science is running as an individual department. This department was started in the year 1971, Primarily only B. Lib & I Sc course was running, in the year 1988 M. Lib & I Sc course was started and to promote research in the field of Library and information science Ph D degree is also being provided. First Ph D degree in was awarded in the year 1994 to Mrs. Maya Verma under the supervision of Prof. A.K. Verma. <https://www.prsu.ac.in/academic-departments/utd-departments/School-of-Studies-in-Library-and-Information-Science/69>



## An Evaluation of the Using Library Resources and Services by the Agriculture Scientists at Indira Gandhi Agriculture University Raipur, Chhattisgarh

<sup>1</sup>Dr. D. S. Mahipal, <sup>2,\*</sup>Dr. Santu Ram Kashyap

S.G. CARS- Jagdalpur,(Bastar), Indira Gandhi Agriculture University, Raipur(C.G.), India.  
SoS in Library & Information Science, PT. Ravishankar Shukla University,  
Raipur(C.G.),India.

dsmahipal82@gmail.com, sr\_kashyap1976@rediffmail.com

\*Corresponding Author: sr\_kashyap1976@rediffmail.com

**Abstract:** The aim of this paper is to identify the resources, services and make them accessible that are available at the Nehru Library, Raipur Chhattisgarh and used by its scientists. The sample for this study consisted of 245 of the 265 agricultural scientists who working at Indira Gandhi Agricultural university, Raipur. Questionnaires have been used for the collection of data under the scope of the study. The results of the study indicate that agriculture scientists visited libraries occasionally due to inadequate library resources. In addition it was found that the majority of agriculture scientists were partially satisfied with library resources and services. Indra Gandhi Agricultural University's library offers a variety of electronic resources and services in conjunction with modern resources. Scientists use the Nehru library for their studies and research. Electronic based services are proving to be an important service for scientists. Scientists are satisfied with the services provided by the library.

**Keywords:** Nehru Library, Library Resources and Services, Indira Gandhi Agriculture University, Raipur, Chhattisgarh

### Introduction:

The University library Known as the heart of the university. It provide relevant resources / information to their users through library resources and services. In this context Nehru Library is functioning as Central University Library for constituent and affiliated colleges of Indira Gandhi Krishi Vishwavidyalaya. 23 constituent Colleges and fifteen private colleges, Research Stations and Krishi Vighyan Kendras (KVKs). The Nehru Library established in 1987 after IGKV came in to existence by bifurcation from JNKVV Jabalpur. Before that it was the library of College of Agriculture, Raipur. It has been recognized as Regional Library of Central India by the Indian Council of Agricultural Research in 2005. The Nehru Library of IGKV has been well equipped with the latest communication media and information technologies like Web based information, CD Rom database search, OPAC and internet browsing as it is well connected through LAN/ BSNL leased line. This library has become a HUB connected on LAN with all automated centralized facilities and acting as a nodal centre for disseminating all kind of agricultural information to its users. The library is linked with various consortiums for online journals. Nehru Library maintains around 60000 collections of books, reference book, reports, theses, monograph, back volumes, journals, CD ROM Database and e-resources.

# **Role of Libraries in The Intellectual Development of India**

## **Editors :**

Dr. Sanjay Kumar Dongre  
Rekhray Sahu  
B.R. Choudhari

## **Organized by**

Library and Information Science Department

&

IQAC

Govt. Bilasa Girls' Post Graduate Autonomous College,  
Bilaspur, (Chhattisgarh)



**SAMATA PRAKASHAN**

Kanpur (Dehat) - 209 303

Organized by  
Library and Information Science Department & IQAC Govt.  
Bilasa Girls' Post Graduate Autonomous College, Bilaspur,  
(Chhatisgarh)

ISBN : 978-93-93403-01-8

Book Name:

Role of Libraries in The Intellectual Development of India

Editors :

Dr. Sanjay Kumar Dongre, Rekhraj Sahu, B.R. Choudhari

© Reserved

First Published : 2022

Typesetting :

Rudra Graphics

*All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, mechanical, photocopying, recording or otherwise, with out prior written permission of the publishers]*

Published by

**SAMATA PRAKASHAN**

159/1 Ward No. 12, Bajrang Nagar, Rura,

Kanpur Dehat (U.P.) - 209 303

Mob. : 9450139012, 9936565601

Email - samataprakashanrura@gmail.com

PRINTED IN INDIA

Printed at Sathak Printer, Kanpur.

## संपादकीय

वर्तमान समय में राष्ट्रीय विकास की चर्चा जोरों पर है, पूरे भारत वर्ष में आर्थिक विकास, सामाजिक विकास, धार्मिक एवं राजनीतिक विकास परन्तु बौद्धिक विकास की चर्चा कोई नहीं कर रहे हैं। देश में समय-समय पर बहुत से क्षेत्रों में आधुनिक क्रांति, हरित क्रांति, श्वेत क्रांति, पीली क्रांति हुई लेकिन क्या ये सब के बावजूद भी हमारा देश विकासशील देश से विकसित देश की श्रेणी में अपना स्थान बना पाया, नहीं बना पाया। यह चिन्तन का विषय है। जब तक देश में बौद्धिक क्रांति (शिक्षा) नहीं होगी, विकसित देश की कल्पना करना निरर्थक है, और बौद्धिक विकास पुस्तकें एवं पुस्तकालय से ही संभव है, आवश्यकता है कि सम्पूर्ण भारत देश में पुस्तकालय की स्थापना एवं उसका विस्तार किया जाये।

सूचना प्रौद्योगिकी के माध्यम से पुस्तकालय एवं शिक्षा में उपयोग कर देश की शिक्षा-प्रसार नीति को संबल बनाया जा सकता है। पुस्तकें एवं पुस्तकालय ही एक ऐसा माध्यम है जिससे बौद्धिक क्रांति संभव हो सकता है। पुराने समय में लोगों के लिए ज्ञान का एक ही स्थान होता था जहाँ पर अध्ययन-अध्यापन हेतु लोग पुस्तकालय में जाते थे। अच्छे पढ़े-लिखे लोग अपनी घर में पुस्तकालय बना लेते थे। पुस्तक पढ़ने का अपना एक अलग ही आनन्द है, आप जितना पुस्तक पढ़ेंगे उतनी ही अपनी अज्ञानता का बोध होगा। पुस्तकालय से ही मनुष्य का सर्वांगीण विकास संभव हो पाता है। प्राचीन से लेकर वैदिक काल में पाण्डुलिपियों का आविष्कार से लेकर पुस्तकों की अन्तिम पड़ाव तक पुस्तकालय की महत्ता को नकारा नहीं जा सकता है।

पुस्तकालय की अनिवार्यता एवं उपादेयता तथा इस सूचना प्रौद्योगिकी की काल में पाठक तक पुस्तकें कैसे पहुँचें, पुस्तकालय में प्रौद्योगिकी का उपयोग कर पाठकों को पुस्तकालय से कैसे कनेक्ट करें। ना आसान हो गया है। इन सब समस्याओं का दूर करते हुए पुस्तकालय स्वयात्न सॉफ्टवेयर कोहा/ डीस्पेश/ आरएफआईडी तकनीक का प्रयोग कर पाठकों की संख्या में इजाफा किया जा सकता है।

पुस्तकालय तनाव से मुक्ति और सकारात्मक चिन्तन का स्थान होता है, ज्ञान पिपासु लोग अपने जिज्ञासुओं की पूर्ति करते हैं। आज से हजारों वर्ष पहले समाज सुधारकों, ऋषि मुनियों, विद्वानों, चिन्तकों द्वारा रचित विचारों का कोश

## अनुक्रम

है। पुस्तकालय किसी भी शैक्षणिक संस्थान की आधार व हृदय स्थल होता है। आज हम जिस गति से औद्योगिकीकरण या अन्य क्षेत्रों में विकास कर रहे हैं। जब तक बौद्धिक दृष्टि से हमारा देश विकास नहीं कर लेगा तब तक विकसित देश की श्रेणी में नहीं जा सकते, विकासशील की अवस्था में ही रहेंगे। प्राचीन और सनातन भारतीय ज्ञान और विचार की परम्परा के आलोक में यह स्पष्ट होता है कि तक्षशिला, नालंदा, विक्रमशिला और वल्लभी जैसे प्राचीन भारत के विश्व स्तरीय संस्थानों ने अध्ययन के विविध क्षेत्रों में शिक्षण और शोध के उंचे प्रतिमान स्थापित किये थे इसी शिक्षा वयवस्था ने चरक, सुश्रुत आर्यभट्ट, वराह मिहिर, भास्कराचार्य, ब्रह्मगुप्त, चाणक्य, माधव, पाणिनी, पतंजलि, नागार्जुन, गौतम, गार्गी, जैसे अनेकों महान विद्वानों को जन्म दिया इन विद्वानों ने वैश्विक स्तर पर ज्ञान के विविध क्षेत्रों जैसे गणित, खगोल विज्ञान, धातु विज्ञान, चिकित्सा विज्ञान, सिविल इंजीनियरिंग, भवन निर्माण, दिशा ज्ञान योग, ललित कला, शतरंज इत्यादि में प्रमाण रूप से मौलिक योगदान किये हैं। किन्तु विदेशी आक्रान्ताओं हमारी सभ्यता एवं संस्कृति को नष्ट करने का प्रयास कर हमारी रचनात्मक एवं साहित्यिक विरासत जला जाले। शायद यदि वह होते तो आज भी हमारा देश बौद्धिक रूप से मजबूत एवं सोने की चिड़िया ही कहलाता।

देश-प्रदेश के कोने-कोने से पथारे ग्रंथालय व्यवसायी, प्रोफेसर एवं छात्र-छात्राओं जिनके मार्गदर्शन एवं भागीदारी से यह कार्यक्रम सफल रहा। मैं उन तमाम साधियों को धन्यवाद ज्ञापित करता हूँ कि जिनके सहयोग के बिना यह कार्यक्रम सफल नहीं हो पाता।

उम्मीद करता हूँ कि संपादकीय टीम द्वारा चयनित रिसर्च पेपर अनुसंधान एवं शोध के क्षेत्र में पुस्तकालय एवं सूचना विज्ञान में संलग्न प्राध्यापकों, छात्र-छात्राओं एवं शोधार्थियों के लिए उपयोगी होगा।

### बी. आर. चौधरी

ग्रंथपाल एवं विभागाध्यक्ष  
पुस्तकालय एवं सूचना विज्ञान विभाग  
शासकीय बिलासा कन्या स्नातकोत्तर  
महाविद्यालय बिलासपुर (छ.ग.)

1. राष्ट्रीय शिक्षा नीति 2020 और पुस्तकालय  
(National Education Policy 2020 and Library)  
**विनोद कुमार खुटे, डॉ. संतू राम कश्यप**  
बौद्धिक विकास में पुस्तकालय की उपादेयता  
**डॉ. संजय कुमार डोंगरे**  
संस्कृत विषय के अध्ययन में ई.पी.जी पाठशाला की भूमिका  
**डॉ. सीमा पाण्डेय**  
21
2. Awareness and Utilization of the Electronic Resources by the  
Undergraduate Students of Indira Gandhi Krishi  
Vishwavidyalaya, Raipur  
**Rekharaj Sahu, Brajesh Tiwari**  
23
3. Use of E-Resources, Mobile Apps and It's Impact on Library Services  
**Ajay Kumar Shrivastava**  
34
4. इंदिरा गाँधी कृषि विश्वविद्यालय, रायपुर (छ.ग.) के अंतर्गत महाविद्यालयों के  
पुस्तकालय वेबसाइट का सामग्री विश्लेषण : एक अध्ययन  
(Content Analysis of Colleges Library Websites Constituent to Indira  
Gandhi Krishi Vishwavidyalaya Raipur (C.G.): A Study)  
**श्रवण यादव, डॉ. हरीश कुमार साहू**  
40
5. वर्तमान संदर्भ में डिजिटल लाइब्रेरी की महत्ता  
**धनकुमार महिलारंग, श्रीमती भुलेश्वरी साहू**  
48
6. Use and importance of Mobile Technology and Application in Library  
Services  
**Anil Kumar Useendi**  
56
7. The Role of Librarian in New Education Policy (NEP) 2020: A Li-  
brarian Point's of View  
**Madan Lal**  
63
8. Blended Library during and post COVID: Best Practices with reference  
to KV Bilaspur  
**Dr. Rajesh Sharma, Praveen Kumar Sahu, Shraddha Sharma** 79

11. Content Analysis of Central University and State Government University Library Websites in Madhya Pradesh State <b>Kundan Jha, Dr. Sarita Mishra</b>	
12. महामारी के दौर में ग्रंथालयों में क्लाउड कम्प्यूटिंग की महत्ता <b>नवीन कुमार ताम्रकार</b>	87
13. पुस्तकालय सूचना सेवाएँ पराम्परिक और आई.सी.टी.के विशेष संदर्भ में <b>सालिक राम, डॉ. सरिता मिश्रा</b>	107
14. पुस्तकालय और पुस्तकालयाध्यक्ष की भूमिका बदलते परिवेश के परिपेक्ष में : एक स्व विचार <b>दिप्ती तिग्गा, डॉ. सरिता मिश्रा</b>	117
15. ग्रंथालय का डिजिटिजेशन तकनीक के विशेष संदर्भ में समीक्षात्मक अध्ययन <b>डॉ. आर.जी. यादव, ओमप्रकाश राठौर</b>	126
16. छत्तीसगढ़ राज्य में स्थापित शिक्षण स्नातकोत्तर महाविद्यालयों के पुस्तकालयों में डिजिटलीकरण एवं प्रौद्योगिकी का उपयोग द्वारा उपयोग एक अध्ययन : रायपुर जिले के विशेष संदर्भ में <b>प्रमोद कुमार कुर्रे, डॉ. गिरजा शंकर पटेल</b>	129
17. महामारी काल में पुस्तकालयों की भूमिका <b>राम कुमार श्रीवास</b>	135
18. कोरोना कालके दौरान पुस्तकालय की भूमिका <b>स्वाती तिवारी</b>	142
19. कोविड-19 प्रभाव और भारत में पुस्तकालय का भविष्य <b>सुनिल कुमार कुर्रे</b>	150
20. पुस्तकालयों में डिजिटलीकरण प्रौद्योगिकी (Digitalization Technology in Libraries) <b>कु श्रेया ताम्रकार</b>	156
21. Transforming Academic libraries into digital libraries : A Review <b>Amrit Kumar Porte</b>	164
22. बौद्धिक विकास के पर्याय बौद्धिकालीन पुस्तकालय एवं नई राष्ट्रीय शिक्षा नीति 2020 <b>बी. आर. चौधरी</b>	170
	179

# 1. राष्ट्रीय शिक्षा नीति 2020 और पुस्तकालय

(National Education Policy 2020 and Library)

\*विनोद कुमार खुंटे

\*\*डॉ. संतू राम कश्यप

सारांश

शिक्षा के क्षेत्र में पुस्तकालय प्रारंभिक शिक्षा से लेकर उच्चतर शिक्षा एवं शोध कार्यों के लिए एक अनिवार्य अंग है। बिना पुस्तकालय के एक मजबूत एवं सशक्त शिक्षा व्यवस्था की कल्पना अशुभी है। पुस्तकालय को शिक्षा का एक अनिवार्य अंग मानते हुए राष्ट्रीय शिक्षा नीति 2020 के द्वारा वर्तमान समय एवं भविष्य को ध्यान में रखकर पुस्तकालय के स्वरूप में बदलाव एवं उसके विकास के लिए महत्वपूर्ण अनुशंसाओं का प्रतिपादन किया गया है।

**शब्द संकेत**

राष्ट्रीय शिक्षा नीति, स्वतन्त्रता, पुस्तकालय, प्रौढ़ शिक्षा, निःशुल्क शिक्षा, वैश्विक महाशक्ति।

**प्रस्तावना**

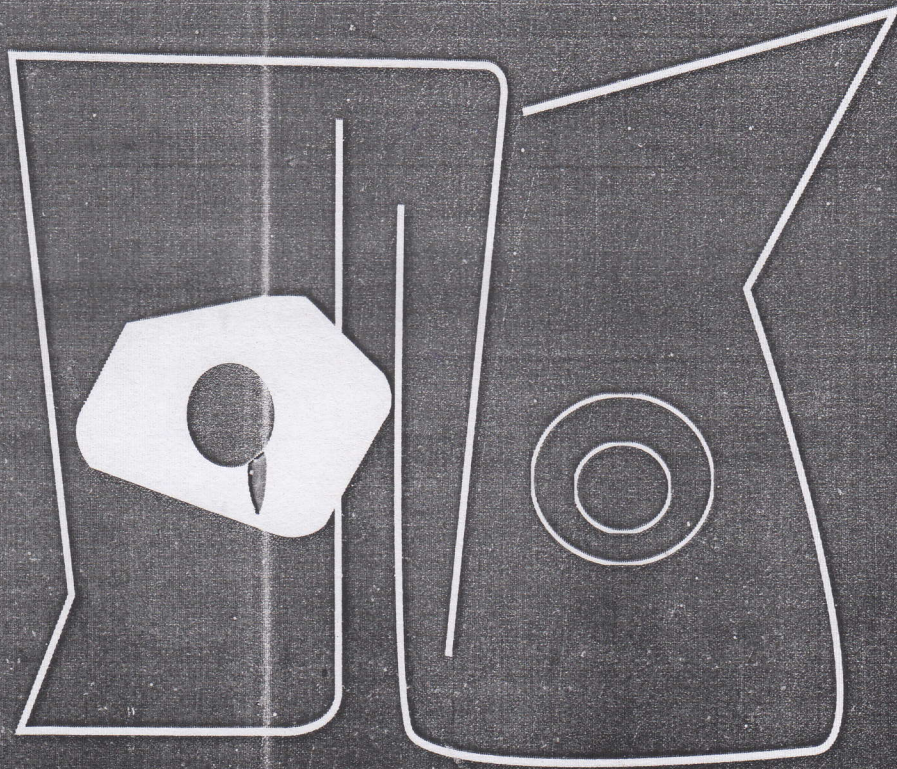
शिक्षा किसी भी राष्ट्र के विकास की आधारशीला है, जो सम्पूर्ण सामाजिक, राजनैतिक, वैज्ञानिक, तकनीकी एवं वैश्विक उन्नति को सुनिश्चित करती है, साथ ही समाज को दिशा प्रदान करती है, किसी भी राष्ट्र का उत्थान उस राष्ट्र में प्रदान की जा रही शिक्षा की गुणवत्ता पर निर्भर करती है जो आने वाले भविष्य में उस राष्ट्र के विकास एवं सफलता का निर्धारण करती है। सरकार द्वारा शिक्षा के स्तर में सुधार करने एवं उचित स्वरूप प्रदान करने के लिए अनेक राष्ट्रीय आयोगों का गठन एवं योजनाओं का निर्माण किया जाता है। साथ ही समय-समय पर आवश्यकता के अनुरूप उन योजनाओं एवं नीतियों में संशोधन भी किया जाता है, जिससे कि बदलते समय एवं आवश्यकता के अनुसार उन्हें अद्यतन स्वरूप प्रदान किया जा सके और ज्यादा से ज्यादा शिक्षा योजनाओं एवं नीतियों को सफलतापूर्वक प्रभाव में लाकर उनका क्रियान्वयन किया जा सके। राष्ट्र में शिक्षा व्यवस्था को सशक्त एवं विकसित करने के लिए जितने भी

# ग्रंथालय विज्ञान

खण्ड 53 अंक 1

ISSN 0973-564X

जनवरी - जून 2022



प्रोफेसर कौला ग्रंथालय  
तथा  
सूचना विज्ञान सन्दान

(विश्वविद्यालय अनुदान आयोग द्वारा वर्ष 2017-2018 एवं 2018-2019 हेतु अनुमोदित  
ग्रन्थालय एवं सूचना विज्ञान विषय की हिन्दी की एकमात्र पत्रिका)

ISSN 0973-564x

## ग्रन्थालय विज्ञान

पूर्व समीक्षित शोध पत्रिका

खण्ड 53 अंक 1  
जनवरी-जून, 2022

मुख्य सम्पादक: डॉ. एस.पी. सूद

सह सम्पादक: डॉ. नीरजा वर्मा

उप सम्पादक: डॉ. अरविन्द कुमार शर्मा

डॉ. अनिल कुमार धीमन्

सहायक सम्पादक: डॉ. गौतम सोनी

उमेश शर्मा

प्रोफसर कौला ग्रन्थालय तथा  
सूचना विज्ञान संदान



## विषय सूची

	ग्रंथालय एवं सूचना विज्ञान क्षेत्र के चर्चित व्यक्तित्व प्रोफेसर रोशन लाल रैना	1
1.	भारतीय ग्रंथालयों में ई-लर्निंग, ई-खोज एवं ई-संसाधनों का प्रबंधन (Management of E-Learning, E-Search and E-Resources in Indian Libraries) डॉ. रश्मि सिकरवाल, डॉ. सरिता वर्मा	3
2.	इलेक्ट्रॉनिक संसाधन : एक परिदृश्य (Electronic Resources: An Overview) डॉ. संतू राम कश्यप	8
3.	सामग्री प्रबंध प्रणाली का ग्रंथालयों में अनुप्रयोग (Application of Content Management System in Libraries) डॉ. भवनाथ पाण्डे, सुश्री ऋजु पाण्डेय	17
4.	शोध में आनलाइन डाटा संग्रह के साधन (Online Data Collection Tools in Research) पूनम गौर, डॉ. नीरजा वर्मा	24
5.	ग्राहक संबंध प्रबंधन और ग्रंथालय (Customer Relation Management and Libraries) डॉ. (श्रीमती) यशोदा रानी, डॉ. अनिल कुमार धीमान	39
6.	ग्रंथालय कार्मिकों के सूचना संबंधी व्यवहार पर वेब सोशल मीडिया का प्रभाव : एक अध्ययन (Impact of Web Social Media on Information Seeking Behaviour of Library Professionals : A Study) रजनी सिंह, डॉ. जितेन्द्र श्रीवास्तव	47
7.	नई शिक्षा नीति 2020 : ग्रंथालय में ग्रंथालयी की भूमिका (New Education Policy 2020 : Role of Librarian in a Library) प्रो. जे.एन. गौतम, रितुराज पाराशर	63
8.	मुक्त शैक्षिक संसाधन (Open Education Resources) सुश्री साहित्यांजलि चंद्र, डॉ. भवनाथ पाण्डे	74
9.	ग्रंथमिति और सामाजिक नेटवर्क विश्लेषण के लिए सॉफ्टवेयर अनुप्रयोग: एक अध्ययन (Software Applications for Bibliometric and Social Network Analysis: A Study) अमृता सिंह जादौन, डॉ. अरविन्द कुमार शर्मा	80

## 2

## इलेक्ट्रॉनिक संसाधन : एक परिदृश्य (Electronic Resources : An Overview)

डॉ. संतू राम कश्यप\*

[इलेक्ट्रॉनिक संसाधनों का परिचय देते हुए इसके प्रकारों की गणना करता है। इसकी विशेषताओं, आवश्यकताएं, लाभ-दोष, समानताएं एवं अंतर इत्यादि का संक्षिप्त वर्णन करता है।]

### 1. प्रस्तावना (Introduction)

आज का युग सूचना क्रांति का युग है, जहाँ पर लगातार सम्पूर्ण विश्व में तीव्र गति से सूचनाओं के प्रकाशन से लेकर इनको प्रचार प्रसार में वृद्धि हो रही है। इसे सूचना विस्फोट के नाम से भी जाना जाता है। इसी परिप्रेक्ष्य में वर्तमान समय में दो प्रकार के सूचना संसाधनों का प्रचलन है, पहला मुद्रित तथा दूसरा अमुद्रित, इनमें से मुद्रित (Printed) सूचना संसाधनों का प्रचलन कई शताब्दियों से चला आ रहा है, लेकिन अमुद्रित (Non Printed) सूचना संसाधनों का प्रचलन कम्प्यूटर तथा सूचना एवं संचार प्रौद्योगिकी (ICT) के आगमन के साथ हुआ है। जिसे इलेक्ट्रॉनिक संसाधन कहा जाता है।

इलेक्ट्रॉनिक संसाधन वह सूचना संसाधन है जो इलेक्ट्रॉनिक स्वरूप में उपलब्ध होते हैं। जिसे इलेक्ट्रॉनिक मशीनों जैसे कम्प्यूटर के माध्यम से बनाया जाता है तथा इलेक्ट्रॉनिक माध्यमों से पढ़ा जाता है। इस प्रकार इनके अनेक लाभ हैं जैसे कम समय में तीव्र गति से सूचना प्राप्त करना, कम्प्यूटर से आसानी पूर्वक पढ़ा जाना, डाउनलोड करना विषयों पर अद्यतन बनाये रखना, एक ही समय में एक संसाधन को अनेकों उपयोगकर्ताओं द्वारा उपयोग किया जाना तथा समय की बचत करना इत्यादि। इस प्रकार आज इलेक्ट्रॉनिक संसाधन मुद्रित संसाधनों के पूरक के रूप में उभर कर सामने आये हैं जिनको शिक्षकों, शोधार्थियों, विद्यार्थियों से लेकर सम्पूर्ण ग्रन्थालय उपयोगकर्ताओं द्वारा उपयोग किया जा रहा है।

### 2. इलेक्ट्रॉनिक संसाधनों के प्रकार (Types of Electronic Resources)

इलेक्ट्रॉनिक संसाधनों के प्रकार निम्नलिखित हैं :

SHORT COMMUNICATION



## Ultradian, circadian, and circaseptan rhythms in the patterns of usage of Facebook messenger

Ananya Diwan<sup>a</sup>, Rakesh Kumar Swain <sup>b</sup>, Sarojini Minz <sup>b</sup>, Arti Parganiha <sup>c</sup>  
and Atanu Kumar Pati <sup>b,c,d</sup>

<sup>a</sup>Center for Basic Sciences, Pt. Ravishankar Shukla University, Raipur, India; <sup>b</sup>School of Zoology, Gangadhar Meher University, Sambalpur, India; <sup>c</sup>School of Life Sciences, Pt. Ravishankar Shukla University, Raipur, India; <sup>d</sup>Center for Translational Chronobiology, Pt. Ravishankar Shukla University, Raipur, India

### ABSTRACT

The Facebook Messenger (FBM) is one of the most popular instant messaging social apps, launched by Facebook in 2010. As of October 2019, there were about 1.3 billion FBM users worldwide. In this study, we analyzed periodicities in the online activity patterns of users in FBM. We did not recruit any subjects in this study; rather four of us used our own FBM accounts to reveal the presence of any rhythms with  $\tau = 12$  h or  $\tau = 24$  h or  $\tau = 168$  h in the patterns FBM usage among our FB friends. We log-transformed the time series data and subjected those to Cosinor rhythmometry. The peaks in the daily pattern of FBM usages, revealed from Cosinor analyses, and harmonics curve fittings validated the presence of multi-frequency rhythms in the longitudinal time-series data captured over a period of 16 days. The underlying basis of the observed multi-frequency rhythms could be attributed to the phenomenon of social synchronization. The current findings might bear commercial applications with special reference to targeted content advertising (TCA).

### ARTICLE HISTORY

Received 10 March 2020  
Accepted 23 March 2020

### KEYWORDS

Ultradian; circadian;  
circaseptan; patterns in FBM  
usage; harmonic curve  
fitting; TCA




## 1. Introduction

The Facebook Messenger (FBM) is one of the most popular instant messaging social apps. The Facebook developed this App in 2008 (Hendrickson 2008; Farber 2008) and launched its messaging platform in 2010 (Siegler 2010). This social media platform enables its users to share image, video, GIF, text messages, voice messages, and pretty stickers to their online friends. These features attract the users towards this Social Networking Apps. Like WhatsApp, it has also voice and video calling facilities. The FBM became instantly popular as it doesn't require any user ID and/or password at the time of login, if a user has an FB account. A user can easily have access to the FBM at any time and from any location. As of October 2019, there were about 1.3 billion FBM users worldwide (Statista.com 2019; <https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/>). It is believed that it may attain a staggering figure of 2.48 billion by 2021. As per the NapoleonCat survey, the

ORIGINAL REPORT



## Circannual production rhythms of seven commercially important fishes in the Chilika lagoon

Prasanti Mishra<sup>a,b</sup>, Amita Kumari Mohanty<sup>a</sup>, Rakesh Kumar Swain <sup>b</sup>,  
Arti Parganiha <sup>c,d</sup> and Atanu Kumar Pati <sup>b,c,d</sup>

<sup>a</sup>Aquaculture Production Division, Central Institute of Freshwater Aquaculture (Indian Council of Agricultural Research), Bhubaneswar, India; <sup>b</sup>School of Zoology, Gangadhar Meher University, Sambalpur, India; <sup>c</sup>School of Studies in Life Science, Pandit Ravishankar Shukla University, Raipur, India; <sup>d</sup>Center for Translational Chronobiology, Pandit Ravishankar Shukla University, Raipur, India

### ABSTRACT

The main objective of this investigation was to delineate spatio-temporal patterns in annual production of seven species of fishes inhabiting the famous Chilika lagoon. The data were collected from 19 landing centers located across four different geographical sectors of the lagoon over a period of two consecutive years. Using Cosinor rhythmometry, statistically significant circannual rhythms of production in all seven species of fishes were validated at the group level either at one or multiple landing centers of the lagoon. The peaks of the circannual rhythms were subjected to Bray–Curtis cluster analysis and similarities among the landing centers apropos the peak timings of the circannual rhythms in production of fish species was determined. Three distinct clusters were witnessed apropos the peaks at different time of the year and at different sectors of the lagoon. This spatiotemporal relationship reflects how temporal abundance of fish species is distributed to avoid conflicts and competitions among themselves along the annual time scale. The findings reported here might help in making strategy to maximize annual fish yield. That will also help in the management of biodiversity of the lagoon.

### ARTICLE HISTORY

Received 11 December 2019  
Accepted 27 March 2020

### KEYWORDS

Spatiotemporal variability; circannual rhythms in fish; production; biodiversity management; chilika lagoon

## 1. Introduction

The species interaction in a community takes place at different levels, namely competition, mutualism and predation (Tulloch et al. 2018). The level and intensity of species interaction also vary depending on the types of the habitat/niche. There are numerous studies on the species interaction in brackish water lagoons. A majority of the studies, reported on species interaction in different lagoons, includes spatial distribution of species in the high marsh (Bortolus et al. 2002), fish species richness and salinity (Sosa-López et al. 2007), intra-annual relationship between zooplankton and abiotic factors (Feike and Heerkloss 2008), co-occurrence of one species with another (Boscutti et al. 2018), effects of global warming and salinisation on the mortality of ephemeral wetland predator (Cuthbert et al. 2019), impact of climate change on species in brackish water lagoon (Bruçet et al. 2009),

**CONTACT** Prasanti Mishra  [mishra.prasanti@gmail.com](mailto:mishra.prasanti@gmail.com)  School of Zoology, Gangadhar Meher University, Amruta Vihar, Sambalpur 768 004, Odisha, India

ARTICLE



## Predictive role of socio-demographic and chronotype on health-related quality of life of cancer patients from southeastern India

Armiya Sultan <sup>a</sup>, Saba Taja<sup>a</sup>, Vivek Choudhary<sup>b</sup> and Arti Parganiha <sup>a,c</sup>

<sup>a</sup>Chronobiology and Animal Behavior Laboratory, School of Studies in Life Sciences, Pandit Ravishankar Shukla University, Raipur, India; <sup>b</sup>Regional Cancer Center, Dr. B.R. Ambedkar Memorial Hospital, Raipur, India; <sup>c</sup>Center for Translational Chronobiology, Pandit Ravishankar Shukla University, Raipur, India

### ABSTRACT

It is well known that cancer and its treatment produce marked impact on the health-related quality of life (HRQoL) of cancer patients. Research concerning impact of chronotype on HRQoL in cancer patients is almost not studied yet, but the interests are growing in several diseases. Present study was carried out to explore the impact of socio-demographics, chronotype and consumption of tobacco, alcohol and sleeping medicine on HRQoL of Indian oncology patients. Self-reported Quality-of-Life questionnaire (EORTC QLQ-C30), Hospital Anxiety and Depression Scale (HADS), and Morningness-Eveningness Questionnaire (MEQ) were administered to the cancer patients (N = 1000) in the native Hindi language. Results revealed that among the socio-demographic factors, only age exhibited significant negative association with physical, role and cognitive functioning and positive association with symptoms, namely fatigue and pain. Interestingly, chronotype was found to be positively associated with emotional functioning and negatively with nausea-vomiting, dyspnoea, diarrhoea and depression. Patients who consumed tobacco, alcohol or sleeping medicine exhibited lower functioning and higher symptoms. Further, treatment of cancer also produced effect on a few measures of HRQoL of patients. In conclusion, age, chronotype and consumption of tobacco, alcohol or sleeping medicine were found to be important determinants of HRQoL of the patients.

### KEYWORDS

Cancer patients; health-related quality of life; socio-demographic; chronotype; addictive habits

## 1. Introduction

In oncological trials and practices, health-related quality of life (HRQoL) is considered as an important end point along with the tumour response rate, and disease-free and overall survival of the cancer patients. HRQoL includes patient's physical, psychological, and social wellbeing (Parganiha et al. 2014; Sultan et al. 2017a, 2018a). It is well known that cancer and its treatment produce marked impact on the anxiety, depression and HRQoL of cancer patients (Mystakidou et al. 2005; Sultan et al. 2017b). However, the impact may depend on the gender, age, type, stage and grade of cancer; type of treatment and its

**CONTACT** Arti Parganiha  [arti.parganiha@gmail.com](mailto:arti.parganiha@gmail.com)  School of Studies in Life Science, Pandit Ravishankar Shukla University, Raipur 492010, India



# Time-of-day and seasonal variations in foraging behavior of street cattle of urban Raipur, India

Bhupendra Kumar Sahu <sup>a</sup>, Arti Parganiha <sup>a,b</sup> and Atanu Kumar Pati <sup>a,b,c</sup>

<sup>a</sup>School of Studies in Life Science, Pandit Ravishankar Shukla University, Raipur, India; <sup>b</sup>Center for Translational Chronobiology, Pandit Ravishankar Shukla University, Raipur, India; <sup>c</sup>School of Zoology, Gangadhar Meher University, Sambalpur, India

## ABSTRACT

We studied time-of-day and seasonal variations in the foraging behavior of street cattle in Raipur city, India. We recorded the foraging behavior of street cattle at 48-time points each day for over three consecutive days at 10 different locations of Raipur city across three distinct seasons of the year. We log-transformed the time series data and employed Single Cosinor to compute the characteristics of time-of-day variation in foraging activity. We also determined the effects of the factors “time-of-day” and “season” on foraging behavior and the number of cattle. We found statistically significant time-of-day variation in foraging pattern with the peaks located mostly at midday hours, irrespective of seasons. The amplitude of foraging was the least in the summer as compared with the rainy and the winter seasons. The factors “time-of-day” and “season” modulated both foraging activity and frequency of cattle on the streets statistically significantly. The observed spatiotemporal patterns in the foraging behavior of cattle on the streets might provide useful information to the stakeholders engaged in mitigating the urban cattle menace in Raipur city and elsewhere in the world.

## ARTICLE HISTORY

Received 25 April 2020  
Accepted 8 July 2020

## KEYWORDS

Time-of-day variation; seasonal variation; foraging behavior; street cattle; cattle menace

## 1. Introduction

Bovine species are familiar to humans. They were domesticated from time immemorial for the purpose of meat and milk. Cattle population has worldwide distribution. A sizable number of cattle, nearly 305 million head (30.44% of the global population), are present in India. This makes India a leading country in the world for cattle population (Cook 2019). Recently released 20<sup>th</sup> Livestock Census report of India (2019) indicated that out of 302.79 million bovine population (Cattle, Buffalo, Mithun, and Yak), 192.49 million consists of cattle (cow and ox) only. The report also revealed a 0.8% increase in the cattle population in India over the data recorded in the last livestock census (19th Livestock Census 2012). A large number of stray street cattle wander freely on the street in urban cities of India. Continuous overexploitation and shrinkage of grassland might be the cause of the above phenomenon (19th Livestock Census 2012; Gowen 2018; Arya et al. 2019; Sahu et al. 2019).

SHORT COMMUNICATION



# Circadian rhythm in the pattern of online usage of Facebook messenger during the COVID-19-triggered lockdown: a sequel to the pre-pandemic study

Rakesh Kumar Swain <sup>a</sup>, Sarojini Minz <sup>a</sup>, Arti Parganiha <sup>b,c</sup>, Ananya Diwan<sup>d</sup>  
and Atanu Kumar Pati <sup>a,b,c</sup>

<sup>a</sup>School of Zoology, Gangadhar Meher University, Sambalpur, India; <sup>b</sup>School of Studies in Life Science, Pandit Ravishankar Shukla University, Raipur, India; <sup>c</sup>Center for Translational Chronobiology, Pandit Ravishankar Shukla University, Raipur, India; <sup>d</sup>Center for Basic Sciences, Pandit Ravishankar Shukla University, Raipur, India

## ABSTRACT

The Government of India imposed the strictest lockdown from 25 March 2020 till 31 May 2020 to control the spread of coronavirus outbreak. Consequently, about 1.38 billion people were under home confinement. Before the COVID-19 pandemic, we studied circadian rhythm (CR) in the usages of Facebook Messenger (FBM), as a group phenomenon, and published the findings in this journal. We thought it would be worthwhile to carry out a sequel study to assess if there are any changes in the CR in the patterns of digital activity of the FBM users during the COVID-19-triggered lockdown. All the authors of this paper harvested real-time data from their FBM account for over 16 consecutive days between 26 March and 17 April 2020. A statistically significant CR in the digital activity pattern of FBM friends of all the authors was validated. Results of one-way repeated measures ANOVA revealed a statistically significant higher Mesor and amplitude of the rhythm in FBM activity patterns during the lockdown; however, acrophase remained unchanged. We concluded that the COVID-19-triggered lockdown did not affect the location of the peaks and the persistence of CR in the online activity patterns of FBM users.

## ARTICLE HISTORY

Received 9 July 2020  
Accepted 14 August 2020

## KEYWORDS

COVID-19 pandemic;  
lockdown; circadian rhythm;  
patterns in FBM usage; pre-  
lockdown

## 1. Introduction

The COVID-19 pandemic provides a unique opportunity to study the impact of lockdown on physiological, psychological, and behavioral responses in the human population. It is very much likely that the physiological and psychosocial behavior of a person under prolonged home confinement would be affected (Majumdar et al. 2020; Sinha et al. 2020). The governments of several countries restricted the people from stepping out of their homes soon after the declaration of COVID-19 as a pandemic. As a consequence, people got little exposure to direct sunlight during

ORIGINAL REPORT



# Does exposure to radiofrequency radiation (RFR) affect the circadian rhythm of rest-activity patterns and behavioral sleep variables in humans?

Margaret Messiah Singh<sup>a</sup>, Priyanka Chandel<sup>a</sup>, Atanu Pati <sup>a,b,c</sup> and Arti Parganiha <sup>a,b</sup>

<sup>a</sup>School of Studies in Life Science, Pandit Ravishankar Shukla University, Raipur, India; <sup>b</sup>Center for Translational Chronobiology, Pandit Ravishankar Shukla University, Raipur, India; <sup>c</sup>Department of Zoology, Gangadhar Meher University, Sambalpur, India

## ABSTRACT

We evaluated the effects of the exposure to radio-frequency radiation emanating from the base transceiver station (BTS) on the characteristics of circadian rest-activity rhythm and behavioral sleep variables in humans. We performed this exploratory field study in a sample of 89 healthy subjects randomly chosen out of 1434 individuals surveyed for the purpose. We divided 89 subjects into five groups, including the control, as a function of distance from the BTS. The E-field strength was higher in the groups of the inter-tower region and between 0 and 150 m away from the BTS. The E-field (distance) did not significantly affect the circadian rhythm parameters and behavioral sleep variables, except a marginal delay in the peak timings of the rest-activity rhythm of subjects in the inter-tower and 300–500 m groups. Notable secondary effects of the factor gender were noticed on circadian amplitude, sleep efficiency, dichotomy index, and wake after sleep onset. We concluded that exposure to radiation from the BTS did not modulate actigraphy-based behavioral sleep variables of people residing around BTS installations. We recommend more extensive field-based studies with rigorous longitudinal designs to validate the effects of radiation from the BTS in humans.

## ARTICLE HISTORY




Received 8 October 2020  
Accepted 16 June 2021

## KEYWORDS

BTS; RF-EMR; actigraphy; rest-activity rhythm; behavioral sleep variables; human

## 1. Introduction

In modern society, we have an intimate association with the telecommunication system comprising mobile phones (MPs) and their base transceiver stations (BTSs). Each BTS operates in the radiofrequency range. According to the Australian Radiation Protection and Nuclear Safety Agency (ARPANSA), the non-ionizing radio-frequency electromagnetic field (RF-EMF) ranges from 3 kilohertz (kHz) to 300 gigahertz (GHz). The number of BTS installations is rapidly rising over the last decade to meet the increasing use of smart-phones for social media, online services, and internet access (Barrile et al. 2009; Kaushal et al. 2012; Haryono and Gunawan 2020). Deployment of BTS in residential areas makes humans exposed to radiofrequency radiation (RFR) persistently. People living in BTS

**CONTACT** Arti Parganiha  [arti.parganiha@gmail.com](mailto:arti.parganiha@gmail.com)  School of Studies in Life Science, Pandit Ravishankar Shukla University, Raipur, India; Center for Translational Chronobiology, Pandit Ravishankar Shukla University, Raipur, India  
 Supplemental data for this article can be accessed [here](#).





# Screening of Obstructive Sleep Apnea (OSA) Risk and Study of Its Predictors in a Population of Adult Indians

Noorshama Parveen<sup>1</sup> · Babita Pande<sup>2</sup> · Atanu Kumar Pati<sup>1,3,4</sup> · Arti Parganiha<sup>1,4</sup>

Received: 31 December 2021 / Accepted: 19 May 2022 / Published online: 18 June 2022  
© The Author(s), under exclusive licence to Springer Nature Singapore Pte Ltd. 2022

## Abstract

**Purpose** The current study is the first attempt to screen obstructive sleep apnea (OSA) risk in adult populations of Chhattisgarh, India. A few predictors of OSA, such as socio-demographic variables, excessive daytime sleepiness (EDS), behavioral sleep variables, and chronotype were also investigated.

**Methods** Five hundred eleven (167 males and 344 females) randomly chosen healthy subjects participated in the study. The STOP-BANG and Modified Berlin Questionnaires (MBQ) were used for the screening of OSA. The Epworth Sleepiness Scale was used to determine excessive daytime sleepiness. The Morningness–Eveningness Questionnaire (MEQ) and Munich Chronotype Questionnaire (MCTQ) were used to determine the chronotype and behavioral sleep variables of each subject.

**Results** It was observed that 11% of the studied population was at risk of OSA obtained through MBQ. The STOP-BANG score significantly differed as a function of gender, family type, habitat, and chronotype. The Principal Component Analysis revealed behavioral sleep variables, demographic variables, EDS, and chronotype as the important correlates of OSA. The variables namely sleep latency and sleep inertia on both workdays and free days contributed to 22% variability in the dataset; whereas age, BMI and BSA together explained 19% variability. The ESS score and other associated factors explained the 20% variability in the dataset.

**Conclusions** The study delivers an early warning and underscores that about 11% of young adults from Chhattisgarh have a higher OSA risk. Sleep latency and sleep inertia could be associated with OSA risk more prominently followed by BMI and BSA.

**Keywords** Obstructive sleep apnea · Excessive daytime sleepiness · Chronotype · Body surface area · Body mass index

## 1 Introduction and Background

Obstructive sleep apnea (OSA) can be defined as an interruption or pause in breathing that occurs more than five times in an hour [1, 2]. It is one of the common sleep-related breathing disorders. OSA reflects cessation in the upper airway of respiration that occurs during sleep, lasting for 10 s or more. A complete cessation is called ‘Apnea,’ whereas incomplete cessation is called ‘Hypopnea.’ In Hypopnea, abnormal shallow breathing occurs, which decreases the oxygen saturation by around 4% or more. The severity of OSA has been categorized into three stages based on the ‘Apnea–Hypopnea Index (AHI)’ [3]. The three stages of OSA are Mild (AHI = 5–15 events/hour), Moderate (AHI = 15–30 events/hour) and Severe (AHI > 30 events/hour) [3]. Loud snoring and excessive daytime sleepiness (EDS) are among the prominent symptoms of OSA. When OSA accompanies EDS then it is termed ‘obstructive sleep

✉ Arti Parganiha  
arti.parganiha@gmail.com

Noorshama Parveen  
noorshama12@gmail.com

Babita Pande  
babitime2014@gmail.com

Atanu Kumar Pati  
akpati19@gmail.com

<sup>1</sup> School of Studies in Life Science, Pandit Ravishankar Shukla University, Raipur 492 010, India

<sup>2</sup> Department of Physiology, All India Institute of Medical Sciences, Raipur 492 099, India

<sup>3</sup> Government of Odisha, Odisha State Higher Education Council, Bhubaneswar 751 002, India

<sup>4</sup> Center for Translational Chronobiology, Pandit Ravishankar Shukla University, Raipur 492 010, India

# Active Exploration of Faces in Police Lineups Increases Discrimination Accuracy

Melissa F. Colloff<sup>1</sup>, Heather D. Flowe<sup>1</sup>, Harriet M. J. Smith<sup>2</sup>, Travis M. Seale-Carlisle<sup>3</sup>,  
Christian A. Meissner<sup>4</sup>, James C. Rockey<sup>5</sup>, Babita Pande<sup>6</sup>, Pratibha Kujur<sup>6</sup>, Noorshama Parveen<sup>6</sup>,  
Priyanka Chandel<sup>6</sup>, Margaret M. Singh<sup>6</sup>, Sraddha Pradhan<sup>6</sup>, and Arti Parganiha<sup>6</sup>

<sup>1</sup> Centre for Applied Psychology, School of Psychology, University of Birmingham

<sup>2</sup> Division of Psychology, Nottingham Trent University

<sup>3</sup> Wilson Center for Science and Justice, School of Law, Duke University

<sup>4</sup> Department of Psychology, Iowa State University

<sup>5</sup> Department of Economics, Birmingham Business School, University of Birmingham

<sup>6</sup> School of Studies in Life Sciences, Pt. Ravishankar Shukla University

Eyewitness identifications play a key role in the justice system, but eyewitnesses can make errors, often with profound consequences. We used findings from basic science and innovative technologies to develop and test whether a novel interactive lineup procedure, wherein witnesses can rotate and dynamically view the lineup faces from different angles, improves witness discrimination accuracy compared with a widely used procedure in laboratories and police forces around the world—the static frontal-pose photo lineup. No novel procedure has previously been shown to improve witness discrimination accuracy. In Experiment 1, participants ( $N = 220$ ) identified culprits from sequentially presented interactive lineups or static frontal-pose photo lineups. In Experiment 2, participants ( $N = 8,507$ ) identified culprits from interactive lineups that were either presented sequentially, simultaneously wherein the faces could be moved independently, or simultaneously wherein the faces moved jointly into the same angle. Sequential interactive lineups enhanced witness discrimination accuracy compared with static photo lineups, and simultaneous interactive lineups enhanced witness discrimination accuracy compared with sequential interactive lineups. These findings were true both when participants viewed suspects who were of the same or different ethnicity/race as themselves. Our findings exemplify how basic science can be used to address the important applied policy issue on how best to conduct a police lineup and reduce eyewitness errors.

This article was published Online First November 18, 2021.

Melissa F. Colloff  <https://orcid.org/0000-0001-6401-4872>

Heather D. Flowe  <https://orcid.org/0000-0001-5343-5313>

Harriet M. J. Smith  <https://orcid.org/0000-0003-2712-5527>

Travis M. Seale-Carlisle  <https://orcid.org/0000-0002-4522-8549>

Christian A. Meissner  <https://orcid.org/0000-0002-6094-5167>

James C. Rockey  <https://orcid.org/0000-0002-2313-5544>

Babita Pande  <https://orcid.org/0000-0002-0545-6002>

Noorshama Parveen  <https://orcid.org/0000-0002-5366-5052>

Arti Parganiha  <https://orcid.org/0000-0001-9764-5566>

This work was supported by the Laura and John Arnold Foundation Grant (to Heather D. Flowe and Christian A. Meissner). Sections of these data were presented by Melissa F. Colloff at the International Meeting of the Psychonomic Society (May 2018), Amsterdam, the Netherlands, and at the Society for Applied Research in Memory and Cognition (June 2019), Cape Cod, Massachusetts, United States. Our data are available at <https://osf.io/2x5tg/> (Experiment 1) and <https://osf.io/b8tvw/> (Experiment 2).

Melissa F. Colloff served as lead for data curation, formal analysis, resources and writing – original draft, contributed equally to writing – review and editing and served in a supporting role for methodology. Heather D. Flowe

served as lead for conceptualization, funding acquisition and methodology, contributed equally to writing – review and editing and served in a supporting role for writing – original draft. Harriet M. J. Smith contributed equally to software and served in a supporting role for writing – review and editing. Travis M. Seale-Carlisle served in a supporting role for writing – review and editing. Christian A. Meissner contributed equally to writing – review and editing and served in a supporting role for methodology. James C. Rockey served in a supporting role for writing – review and editing. Babita Pande served in a supporting role for writing – review and editing. Pratibha Kujur served in a supporting role for writing – review and editing. Noorshama Parveen served in a supporting role for writing – review and editing. Priyanka Chandel served in a supporting role for writing – review and editing. Margaret M. Singh served in a supporting role for writing – review and editing. Sraddha Pradhan served in a supporting role for writing – review and editing. Arti Parganiha served in a supporting role for writing – review and editing. Babita Pande, Pratibha Kujur, Noorshama Parveen, Priyanka Chandel, Margaret Singh, Sraddha Pradhan, and Arti Parganiha all also served in a supporting role for data curation.

Correspondence concerning this article should be addressed to Melissa F. Colloff, Centre for Applied Psychology, School of Psychology, University of Birmingham, Edgbaston, Birmingham B15 2TT, United Kingdom. Email: [m.colloff@bham.ac.uk](mailto:m.colloff@bham.ac.uk)

**Original Research**

DOI : <http://doi.org/10.22438/jeb43/3/MRN-1807>

# Determination of short-interval time estimates in humans exposed to radiofrequency electromagnetic radiation

P. Chandel<sup>1</sup>, M.M. Singh<sup>1</sup>, A.K. Pati<sup>1,2,3</sup>, V. Choudhary<sup>4</sup> and A. Parganiha<sup>1,2\*</sup>

<sup>1</sup>School of Studies in Life Science, Pandit Ravishankar Shukla University, Raipur-492 010, India

<sup>2</sup>Center for Translational Chronobiology, Pandit Ravishankar Shukla University, Raipur-492 010, India

<sup>3</sup>Professor Emeritus at Kalinga Institute of Social Sciences – Deemed to be University, Bhubaneswar-751 024, India

<sup>4</sup>Regional Cancer Center, Pt. Jawaharlal Nehru Medical College, Dr. B.R. Ambedkar Memorial Hospital, Raipur-492 001, India

\*Corresponding Author Email : [arti.parganiha@gmail.com](mailto:arti.parganiha@gmail.com)

Received: 22.02.2021

Revised: 26.08.2021

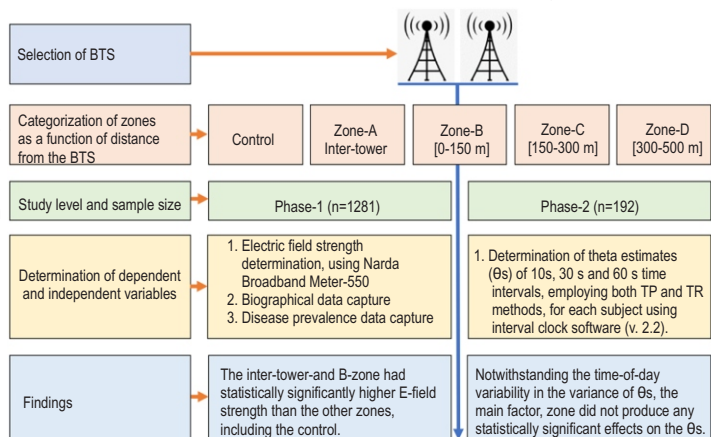
Accepted: 13.11.2021

**Abstract**

**Aim:** The present study aimed at evaluating the effects of radiofrequency electromagnetic radiation exposure on short-interval time estimates in humans living in the vicinity of base transceiver stations.

**Methodology:** The study was conducted in Phase-1 and Phase-2 with 1281 and 192 subjects, respectively. Four groups with one control were identified in each phase depending on the distance from the ground-based transceiver stations. The cognitive ability of the subjects of each group was determined by measuring short-interval time estimates, namely 10 s, 30 s, and 60 s, with time production and time reproduction methods using the Interval Clock software (Version 2.2). The electric field strength at each participant's house was determined using the Narda Broadband Meter-550 with a probe EF0-391.

**Results:** ANOVA results demonstrated a statistically significant difference in electric field strength among different zones around the installations of base transceiver stations ( $F_{4,1274} = 50.071$ ;  $p < 0.001$ ). It was significantly higher in the inter-tower zone than in all other zones. The prevalence of various clinical problems was higher among the individuals living in the inter-tower zone. ANCOVA results revealed that the main factors zone, gender, and year of residence, did not significantly affect any short-interval time estimates. However, a statistically significant 'time of the day' variation in most of the target short-interval time estimates with both the methods for all the studied groups, except the inter-tower zone, was observed.



**Interpretation:** The radiofrequency electromagnetic radiation emitted from base transceiver stations did not significantly impact the ability to estimate short-time intervals in humans.

**Key words:** Base transceiver station, Electric-field strength, Narda Broadband Meter-550, Radiofrequency electromagnetic radiation, Short-interval time estimation.

**How to cite :** Chandel, P., M.M. Singh, A.K. Pati, V. Choudhary and A. Parganiha: Determination of short-interval time estimates in humans exposed to radiofrequency electromagnetic radiation. *J. Environ. Biol.*, **43**, 369-376 (2022).

## Genotoxic impacts of long term exposure of Arsenic and Fluoride to Cat Fish, *Clarias batrachus*

Purva Mishra<sup>1</sup>, Aditi Niyogi Poddar<sup>2\*</sup>

<sup>1,2</sup>SoS in Life Science, Pt. Ravishankar Shukla University, Raipur, India

\*Corresponding author: [adinpod@gmail.com](mailto:adinpod@gmail.com), Tel: +918839440215

Available online at: [www.isroset.org](http://www.isroset.org)

Received: 22/Oct/2021, Accepted: 20/Nov/2021, Online: 31/Dec/2021

**Abstract** - Arsenic and Fluoride are very common ground water pollutants, contributed by natural and anthropogenic sources leading to serious health effects in both terrestrial and aquatic organisms. The current research was carried out to identify the relationship between arsenic and fluoride, using *Clarias batrachus* (common cat fish) as an experimental model. The study includes seven groups (Group I to VII), one control (Group I) and other six (Group II, III, IV, V, VI, VII) exposed to different concentration of arsenic and fluoride individually and in combination. Long term exposure of 60 days was carried out for each group, with no toxicant added in Group I. Blood samples were collected from each experimental group on 60<sup>th</sup> day and COMET assay was performed to check genotoxicity. Parameters like Head DNA percentage, tail DNA Percentage, comet length, tail moment were calculated from comet images. Results revealed maximum DNA damage in group V, which was exposed to arsenic alone, concluding arsenic being more toxic than fluoride. Also, antagonistic relationship was established between arsenic and fluoride.

**Keywords** - Arsenic, Fluoride, *Clarias batrachus*, Genotoxicity

### I. INTRODUCTION

Increasing anthropogenic activities are the key to aquatic and terrestrial pollution across the globe. Arsenic and Fluoride are very common ground water pollutants, contributed by both natural and human caused reasons. Concurrent occurrence of fluoride and arsenic is widespread in many states of India, China, Bangladesh and South East Asia. Following their exposure, severe health complications arise namely Arsenicosis and Fluorosis, respectively [1].

Fluoride gets accumulated in aquatic invertebrates and vertebrates, through food and water. Once absorbed, it is distributed and accumulated in various organs and body parts [2]. The tendency of fluoride accumulation is found more in bony tissues than in soft tissues [3]. Fluoride also alters numerous hematological parameters [4] and interferes with various enzymatic (SOD, Catalase) and non-enzymatic activities (GSH, LPO) [5]. It has propensity to bind with the DNA molecule and distort its normal structure, and also induces generation of free radicals, ultimately causing DNA damage [6].

Arsenic, on the other hand is a non essential heavy metal which is mainly contributed by coal burning industries [7], generally present in its two forms organic and inorganic; inorganic being the more toxic one [8]. Aquatic organisms get exposed to arsenic through food/dietary sources and via water. Arsenic intrudes in the food chain and hence has bioaccumulative properties [9]. Accumulation of arsenic in fishes takes place in different organs like liver,

kidney and gills depending upon the source of exposure [10]. Arsenobetaine, a water-soluble arsenic compound is usually found in marine living beings, which affects the organism and also can have adverse effects on humans indirectly [11]. Arsenic inhibits various enzyme activities involved in DNA repair leading to DNA damage. It brings about oxidative stress and free radicals affecting DNA and various cellular activities [6].

Contradictory literatures are available for both antagonistic and synergistic relationship of fluoride and arsenic. However, adverse health consequences of arsenic and fluoride exposure individually have been explored more, in comparison to their combination effects [12].

The research paper is further described as follows; section II mentions about the methods acquired to carry out the experiment, section III deals with the finding of the research carried out and also the discussion in which our results were supported by other researchers. Future scope and conclusions are narrated in section IV, followed by acknowledgement and finally the references.

### II. RELATED WORK

Research reports are available confirming concurrent presence of arsenic and fluoride in various water bodies; but a very little work has been explored about the effects of both toxicants on aquatic organisms. However, many reports are available on rats. Arsenic and fluoride lead to increased activities of glutathione peroxidases, SOD & catalase, and also reduce levels of glutathione and ascorbic

acid [13]. Similar results are available in ovary of rats [14] and blood, liver and brain of rats, exposed to different concentrations of arsenic and fluoride, concluding antagonistic connection between them [15]. Correspondingly, antagonistic associations were noticed between the two, wherein increased ROS and lipid peroxidation were observed in groups of rats exposed to arsenic and fluoride separately [16].

Several conflicting publications are also available explaining synergistic association of fluoride and arsenic. Reports have been published, observing less DNA damage in groups of rats exposed to both arsenic and fluoride in combination, demonstrating synergistic effects between the two [17].

### III. METHODOLOGY

Experimental model, *Clarias batrachus* were selected for the study and were purchased from local market. Before acclimatization, fishes were immersed in 1% KMnO<sub>4</sub> solution, to avoid any skin diseases. Five fishes in each water tank of 50L capacity were acclimatized for 15 days with continuous supply of oxygen and water, with room temperature maintained at 27°C. They were fed daily once with Taiyo fish food.

Sodium fluoride (NaF) (Himedia laboratory) and Arsenic trioxide (As<sub>2</sub>O<sub>3</sub>) (Sigma Aldrich) of desired concentration were used to expose *Clarias batrachus*. Seven experimental groups were formed to study the effects of fluoride and arsenic individually and in combinations. Group I (Control), Group II (10 mgL<sup>-1</sup>NaF), Group III (20 mgL<sup>-1</sup>NaF), Group IV (1 mgL<sup>-1</sup>As<sub>2</sub>O<sub>3</sub>), Group V (2 mgL<sup>-1</sup>As<sub>2</sub>O<sub>3</sub>), Group VI (10 mgL<sup>-1</sup>NaF + 1 mgL<sup>-1</sup>As<sub>2</sub>O<sub>3</sub>), Group VII (20 mgL<sup>-1</sup>NaF + 2 mgL<sup>-1</sup>As<sub>2</sub>O<sub>3</sub>)

Long term exposure of 60 days was carried out for each group, with no toxicant added in Group I, and the desired toxicant were added in the following groups. Blood samples were collected from each experimental group on 60<sup>th</sup> day. 1.0ml each of blood samples were collected in polypropylene vials/tubes coated with heparin. Samples were stored at 4°C for about a week or at a temperature of -20°C, until further analysis.

#### Comet Assay:

Samples were then analyzed for DNA damage by using COMET assay technique [18], a SCGE (Single Cell Gel electrophoresis) of blood cell, which signifies the amount of DNA impairment. The procedure involves preparation of base slides, using layers of LMPA (Low Melting Point Agarose) and NMA (Normal Melting agarose). Blood samples collected were dissolved in PBS (Phosphate Buffer Saline) solution for isolation of blood cells. Samples were then placed on prepared base slide and coated with agarose layer, and cover slips gently placed over it. Microgel slides were subjected to electrophoresis

for about 20 minutes (15 volts & 300 mill amperes). Slides were stained with EtBr (Ethidium bromide) and immediately visualized under fluorescent microscope (Leica DM 1000).

Visual scoring method developed by Comet assay forum ([www.cometassayindia.org](http://www.cometassayindia.org)) was used. Around 100 cells were counted per slide & analyzed for damage. CaspLab (Comet assay Software Project 1.2.3b), was also used for calculating comet length, percentage of DNA in head and tail region in COMET images.

### IV. RESULTS AND DISCUSSIONS

#### Results

DNA damage was analyzed using Comet assay technique in blood samples of control and experimental fishes of different concentration of NaF & As<sub>2</sub>O<sub>3</sub>. Least DNA damage was found in control samples with maximum number of 'Type 0' and minimum number of 'Type 4' DNA damage categories. Greatest damage was observed in group V (2µgL<sup>-1</sup>As) with maximum 'Type 4' and minimum 'Type 0' (Figure 1). Less percentage of DNA damage was found to be observed in groups exposed to both fluoride and arsenic (group VI & VII), compared to groups exposed only to arsenic (group IV & V).

Highest percentage of DNA in head region was observed in control group (Figure 2). Order of Head DNA (%) witnessed was; group I (99.4±0.29) > group II > group III > group VI > group IV > group VII > group V (36.60±5.32). However, tail DNA (%) was found maximum in group V (63.39±9.22) and least in group I. Decreasing order of tail DNA was found in group V, followed by group VII, group IV, group VI, group III, group II, group I (0.56±0.82).

Highest length of the comet was found in group V (304±3.21) followed by group VII, group IV, group VI, group III, group II. And least length was seen in group I (40.4±2.20) (Figure 3)

Tail moment was also estimated, which is the product of tail DNA percent & tail length of the comet. Highest tail moment was measured in group V and lowest was detected in control group (Figure 4).

COMET images (Figure 5), using blood samples collected from fishes of each group was allowed to run in electrophoresis (SCGE) and were observed under fluorescent microscope. Maximum DNA damage, with long comets were observed in group V (arsenic treated) and least DNA damage were reported in control samples (group I). DNA damage was found be highest in arsenic exposed groups than in fluoride exposure groups. Confirming the antagonistic nature of arsenic and fluoride, DNA damage was low in groups exposed to arsenic and fluoride together as compared to groups exposed to fluoride and arsenic individually.

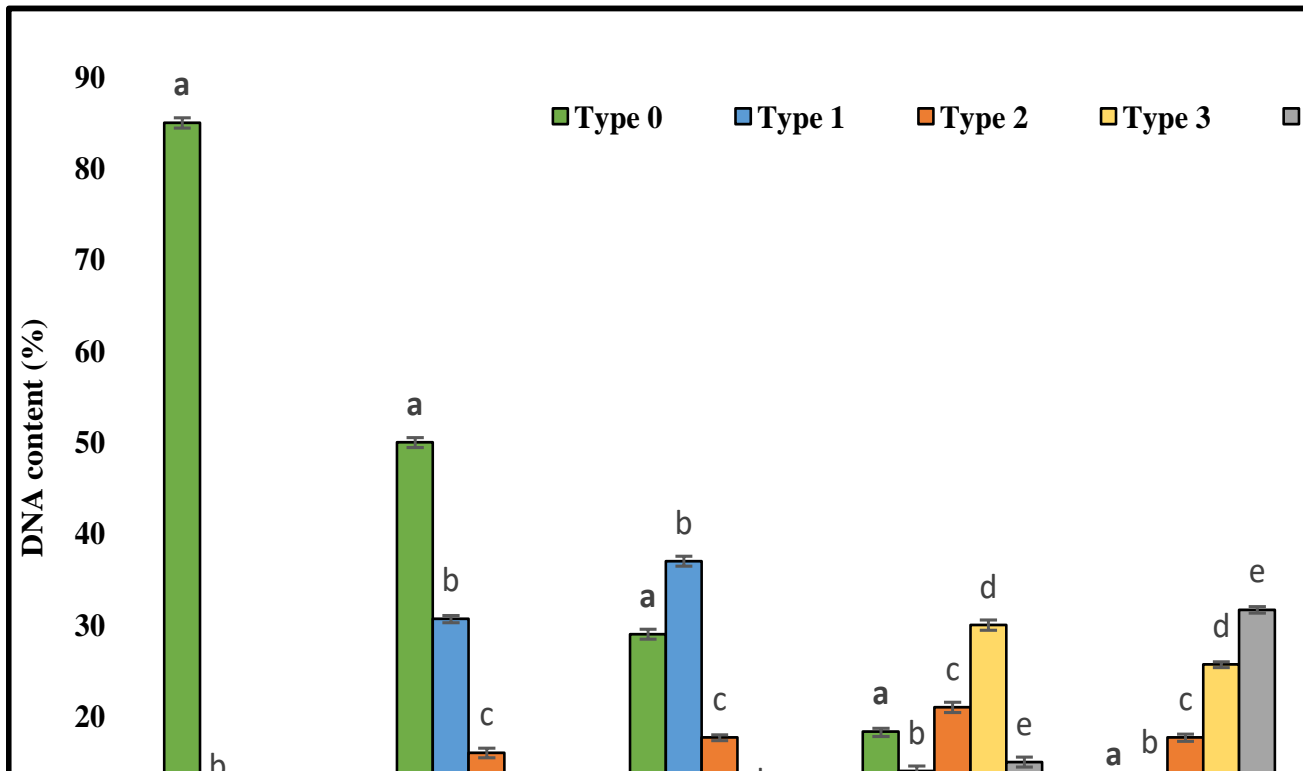


Figure 1. DNA damage (percentage) in control and different exposed groups of fluoride & arsenic (separately & in combination) after 60 days. Alphabets represents significance ( $P < 0.001$ ) between different types of DNA damage (0 to 4). No significant difference was observed between different exposure groups Means bearing different letters are statistically significant from each other (based on Duncan's multiple - range test).

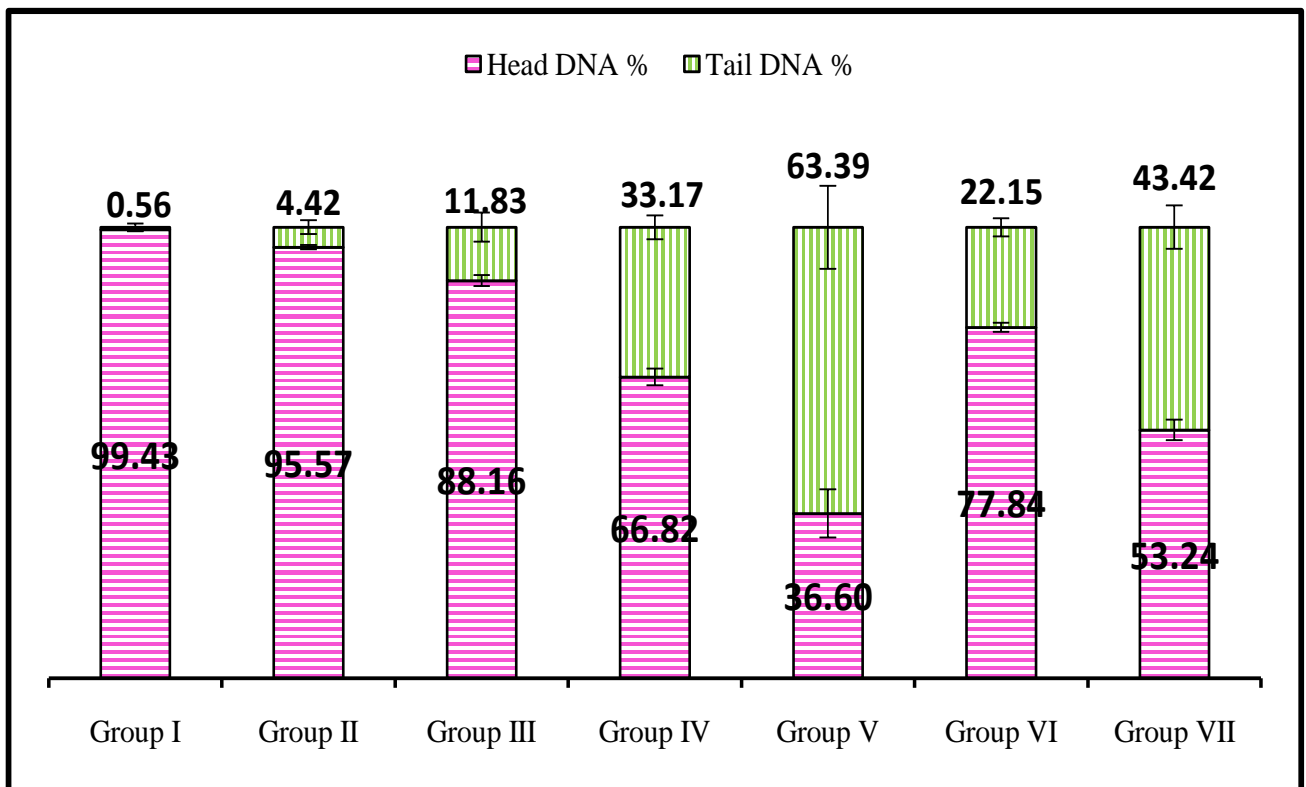


Figure 2. Percentage of DNA (Head and tail) in control and different experimental groups after 60 days of exposure.

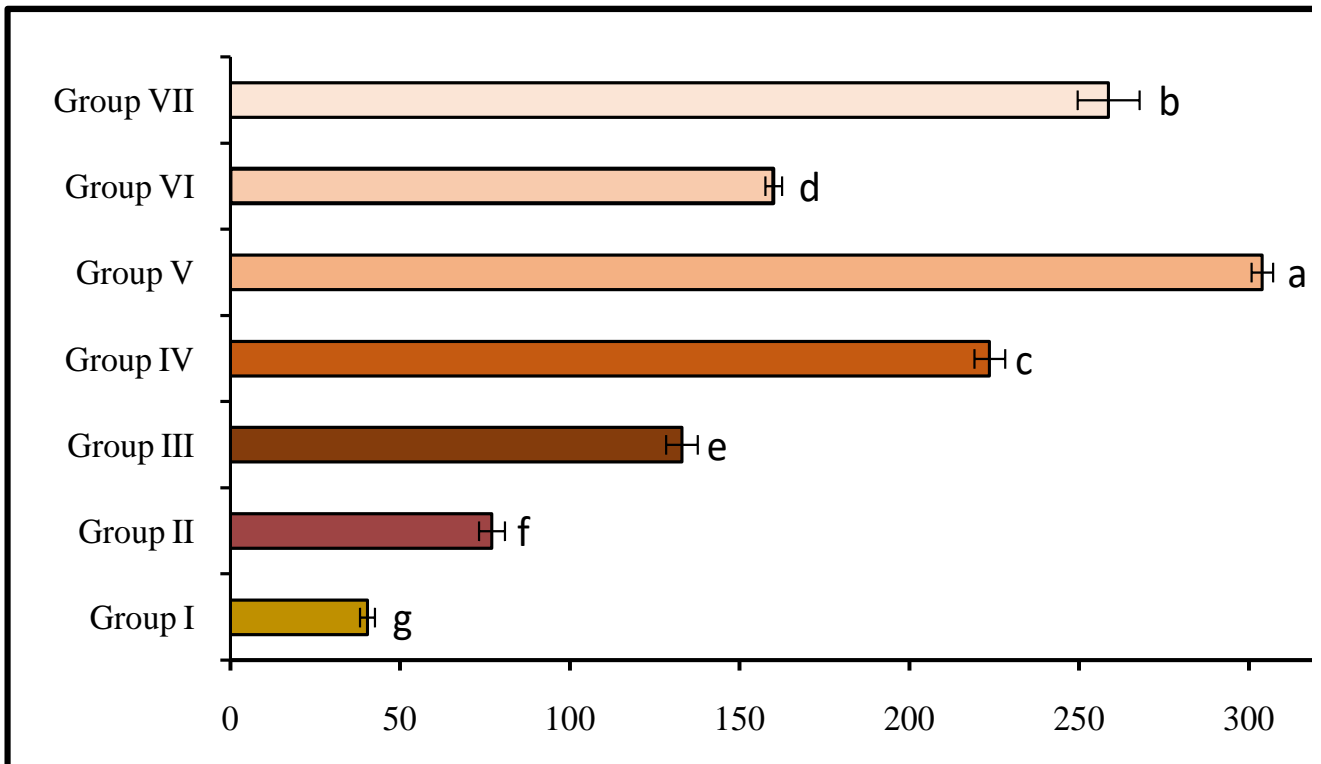


Figure 3. Comet length (pixel) in control and different experimental groups after 60 days of exposure. Alphabets represents significance ( $P < 0.05$ ) between different treatments. Means bearing different letters are statistically significant from each other (based on Duncan's multiple - range test).

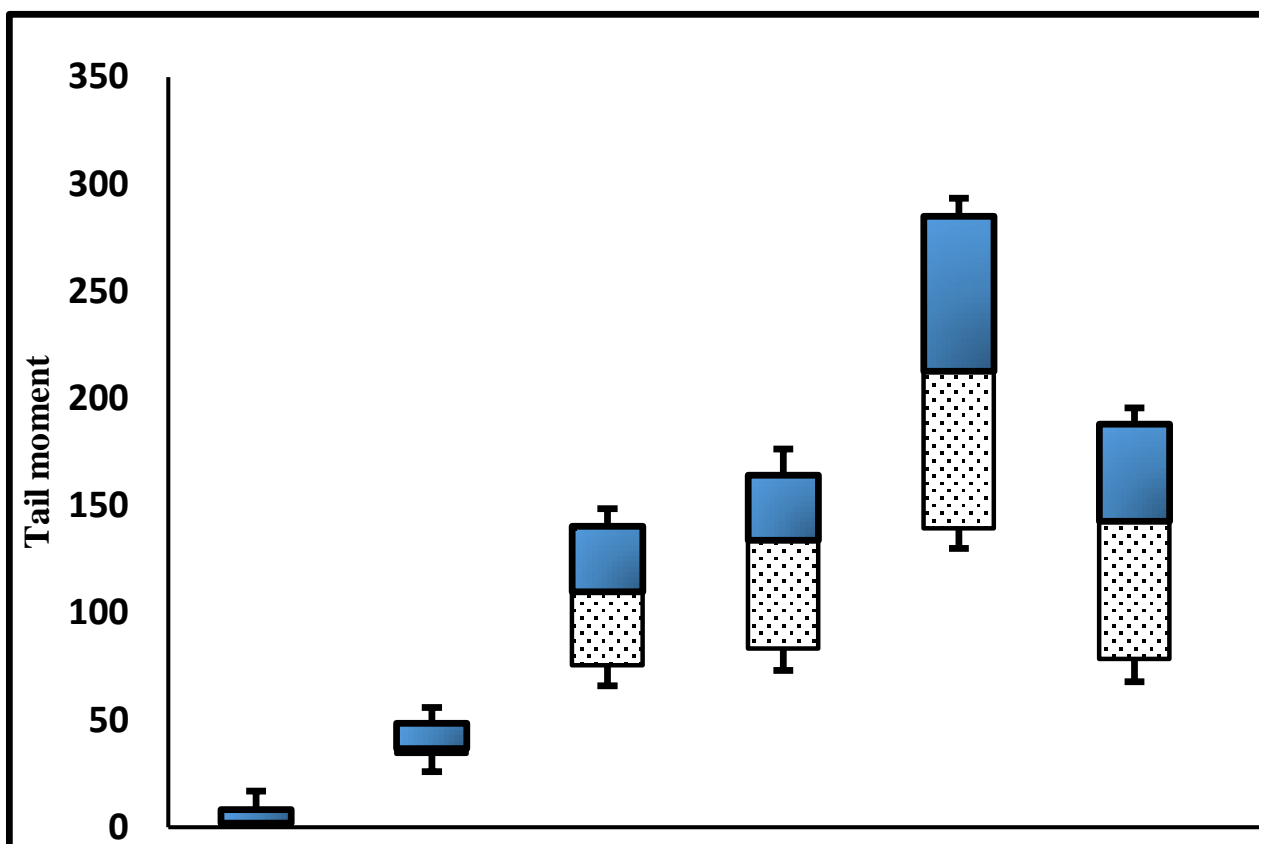


Figure 4. Tail moment (Tail DNA % \* Tail length) in control and different experimental groups after 60 days of exposure.

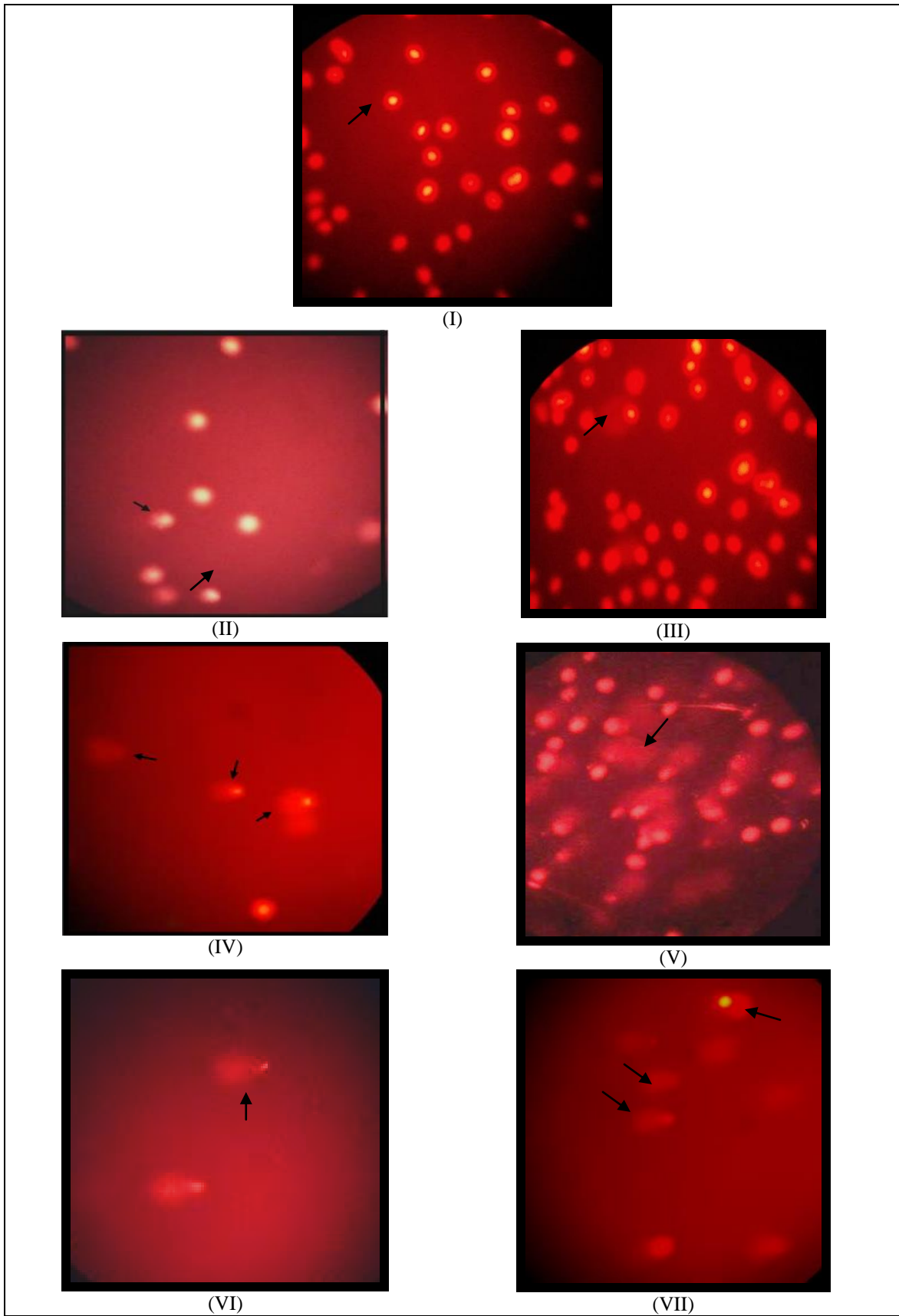


Figure 5. COMET images, of blood cells collected from different groups (I to VII) after 60 days of exposure, observed under fluorescent microscope.



## Discussion

Two commonly used techniques for testing genotoxicity in fish model are COMET assay and CAT (Chromosomal Aberration Test) [19]. In the field of ecotoxicology fishes considered as established models, where in the most reliable technique adopted for accessing DNA damage is COMET assay [20]. A study in *Clarias batrachus* reported increased Chromosomal aberration with increasing fluoride exposure [21]. Similar observations were reported in mice bone marrow, when tested for genotoxicity. Swiss albino mice were exposed to different sub lethal concentrations of sodium fluoride via drinking water, and breaks in chromosomal strands, appearance of micro nuclei was noticed [22]. Analogous experiments were conducted in Wistar rats, with a long-term exposure to fluoride, and analogous results were witnessed [23].

We agree with [24], considering arsenic a potent carcinogen; which he demonstrated using human lung cell lines and reported increased frequency of double stranded DNA breaks while performing Neutral COMET assay technique. Complimentary reports were established in *Oreochromis mossambicus* when exposed to different concentration of arsenic [25].

Antagonistic relationship between arsenic and fluoride was established by [26], where mice exposed to arsenic and fluoride separately has more DNA damage than to the group of mice with co-exposure of arsenic and fluoride, which is further supported by our investigations. In an experiment conducted by [27], arsenic and fluoride (singly and separately) were exposed to human peripheral lymphocytes cell cultures for 24h, ensuing DNA damage in all the exposed groups compared to control groups. Besides, comet length was found to be high in treated cultures; also, DNA percentage in head of comet was less and tail DNA% was more in exposed groups. However reverse condition was observed in non-treated groups. Antagonistic relationship between arsenic and fluoride is estimated in the present report and is further supported by the above study. Single strand breaks in DNA were observed in rat lymphocytes with the aid of Comet assay technique, when they were treated with arsenic, fluoride and co-exposure of arsenic & fluoride [28]. Comets with visibly long tails were seen in chronic fluoride (28 weeks) and arsenic treated groups in comparison to control, which are also analogous to the current work. Similar results were obtained [29], following exposure of fluoride and arsenic to human blood lymphocyte cultures for 24 hours. A noticeable lengthy comet tail was recognized in exposed cell cultures, indicating DNA damage.

Antagonistic relationship between arsenic & fluoride is due to formation of certain compounds like  $\text{AsF}_3$ ,  $\text{AsF}_5$  and  $\text{AsF}_6^-$ . Arsenic has an empty d orbital, giving it an affinity towards any electronegative element, like fluoride. Arsenic (III) undergoes  $\text{SP}_3$  hybridization with fluoride and forms  $\text{AsF}_3$  & when present in arsenic (V) go through  $\text{SP}_3\text{d}$  hybridization to form  $\text{AsF}_5$ , thereby reducing the individual effect of each [30].

## V. CONCLUSION AND FUTURE SCOPE

Arsenic and Fluoride are two serious inorganic water pollutants worldwide. Extensive work has been done with reference to both fluoride and arsenic in combination, but a little has been explored in *Clarias batrachus*. Different views and reviews are obtainable for fluoride and arsenic relationship with each other. Our work has definitely brought clarity to their relationship between As & F<sup>-</sup> when studied together. DNA damage was found be highest in arsenic exposed groups than in fluoride exposed groups and groups of As+F<sup>-</sup> exposure. Confirming the antagonistic nature of arsenic and fluoride, DNA damage was low in groups exposed to arsenic and fluoride together as compared to groups exposed to fluoride and arsenic individually. Estimation of accumulation status and biochemical effects of arsenic and fluoride would be an important tool for calculating ecological risk assessment.

## ACKNOWLEDGMENT

The author is thankful to SOS Life sciences, Pandit Ravishankar Shukla University for support and providing lab facilities to carry out the required work.

## REFERENCES

- [1]. P.K. Jha, P. Tripathi, "Arsenic and fluoride contamination in groundwater: A review of global scenarios with special reference to India" *Ground water for Sustainable Development*, Vol.13, pp. 100576, 2021.
- [2]. X. Shi., P. Zhuang, L. Zhang, G. Feng, L. Chen, J. Liu, R. Wang, "The bioaccumulation of fluoride ion (F<sup>-</sup>) in Siberian sturgeon (*Acipenser baerii*) under laboratory conditions" *Chemosphere*, Vol. 75, Issue.3, pp. 376-380, 2009.
- [3]. M. Sands, S. Nicol, A. McMinn, "Fluoride in Antarctic marine crustaceans" *Marine Biology*, Vol. 132, pp. 591-598, 1998.
- [4]. A. Chauhan, H. Singh, R. Singh, "Sodium Fluoride toxicity on blood parameter and catalase activity of Indian fresh water larvicidal fish *Channa striatus*" *Current World Environment*, Vol. 9, pp. 952-956, 2014.
- [5]. N. Singh, M. Tripathi, "Alteration in antioxidant biomolecules after the exposure to fluoride in fresh water fish *Heteropneustes fossilis*" *Journal of Ecophysiology and Occupational Health*, Vol. 16, Issue. 3&4, pp. 66-71, 2016.
- [6]. S. Chouhan, S.J.S. Flora, "Arsenic and fluoride: two major ground water pollutants" *Indian Journal of Experimental Biology*, Vol. 48, Issue. 7, pp. 666-678, 2010.
- [7]. S. K. Soni, R. Pandey, "Interaction of Hazardous Heavy Metals with Humans and Environment and their Toxicological Impacts" *International Journal of Scientific Research in Biological Sciences*, Vol.8, Issue.5, pp.39-45, 2021.
- [8]. D. Fattorini, C.M. Alonso-Hernandez, M. Diaz-Asencio, A. Munoz-Caravaca, F.G. Pannacchiulli, M. Tangherlini, F. Regoli, "Chemical speciation of arsenic in different marine organisms: Importance in monitoring studies" *Marine Environmental Research*, Vol. 58, Issue. 2-5, pp. 845-850, 2004.
- [9]. S. Suhendrayatna, A. Ohki, T. Nakajima, S. Maeda, "Studies on the accumulation and transformation of arsenic in fresh water organisms I. Accumulation, transformation and toxicity of arsenic compounds on the Japanese medaka, *Oryzias latipes*" *Chemosphere*, Vol. 46, Issue. 2, pp. 319-324, 2002.
- [10]. B. Kumari, V. Kumar, A.K. Sinha, J. Ahsan, A. K. Ghosh, H. Wang, G. DeBoeck, "Toxicology of arsenic in fish and aquatic systems" *Environmental Chemistry Letters*, Vol. 15, pp. 43-64, 2017.

- [11]. C.M. Liao, B.C. Chen, S. Singh, M.C. Lin, C.W. Liu, B.C. Han, "Acute toxicity and bioaccumulation of arsenic in tilapia (*Oreochromis mossambicus*) from a black foot disease area in Taiwan" *Environmental Toxicology: An International Journal*, Vol. 18, pp. 252-259, 2003.
- [12]. S. Jiang, J. Su, S. Yao, Y. Zhang, F. Cao, F. Wang, S. Xi, "Fluoride and arsenic exposure impairs learning and memory and decreases mGluR5 expression in the hippocampus and cortex in rats" *PLoS One*, Vol. 9, pp. e96041, 2014.
- [13]. N.J. Chinoy, S.D. Shah, "Biochemical effects of sodium fluoride and arsenic trioxide toxicity and their reversal in the brain of mice" *Fluoride*, Vol. 37, pp. 80-87, 2004.
- [14]. D.D. Jhala, N.J. Chinoy, M.V. Rao, "Mitigating effects of some antidotes on fluoride and arsenic induced free radical toxicity in mice ovary" *Food and Chemical Toxicology*, Vol. 46, pp. 1138-1142, 2008.
- [15]. S.J.S. Flora, V. Pachauri, M. Mittal, D. Kumar, "Interactive effect of arsenic and fluoride on cardio-respiratory disorders in male rats: possible role of reactive oxygen species" *Biometals*, Vol. 24, pp. 615-628, 2011.
- [16]. K.T. Liu, G. Wang, L. Ma, P. Jang, B.Y. Xiao, C. Zhang, "Adverse effects of combined arsenic and fluoride on liver and kidney in rats." *Fluoride*, Vol. 32, pp. 243-247, 1999.
- [17]. C. Zhang, B. Ling, J. Liu, G. Wang, "Effect of fluoride-arsenic exposure on the neurobehavioral development of rat's offspring" *Wei Sheng Yan Jiu*, Vol. 28, Issue. 6, pp. 337-338, 1999.
- [18]. N.P. Singh, M.T. McCoy, R.R. Tice, E.L. Schneider, "A simple technique for quantitation of low levels of DNA damage in individual cells" *Experimental Cell Research*, Vol. 175, Issue.1, pp. 184-191, 1988.
- [19]. R.K. Garg, N. Batav, R. Sharma, "Genotoxicity assessment using micronucleus assays in *Sperata seenghala* at in-situ level from lower lake and Shahpura lake Bhopal" *India. Journal of Environmental Research and Development*, Vol. 6, Issue.4, pp. 1040-1043, 2012.
- [20]. R. Pandrangi, M. Petras, S. Ralph, M. Vrzoc, "Alkaline single cell gel (comet) assay and genotoxicity monitoring using bullheads and carp" *Environmental and Molecular Mutagenesis*, Vol. 26, Issue. 4, pp. 345-356, 1995.
- [21]. N. Tripathi, S. Bajpai, M. Tripathi, "Genotoxic alterations induced by Fluoride in Asian catfish, *Clarias batrachus* (Linn)" *Fluoride*, Vol. 42, Issue.4, pp. 292-296, 2009.
- [22]. S. Podder, A. Chattopadhyay, S. Bhattacharya, M.R. Ray, "Differential in vivo genetic effect of lower and higher concentration of fluoride in mouse bone marrow cells" *Fluoride*, Vol.41, Issue.4, 301-307, 2010.
- [23]. J. Radovanovic, B. Antonijevic, S. Kolarevic, S. Milutinovic-Smiljanic, J. Mandic, B. Vukovic-Gacic, M. Bulat, Z. Čurčić, M. Kračun-Kolarević, K. Sunjog, J. Kostić-Vuković, J. Jovanović Marić, E. Antonijević-Miljaković, D. Đukić-Čosić, A. BuhaDjordjevic, D. Javorac, K. Baralić, Z. Mandinić, J. Kostic-Vukovic, "Genotoxicity of fluoride subacute exposure in rats and selenium intervention" *Chemosphere*, Vol. 266, pp. 128978, 2020.
- [24]. H. Xie, S. Huang, S. Martin, J. P. Wise Sr, "Arsenic is cytotoxic and genotoxic to primary human lung cells" *Mutation Research/Genetic Toxicology and Environmental Mutagenesis*, Vol. 760, pp. 33-41, 2014.
- [25]. M.K. Ahmed, M. Habibullah-Al-Mamun, M.A. Hossain, M. Arif, E. Parvin, M.S. Akter, M.S. Khan, M.M. Islam, "Assessing the genotoxic potentials of arsenic in Tilapia (*Oreochromis mossambicus*) using alkaline comet assay and micronucleus test" *Chemosphere*, Vol. 84, pp. 143-149, 2011.
- [26]. S.J.S. Flora, M. Mittal, D. Mishra, "Co-exposure to arsenic and fluoride on oxidative stress, glutathione linked enzymes, biogenic amines and DNA damage in mouse brain" *Journal of the Neurological Sciences*, Vol. 285, Issue. 1-2, pp. 198-205, 2009.
- [27]. H. Tiwari, M. V. Rao, "Curcumin supplementation protects from genotoxic effects of arsenic and fluoride" *Food and Chemical Toxicology*, Vol. 48, Issue.5, pp. 1234-1238, 2010.
- [28]. S.J.S. Flora, M. Mittal, V. Pachauri, N. Dwivedi, "A possible mechanism for combined arsenic and fluoride induced cellular and DNA damage in mice" *Metallomics*, Vol. 4, pp. 78-90, 2012.
- [29]. H. Pant, M.V. Rao, "In vitro melatonin supplementation against genetic toxicity by arsenic and fluoride" *Advance in Bioresearch*, Vol. 1, Issue. 2, pp. 17-24, 2010.
- [30]. G. Sahu, S. Pervez, A. N. Poddar, "Combined Toxicity and Bioconcentration of Fluoride and Arsenic in African Catfish *Clarias gariepinus* (Burchell, 1822)" *International Journal of Environment, Agriculture and Biotechnology*, Vol. 2, Issue. 2, pp. 968-976, 2017.

#### AUTHORS PROFILE

Dr Aditi Niyogi Poddar pursued her MSc (1980), PhD (1984) from the SoS in Lifescience, Pandit Ravishankar Shukla University, Raipur Chhattisgarh, India and is continuing as a Professor in the same department with 37 years of teaching and research experience.



She has published 38 research papers in reputed national and international journals including Scopus, Web of science and SCI. Her research fields are Parasitic diseases and Environmental toxicology.

Mrs. Purva Mishra is currently a Research Scholar under the guide ship of Dr. Aditi Niyogi Poddar, SoS in Life Sciences Pandit Ravishankar, Shukla, University.



She has submitted her thesis entitled "Toxicokinetics of Arsenic and Fluoride On Cat fish". Her area of interest is Environmental toxicology, Aquatic Pollution, Heavy metal toxicity.

## FLUORIDE AND ARSENIC : BIOACCUMULATORY POTENTIAL AND THEIR COMBINED TOXIC IMPACT ON THE BEHAVIOR OF FRESHWATER CATFISH, *CLARIAS BATRACHUS* LINN. 1758

Gamini Sahu and Aditi Niyogi Poddar\*

School of Life Sciences, Pt. Ravishankar Shukla University, Raipur - 492 010, India.

\*e-mail: [adinpod@gmail.com](mailto:adinpod@gmail.com)

(Received 12 July 2021, Accepted 13 September 2021)

**ABSTRACT :** Fluoride and arsenic, upon release into the environment, often accumulate rapidly in aquatic habitats and are taken up by aquatic organisms subsequently entering into the food chain. This study comprises of examining the tissue distribution of arsenic and fluoride in the freshwater catfish, *Clarias batrachus* chronically exposed to them in combination. Fishes were exposed to a range of aqueous arsenic trioxide and sodium fluoride, both individually and in combination, and sampled at 24, 48, 72 and 96 hours. Levels of fluoride and arsenic in the liver, kidney, bone and blood of *Clarias batrachus* demonstrated significantly a direct relationship with the exposure medium. Fluoride level in bone was the highest whereas; the lowest level was observed in the muscle. Arsenic level in the liver was the highest whereas; the lowest level was observed in the bone at the end of 96 hours, among all tissues, at the same concentration and sampling time. Impact on behavior was studied in terms of air gulping, opercular movement, swimming activity, body position and food sensitivity. Control fish remained normal throughout the experimental period (28 d), but treated fishes were very restless, with loss of equilibrium, and a significant increase ( $P < 0.01$ ) in the number of opercular movements and air gulping. Our results suggest that elevated levels of fluoride and arsenic exposure cause bioaccumulation in the fish body, which ultimately may be harmful to humans.

**Key words :** Bioaccumulation, biotransformation, methylation, biotransformation, TISAB.

**How to cite :** Gamini Sahu and Aditi Niyogi Poddar (2022) Fluoride and arsenic : Bioaccumulatory potential and their combined toxic impact on the behavior of freshwater catfish, *Clarias batrachus* Linn. 1758. *J. Exp. Zool. India* **25**, 435-441. DocID: <https://connectjournals.com/03895.2022.25.435>

### INTRODUCTION

Civilization and the rapid spread of industrialization have compelled developing countries to face the crisis of aquatic pollution. A large number of polluted products, especially heavy metals are constantly being drained, untreated into rivers, close at hand. These products readily get dissolved in water and are the major persistent elements in aquatic ecosystems. Chromium, lead, mercury, arsenic and cadmium, rank among the priority metals and are viewed as systemic toxicants inciting numerous organ damages, even at lower levels of exposure (Olsson *et al.*, 1998). They also influence cellular organelles and various enzymes involved in the metabolic process, detoxification, and damage repair (Wang and Shi, 2001). Besides, DNA molecules and nuclear proteins are also damaged, possibly leading to carcinogenesis or apoptosis (Beyersmann and Hartwig, 2008). Obviously, the impact of heavy metals on the aquatic ecosystem is a

global concern (Yousafzai *et al.*, 2008).

In the present scenario, unfortunately, a billion people in the world are drinking unhealthy water regularly (Borah *et al.*, 2011). To meet the need for clean drinking water of these thirsty billions, indiscriminate fracturing of rocks to dig bore wells has consequently lead the emergence of two major public-health problems, *viz.*, groundwater contamination with excess fluoride and arsenic. The chief sources of high fluoride in water resources are fluoride-bearing minerals existing in rocks and soils (Jha *et al.*, 2011).

Aquatic animals are capable of taking up fluoride directly from water or to a lesser extent through food. In fish, fluoride may accumulate from the food chain (Shi *et al.*, 2009). Roughly, 80-90% of the total ingested fluoride is absorbed from the gastrointestinal tract by passive diffusion (Whitford, 1996). Fluoride is distributed more rapidly in well-perfused tissues, such as the heart, lung,

and liver than less perfused tissues, such as skin, resting skeletal muscles and adipose tissue (WHO, 2002).

The major cause of arsenic concentration in groundwater and alluvial plain is desorption and dissolution of arsenic-bearing minerals and alluvial sediments (Shankar *et al*, 2014). Usage of arsenic-containing insecticides, fungicides, and herbicides in agriculture and wood preservatives, burning of fossil fuels and mining are anthropogenic sources (Nriagu *et al*, 2007). In its diverse chemical forms, arsenic too is bioaccumulative and enters the food chain (Suhendrayatna *et al*, 2002).

Fluoride and arsenic are found to co-occur in groundwater in many countries, including Argentina, China, Mexico, Pakistan Australia, Japan, Korea and Chile (Ahn, 2012). Many industries, by the improper release of their wastewaters, add to the possibilities of combined exposure to arsenic and fluoride. Co-exposure to fluoride and arsenic may lead to more complicated adverse health effects than exposure to fluoride and arsenic alone. Such observations could be attributed to the possible interaction between arsenic and fluoride in biological sites. In various studies, more contradictory results have been reported in which synergistic and antagonistic effects have been observed (Chouhan and Flora, 2010; Jiang *et al*, 2014).

Fish act as competent bioindicators of water quality (Al-Ghanim *et al*, 2016), due to their quality to accumulate metals in their muscles (Zhao *et al*, 2012) causing physiological, biochemical, and genetic alterations in their body (Javed and Usmani, 2017). Changes in certain fish behaviors, such as cough rate and avoidance reactions, predator avoidance, feeding behavior, learning, social interactions, and a variety of locomotor behaviors are very sensitive indicators of sublethal exposure to metals. Thus, behavioral alterations in aquatic organisms could be used as tools for risk assessment in aquatic ecosystems. This research work deals with an assessment of the bioaccumulatory potential of fluoride and arsenic and their combined toxic impact on the behavior of freshwater catfish *Clarias batrachus* Linn.1758.

## MATERIALS AND METHODS

### Procurement of experimental model and its maintenance

*Clarias batrachus* Linn. 1758 was used as the fish model throughout the toxicological investigations. Live and healthy fishes were procured from fish hatcheries, situated in Raipur, Chhattisgarh and acclimatized under laboratory conditions for a minimum of 15 days pre-exposure. Maintenance was done in natural freshwater (24°C±1) with sufficient oxygen supply and a clean

environment. Taiyo pellet fish food was fed to fishes during acclimatization and experimental period.

Results of previous acute toxicity tests (LC<sub>50</sub>) were used for chronic toxicity studies. The acute value was divided by 10 to provide a margin of safety and the resulting chronic estimate was used for chronic toxicity tests (Hoffman *et al*, 2003). Sodium fluoride (NaF, Himedia, Mumbai) and arsenic trioxide (As<sub>2</sub>O<sub>3</sub>, Sigma, USA) were selected as toxicants for individual and combined toxicity tests. 50 fishes were randomly distributed into five groups of 10 fishes per aquarium with 50L of water and treated as follows for a duration of 28 days- Group I (1.5 mgL<sup>-1</sup> Arsenic); Group II (30 mgL<sup>-1</sup> Fluoride); Group III (15 mgL<sup>-1</sup> Fluoride + 0.75 mgL<sup>-1</sup> Arsenic); Group IV (30 mgL<sup>-1</sup> Fluoride + 1.5 mgL<sup>-1</sup> Arsenic); Group V (control animals in normal water).

Two fishes from each aquarium were removed and anesthetized with MS-222 solution (100mgL<sup>-1</sup>). Blood and tissue (liver, kidney and muscle, bone) samples were carefully dissected and collected weekly for up to 28 days along with water samples for the different analyses.

### Quantification of Fluoride content

#### Fluoride digestion and Sample preparation :

About 100mL of water samples were collected in polyethylene vials and kept in a refrigerator at 4°C until further analysis. Fluoride content was estimated by direct determination method using TISAB buffer in 1:1 ratio for both samples and standards. Blood samples of about 0.5mL were collected in heparinized polypropylene vials and kept in a refrigerator at 4°C temperature until further analysis. Direct analysis was done without any pretreatment of the sample, diluting with TISAB II buffer in the ratio 1:1. Tissue and bone (Labiotkowski-Arendarczyk *et al*, 2015) samples were digested and TISAB II buffer (1:1) was added. Fluoride content was measured by the direct determination method (Birkel *et al*, 1970; Labiotkowski-Arendarczyk *et al*, 2015).

**Estimation of fluoride :** Estimation of fluoride was done using Thermo Scientific 9609 BNWP Ion-selective electrode (manual and ASTM D1179-72 B, 1976).

### Quantification of Arsenic content

Water, blood, tissue and bone samples were collected and stored as mentioned above in fluoride analysis. Preparation of water, blood and tissue samples are given below:

#### Arsenic digestion and Sample preparation :

Water (APHA, 2005; Chaurasia *et al*, 2013), blood (Chaurasia *et al*, 2013), tissues (liver, kidney and muscles) (Pazhanisamy *et al*, 2007) and bone (Akan *et al*, 2012)

samples were digested according to standard methods. After the accomplishment of complete digestion, the digested samples were made up to 25mL with distilled water and stored at 4°C for analysis.

Prior to analysis, all the standards, samples, and blank were incubated with 2.5mL each of 5% ascorbic acid, concentrated HCl and 5% KI, for an hour.

**Analysis and estimation of arsenic :** Estimation of arsenic from digested samples was done by Hydride Generation Atomic Absorption Spectrometer (AA8000 Lab India Atomic absorption Spectrophotometer Ltd.).

### Behavior study

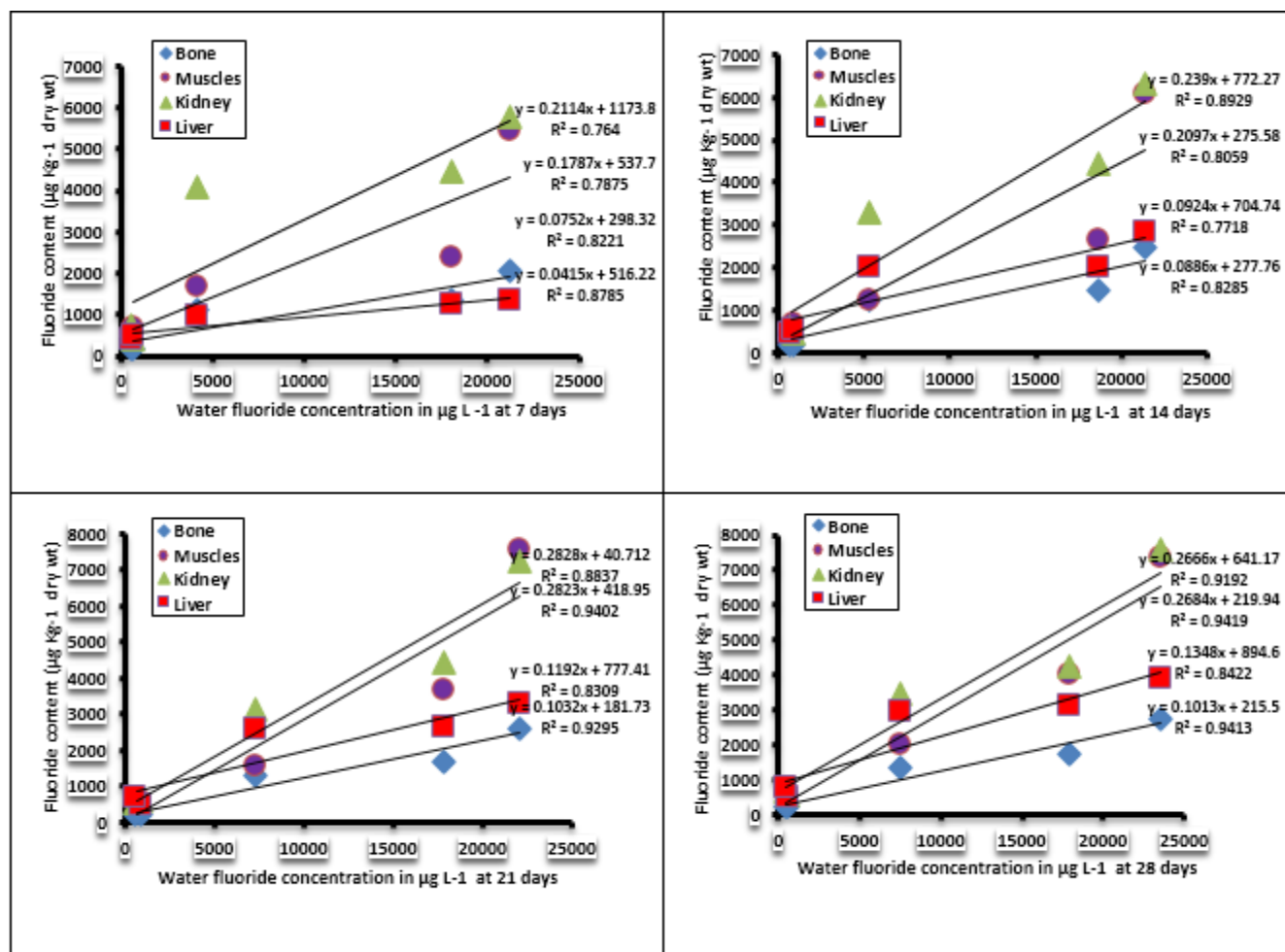
During the experiment days, fish were regularly checked for any changes in their behavioral aspects, such as air gulping, operculum movements, swimming patterns, equilibrium, and feeding activities. Opercular movements were noted per minute and air gulps for every 15 minutes.

### Statistical analysis

Statistical analysis was done through statistical software. Linear regression was done in MS Excel 2007.

## RESULTS

Fig. 1(A to D) represents fluoride and Fig. 2 (A to D) represents arsenic contents in exposure medium (water) and blood, liver, kidney, muscles and bones of *Clarias batrachus* when exposed respectively, to sodium fluoride and arsenic trioxide for 28 days. The concentrations of fluoride and arsenic were high in the exposure medium (water) of fluoride and arsenic alone groups, respectively as compared from their co-exposure groups throughout 28 days. Fluoride accumulation in *Clarias batrachus* demonstrated that as the concentration of fluoride increased in the exposure medium, more fluoride accumulated within the organism. Hence, after 7, 14, 21 and 28 days of exposure, the levels of fluoride in tissues, blood, and bone were increased with increasing water fluoride concentration and exposure duration. The distribution pattern of fluoride was in decreasing order of liver > bone > kidney > muscles > blood. Fluoride level in the liver was the highest ( $4817.73 \pm 238.64 \mu\text{g Kg}^{-1}$  dry weight) whereas; the lowest level was in the muscle tissue ( $2735.71 \pm 133.26 \mu\text{g Kg}^{-1}$



**Fig. 1 :** Linear regression of fluoride levels in different tissues from *Clarias batrachus* with fluoride level in exposure medium (water) at 7 (A), 14(B), 21(C), 28 days (D).

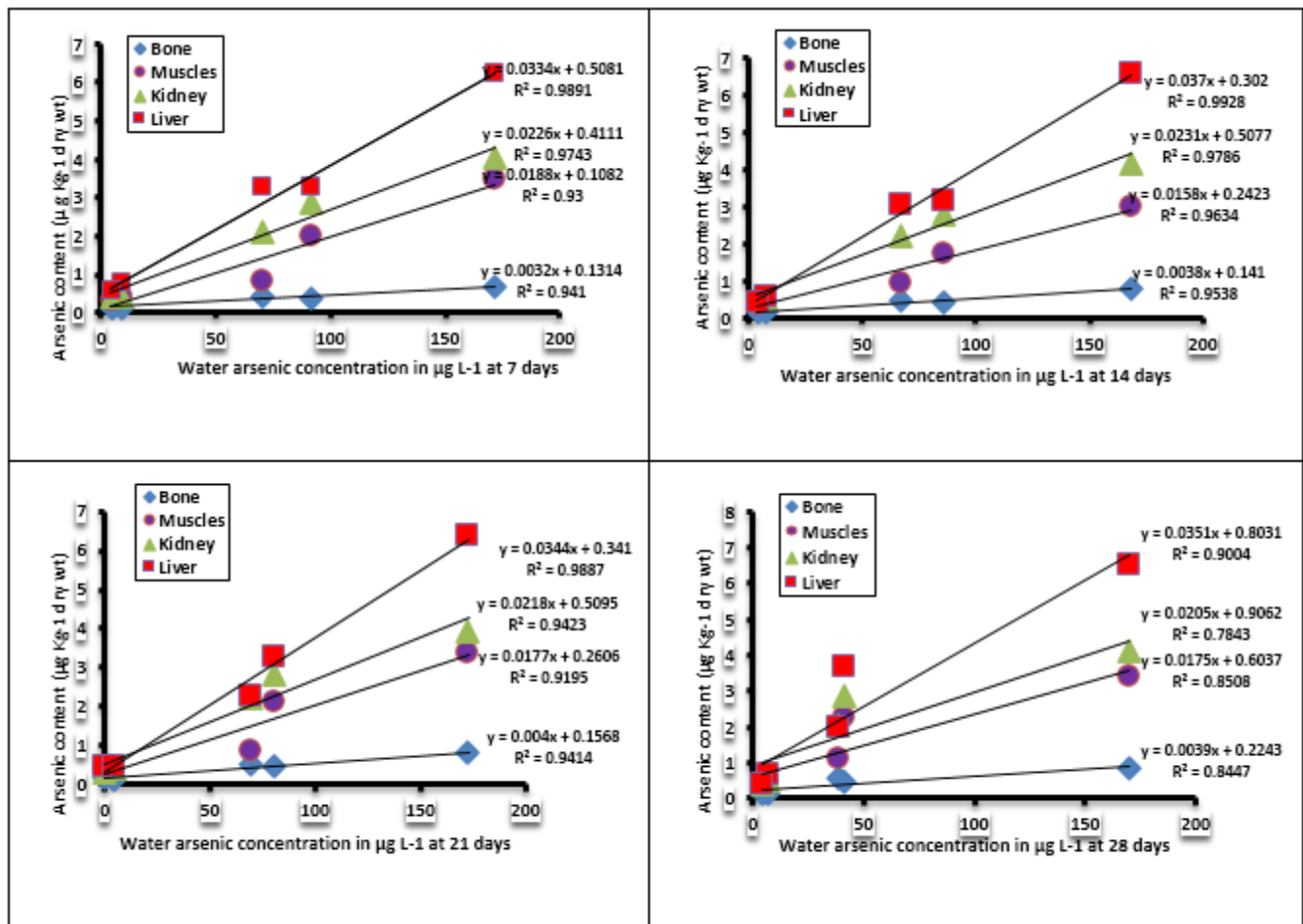


Fig. 2 : Linear regression of arsenic levels in different tissues from *Clarias batrachus* with fluoride level in exposure medium (water) at 7 (A), 14(B), 21(C), 28 days (D).

Table 1 : Behavioral response of *Clarias batrachus* exposed to various concentrations of arsenic trioxide and sodium fluoride up to 28 days.

Parameters	Experiment groups				
	Group I	Group II	Group III	Group IV	Group V
Air gulping (per 15 min)	11.33±2.08 <sup>a</sup>	10.67±1.45 <sup>a</sup>	8.33±0.88 <sup>a</sup>	11.00±1.20 <sup>a</sup>	3.33±0.88 <sup>b</sup>
Opercular movement (per min)	41.33±1.45 <sup>b</sup>	38.00±1.15 <sup>a</sup>	36.33±1.20 <sup>a</sup>	37.00±1.73 <sup>a</sup>	30.00±1.15 <sup>c</sup>
Swimming movement (7-28 d)	ES	ES	ES	ES	U
Body position (7-28 d)	SV	SV	SV	SV	B
Equilibrium (7-28 d)	EL	EL	EL	EL	N
Food sensitivity (7-28 d)	VL	L	L	L	N

Mean±SE (n=3); (Group I- 1.5 mg L<sup>-1</sup> As; Group II- 30 mg L<sup>-1</sup> F; Group III- 0.75 mg L<sup>-1</sup> As + 15 mg L<sup>-1</sup> F; Group IV- 1.5 mg L<sup>-1</sup> As + 30 mg L<sup>-1</sup> F; Group V- Control). U uniform, ES erratic and speedy movements, SV swimming vertically near the upper surface of the water, B at the bottom, EL equilibrium lost, N normal, VL very low, L low.

dry weight) at the end of 28 days. The distribution pattern of arsenic was in decreasing order of liver > kidney > muscles > bone > blood. Arsenic level in the liver was

the highest (6.515±0.14 μg Kg<sup>-1</sup> dry weight) whereas; the lowest level was observed in the bones (0.834±0.02 μg Kg<sup>-1</sup> dry weight) at the end of 28 days.

## Behavioral study

Behavioral changes (air gulping, opercular movement, swimming activity, body position, and food sensitivity) are depicted in Table 1. The number of air gulps (per 15 min for 7-28 days) increased ( $P < 0.01$ ) from  $3.33 \pm 0.88$  in the control group to  $11.33 \pm 2.08$  in the exposed Group I ( $1.5 \text{ mg L}^{-1} \text{ As}$ ). A significant increase ( $P < 0.01$ ) in the number of opercular movements (per min, 7-28 d) was recorded in treatment groups as compared to control. The recorded values ranged from  $10.00 \pm 1.15$  in the control group to  $41.33 \pm 1.45$  in Group I ( $1.5 \text{ mg L}^{-1} \text{ As}$ ) exposed group. During the experiment period, treated fishes were very restless while control fishes were very calm and spent most of the time at the bottom. The swimming activity of experimental fishes was found to be erratic and rapid; with body slanted head upside. However, control fish remained normal and swam horizontally throughout the experimental period (28 d). Equilibrium was lost in all treated groups as compared to control fishes. Fishes mostly hung vertically with mouth pointed towards the surface and slow response to food. Sometimes they started following and biting other fishes.

## DISCUSSION

As a consequence of their accumulation in various tissues, the intakes of fluoride and arsenic damage the cellular structures. Fluoride gets easily absorbed in fish tissues although preferably it is accumulated more in bones as fluoride has a high affinity for Calcium. Shi *et al* (2009) reported a significant increase in fluoride concentration in bone, cartilage, skin, and gill of Siberian sturgeon exposed to fluoride for 90 days. Accumulation of fluoride at a water concentration of  $\geq 4 \text{ mg L}^{-1}$  leads Siberian sturgeon up to the level of  $3204.4 \text{ mg Kg}^{-1}$  in bone,  $1401.2 \text{ mg Kg}^{-1}$  in cartilage,  $389.4 \text{ mg Kg}^{-1}$  in gills,  $100.1 \text{ mg Kg}^{-1}$  in the skin. Our observation that more accumulation of fluoride takes place in bone than other tissues conforms to previous studies by other workers (Shi *et al*, 2009; Ganta *et al*, 2015). Not only bones, but fluoride also targets soft tissues including the kidney, liver, muscles, gills, gut, pylorus, spleen brain and testis, etc. (Sewelam, 2017; Shi *et al*, 2009; Inkielewicz and Krechniak, 2003). In the present study, fluoride accumulation in soft tissue was observed in a dose-dependent manner with the highest in the liver followed by kidney and muscles. This is concordant with the previous findings conducted on fluoride-treated Siberian sturgeon that liver, gut and pylorus accumulated more fluoride than muscles and their accumulation was in a dose-dependent manner (Shi *et al*, 2009).

The liver is the chief organ by way of metabolic

functions involved in the uptake, accumulation, detoxification and excretion of toxic elements. It is one of the sensitive organs of teleost fishes that show a change in biochemistry, histoarchitecture and physiology following exposure to environmental pollutants (Puntoriero *et al*, 2018). Biotransformation of arsenic primarily occurs in the liver and tends to accumulate thereby binding with thiol or  $-SH$  group of protein of liver. In the present study, arsenic accumulated more in the liver than other tissues (kidney, muscles, bone) in both short term and long term exposures, which is in agreement with other findings (Kumari *et al*, 2017; Begum *et al*, 2013; Pazhanisamy *et al*, 2007; Zhang *et al*, 2007). In the present work, the kidney also accumulated a significant level of arsenic after liver. Electrothermal atomic absorption spectroscopy of arsenic reveals the maximum amount of arsenic in the liver and kidney after acute poisoning (Ratnaik, 2003). Muscle contributes major mass to fish and is also the most commonly consumed portion by human beings. In the present study, the accumulation of arsenic and fluoride was very low in muscles, since muscles are not an active site of detoxification and have weak accumulating potential. The present study is also in agreement with Sahu *et al* (2017), who observed that fishes (*Clarias gariepinus*) exposed to different sub-lethal concentrations of sodium fluoride and arsenic trioxide for 96 hours showed a significant increase in tissue fluoride and arsenic concentration with increasing water fluoride and arsenic concentration.

In the present study, altered behavior response in treated fishes, such as, increased rate of air gulping and rapid opercular movements, loss of equilibrium, erratic swimming, hanging, restlessness and decreased food consumption were observed, which depict beyond doubt, a stressful environment due to the presence of toxicant. Increased air gulping and operculum movement are due to the formation of mucus layer over the fish exposed surface, act as a barrier to entry of toxicants. Increased mucus secretion could also block the respiratory surface thus compelling fishes to increase air gulping to meet their oxygen demand.

Erratic swimming and loss of equilibrium observed in the present study may be due to impairment of the nervous system that is responsible for vital activities. Acetylcholinesterase is an enzyme that hydrolyzes a naturally occurring neurotransmitter acetylcholine. Previous studies reported that arsenic and fluoride decrease the activity of acetylcholinesterase in rats (Tolins *et al*, 2014; Bharti and Srivashtava, 2011). Anorexia in treated fish as compared to control ones further corroborates toxic effects. Similar findings were reported

by Anguirre-Sierra *et al* (2013) and Yallappa and Nuzhat (2017) in *Austropotamobius pallipes* and *Cyprinus carpio*, respectively.

Previous studies indicating conflicting reports about antagonism or synergism between arsenic and fluoride include; Li *et al* (1999), Liu *et al* (1999), Mittal and Flora (2006) and Jhala *et al* (2008). Results from the present study suggest that during co-exposure, arsenic and fluoride concentration decreased significantly in exposed water, blood, bone and soft tissues of exposed fish as compared to their exposure, which is in agreement with the work of Sahu *et al* (2017) and Flora *et al* (2012). Decreased accumulation in arsenic and fluoride co-exposed groups can be explained by the fact that sodium fluoride is an ionic compound and gets completely dissolved in an aqueous medium. Thus, fluoride could inhibit the ionization of arsenic compounds hence, reducing their toxicity (Sahu and Kumar, 2021). Fluoride is a highly electronegative element and arsenic can directly react with halogens and other nonmetals, but predominantly bind with halogens due to their high electro-negativity. In trivalent oxidation state ( $As^{3+}$ ) arsenic binds with fluoride and forms  $AsF_3$ , in pentavalent form ( $As^{5+}$ ) it forms  $AsF_5$  (Mittal and Flora, 2006). This indicates that the interaction mechanism of fluoride and arsenic in the development of endemic disease is complicated and may be affected by many uncertain factors.

## CONCLUSION

Arsenic accumulated more in the liver than other tissues, while fluoride accumulated more in bone and very least in muscles in 28 days of exposure. Concomitant exposure to arsenic and fluoride was found to decrease in blood, bone, and soft tissues arsenic and fluoride concentration. Arsenic and fluoride altered behavioral activities in *Clarias batrachus* in a dose and time-dependent manner. Even at very low concentrations, arsenic trioxide seemed to be more effective in causing behavioral alterations as compared from sodium fluoride. The treatments with fluoride and arsenic alone resulted in greater effects than those produced by their combination suggesting antagonism between them.

## ACKNOWLEDGEMENT

Sincere thanks are due University Grants Commission for providing UGC-BSR fellowship to Gamini Sahu as financial assistance and to the Head, School of Life Science for providing lab facilities.

## REFERENCES

Aguirre-sierra A, Alonso L and Camargo J A (2013) Fluoride bioaccumulation and toxic effects on the survival and behavior of the endangered white-clawed crayfish *Austropotamobius*

- pallipes* (Lereboullet). *Arch. Environ. Con. Tox.* **65**, 244-250.
- Ahn J S (2012) Geochemical occurrences of arsenic and fluoride in bedrock groundwater: a case study in Geumsan County, Korea. *Environ. Geochem. Health* **34**, 43-54.
- Akan J C, Mohmoud S, Yikala B S and Ogugbuaja V O (2012) Bioaccumulation of some heavy metals in fish samples from river Benue in Vinikilang, Adamawa State, Nigeria. *Am. J. Analyt. Chem.* **3**, 727-736.
- Al-Ghanim K A, Mahboob S, Seemab S, Sultana S, Sultana T, Al-Misned F and Ahmed Z (2016) Monitoring of trace metals in tissues of *Wallago attu* (lanchi) from the Indus river as an indicator of environmental pollution. *Saudi J. Biol. Sci.* **23**, 72-78.
- APHA (2005) *Standard Methods for the Examination of Water and Wastewater*. 21st Edition, American Public Health Association/American Water Works Association/Water Environment Federation, Washington DC.
- Begum A, Mustafa A I, Amin M N, Banu N and Chowdhury Y R (2013) Accumulation and histopathological effects of Arsenic in tissues of shingi fish (stinging catfish) *Heteropneustes fossilis* (Bloch, 1794). *J. Asiat. Soc. Bangladesh Sci.* **39**, 221-230.
- Benramdane L, Accominotti M, Fanton L, Malicier D and Vallon J J (1999) Arsenic speciation in human organs following fatal arsenic trioxide poisoning-a case report. *Clin. Chem.* **45**, 301-306.
- Beyersmann D and Hartwig A (2008) Carcinogenic metal compounds: recent insight into molecular and cellular mechanisms. *Arch. Toxicol.* **82**, 493-512.
- Bharti V K and Srivastava R S (2011) Effect of pineal proteins at different dose levels on fluoride-induced changes in plasma biochemicals and blood antioxidant enzymes in rats. *Biol. Trace Elem. Res.* **141**, 1-3.
- Borah J (2011) A Comparative Study of Groundwater with special reference to fluoride concentration in some parts of the Dibrugarh district, Assam, India. *Adv. Appl. Sci. Res.* **2**, 318-322.
- Chaurasia N, Pandey S K and Devendra M (2013) Determination of Arsenic content in the water and blood samples of Balia region using Hydride Generation Atomic Absorption Spectrophotometer. *Res. J. Forensic Sci.* **1**, 1-3.
- Chouhan S and Flora S J S (2010) Arsenic and fluoride: two major groundwater pollutants. *Indian J. Exp. Biol.* **48**, 666-678.
- Ganta S, Yousuf A, Nagaraj A, Pareek S, Sidiq M, Singh K and Vishnani P (2013) Evaluation of fluoride retention due to most commonly consumed estuarine fishes among fish consuming population of Andhra Pradesh as a contributing factor to dental fluorosis: a cross-sectional study. *J. Clinic. Diag. Res.* **9**, 11-15.
- Hamilton M (1992) Water fluoridation: a risk assessment perspective. *J. Environ. Health* **54**, 27-32.
- Hoffman D J, Rattner B A, Burton G A and Cairns J (2003) *Handbook of ecotoxicology*. 2nd eds. CRC press company, Washington DC, pp 21-23.
- Inkielewicz I and Krechniaka J (2003) Fluoride content in soft tissues and urine of rats exposed to sodium fluoride in drinking water. *Fluoride* **36**, 263-266.
- Javed M and Usmani N (2019) An overview of the adverse effects of heavy metal contamination on fish health. *Proc. Natl. Acad. Sci., India, Sect. B Biol. Sci.* **89**, 89-403 DOI: 10.1007/s40011-017-0875-7.
- Jha S K, Mishra V K, Sharma D K and Damodaran T (2011) Fluoride



- in the environment and its metabolism in humans. *Rev. Environ. Contam. T.* **211**, 121-142.
- Jiang S, Su S, Yao S, Zhang Y, Cao F, Wang F, Wang H, Li J and Xi S (2014) Fluoride and arsenic exposure impairs learning and memory and decreases mGluR5 expression in the hippocampus and cortex in rats. *PLoS One* **9**, e96041.
- Kumari B, Kumar V, Sinha A K, Ahsan J, Ghosh A K, Wang H and DeBoeck G (2017) Toxicology of arsenic in fish and aquatic systems. *Environ. Chem. Lett.* **15**, 43-64.
- Labiotkowski-Arendarczyk N, Kosik-Bogacka D I, Kalisinska E, Sokolowski S, Lebiotkowski M, Baranowska-Bosiacka I, Gutowska I and Chlubek D (2015) Bone fluoride content in patients after hip and knee joint surgery. *Fluoride* **48**, 223-233.
- McIvor M (1990) Acute fluoride toxicity: pathophysiology and management. *Drug Saf.* **5**, 79-85.
- Mittal M and Flora S J S (2006) Effects of individual and combined exposure to sodium arsenite and sodium fluoride on tissue oxidative stress, arsenic and fluoride levels in male mice. *Chem-Biol. Interact.* **162**, 128-39.
- Nriagu J, Bhattacharya P, Mukherjee A, Bundschuh J, Zevenhoven R and Loeppert R (2007) Arsenic in soil and groundwater: an overview. In: *Trace Metals and other Contaminants in the Environment* (Bhattacharya P, Mukherjee A, Bundschuh J, Zevenhoven R and Loeppert R eds.), pp. 3-60, Elsevier, Amsterdam, The Netherlands.
- Olsson P E, Kling P and Hogstrand C (1998) Mechanisms of heavy metal accumulation and toxicity in fish. *Metal Metabolism in Aquatic Environments* 321-350.
- Pazhanisamy K, Vasanthy M and Indra N (2007) Bioaccumulation of arsenic in the freshwater fish *Labeo rohita* (Hamilton). *The Bioscan* **2**, 67-69.
- Pickford K A, Thomas-Jones R E, Wheals B, Tyler C R and Sumpter J P (2003) Route of exposure affects the oestrogenic response of fish to 4-tert-nonylphenol. *Aquat Toxicol.* **65**, 267-279.
- Puntoriero M L, Cirelli A F and Volpedo A V (2018) Histopathological changes in liver and gills of *Odontesthes bonariensis* inhabiting a lake with high concentrations of arsenic and fluoride (Chasicó Lake, Buenos Aires province). *Rev. Int. Contam. de Ambient.* **34**, 69-77.
- Ratnaike R N (2003) Acute and chronic arsenic toxicity. *Postgrad. Med. J.* **79**, 391-396.
- Sahu G, Pervez S and Poddar A N (2017) Combined toxicity and bioconcentration of fluoride and arsenic in African catfish *Clarias gariepinus* (Burchell, 1822). *Int. J. Environ. Agric. Biotechnol.* **2**, 2456-1878.
- Sahu G and Kumar V (2021) The toxic effect of fluoride and arsenic on behavior and morphology of catfish (*Clarias batrachus*). *Nat. Environ. Pol. Technol.* **20**, 371-375.
- Sewelam A S (2017) Toxicity of sodium fluoride in the liver of albino rat and the beneficial effect of calcium in reversing fluoride toxicity: histological, ultrastructural and immunohistochemical studies. *Egypt. J. Hosp. Med.* **69**, 2562-2582.
- Shankar S, Shanker U and Shikha (2014) Arsenic Contamination of Groundwater: A Review of Sources, Prevalence, Health Risks, and Strategies for Mitigation. *Sci. World J.* <https://doi.org/10.1155/2014/304524>.
- Shi X, Zhuang P, Zhang L, Feng G, Chen L, Liu J, Qu L and Wang R (2009) The bioaccumulation of fluoride ion (F<sup>-</sup>) in Siberian sturgeon (*Acipenser baerii*) under laboratory conditions. *Chemosphere* **75**, 376-380.
- Suhendrayatna S, Ohki A, Nakajima T and Maeda S (2002) Studies on the accumulation and transformation of arsenic in freshwater organisms I. Accumulation, transformation, and toxicity of arsenic compounds on the Japanese Medaka, *Oryzias latipes*. *Chemosphere* **46**, 319-24.
- Tolins M, Ruchirawat M and Landrigan P (2014) The developmental neurotoxicity of arsenic: cognitive and behavioral consequences of early life exposure. *Ann. Glob. Health* **80**, 303-314.
- Wang S and Shi X (2001) Molecular mechanisms of metal toxicity and carcinogenesis. *Mol. Cell. Biochem.* **222**, 3-9.
- Whitford G M (1996) The metabolism and toxicity of fluoride. *Monogr. Oral Sci.* **16**, 1-153.
- WHO (2002) Fluorides. *Geneva, World Health Organization (Environmental Health Criteria, 227)*.
- Yallappa S and Asiya Nuzhat F B (2017) Toxic effect of biochemical and morphological changes on carp (*Cyprinus carpio*) exposed to cadmium chloride. *Int. J. Zool. Stud.* **2**, 222-228.
- Yousafzai A M, Khan A R and Shakoori A R (2008) Heavy metal pollution in river Kabul affecting the inhabitant fish population. *Pak. J. Zool.* **40**, 331-339.
- Zhang M, Wang A, He W, He P, Xu B, Xia T, Chen X and Yan K (2007) Effects of fluoride on the expression of NCAM, oxidative stress, and apoptosis in primary cultured hippocampal neurons. *Toxicol.* **236**, 208-216.
- Zhao S, Feng C, Quan W, Chen X, Niu J and Shen Z (2012) Role of living environments in the accumulation characteristics of heavy metals in fishes and crabs in the Yangtze River Estuary, China. *Mar. Pollut. Bull.* **64**, 1163-1171.

## ANTIMICROBIAL EFFICACY OF BIOACTIVE COMPOUNDS OF RARE ENDOPHYTIC ACTINOBACTERIA, *Actinoalloteichus cyanogriseus* SIR5 (MK793584)

Geetika Wag<sup>✉</sup>, Sunita Datla and Ashwini Kumar Gupta

Microbiology Research Laboratory, School of Studies in Life Science, Pt. Ravishankar Shukla University, Raipur-492010, Chhattisgarh, India

<sup>✉</sup>Corresponding Author: [geet.mun08@gmail.com](mailto:geet.mun08@gmail.com)

### ABSTRACT

To address the problem of antibiotic resistance in pathogens, our research aimed for endophytic actinobacteria, producers of a diverse array of significant bioactive metabolites. Endophytic actinobacteria SIR5 was isolated from roots of *Sphaeranthus indicus* Linn. and was identified to be *Actinoalloteichus cyanogriseus* via 16S rRNA sequencing. With the accession number MK793584, the gene sequence was deposited to NCBI. In the current study, a rare actinobacteria *Actinoalloteichus cyanogriseus*, has been reported as an endophyte for the first time. Both Microbial Type Culture Collection (MTCC) and Clinical Cultures (CC) were used to investigate the antimicrobial property of the bioactive chemicals synthesized by *A. cyanogriseus* SIR5. A significant zone of inhibitions was recorded against clinical cultures: *B. cereus* (12.16±0.16 mm), *Candida albicans* (12.83±0.44 mm), *E. coli* (15.33±0.33 mm), *S. epidermidis* (11.50±0.28 mm) and MTCC pathogens: *B. cereus* (11.16±0.16 mm), *B. subtilis* (13.33±0.16 mm), *P. aeruginosa* (13.33±0.33 mm), *S. epidermidis* (12.33±0.33 mm). The production of bioactive compound was enhanced by optimization using one factor at a time (OFAT), which was achieved with modified ISP-4 medium (starch - 1% w/v, NH<sub>4</sub>NO<sub>3</sub> - 1% w/v, CaCO<sub>3</sub> - 2 g/l, K<sub>2</sub>HPO<sub>4</sub> - 1 g/l, MgSO<sub>4</sub> - 1 g/l, NaCl - 1g/l, trace solution - 1 ml/l) with inoculum size - 13%, incubation period - 16 days, pH - 8.0 and temperature - 28°C.

**Keywords:** *Actinoalloteichus cyanogriseus*, Bioactive Compounds, Antimicrobial Activity, Endophytic Actinobacteria

RASĀYAN J. Chem., Vol. 14, No.3, 2021

### INTRODUCTION

The increased multidrug resistance (MDR) in pathogens as a result of anthropogenic activities in addition to natural processes (through hereditary changes, efflux pump,  $\beta$  lactamases, etc.) is alarming for public health and modern medicine.<sup>1,2</sup> The situation has resulted in reduced effectiveness of approved antibiotics and thus efforts are being made to find efficient and broad-spectrum antibiotics from actinobacteria which are potential producers of diverse metabolites. Since currently available antibiotics are mainly derived from soil actinobacteria, research on endophytic actinobacteria is underway to replace repetitive discovery of known antibiotics. Endophytic actinobacteria are more likely to be involved in the metabolic pathway of the host plant and thus chances of production of some potential novel bioactive metabolites in addition to chemically similar ones are more.<sup>3</sup> Taxane (taxol), an anticancer compound produced by the plants *Taxus brevifolia* and *Taxus baccata*, has also been obtained from its endophyte *Micromonospora* sp. and *Kitasatospora* sp. respectively,<sup>4</sup> possibly evidencing the involvement of both in their metabolism. Thus to ascertain more efficient compounds, recent research has focused on rare endophytic actinobacteria, an underexplored group of microorganisms.

In this study, a rare actinobacteria, *Actinoalloteichus cyanogriseus* strain SIR5 was procured from the root tissue of medicinal weed *Sphaeranthus indicus* from Raipur, Chhattisgarh and its antimicrobial activity was observed against MTCC and Clinical pathogens. Previously, *A. cyanogriseus* has been isolated from the soils of China and the strain was authenticated to be of family *Pseudonocardiaceae*, based on phylogenetic analysis.<sup>5</sup> Bioactive alkaloids, caeruleomycins and cyanogramide, obtained from marine *A. cyanogriseus*, exhibited significant antibacterial, antifungal, anticancer and antiamoebic activity.<sup>6-8</sup>

# Characterization of a novel keratinase from *Chrysosporium tropicum*

Sarkar Ashis Kumar<sup>1\*</sup> and Gupta Ashwini Kumar<sup>2</sup>

<sup>1</sup> Faculty of Science, Shri Rawatpura Sarkar University, Raipur 492016, Chhattisgarh, INDIA

<sup>2</sup> School of Life Sciences, Pandit Ravishankar Shukla University, Raipur 492010, Chhattisgarh, INDIA  
\*toashis@gmail.com

## Abstract

A keratinophilic fungus *Chrysosporium tropicum* was isolated from poultry farm soil and screened for extracellular keratinase activity. The fungus was cultured in basal salts medium and keratinase production was assessed. The novel keratinase was purified by Sephadex G-100 column chromatography and characterized. The molecular weight of the enzyme was estimated to be 14.5 KDa by sodium dodecyl sulfate-polyacrylamide gel electrophoresis (SDS-PAGE). The optimum pH and temperature of the keratinase were found to be 7.5 and 40°C respectively.

The  $K_m$  for keratin powder from human hair was 6.67 mg and the  $V_{max}$  of novel keratinase was determined to be 0.33 mg ml<sup>-1</sup> by the Lineweaver-Burk plot. The enzyme activity was almost completely inhibited by phenylmethylsulphonyl fluoride (PMSF) suggesting that the keratinase belongs to the serine protease family.

**Keywords:** Keratinophilic fungi, *Chrysosporium tropicum*, extracellular keratinase, purification.

## Introduction

Keratin, an insoluble fibrous protein, is non-degradable by common proteases such as pepsin, trypsin, papain etc. because of the presence of high degree disulfide cross-linking. The keratinous wastes generally are feathers, hair, nails, horn, hoofs, skin, scales and wool. Globally the most abundant keratinous materials are poultry feathers which are increasing annually with rising global production and consumption<sup>18</sup>. Feathers contain around 90% keratin protein and the traditional methodology to degrade those leads to the destruction of valuable amino acids needed to prepare protein-rich feather meal.

Traditionally feathers are degraded by alkali hydrolysis and steam pressure cooking, consuming a huge amount of energy and producing waste which leads to environmental hazards<sup>8,11</sup>. Numerous microorganisms, actinomycetes, bacteria and fungi, are responsible for keratin utilization in nature and thrive on it. These organisms produce proteolytic enzymes keratinase having keratinolytic ability which naturally degrades keratin wastes<sup>3,20</sup>.

Keratinophilic or keratinolytic fungi are closely related to dermatophytes and have the capability of tissue invasion<sup>21</sup>.

Enzyme keratinase has been purified and characterized, produced by various microorganisms such as fungi<sup>1,9,13,16,17</sup>, bacteria<sup>2,11</sup> and a few *Streptomyces* species<sup>6</sup>. The keratinase produced by these organisms showed specific activity on insoluble keratin. The production of extracellular keratinase was governed by several factors like temperature, pH, carbon and nitrogen sources and types of keratin substrates.

The characterization of keratinase is warranted for important biotechnological applications in industrial processes<sup>1</sup>. The industrial application of keratinase varies hugely as it has been used for dehairing of skin and hides, preparation of feather meal and nitrogen fertilizers from poultry feathers. The present study deals with the production, purification and characterization of extracellular keratinase from *Chrysosporium tropicum* (NFCCI-3317) isolated from a poultry farm soil.

## Material and Methods

**Isolation and maintenance of culture:** *C. tropicum* (NFCCI-3317) was isolated from the poultry farm soil of Raipur, India. The fungus was maintained in Sabouraud's dextrose agar (pH 5.60) at 26±2°C.

**Production of keratinase enzyme:** For production of extracellular keratinase enzyme, basal salts medium [KH<sub>2</sub>PO<sub>4</sub> - 1.5g; MgSO<sub>4</sub>.7H<sub>2</sub>O - 0.025g; FeSO<sub>4</sub>.7H<sub>2</sub>O - 0.015g; ZnSO<sub>4</sub>.7H<sub>2</sub>O - 0.005g and CaCl<sub>2</sub> - 0.025g in 1 litre, deionized distilled water, pH - 7.0] was used for the fungus. Erlenmeyer flasks (150 ml) containing 50 ml of this medium supplemented with 500 mg of defatted and pre-sterilized human hairs (1 cm length) as a substrate were inoculated and incubated at 27°C for 6 weeks in static condition. Six test flasks and one control set were maintained for observations. Each test flask was inoculated with a 6 mm disc from 7-day old fungal culture. Flasks containing the medium with a disc of agar without the fungus served as control. After the incubation period, culture filtrates from each flask were filtered through Whatmann filter paper no. 42 and centrifuged at 5000 rpm for 5 min. The supernatant was used for the estimation of extracellular keratinase enzyme and protein.

**Assay of keratinase activity:** To assess the keratinase activity, the method of Yu et al<sup>23</sup> was followed with some modifications. 50 mg of human hairs (4-5 mm in length) were suspended in 4.5 ml of 0.028M phosphate buffer to which 0.5 ml of culture filtrate was added as an enzyme source. The reaction mixture was incubated at 37°C for 1 h and then immersed in ice water for 10 min to stop the



Received on 17 April 2022; received in revised form, 15 June 2022; accepted 14 September 2022; published 01 December 2022

## PHYTOCHEMICAL ASSESSMENT AND SYNERGISTIC BIOEFFICACY OF *CURCUMA CAESIA* (ROXB.) FROM BASTAR AGAINST MULTI-DRUG RESISTANT HUMAN PATHOGENS

Dhananjay Pandey<sup>1,\*2</sup> and A. K. Gupta<sup>1</sup>

School of Studies in Life Science<sup>1</sup>, Pt. Ravishankar Shukla University, Raipur - 492010, Chhattisgarh, India.

Department of Botany<sup>2</sup>, Government Naveen Girls College, Surajpur - 497229, Chhattisgarh, India.

### Keywords:

Phytochemicals, Bastar, Bioactive compound, Synergism, Multi-drug resistant, Human pathogens

### Correspondence to Author:

Dr. Dhananjay Pandey

Assistant Professor,  
Department of Botany,  
Government Naveen Girls College,  
Surajpur - 497229, Chhattisgarh,  
India.


E-mail: pandey.dhananjay333@gmail.com

**ABSTRACT:** The current research is an attempt to investigate the antibacterial and synergistic bioefficacy of *Curcuma caesia* (Roxb.) versus human pathogenic bacteria viz., *Bacillus cereus*, *Bacillus subtilis*, *Staphylococcus aureus*, *Staphylococcus epidermidis*, *Escherichia coli*, *Klebsiella pneumonia*, *Pseudomonas aeruginosa* and *Proteus vulgaris* procured from IMTECH, Chandigarh, India. Agar well diffusion assay was performed, and one-way ANOVA examined the outcome. The qualitative phytochemical examination revealed a positive test for flavonoids, glycosides, phytosterols, resins, saponins, and tannins. However, the quantitative estimation of phytochemicals revealed that the root sample contains highest amount of flavonoid followed by total phenol, saponin and alkaloid. The bioactive extract was purified using column chromatography. The purified fraction and commercially available antibacterials viz., tetracycline, streptomycin, and penicillin was evaluated for their synergistic or antagonistic efficacy counter to multi-drug resistant human pathogenic bacteria. The outcome divulge that a purified fraction of *C. caesia* was found to act synergistically with tetracycline against all the bacterial cultures under investigation. The results with streptomycin showed maximum synergistic activity against *B. cereus*. However, penicillin and purified fraction exhibit utmost synergistic activity against *S. epidermidis* and *B. subtilis*. The results revealed that the methanolic root extract of *C. caesia* bears a potential bioactive phytocompound conferring enhanced synergism.

**INTRODUCTION:** The antibiotic resistance exhibited by multi-drug resistant human pathogenic microorganisms is a burning issue and is of serious global concern<sup>1</sup>. The clinical pathogenic bacterial strains possess the immense genetic potential to attain and transmit resistance against frequently used antibiotics<sup>2,3</sup>.

The profuse use of antibiotics to cure infectious ailments induced the emergence of multi-drug resistant human pathogenic bacteria leading to a decline in health benefits over the past few decades<sup>4,5</sup>. One of the best choices to combat this great resistance issue is the implication of combination therapy<sup>6</sup>.

In the current scenario, combination therapy is a great boon to mankind, especially for patients suffering from severe infections due to MDR human pathogenic bacteria<sup>7</sup>. Synergism is a constructive interplay when two drugs amalgamate and employ an inhibitory outcome exceeding the sum of their discrete results<sup>8</sup>.

	QUICK RESPONSE CODE
	DOI: 10.13040/IJPSR.0975-8232.13(12).5129-38
This article can be accessed online on <a href="http://www.ijpsr.com">www.ijpsr.com</a>	
DOI link: <a href="http://dx.doi.org/10.13040/IJPSR.0975-8232.13(12).5129-38">http://dx.doi.org/10.13040/IJPSR.0975-8232.13(12).5129-38</a>	

# Research and Publication Ethics - Evaluation of participants

21.03.2022 to 26.03.2022

Sr. No.	Name of the Candidate	Result
1	Ku. Payal	Succeeded
2	Shrawan Yadav	Succeeded
3	Vinod Kumar Khunte	Succeeded
4	Ku. Asha Gupta	Succeeded
5	Ankita Bhoi	Succeeded
6	Labya Prabhas	Succeeded
7	Benu Prasad Sidar	Succeeded
8	Likesh Patel	Succeeded
9	Pradeep Barman	Succeeded
10	Abhishek Katakwar	Succeeded
11	Suman Dhritlahare	Succeeded
12	Kavita Patel	Succeeded
13	Shailendra Wasnik	Succeeded
14	Arti Gajendra	Succeeded
15	Sandeep Kumar Tiwari	Succeeded
16	Onkar Prasad	Succeeded
17	Roopam Jain	Succeeded
18	Pritam Kumar Dass	Succeeded
19	Lokesh Kumar Sahu	Succeeded
20	Pankaj Kumar Bharti	Succeeded
21	Khushabu	Succeeded
22	P. Riya Ritika Singh	Succeeded
23	Nisha Singh	Succeeded
24	Sanjay Kumar	Succeeded
25	Chandrakanta Sethi	Succeeded
26	Gyanendra Bhoi	Succeeded
27	Alok Kumar Chaurasiya	Succeeded
28	Upasana Vishwakarma	Succeeded
29	Apurva Sharma	Succeeded
30	Durgesh Nandini Joshi	Succeeded
31	Nikita Raghuvanshi	Succeeded
32	Suryakant Manikpuri	Succeeded
33	Yogyata Chawre	Succeeded
34	Ankita Beena Kujur	Succeeded
35	Shubhra Sinha	Succeeded
36	Gayatri Patel	Succeeded
37	Smt. Neha Pillay	Succeeded
38	Abhishek Katendra	Succeeded
39	Angel Minj	Succeeded
40	Reena Suryawanshi	Succeeded
41	Jai Singh Sarswat	Succeeded
42	Dharana Agrawal	Succeeded
43	P. Veena Swami	Succeeded
44	Temin	Succeeded
45	Shruti Reddy	Succeeded
46	Anjali Xalxo	Succeeded
47	Prakhar Mishra	Succeeded
48	Zeenat Sultana	Succeeded
49	Anurag Tiwari	Succeeded
50	Smt Sarita Sharma	Succeeded

27/3/22

**Review article****PYRETHROID INDUCED TERATO-GENICITY AND GENOTOXICITY**

Ajay Singh Shakya\*, Ajay Kumar and S. K. Prasad

School of Studies in Life Science, Pt. Ravishankar Shukla University, Raipur - 492 010, India.

\*e-mail : [ajaysinghshakya556@gmail.com](mailto:ajaysinghshakya556@gmail.com)

(Received 3 October 2021, Revised 30 November 2021, Accepted 18 December 2021)

**ABSTRACT :** Pesticide has become an integral part of modern agriculture. Pyrethroids are biodegradable that is why uses of this pesticide being in large amounts, and due to their not being used properly, they affect harmful insects as well as many beneficial insects and many different types of organisms and humans. Produced effects such as neurotoxic, genotoxic and teratogenic effects. Cypermethrin (CYP), a class-II type of pyrethroid pesticide has been studied in many organisms for its various adverse effects, but its teratogenic and genotoxic effect has not been much studied in birds. So, in this review conclude the genotoxic and teratogenic potential of different type of pyrethroid in various animals.

**Key word :** Pyrethroid, teratogenicity, genotoxicity.

**How to cite :** Ajay Singh Shakya, Ajay Kumar and S. K. Prasad (2022) Pyrethroid induced terato-genicity and genotoxicity. *Biochem. Cell. Arch.* 22, 4019-4024. DOI: <https://doi.org/10.51470/bca.2022.22.2.4019>, DocID: <https://connectjournals.com/03896.2022.22.4019>

**INTRODUCTION**

Pesticides are chemical, which is used against pests in agriculture, animal husbandry and public health. Against the targeted species these chemicals are highly effective, thus became the inseparable part of modern agriculture. Pesticides are divided into organophosphate, organochlorines, carbamate and pyrethroid based on their chemical structure. Due to the rapid biodegradable of pyrethroid, it is being used in place of carbamide, organophosphate and organochloride (Kaushik *et al*, 2018).

Pyrethroid is a group of synthetic pesticide, which is similar to the natural pesticide pyrethrum and produced by the flower of pyrethrum plant of chrysanthemum genus of Compositae family native to Asia and northeastern Europe. As an insecticide, these pyrethroids are used in agriculture, disinfection and ectoparasitic disease (Heudorf and Angerer, 2001). Pyrethroid bind to voltage-sensitive Na- channel and convert their gating kinetics, thereby nerve function are disrupted and generate acute neurotoxic effects in insect as well as non-target organism (Choi and Soderlund, 2006). Studied suggest that in non-targeted species teratogenicity, reproductive toxicity and genotoxicity could be induced by pyrethroid.

**Type of pyrethroid**

On the basis of chemical structure pyrethroids are classify in two type -

Type I and type II (Kaushik *et al*, 2018).

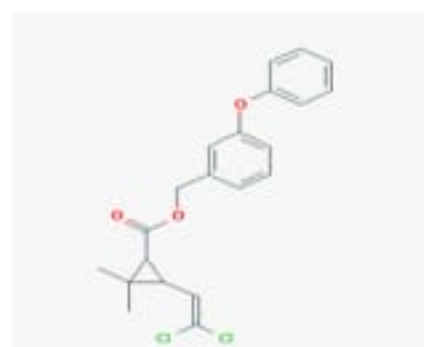
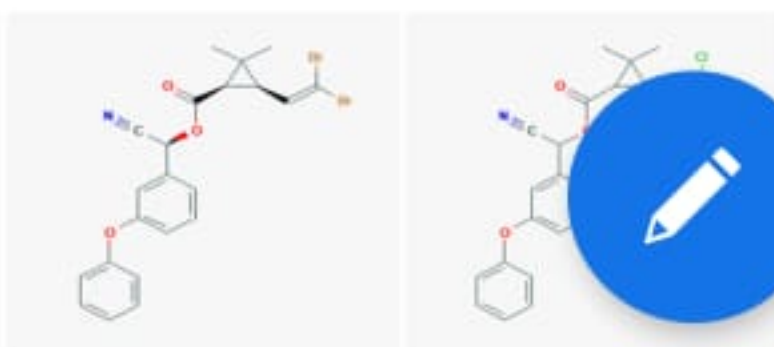
**Type I** - Pyrethroid that have without cyano group.

**Type II** - Pyrethroid that have contained cyano group

Type I	Type II
Permethrin	Cypermethrin
Bioallethrin	Deltamethrin
Tefluthrin	Fenvalerate
Allethrin	$\lambda$ -cyhalothrin
Tetramethrin	$\alpha$ -cypermethrin
Resmethrin	$\beta$ -cypermethrin
Bioresmethrin	Esfenvalerate
Prallethrin	Cyfluthrin

**Teratogenicity and genotoxicity**

The development of any type of structural and functional defects during fetal development is called teratogenicity. Genotoxicity refers to processes that alter the structure, information content, or segregation of DNA and that are not necessarily associated with mutagenicity (Pellevoisin *et al*, 2018).

**Type I****Type II**

## Total Chlorophyll Determination in Leafy Vegetables Cultivated in Hydroponics and Soil

Labya Prabhas<sup>1</sup>, Dr. Amia Ekka<sup>2</sup>

<sup>1</sup>Assistant Professor, School of Studies in Life Science,  
Pt. Ravishankar Shukla University, Raipur, Chhattisgarh, India.

<sup>2</sup>Professor, School of Studies in Life Science, Pt. Ravishankar Shukla University, Raipur,  
Chhattisgarh, India.

### ABSTRACT:

There are many factors that can be used to describe the growth outline of the plant. Qualitative and quantitative estimation of phyto-chemical composition of the plant's can directly reflects the growth pattern. These may also reflects the nutraceutical values of the plant for human consumption. Selected plant species are leafy vegetables and popular among the people of central India. Cultivation of selected plant's species is carried out in two different ways. Traditional method of plant cultivation includes soil based cultivation and other is hydroponic technique. In hydroponics, there is no need of soil, liquid media remains in direct contact with the seed and root of the plant. Hydroponically grown *S. oleracea* L (1.447 mg/g) was recorded with highest amount of chlorophyll, followed by *M. arvensis* (1.338 mg/g), *C. sativum* (1.162 mg/g), *T. F. graceum* L. (1.097 mg/g), *C. oltorius* L. (1.060 mg/g), *A. viridis* (0.917 mg/g) and *C. arietinum* (0.643 mg/g). On the other hand total chlorophyll content in soil cultivated plants was found highest in *M. arvensis* (1.206) followed by *S. oleracea* L. (1.085), *C. sativum* (1.046 mg/g), *T. F. graceum* L. (0.906), *C. oltorius* L. (0.859 mg/g), *C. arietinum* (836 mg/g) and *A. viridis* (0.794). This study may reveal the compatibility and acceptance of hydroponics for plant cultivation. Chlorophyll content was consistently high in most of the experimental plants cultivated in hydroponic system as compared to soil cultivated plants.

**Keyword:** Phyto-chemical, nutraceutical, hydroponics, total chrolophyll, protein content, carbohydrate, recognize, suitable.

### INTRODUCTION:

Plant is composed of various type of light capturing pigment like chrolophyll, carotenoid and much other type of pigments. Chlorophyll is an important fraction of photosynthetic machinery. Amount of chlorophyll directly represent the number of chloroplast in plant cell. Richness in chlorophyll molecules is responsible for capturing sunlight and conversion into sugar compound. Hence, optimum rate of production of sugar inside plant cell mainly depends upon amount chlorophyll molecule. If optimum sugar is produced and stored by plant then this will result imitate optimum growth of plant too. It means chlorophyll is an important tool which is directly associated with growth of the plant. Chlorophyll is found in

## A Review on Hydroponics: A Sustainable Approach for Plant Cultivation

Received: 22 August 2022, Revised: 28 September 2022, Accepted: 24 October 2022

Mr. Labya Prabhas and Prof. Amia Ekka

School of Studies in Life Science, Pt. Ravishankar Shukla University, Raipur (Chhattisgarh – India)

\*labya\_127@yahoo.co.in

### Keywords

Sustainable development, threshold limit, resources, challenge, plant cultivation, land area, water consumption, compatible, morphology.

### Abstract

Sustainable development is really a matter of concern now days. Many natural events prove that Earth is reaching nearby its threshold limit in terms of natural resources. Saving its natural resources with maintaining rate of development for any country is a major challenge. Especially in case of agriculture, rate of utilization of land area and water consumption is really high. Some effort towards modification in traditional methods of plant cultivation is essential but with rise in total plant productivity or without affecting previous rate of productivity is required. Hydroponics, a novel or non popular plant cultivation technique is showing some assurance towards sustainable development. Hydroponics is a method of plant cultivation without soil. Amount of water requirement is really very less as compared to soil based technique. Some of the plant species is very much compatible for hydroponic cultivation. They include mostly herbaceous or plants with small morphology. An earlier report proves that the existence of hydroponic for plant cultivation in all the seven continents of the world map. Which indicates that world is ready to adopt modification and novel approaches over traditional method of plant cultivation.

### 1. Introduction

Water is souvenir from the nature to us. Existence of all life kind depends upon water prosperity of the Earth. Consumption level may vary from species to species among all living organism but this cannot elucidate importance water in their life. All life forms including unicellular to multicellular organisms is composed of water as a major part in their total cadaver. Life cycle of higher organism like humans and plants are extensively affected by availability of water type for their use. A well known fact that everyday rise in human population is directly compelling us to thing about food scarcity and food security. We are well aware that food resources are the major concern for the existence of mass population. Existence of human population also affects almost all other living species directly and indirectly in food web, but without continuous supply of useable water

resources and food, there is a threat of mass destruction. Now, there is a need to find out some new ideas and creative work out that can help to ensure existence of living beings for longer time with available and limited resources, specially water and food.

Agriculture provides us a major part of food and energy resources. This is followed by dairy and animal farming in well support. But question is "what are the basic needs in agriculture?" Yes, the answer is Sunlight, Water and Nutrition. Apart from sunlight, water also helps in transportation of various mineral and ions from soil to plant body. It means supply of nutrition also depends upon water flow from outside plant cell to inside. If importance of water is significant and only limited resources are available with us then it's certainly a matter of discussion. Because limited water resources and rate of consumption and pollution in water body is hospitable for upcoming troubles.



## A Review on Hydroponics: A Sustainable Approach for Plant Cultivation

Received: 22 August 2022, Revised: 28 September 2022, Accepted: 24 October 2022

Mr. Labya Prabhas and Prof. Amia Ekka

School of Studies in Life Science, Pt. Ravishankar Shukla University, Raipur (Chhattisgarh – India)

\*labya\_127@yahoo.co.in

### Keywords

Sustainable development, threshold limit, resources, challenge, plant cultivation, land area, water consumption, compatible, morphology.

### Abstract

Sustainable development is really a matter of concern now days. Many natural events prove that Earth is reaching nearby its threshold limit in terms of natural resources. Saving its natural resources with maintaining rate of development for any country is a major challenge. Especially in case of agriculture, rate of utilization of land area and water consumption is really high. Some effort towards modification in traditional methods of plant cultivation is essential but with rise in total plant productivity or without affecting previous rate of productivity is required. Hydroponics, a novel or non popular plant cultivation technique is showing some assurance towards sustainable development. Hydroponics is a method of plant cultivation without soil. Amount of water requirement is really very less as compared to soil based technique. Some of the plant species is very much compatible for hydroponic cultivation. They include mostly herbaceous or plants with small morphology. An earlier report proves that the existence of hydroponic for plant cultivation in all the seven continents of the world map. Which indicates that world is ready to adopt modification and novel approaches over traditional method of plant cultivation.

### 1. Introduction

Water is souvenir from the nature to us. Existence of all life kind depends upon water prosperity of the Earth. Consumption level may vary from species to species among all living organism but this cannot elucidate importance water in their life. All life forms including unicellular to multicellular organisms is composed of water as a major part in their total cadaver. Life cycle of higher organism like humans and plants are extensively affected by availability of water type for their use. A well known fact that everyday rise in human population is directly compelling us to thing about food scarcity and food security. We are well aware that food resources are the major concern for the existence of mass population. Existence of human population also affects almost all other living species directly and indirectly in food web, but without continuous supply of useable water

resources and food, there is a threat of mass destruction. Now, there is a need to find out some new ideas and creative work out that can help to ensure existence of living beings for longer time with available and limited resources, specially water and food.

Agriculture provides us a major part of food and energy resources. This is followed by dairy and animal farming in well support. But question is "what are the basic needs in agriculture?" Yes, the answer is Sunlight, Water and Nutrition. Apart from sunlight, water also helps in transportation of various mineral and ions from soil to plant body. It means supply of nutrition also depends upon water flow from outside plant cell to inside. If importance of water is significant and only limited resources are available with us then it's certainly a matter of discussion. Because limited water resources and rate of consumption and pollution in water body is hospitable for upcoming troubles.

## Total Chlorophyll Determination in Leafy Vegetables Cultivated in Hydroponics and Soil

Labya Prabhas<sup>1</sup>, Dr. Amia Ekka<sup>2</sup>

<sup>1</sup>Assistant Professor, School of Studies in Life Science,  
Pt. Ravishankar Shukla University, Raipur, Chhattisgarh, India.

<sup>2</sup>Professor, School of Studies in Life Science, Pt. Ravishankar Shukla University, Raipur,  
Chhattisgarh, India.

### ABSTRACT:

There are many factors that can be used to describe the growth outline of the plant. Qualitative and quantitative estimation of phyto-chemical composition of the plant's can directly reflects the growth pattern. These may also reflects the nutraceutical values of the plant for human consumption. Selected plant species are leafy vegetables and popular among the people of central India. Cultivation of selected plant's species is carried out in two different ways. Traditional method of plant cultivation includes soil based cultivation and other is hydroponic technique. In hydroponics, there is no need of soil, liquid media remains in direct contact with the seed and root of the plant. Hydroponically grown *S. oleracea* L (1.447 mg/g) was recorded with highest amount of chlorophyll, followed by *M. arvensis* (1.338 mg/g), *C. sativum* (1.162 mg/g), *T. F. graceum* L. (1.097 mg/g), *C. oltorius* L. (1.060 mg/g), *A. viridis* (0.917 mg/g) and *C. arietinum* (0.643 mg/g). On the other hand total chlorophyll content in soil cultivated plants was found highest in *M. arvensis* (1.206) followed by *S. oleracea* L. (1.085), *C. sativum* (1.046 mg/g), *T. F. graceum* L. (0.906), *C. oltorius* L. (0.859 mg/g), *C. arietinum* (836 mg/g) and *A. viridis* (0.794). This study may reveal the compatibility and acceptance of hydroponics for plant cultivation. Chlorophyll content was consistently high in most of the experimental plants cultivated in hydroponic system as compared to soil cultivated plants.

**Keyword:** Phyto-chemical, nutraceutical, hydroponics, total chrolophyll, protein content, carbohydrate, recognize, suitable.

### INTRODUCTION:

Plant is composed of various type of light capturing pigment like chrolophyll, carotenoid and much other type of pigments. Chlorophyll is an important fraction of photosynthetic machinery. Amount of chlorophyll directly represent the number of chloroplast in plant cell. Richness in chlorophyll molecules is responsible for capturing sunlight and conversion into sugar compound. Hence, optimum rate of production of sugar inside plant cell mainly depends upon amount chlorophyll molecule. If optimum sugar is produced and stored by plant then this will result imitate optimum growth of plant too. It means chlorophyll is an important tool which is directly associated with growth of the plant. Chlorophyll is found in

## Total Protein and Carbohydrate Determination in Leafy Vegetables Cultivated in Hydroponics and Soil

Labya Prabhas<sup>1\*</sup>, Dr. Parvez A. Khan<sup>2</sup>, Dr. Megha Agrawal<sup>3</sup>, Dr. Amia Ekka<sup>4</sup>

<sup>1</sup>Assistant Professor, School of Studies in Life Science, Pt. Ravishankar Shukla University, Raipur, Chhattisgarh, India.

<sup>2</sup>Research associate, School of Studies in Life Science, Pt. Ravishankar Shukla University, Raipur, Chhattisgarh, India.

<sup>3</sup>Assistant Professor, Gurukul Mahila Mahavidyalaya, Kalibadi, Raipur, Chhattisgarh, India.

<sup>4</sup>Professor, School of Studies in Life Science, Pt. Ravishankar Shukla University, Raipur, Chhattisgarh, India.

(Corresponding author: Labya Prabhas, labya\_127@yahoo.co.in)

(Received 16 September 2022, Accepted 05 November, 2022)

(Published by Research Trend, Website: www.researchtrend.net)

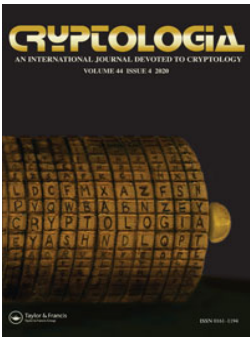
**ABSTRACT:** In this study we are aiming to analyze the effect of change in plant cultivation technique associated with plant growth. Not only morphologically many anatomical and estimation of many phytochemicals can be considered to analyze the effect of plant cultivation technique. Seven leafy vegetable plant species were selected i.e. *Amaranthus viridis*, *Trigonella foenum graceum L.*, *Chorchorus olerarius L.*, *Coriandrum sativum*, *Mentha arvensis*, *Cicer arietinum*, *Spinacia oleracea L.* for cultivating under hydroponic system and in soil. Estimation of amount of protein, carbohydrate and moisture content were aimed to determine the effect on growth of the plant in hydroponics and soil cultivation technique. Hydroponically cultivated leafy plants was found rich in protein except *C. olerarius* (3.6 mg/g) and *T.F. graceum L.* (3.7 mg/g) as compared to soil cultivated plant *C. olerarius* (4.9 mg/g) and *T.F. graceum L.* (4.4 mg/g). Similarly carbohydrate content was also consistently high in hydroponically cultivated leafy plants except one species of *S. oleracea L.* (3.9 mg/g) and it was found as 4.11 mg/g in soil cultivated leafy plant. Somehow growth rate was high in hydroponics under optimum condition. Some important factors in lifecycle of the plant like flowering and fruiting are still to be achieved.

**Keywords:** Plant cultivation, phyto-chemicals, hydroponics, soil cultivation, protein, carbohydrate, moisture, optimum.

### INTRODUCTION

Food is consumed by all living organism to obtain nutritional support, necessary for their growth and survival. A big part of food resources are obtained from the plant by the humans like many other higher animals. Plant consumes energy from sunlight and prepares food for own benefits. Plant uses their stored food material for maintaining their own health and metabolic activities including giving rise to fruits and flower. Food is stored by the plants in form of protein and carbohydrates are also used by other higher organisms called consumers like human beings and animals belong to category of herbivores and omnivores too. Now the important thing is that the nutraceutical value of the food. If food is rich in various type of nutrients and minerals. It will directly reflect to the good health of the organisms who is consuming it as a source of nutrition. Leafy vegetables are one of an important part of nutrition for the people who live in Asia, especially in south Asian country like India. Varieties of leafy vegetables are found and listed in edible resources under Indian Territory. Some of them are cultivated by farmers and local cultivators. Some are also available

seasonally and are of wild type. Some of the popular leafy vegetables in central India are *Oxalis corniculata*, *Cordia myxa* Roxb., *Cicer arietinum*, *Cassia tora*, *Amaranthus viridis L.*, *Chorchorus olerarius*, *Leucas cephalotes*, *Amaranthus gangeticus L.*, *Amaranthus tricolor L.*, *Trigonella foenum graceum L.*, *Spinacea oleracea L.*, *Spinacea glabra L.*, *Basella rubra L.*, *Brassica campestris L.*, *Coriandrum sativum*, *Mentha arvensis*, *Allium cepa*, *Merremia emarginata* Burmf., *Moringa pterygosperma* Lam., *Ipomoea batatas* Lam., *Ipomoea aquatic* Frosk etc. These are only few examples as the climate and region of the Asiatic region changes, plant diversity also varies significantly. Almost all kind of leafy vegetables species are well known for their nutritional values obtained by analyzing various kinds of fibers, vitamins, minerals, protein content, carbohydrate, lipid, and total moisture. Hence, reason behind the obtaining optimum growth by the plant would be maximum amount of stored nutrients. Rise in popularity and consumption of leafy vegetables causes limited productivity and high demand. This situation causes search of new technique and technology over traditional methods of obtaining nutritional resources. Modification and change is must



## Cryptanalysis and improvement of authentication scheme for roaming service in ubiquitous network

Shaheena Khatoon & Balwant Singh Thakur

To cite this article: Shaheena Khatoon & Balwant Singh Thakur (2020) Cryptanalysis and improvement of authentication scheme for roaming service in ubiquitous network, Cryptologia, 44:4, 315-340, DOI: [10.1080/01611194.2019.1706061](https://doi.org/10.1080/01611194.2019.1706061)

To link to this article: <https://doi.org/10.1080/01611194.2019.1706061>



Published online: 10 Feb 2020.



Submit your article to this journal [↗](#)



Article views: 109



View related articles [↗](#)




View Crossmark data [↗](#)



Citing articles: 3 View citing articles [↗](#)



# Cryptanalysis and improvement of authentication scheme for roaming service in ubiquitous network

Shaheena Khatoon  and Balwant Singh Thakur

## ABSTRACT

The paper analyzes a recently proposed secure authentication and key agreement scheme for roaming service in a ubiquitous network. In 2018, Lee et al. proposed a biometric-based anonymous authentication scheme for roaming in ubiquitous networks. But, we found that Lee et al. scheme is prone to the off-line dictionary attack when a user's smart device is stolen, replay attack due to static variables and de-synchronization attack when an adversary blocks a message causing failure of authentication mechanism. Further, the scheme lacks no key control property and has incorrect XOR calculation. In the sequel, we presented an improved biometric based scheme to remove the weaknesses in Lee et al.'s scheme, which also does not require an update of identity in every session, hence preventing de-synchronization attack. Also, the security of the proposed schemes were analyzed in a widely accepted random oracle model. Further, computational and communication cost comparisons indicate that our improved scheme is more suitable for ubiquitous networks.

## KEYWORDS

cryptanalysis; elliptic curve  
cryptography;  
random oracle

## 1. Introduction

Ubiquitous networks provide uninterrupted remote operations to a globally roaming mobile user  $MU$  by connecting to a home agent ( $HA$ ) via a foreign agent ( $FA$ ). The mobile users get access to the desired services at any time and place even if he/she is out of the coverage of his/her home network. But, such communications rely on public networks which are susceptible to various security threats. An adversary can intercept, eavesdrop, delete, modify or replay the messages communicated over public networks. Consequently, a secure mutual authentication in the communication has become a vital issue, leading researchers to focus their interests on secure authentication schemes. At the same time, it is also essential to protect the user's identity from being traced. Hence, to respect the privacy of the user, researchers investigate various cryptographic techniques to hide the real identity of a user. In recent year, numerous authentication and key agreement schemes have been proposed to provide robust security in ubiquitous

**CONTACT** Shaheena khatoon  [shaheenataj.28@gmail.com](mailto:shaheenataj.28@gmail.com)  PT. RAVISHANKAR SHUKLA UNIVERSITY, S.o.S Mathematics, Great Eastern Rd, Amanaka, Raipur, Chhattisgarh 492010, Raipur 492010, India.

Color versions of one or more of the figures in the article can be found online at [www.tandfonline.com/ucry](http://www.tandfonline.com/ucry).

networks. Initially, two-factor authentication schemes received much attention with numerous schemes proposed. However, Several weaknesses of two-factor schemes have been identified such as: passwords are easy to break; smart cards can be misappropriated, and are also subject to differential power attacks. Consequently, biometric-based user authentication protocols have been introduced and are considered better and more reliable alternatives than traditional password-based authentication schemes. Biometric methods are unique and quantifiable methods for recognizing a human being. However, biometric information is prone to various noises during the acquisition process and the reproduction of actual biometric data is generally difficult (Bellovin and Merritt 1992). Bio-hash function and fuzzy extractor (Jung et al. 2017; Odelu et al. 2017; Wazid et al. 2016) are two commonly used techniques to address these kinds of problems.

## 2. Related work

The first authentication scheme for ubiquitous networks was put forward by Zhu and Ma (2004). It was a password based authentication scheme which provides anonymity to the user. In the later years, Lee et al. (2006) revealed that their scheme was not secure. Their scheme does not resist forgery attack and is unsuccessful in achieving perfect backward secrecy and mutual authentication. Lee et al. (2006) proposed an improved scheme to overcome the security issues of the Zhu and Ma (2004) scheme. Their scheme was proved insecure by Wu et al. (2008). Wu et al. (2008) analyzed Zhu and Ma (2004) and Lee et al. (2006) schemes and demonstrated that both the schemes fail to achieve user anonymity and also showed that Lee et al. (2006) scheme also fails to provide perfect backward secrecy. In the sequel, Wu et al. (2008) also presented an improved scheme to overcome the security issues of the previous schemes. Later, Mun et al. (2012) analyzed Wu et al. (2008) scheme and proved that the scheme was unable to provide user anonymity and perfect forward secrecy and they presented an enhanced password-based authentication scheme to overcome these weaknesses. The Mun et al. (2012) scheme was analyzed by Zhao et al. (2014). They proved that Mun et al. (2012) was unable to resist impersonation attacks and insider attacks and fails to achieve user anonymity.

In 2011, Chen et al. (2011) proposed a provably secure, lightweight, anonymous user authentication scheme for the global mobility network. However, their scheme was proved insecure by Xie et al. (2014). Chen et al. (2011) scheme was not able to achieve session key security and user privacy. In 2011, He et al. (2011) proposed a design of an efficient password-based authentication scheme for ubiquitous networks. Jiang et al. (2013) demonstrated various security pitfalls in He et al.'s Scheme (Chen

et al. 2011): it fails to resist off-line password guessing, server-spoofing, replay and privileged-insider attacks. Jiang et al. proposed an improved password-based authentication scheme which was analyzed by Wen et al. (2013). They proved that Jiang et al.'s Scheme (Jiang et al. 2013) is vulnerable to stolen-verifier, server spoofing, replay and denial-of-service attacks and fails to provide forward secrecy. They also proposed an improved scheme which was independently analyzed by Farash et al. (2017) and Gope and Hwang (2015). It was commonly found that Wen et al.'s Scheme (Wen et al. 2013) is insecure against the known attacks i.e. the scheme cannot resist off-line password-guessing attacks once an adversary steals/finds the smart card of the user. Then, Farash et al. (2017) and Gope and Hwang (2015) independently proposed improved authentication schemes. But, both Wu et al. (2017) and Chaudhry et al. (2017) showed that Farash et al. (2017) scheme have a number of security issues. Farash et al.'s scheme does not provide user-anonymity, discloses the secret parameters of the mobile node (MN) and the session key and leads to mobile node impersonation attacks. Wu et al. (2017) also demonstrated that Gope and Hwang (2015) are vulnerable to various attacks. In 2016, Karuppiyah et al. (2016) proved that the scheme of Farash et al. (2017) is vulnerable to replay attacks and off-line password-guessing attacks and does not provide session key security, perfect forward secrecy and user anonymity. Karuppiyah et al. (2016) proposed an improved DLP-based authentication and key agreement scheme. Arshad and Rasoolzadegan (2017) showed that the scheme of Karuppiyah et al. is vulnerable to off-line password-guessing attacks and does not provide perfect forward secrecy. Table 1 provides a summary of the flaws of the previously mentioned schemes.

Recently, in 2018 Lee et al. (2018) showed that Chaudhry et al.'s Scheme (Chaudhry et al. 2017) is vulnerable to stolen-mobile devices and user impersonation attacks and has incorrect login-input detection, incorrect password change phase and the absence of the revocation-phase. They proposed an improved biometric-based authentication scheme for roaming in ubiquitous networks. They claimed that their scheme is secure against the various known attacks and is lightweight compared with the earlier scheme. However, we found that Lee et al. scheme is prone to the following attacks: off-line dictionary attack, replay attack and de-synchronization attack. Further, the scheme lacks no key control property, and has incorrect XOR calculations. Hence, we propose an improved scheme and analyze the security of the proposed scheme in a widely accepted random oracle model. The proposed scheme is more secure and lightweight as compared with Lee et al.'s schemes. Heuristic analysis is also conducted.

The remainder of this paper is organized as follows: preliminaries are given in Section 3, Lee et al's scheme is analyzed in the Sections 4 and in

**Table 1.** Related authentication scheme for roaming in ubiquitous networks.

Protocol	Year	Major attacks
Zhu and Ma (2004)	2004	Scheme do not resist forgery attack, is unsuccessful in achieving perfect backward secrecy and mutual authentication, and do not preserve the user anonymity.
Lee et al. (2006)	2006	Scheme fails to provide perfect backward secrecy and do not preserve the user anonymity.
Wu et al. (2008)	2008	Scheme do not provide user anonymity and a perfect forward secrecy.
Chen et al. (2011)	2011	Scheme do not provide session key security and user privacy.
He et al. (2011)	2011	Scheme is prone to number of attacks namely, off-line password guessing, server-spoofing, replay and privileged-insider attacks.
Mun et al. (2012)	2012	Scheme cannot resist impersonation attacks and insider attacks and also does not provide user anonymity.
Jiang et al. (2013)	2013	Scheme is vulnerable to stolen-verifier, server spoofing, replay, and denial-of-service attacks and fails to provide forward secrecy
Wen et al. (2013)	2013	Scheme cannot resist off-line password-guessing attacks once an adversary steals/finds the smart card of the user.
Karuppiah et al. (2016)	2016	Scheme was vulnerable to off-line password-guessing attacks and do not provide perfect forward secrecy.
Farash et al. (2017)	2017	Scheme do not provide user-anonymity and the discloses the secret parameters of the mobile node (MN) and the session key and leads to mobile node impersonation attacks.
Chaudhry et al. (2017)	2017	Scheme is vulnerable to stolen-mobile devices and user impersonation attacks and has incorrect login-input detection, incorrect password change phase, and the absence of the revocation-phase.
Lee et al. (2018)	2018	Scheme is prone to the following attacks; off-line dictionary attack attack, replay attack and de-synchronization attack. Further, the scheme lacks no key control property, and has incorrect XOR calculation.

Section 5.2 we propose an enhanced scheme. The formal security analysis is given in Section 6, the heuristic and performance analyses are given in Sections 7 and 8, respectively, and are followed by the conclusion.

### 3. Preliminaries

Elliptic Curve Cryptography (ECC), computational problems, a typical model of ubiquitous network, their security requirements and adversary capabilities are briefly discussed in the present section.

#### 3.1. Elliptic curve cryptography (ECC)

Elliptic curve cryptography (ECC) is a widely known public-key cryptography based on the algebraic structure of elliptic curves over finite fields. An elliptic curve consists of the points satisfying the following:

$$y^2 = x^3 + ax + b.$$



The public parameters of the elliptic curve are  $(p, a, b, G, n, h)$  where:

- $F(p)$ : the finite field over  $p$ , where  $p$  is a prime and represents the size of the finite field.
- $(a, b)$ : the parameters of elliptic curves  $y^2 = x^3 + ax + b$ .
- $G(x_p, y_p)$ : generator point but  $G \neq 0$ .
- $n$ : the order of the base point  $G$ .
- $h$ : cofactor, an integer,  $h = F(p)/n$ .

### 3.2. Computational problems

Consider large primes  $p$  and  $q$ , and let  $F_p$  be a finite field,  $E/F_p$  be an elliptic curve over  $F_p$ , and  $G$  be a subgroup of  $E/F_p$  whose order is  $q$ . Then, for any integers  $a, b \in \mathbb{Z}_p^*$  and a randomly generated point  $P$  in  $G$ , we can define the following problems:

- Elliptic curve discrete logarithm problem (ECDLP) [?]: Given  $(P, aP)$ , it is impossible to compute  $a$  within polynomial time.
- Elliptic curve computational Diffie–Hellman problem (ECCDHP) [?]: Given  $(aP, bP)$ , it is impossible to compute  $abP$  within polynomial time.

### 3.3. A typical model of ubiquitous network

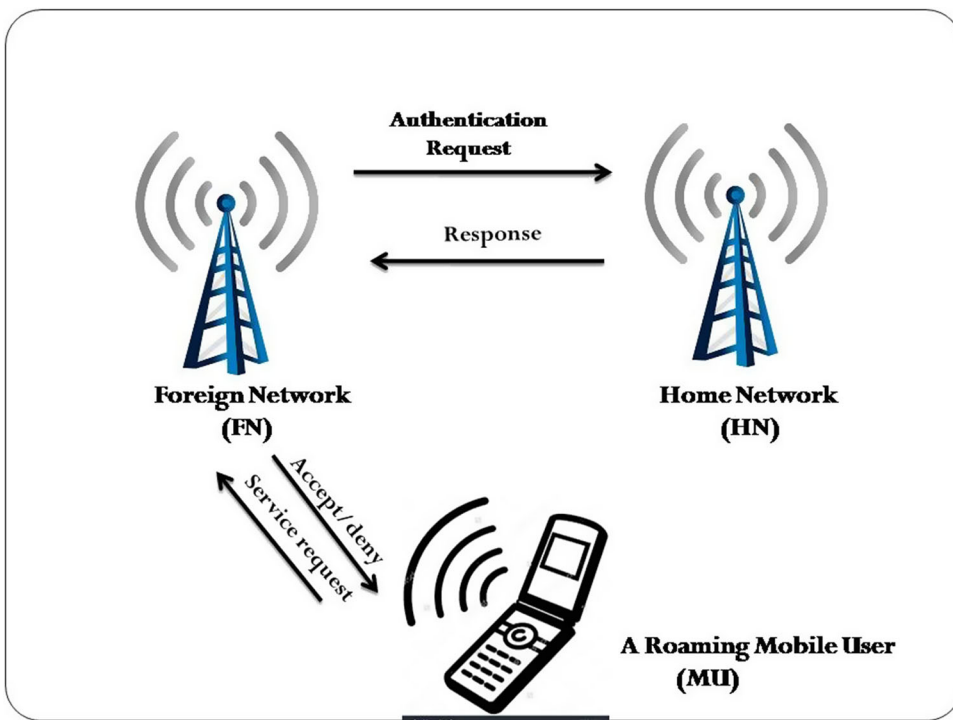
Ubiquitous networks enables mobile users  $MU$  to connect to available, while he/she roams from one place to another (Jiang et al. 2013). In an ubiquitous network mobile user  $MU$  is able to access the service of the home network  $HN$ , while roaming outside the home network  $HN$  via a foreign network  $FN$  which has a prior agreement with the home network  $HN$ . The mutual authentication and sharing of the session key between  $MU$  and  $FN$  with the support of the  $HN$  is depicted in Figure 1. The brief description of the mutual authentication process is as follows:

- (1) Mobile user  $MU$  sends a service request to the foreign network  $FN$ .
- (2) Foreign network  $FN$  sends an authentication request to the home network  $HN$ .
- (3) The home network  $HN$  checks the authenticity of the the mobile user  $MU$  and sends a response to the foreign network.
- (4) Finally, on the basis of the received response the foreign network  $FN$  accepts or rejects the request of the mobile user  $MU$ .

### 3.4. Security requirements

The security requirements for a ubiquitous networks are as follows:

- Mutual authentication: Mutual authentication enables the participants to authenticate each other (He et al. 2016; Lee et al. 2013). The home network should ensure the authentication between the user and foreign network.



**Figure 1.** A typical model for a ubiquitous network.

- **User anonymity:** It is a privacy protection requirement for individual users though it is not directly related to system security. Many systems have such a requirement including distributed systems (Wang et al. 2017) User anonymity is protected to prevent foreign network *FN* or any adversary from computing the user's identity or linking the transcript to the same user. Also, the user location should not be revealed to anyone.
- **Key agreement:** The foreign network and user must share a secret session key for confidential communication.
- **User friendly:** A user friendly scheme enables a mobile user to select the password freely and change it locally (Wang and Wang 2016) when he/she finds the smart card insecure, he/she can revoke it and re-register to the system with their original identity.
- The proposed scheme should be secure enough to resist the known attacks.

### 3.5. Adversary capabilities

The adversary *A* is supposed to have the following capacities:

- The adversary *A* has full control over the communication channel, i.e., *A* can modify, intercept, delete and resend any legitimate message (Dolev and Yao 1983; Eisenbarth et al. 2008; Kumari et al. 2016).

- The adversary  $A$  can enumerate all the items in  $D_{pw} \times D_{id}$  in polynomial time, where  $D_{pw}$  and  $D_{id}$  denote the password space and the identity space respectively (Ignatenko and Willems 2009; Jiang et al. 2017; Wang et al. 2015).
- All the public parameters are known to  $A$  including the user's biometrics (He and Wang 2015; Jiang et al. 2017; Wang and Xu 2017).
- $A$  cannot extract private key of  $HN$ .
- The shared key between  $HN$  and  $FN$  cannot be exposed to  $A$ .

## 4. Cryptanalysis of lee et al.'s scheme

### 4.1. A brief review of lee et al.'s scheme

The following section, briefly discusses the various phases of the Lee et al. (2018) scheme. The scheme consist of the following phases: (1) registration, (2) login and authentication, (3) password changing and (4) revocation. We will discuss only the login and registration phases in detail as these are the relevant phases when discussing the various pitfalls in the scheme.

### 4.2. Registration

The registration phase for the mobile user  $MN_i$  involves the following operations:

- (1)  $MN_i \rightarrow HA_k : (ID_{mi}, PWB_{mi})$ .  
 $MN_i$  inputs identity and password of its choice  $ID_{mi}$  and  $PW_{mi}$  and imprints  $BIO_{mi}$ . Mobile device calculates  $PWB_{mi} = h(PW_{mi}|BIO_{mi})$  and send registration request  $(ID_{mi}, PWB_{mi})$  securely to  $HA_k$ .
- (2)  $HA_k \rightarrow MN_i : (PID_{mi}, A_{mi}, B_{mi}, r_A)$ .  
 $HA_k$  verifies the identity of  $MN_i$  and computes  $RID_{mi} = E_{h(K_H)}(ID_{mi})$ .  $HA_k$  searches  $RID_{mi}$  in the database to verify the presence of an already registered user with the same  $ID_{mi}$  if this is verified  $HA_k$  requests a new identity from  $MN_i$ . Else,  $HA_k$  randomly generates  $r_A$  and  $r_D$ , and calculates  $PID_{mi} = E_{h(K_H)}(ID_{mi}||r_D)$ ,  $A_{mi} = h(ID_{mi}||PWB_{mi})$  and  $B_{mi} = h(ID_{mi}||r_A||PWB_{mi}) \oplus .h(K_H||ID_{mi})$ . If  $MN_i$  is a new user,  $HA_k$  sets  $I_{mi}$  to zero otherwise,  $I_{mi} = I_{mi} + 1$ .  $HA_k$  then stores  $(I_{mi}, PID_{mi}, RID_{mi})$  as a tuple in the database and it sends  $PID_{mi}, A_{mi}, B_{mi}, r_A$  to  $MN_i$  via a secure channel.
- (3)  $MN_i$  stores all of the received parameters into the mobile device.

### 4.3. Login and authentication

This phase is executed between  $MN_i$  and  $FA_j$ . They authenticate each other and agree upon a common session key with the support of  $HA_k$ . The details of this phase are as follows:

- (1)  $MN_i \rightarrow FA_j : (M_1 = PID_{mi}, MV_2, MV_3, ID_{hk})$ .  
 $MN_i$  enters his/her  $ID_{mi}$ ,  $PW_{mi}$  and  $BIO_{mi}$ , the mobile device calculates  $PWB_{mi} = h(PW_{mi} || H(BIO_{mi}))$  then verifies the value  $A_{mi} = h(ID_{mi} || PWB_{mi})$ . If equation does not hold  $MN_i$  terminates the user's login request. Else, mobile device randomly generates  $n_{mi}$  and calculates  $MV_1 = B_{mi} \oplus h(ID_{mi} || r_A || PWB_{mi})$ ,  $MV_2 = h(MV_1 || ID_{mi} || n_{mi})$  and  $MV_3 = MV_1 \oplus n_{mi}$ . Then, it sends the login request message  $(M_1 = PID_{mi}, MV_2, MV_3, ID_{hk})$  to  $FA_j$ .
- (2)  $FA_j \rightarrow HA_k : (M_2 = ID_{fj}, FV_2, FV_3, M_1)$   
 $FA_j$  randomly generates  $n_{fj}$  and calculates  $FV_1 = h(K_{FH} || MV_2 || MV_3)$ ,  $FV_2 = FV_1 \oplus n_{fj}$  and  $FV_3 = h(FV_1 || FV_2 || n_{fj})$ . Then, it sends the message  $(M_2 = ID_{fj}, FV_2, FV_3, M_1)$  to  $HA_k$ .
- (3)  $HA_k \rightarrow FA_j : (M_3 = PID_{mi}^{new}, HV_1, HV_2)$ .  
 $HA_k$  checks  $ID_{fj}$  to find its corresponding  $K_{FH}$  and calculates  $FV_1^* = h(K_{FH} || MV_2 || MV_3, n_{fj}^*) = FV_1^* \oplus FV_2$  and verifies  $FV_3 = h(FV_1^* || FV_2 || n_{fj}^*)$ . If verification equation does not hold  $HA_k$  terminates this phase; else  $HA_k$  calculates  $\{ID_{mi}^*, r_D\} = D_{h(K_H)}(PID_{mi})$ ,  $MV_1^* = h(K_H || ID_{mi}^*)$ ,  $n_{mi}^* = MV_1^* \oplus MV_3$  and verifies  $MV_2 = h(MV_1^* || ID_{mi} || n_{mi})$ . If verification equation does not hold,  $HA_k$  terminates this phase; else  $HA_k$  randomly generates  $r_D^{new}$  and calculates  $PID_{mi}^{new} = E_{h(K_H)}(ID_{mi}^* || r_D^{new})$ ,  $SK_{fj} = h(MV_1^* || ID_{mi}^* || ID_{fj} || n_{mi}^*)$ ,  $HV_1 = SK_{fj} \oplus h(K_{FH} || n_{fj}^*)$  and  $HV_2 = h(K_{FH} || SK_{fj} || ID_{hk})$ .  $HA_k$  then replaces  $PID_{mi}$  with  $PID_{mi}^{new}$  and sends the message  $(M_3 = PID_{mi}^{new}, HV_1, HV_2)$  to  $FA_j$ .
- (4)  $FA_j \rightarrow MN_i : (M_4 = PID_{mi}^{new}, ID_{fj}, FV_4)$ .  
 $FA_j$  calculates  $SK_{fj} = HV_1 \oplus h(K_{FH} || n_{fj})$  and verifies the equation  $HV_2 = h(K_{FH} || SK_{fj} || ID_{hk})$ . If verification equation does not hold,  $FA_j$  terminates; else calculates  $FV_4 = h(SK_{fj} || ID_{fj})$ . Then, it sends the message  $(M_4 = PID_{mi}^{new}, ID_{fj}, FV_4)$  to  $MN_i$ .
- (5)  $MN_i$  calculates  $SK_{mi} = h(MV_1 || ID_{mi} || ID_{fj} || n_{mi})$  and  $FV_4^* = h(SK_{mi} || ID_{fj})$  and checks the validity of the session key by verifying the equation  $FV_4^* = FV_4$ . If equation does not hold  $MN_i$  terminates the connection; else  $MN_i$  authenticates  $FA_j$  and has successfully established the same session key,  $SK$ . Lastly,  $MN_i$  replaces  $PID_{mi}$  with  $PID_{mi}^{new}$ .

#### 4.4. Security and design flaws in the lee's et al. scheme

##### (1) Off-line dictionary attack:

This attack enables an adversary to get the password either by intercepting a public message or stealing the smart card. In Lee et al.'s scheme, the adversary can steal the smart card and guess the password of the user. In accordance with the capabilities of the adversary  $A$  as discussed in [subsection 3.5](#) it can be assumed that  $A$  has somehow acquired the mobile device

of the mobile user  $MN_i$  and has revealed the parameter stored in it. Additional  $A$  had also acquired the biometrics  $BIO_{mi}$  by a malicious terminal or by some other way. Then  $A$  can obtain  $MN_i$  password  $PW_i$  as follows:

- (a) Suppose  $A$  guesses  $PW_{mi}$  to be  $PW_{mi}^*$  and  $ID_{mi}$  to be  $ID_{mi}^*$  from the dictionary space  $D_{pw}$  and  $D_{id}$ .
- (b) Then the adversary  $A$  enters  $ID_{mi}^*$  and  $PW_{mi}^*$  and imprints  $BIO_{mi}$ .
- (c) Then the device computes  $PWB_{mi}^* = h(PW_{mi}^* || H(BIO_{mi}))$
- (d) Then the device verifies the value  $A_{mi} = h(ID_{mi}^* || PWB_{mi}^*)$
- (e) Repeats the steps 1-4 of this algorithm till the correct value of  $PW_M$  and  $ID_M$  are obtained.

The time complexity of the above attack is  $O(|D_{pw}| * |D_{id}| * 2T_h)$ , where  $|D_{pw}|$  is the number of password in  $D_{pw}$  and  $T_h$  is the running time for hash computation. Further, it is observed (Wang and Wang 2016; Wang et al. 2017) that  $|D_{id}| < |D_{pw}| < 10^6$ . Thus, the above attack is quiet efficient.

## (2) Replay attack:

This attack enables the adversary to intercept the contents to act as a session member and avail undue advantages. In Lee et al.'s scheme, the authentication equation involves all static variables which do not change with every login request causing replay attack. Suppose the adversary  $A$  has eavesdropped the communication channel between a legal users  $MN_i$  and  $FA_j$  and recorded a previous login request message  $M_1 = (PID_{mi}, MV_2, MV_3, ID_{hk})$ . The adversary can login to the server by sending the eavesdropped login request message ( $M_1$  to  $FA_j$  in the following way:

- (a) The adversary  $A$  sends the message  $M_1 = (PID_{mi}, MV_2, MV_3, ID_{hk})$  to  $FA_j$ .
- (b) Upon receiving  $M_1$ ,  $FA_j$  will randomly generates  $n_{fj}$  and calculates,  $FV_1$ ,  $FV_3$  (as explained earlier) and sends the message  $M_2 = (ID_{fj}, FV_2, FV_3, M_1)$  to  $HA_k$ .
- (c)  $HA_k$  will authenticate  $ID_{fj}$  by verifying the equation  $FV_3 = h(FV_1^* || FV_2 || n_{fj}^*)$ . Then,  $HA_k$  calculates  $\{ID_{mi}^*, r_D\} = D_{h(K_H)}(PID_{mi})$ ,  $MV_1^* = h(K_H || ID_{mi}^*)$ ,  $n_{mi}^* = MV_1^* \oplus MV_3$  and verifies  $MV_2 = h(MV_1^* || ID_{mi}^* || n_{mi}^*)$ . Here, we observe that this authentication equation will hold as it involves only static variables which do not change with every login request. Then,  $HA_k$  randomly generates  $r_D^{new}$  and calculates,  $PID_{mi}^{new} = E_{h(K_H)}(ID_{mi}^* || r_D^{new})$ ,  $SK_{fj} = h(MV_1^* || ID_{mi}^* || ID_{fj} || n_{mi}^*)$ ,  $HV_1 =$

$SK_{ff} \oplus h(K_{FH} || n_{ff}^*)$  and  $HV_2 = h(K_{FH} || SK_{ff} || ID_{hk})$  sends the message  $M_3 = (PID_{mi}^{new}, HV_1, HV_2)$  to  $FA_j$ .

- (d) Furthermore,  $FA_j$  sends the message  $M_4 = (PID_{mi}^{new}, ID_{ff}, FV_4)$  to the adversary. Although he/she cannot calculate the session key, he/she is successful as long as the server accepts the login request. Hence, since the server authenticated the adversary as the legal user and accepted his/her login request, the adversary ignores the received message  $M_4$ . Therefore, since an adversary can impersonate a legal user and login to the server by replaying an old login request message, we can conclude that Lee's et al. scheme is vulnerable to replay attacks.

### (3) Absence of no key control property:

The no key control property of an authentication scheme ensures that none of the users have control over others. That is none of the users or even an adversary can force the other users' session keys to be a preselected value, or a value within a set consisting of a small number of elements. Hence, we can say that an authentication scheme has the no key control property if the session key is computed with the contributions of all the participants. In Lee et al.'s Scheme (Lee et al. 2018), the session key agreed between  $MN_i$  and  $FA_j$  is  $SK = h(MV_1 || ID_{mi} || ID_{ff} || n_{mi})$ . We observe that,  $MV_1$  is calculated by  $MN_i$ ; also the mobile user  $MN_i$  chooses the random number  $n_{mi}$  and the identity  $ID_{ff}$  is a publicly known parameter. Hence, we can conclude that  $FA_j$  has no contribution on the session key. Therefore, the no key control property is absent in Lee et al's authentication scheme.

### (4) De-synchronization attack:

This attack jeopardizes secure communication between the patient and the server by removing synchronization between them. De-synchronization attack violates completeness property of authentication i.e. a legal entity will not be authenticated by a valid server. If the message  $M_4$  is blocked by an adversary  $A$  or fails to reach the mobile user (due to network problem or some other technical issue), the update between  $MN_i$  and  $HA_k$  will not be synchronized, meaning that  $HA_k$  will replace  $PID_{mi}$  with  $PID_{mi}^{new}$  but  $MN_i$  will fail to do this causing de-synchronization attack.

### (5) Incorrect XOR calculation:

In Lee et al's scheme it is assumed that the lengths of random number and hash function are 64 bits and 160 bits respectively. In bitwise XOR function bit size of the operand should be the same to get the correct result. For instance, if the variable A and B are the same size (say 32 bits), the XOR operation of A and B gives the correct result. Now, If the bit size of the A

**Table 2.** Description of attacks on Lee's et al. scheme.

Attack	Cause	Impact	Remedy in the proposed scheme
Off-line dictionary attack	due to weak password and no limit on the wrong input of password	reveals the password of the user	strong password and limit the number of wrong password input
Replay attack	verification message involves static variables which do not change with the session	adversary can impersonate a legal user	fresh timestamp is used in every session
De-synchronization attack	adversary blocks the message	legal user will not be authenticated by the server	the proposed scheme does not require update of identity hence not vulnerable to attack

is 32 bits and that of B is 64 bits and we apply XOR operation result would be 64 bits for the operands A and B. But, this operation is not logically correct. In Lee et al's scheme, it is assumed that the lengths of random number and hash function are 64 bits and 160 bits respectively. Hence, XOR calculation of  $MV_3 = MV_1 \oplus n_{mi}$  and  $FV_2 = FV_1 \oplus n_{ff}$  is technically incorrect. Consequently, the scheme is not technically correct in terms of XOR calculation.

In the following Table 2 we describe the various attacks on the Lee's et al. scheme, its cause, impact and remedies in the proposed scheme.

## 5. The proposed scheme

This section presents an improved scheme which is resistant against various known attacks and provides necessary security attributes. The proposed scheme consists of the following phases: 1) User registration phase, 2) Login and authentication phase, 3) Password change phase, 4) Revocation phase, and 5) Re-registration phase. During the initialization process of the proposed scheme, the home agent chooses an elliptic curve  $E/F_p$  and a generator  $G$  with the large order  $n$  and a random number  $x \in Z_p^*$  as its master secret key. After that  $HN$  generates its public key  $Q = xG$ . Moreover, it chooses a secure one-way hash function  $h(\cdot)$  and publishes  $(p, a, b, G, n, Q, h(\cdot))$  and keeps  $x$  secret. Furthermore, each foreign agent shares a unique long-term secret key  $K_{FH}$  with the home agent. For clarity, the notations in Table 3 are used throughout the paper.

### 5.1. Registration phase

A mobile user  $MU_i$  registers a home network in the following way:

- (1)  $MU_i \Rightarrow HN : Reg_i = \{h(ID_i), MP_i\}$ .  
 $MP_i = h(h(ID_i)||PW_i||x_i)$ , where  $x_i \in Z_p^*$  is randomly generated by mobile device.

- (2)  $HN \Rightarrow MU_i : \{e_i, S_i, p, a, b, G, n, Q, h(\cdot)\}$ .

Upon receiving the registration request  $HN$  checks  $h(ID_i)$  in its

database and if it exists, asks the user to choose another  $ID_i$ , otherwise computes  $S_i = h(h(ID_i)||x)$ , and  $e_i = MP_i \oplus S_i$ . Also,  $HN$  record  $(h(ID_i), List)$  in its database, and  $List$  counts the number of failed login attempt of a mobile user, and it is initialized to NULL. If the  $List$  value is greater than the threshold value, the corresponding mobile device will be discarded till the user re-registers.

- (3) Upon receiving the message from,  $MU_i$  imprints his/her biometrics  $Bio_i$ , generates  $H(BIO_i)$ ,  $B_i = x_i \oplus H(BIO_i)$ .  $MU_i$  stores  $\{B_i, MP_i, H(\cdot)\}$  in the mobile device. Finally, the mobile device includes  $\{e_i, S_i, p, a, b, G, n, Q, h(\cdot), H(\cdot), B_i, MP_i\}$ .

Figure 2, briefly summarizes the registration phase.

Table 3. Basic notation.

Notations	Description
$MU_i$	Mobile user.
$FN$	Foreign network.
$HN$	Home network
$ID_i, PW_i, Bio_i$	Identity, password and biometric information respectively of any user $i$ .
$x$	Master secret key of $HN$ .
$Q$	Public key pair $HN$ where $Q = xG$ .
$K_{FH}$	A pre-shared secret key between $FN$ and $HN$ .
$h(\cdot)$	A cryptographic secure hash function.
$H(\cdot)$	Bio-hashing.
$E/F_p$	An elliptic curve.
$G$	A base point of an elliptic curve.
$rG$	Point multiplication, where $rG = G + G + \dots + G$ , $r$ times.
$T_i, 1 \leq i \leq 5$	Time stamp.
$\rightarrow$	An insecure channel.
$\Rightarrow$	A secure channel.
$\parallel$	Concatenation.
$\oplus$	XOR operation.

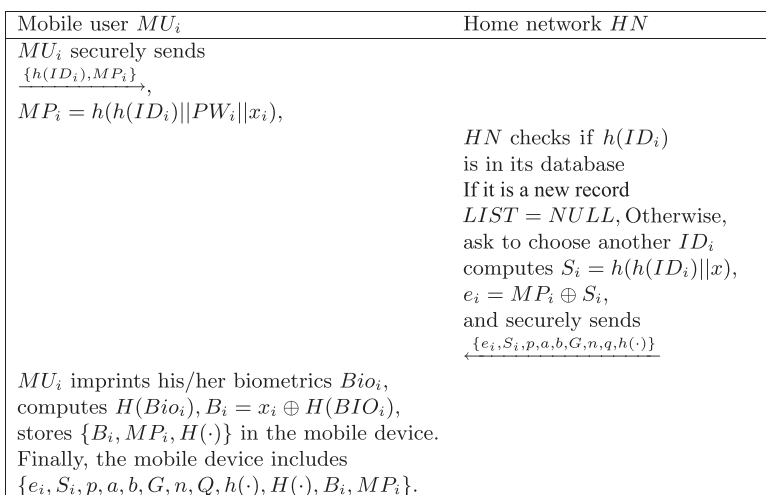


Figure 2. Registration phase.



## 5.2. Login and authentication phase

This phase enables  $FN$  to authenticate the request of  $MU_i$  and negotiate a session key with the help of  $HN$ . Here,  $K_{FH}$  is a pre-shared secret key between  $HN$  and  $FN$ . Figure 3 briefly summarizes the login and authentication phase.

Mobile user $MU_i$	Foreign network $FN$	Home network $HN$
enters $ID_i^*$ , $PW_i^*$ , $BIO_i^*$ , The device computes: $H(BIO_i^*)$ , $x_i^* = B_i \oplus H(BIO_i^*)$ , $MP_i^* = h(h(ID_i^*)    PW_i^*    x_i^*)$ , If $MP_i \neq MP_i^*$ , aborts Else, Generate $K_1 \in Z_n^*$ Computes: $A = K_1 G$ , $K_{mh} = h(T_1    K_1 Q)$ , $M_1 = ID_{mi} \oplus K_{mh}$ $M_2 = h(k_1 Q    M_1    S_i    T_1)$ $\overleftarrow{M_{MF} = \{A, M_1, M_2, T_1\}}$	checks $T_1$ , Generate $K_2 \in Z_n^*$ computes: $B = K_2 G$ , $M_3 = h(B    ID_F    K_{FH}    T_2)$ $\overleftarrow{M_{FH} = \{ID_F, M_{MF}, M_3, B, T_2\}}$	checks $T_2$ , compute: $M_3^* = h(B    ID_F    K_{FH}    T_2)$ IF $M_3^* = M_3$ , computes: $K_{mh}^* = h(T_1    x.A)$ , $ID_i^* = M_1 \oplus K_{mh}^*$ , and $S_i^* = h(ID_i    x)$ search $ID_i$ in the database, if registered checks $List$ , if $List \geq$ threshold value, terminates Else, computes $M_2^* = h(xA    M_1    S_i    T_1)$ if $M_2^* \neq M_2$ , terminates Else, computes: $M_4 = h(A    B    K_{FH}    M_3    T_2)$ and $M_5 = h(xA    B    S_i    M_2    T_2)$ $\overleftarrow{M_{HF} = \{M_4, M_5, ID_F, T_3\}}$
checks $T_4$ computes $M_5^* = h(K_1 Q    B    S_i    M_2    T_2)$ if $M_5^* \neq M_5$ terminates Else, computes $SK = h(K_1 B) = h(K_1 K_2 G)$ $M_6^* = h(A    B    SK    T_4)$ if $M_6^* \neq M_6$ , terminates Else, computes $M_7 = h(M_5    M_2    SK    T_5)$ $\overleftarrow{M_{MF'} = \{M_7, T_5\}}$	checks $T_3$ then computes: $M_4^* = h(A    B    K_{FH}    M_3    T_2)$ if $M_4^* \neq M_4$ , terminates Else, computes: $SK = h(K_2 A) = h(K_1 K_2 G)$ $M_6 = h(A    B    SK    T_4)$ $\overleftarrow{M_{FM} = \{B, M_5, M_6, T_4\}}$	
	checks $T_5$ computes $M_7^*$ if $M_7^* \neq M_7$ , terminates Else, accepts $MU_i$ 's request and allow to access its network service	

Figure 3. Login and authentication phase.

- (1)  $MU_i \rightarrow FN : M_{MF} = \{A, M_1, M_2, T_1\}$ .  
 $MU_i$  enters his/her identity  $ID_i^*$ ,  $PW_i^*$ , and  $BIO_i^*$ , then the mobile device computes  $h(ID_i^*), H(BIO_i^*), x_i^* = B_i \oplus H(BIO_i^*), MP_i^* = h(h(ID_i^*) || PW_i^* || x_i^*)$ , If  $MP_i \neq MP_i^*$ , the mobile device rejects the request (Note: here, the number of failed attempts should be limited to some finite number). Otherwise, mobile device randomly generates a number  $K_1 \in Z_n^*$  and computes  $A = K_1G, K_{mh} = h(T_1 || K_1Q)$ ,  $M_1 = h(ID_i^*) \oplus K_{mh}$  and  $M_2 = h(K_1Q || M_1 || S_i || T_1)$ . Mobile device then sends the login request  $M_{MF} = \{A, M_1, M_2, T_1\}$  to  $FN$ .
- (2)  $FN \rightarrow HN : M_{FH} = \{ID_F, M_{MF}, M_3, T_2\}$ .  
The  $FN$  first checks the freshness of  $T_1$ , then randomly generates a number  $K_2 \in Z_n^*$  and computes  $B = K_2G, M_3 = h(B || ID_F || K_{FH} || T_2)$ . The  $FN$  forwards the message  $M_{FH} = \{ID_F, M_{MF}, M_3, B, T_2\}$  to  $HN$ .
- (3)  $HN \rightarrow FN : M_{HF} = \{M_4, M_5, T_3\}$ .  
 $HN$  first checks  $T_2$ , then authenticates  $FN$  by calculating  $M_3^* = h(B || ID_F || K_{FH} || T_2)$ . If  $M_3^* = M_3$  computes  $K_{mh}^* = h(T_1 || xA), h(ID_i^*) = M_1 \oplus K_{mh}^*$ , and  $S_i^* = h(Ih(D_i^*) || x)$  then it searches for  $h(ID_i^*), List$  in the database. If the mobile user is a registered user it checks the value of  $List$  if  $List \geq$  threshold value the  $HN$  rejects the request else sets  $List = List + 1$  and computes  $M_2^* = h(xA || M_1 || S_i || T_1)$ . Then,  $HN$  verifies the calculated and obtained values if  $M_2^* \neq M_2$   $HN$  rejects the request. Otherwise, it computes  $M_4 = h(A || B || K_{FH} || M_3 || T_2)$  and  $M_5 = h(xA || B || S_i || M_2 || T_1)$  and sends  $M_{HF} = \{M_4, M_5, T_3\}$  to the  $FN$ .
- (4)  $FN \rightarrow MU_i : M_{FM} = \{B, M_5, M_6, T_4\}$ .  
Upon receiving the message  $FN$  checks  $T_3$  then computes  $M_4^* = h(A || B || K_{FH} || M_3 || T_2)$ , if  $M_4^* \neq M_4$   $FN$  rejects the request. Otherwise, it computes  $SK = h(K_2A) = h(K_1K_2G), M_6 = h(A || B || SK || T_4)$  and sends  $M_{FM} = \{B, M_5, M_6, T_4\}$  to  $MU_i$ .
- (5)  $MU \rightarrow FN : M_{MF'} = \{M_7, T_5\}$ .  
Upon receiving the message  $MU_i$  checks freshness of  $T_4$  then computes  $M_5^* = h(K_1Q || B || S_i || M_2 || T_1)$  if  $M_5^* \neq M_5$   $MU_i$  rejects the request. Otherwise, it computes  $SK = h(K_1B) = h(K_1K_2G)$  and  $M_6^* = h(A || B || SK || T_4)$  if  $M_6^* \neq M_6$  rejects the request. Else, it computes  $M_7 = h(M_5 || M_2 || SK || T_5)$  and sends the message  $M_{MF'} = \{M_7, T_5\}$  to  $FN$ .
- (6) Upon receiving the message  $M_{MF'}$  checks  $T_5$  then computes  $M_7^*$  and verifies it with the obtained value. if  $M_7^* \neq M_7$   $FN$  rejects the request. Otherwise, it authenticates  $MU_i$  and accepts his/her request and allows access to its network service.

### 5.3. Password change phase

Any mobile user can change his/her password independently without the help of home network through the following steps:

$MU_i$  inputs  $ID_i$ ,  $PW_i$  and new password  $PW_i^{new}$ ,  
 The mobile device computes:  
 $H(BIO_i^*)$ ,  $x_i^* = B_i \oplus H(BIO_i^*)$ ,  
 $MP_i^* = h(h(ID_i^*) || PW_i^* || x_i^*)$ ,  
 If  $MP_i \neq MP_i^*$ , rejects the request  
 Otherwise computes:  
 $MP_i^{new} = h(h(ID_i^*) || PW_i^{new} || x_i^*)$   
 finally replaces  $MP_i$  with  $MP_i^{new}$ .

**Figure 4.** Password change phase.

- (1)  $MU_i$  inputs  $ID_i$ ,  $PW_i$ ,  $BIO_i$  and new password  $PW_i^{new}$ .
- (2) The mobile device computes  $H(BIO_i^*)$ ,  $x_i^* = B_i \oplus H(BIO_i^*)$ ,  $MP_i^* = h(h(ID_i^*) || PW_i^* || x_i^*)$ , If  $MP_i \neq MP_i^*$ , the mobile device rejects the request. Otherwise mobile device computes  $MP_i^{new} = h(h(ID_i^*) || PW_i^{new} || x_i^*)$  and replaces  $MP_i$  with  $MP_i^{new}$ .

Figure 4, briefly summarizes the password change phase.

#### 5.4. Revocation phase

Any mobile user can protect the account from being misused whenever his/her mobile device is breached by revoking the device in the following way:

- (1)  $MU_i$  must first get authenticated by the device in the manner found in step 1 of the login and authentication phase (5.2).
- (2)  $MU_i \rightarrow HN : \{ID_i, MP_i, M_2, T_1, revoke-request\}$ , here  $MP_i, M_2$  are calculated by mobile device as described in 5.2
- (3) Upon receiving the revocation request from  $MU_i$ ,  $HN$  first authenticates  $MU_i$ . If  $MU_i$  is a legal user  $HN$  sets  $List$  greater than threshold value and revokes the mobile device, which means that nobody can log in to the network with the device until  $MU_i$  re-register himself/herself.

#### 5.5. Re-registration phase

After revocation of a mobile device a user  $MU_i$  can re-register in the following way:

- (1)  $MU_i \rightarrow HN : \{ID_i, MP_i, re-register\}$ .
- (2) Firstly,  $HN$  looks for  $ID_i$  in its database, checks whether  $List \geq$  the threshold value. If so,  $HN$  believes the card is suspended. Then, the user re-registers in accordance with the steps in Section 5.

### 6. Formal security analysis using random oracle model

In this section, we describe the formal security analysis using the real-or-random (R-OR) model proposed by Abdalls et al. (Abdalla et al. 2005).

In the proposed scheme there are three participants, a mobile user  $MU_i$ , home network  $HN$  and a foreign network  $FN$ .

- (1) Instance:  $\prod_H^t$ ,  $\prod_F^u$  and  $\prod_{MU_i}^v$  denote the instance  $t$  of  $FN$ ,  $u$  of  $FN$  and instance  $v$  of  $MU_i$ . These instances are called oracles.
- (2) SID: SID(session identifier) is the concatenation of all the messages sent and received by that oracle.
- (3) Open Oracle: If an oracle  $\prod_H^t$  reveals the accepted session key in any state, then the oracle is considered opened in that state.
- (4) Partner Oracle: If two oracles say  $\prod_H^t$  and  $\prod_F^u$  possess the same SID they are called partners.
- (5) Fresh Oracle: An unopened and uncorrupted oracle is said to be fresh.
- (6) Adversary: In the R-OR model the adversary  $A$  has the ability to control all communications and can put the following queries:
  - $\text{Execute}(\prod_H^t, \prod_F^u)$ : This query is executed by any adversary  $A$  to launch an eavesdropping attack, by sending this query  $A$  tries to get messages communicated between honest participants.
  - $\text{Send}(\prod_H^t, m)$ : This query launches an active attack. In this query  $A$  communicates a message  $m$  to a participant instance  $\prod_H^t$  and records the response message.
  - $\text{CorruptMD}(\prod_{MU_i}^v)$ : Lost/stolen mobile device attack is launched by this query. This query reveals the details stored in the mobile device.
  - $\text{Test}(\prod_H^t)$ : The semantic security of the session key  $SK$  is modeled by the query and follows the R-OR model indistinguishability (Abdalla et al. 2005).  $A$  can make a test query to some fresh oracle at any time. At the beginning of the experiment, a fair unbiased coin  $c$  is flipped, if answer is 1, the output is a randomly chosen session key. Otherwise the output is the agreed session key of the test oracle.
- (7) Semantic security of the session key: In the R-OR model the adversary  $A$  challenges the experiment to distinguish between the real session key  $SK$  of the instance and the random session key.  $A$  can execute a number of Test queries to either the user instance or the server instance. The result of the Test query must be consistent with respect to a random bit  $c$ . At the end of the experiment  $A$  returns a bit  $c'$ . If  $c' = c$ ,  $A$  wins the game. Let  $Succ$  denote the event that  $A$  wins the game. The advantage of breaking the semantic security of the protocol is  $Adv_P^{ake} = 2|Pr[Succ] - 1|$ . Therefore, if  $Adv_P^{ake} \leq \eta$  for any sufficiently small  $\eta > 0$   $P$  is a secure authentication protocol in the R-OR sense.

- (8) **Random oracle:** In this paper, all participants and the adversary  $A$  use a one-way hash function  $h(\cdot)$  modeled as a Hash oracle.

The following difference lemma will be used in the formal security proof.

**Lemma 6.1** (Difference lemma). (Lee 2015) *Let  $Succ_1$ ,  $Succ_2$ , and  $Succ_3$  denote the events defined in some probability distribution. Let  $Succ_1 \wedge Succ_3 \iff ?Succ_2 \wedge ?Succ_3$ . Then, we have*

$$|Pr[Succ_1] - Pr[Succ_2]| \leq Pr[Succ_3]$$

The following theorem will establish the semantic security of the session key.

**Theorem 6.2.** *Assume that an adversary  $A$  is operating within polynomial time  $t$  for the proposed scheme  $P$  in a random oracle. Assume  $D$  represents uniformly distributed password dictionary and  $l$  denotes bit size of the biometrics key  $BIO_i$ . The probability of  $P$ 's session key security being broken by  $A$  is as follows:*

$$Adv_P^{ake} \leq \frac{q_h^2}{|Hash|} + \frac{q_{send}}{2^l \cdot |D|} + 2Adv^{ECCDHP}(t),$$

where  $q_h$ ,  $|HASH|$ ,  $q_{send}$ ,  $|D|$ , and  $Adv^{ECCDHP}(t)$  denote the number of Hash queries, the range space of the one-way hash function, the number of Send queries, the size of  $D$ , and the advantage of  $A$  in breaking the ECCDHP, respectively.

*Proof.* We begin with defining a sequence of games  $G_i$ ,  $0 \leq i \leq 4$ . Here,  $Succ_i$  represents the success of  $A$  in guessing the bit  $c$  in the game  $G_i$ . The proposed scheme runs from game  $G_0$  to game  $G_4$ , and in the conclusion of the proof it will show that  $A$  has a negligible advantage to break session key (SK)-security of  $P$ .

- **Game  $G_0$ :** This game is a real attack by the adversary against protocol  $P$  in the random oracle. Where the bit  $c$  is chosen at the beginning of this game. By definition, we have

$$Adv_P^{ake}(A) = 2Pr[Succ_0] - 1 \tag{6.1}$$

- **Game  $G_1$ :** This game simulates an eavesdropping attack of an adversary  $A$  using the Execute ( $\prod^u, \prod^v$ ) oracle. The attacker also queries the Test oracle and checks whether the result is a real session key  $SK$  or some other random value. The session key  $SK$  is computed by the foreign network  $FN$  as  $SK = h(K_2B) = h(K_1K_2G)$  and the mobile user  $MU_i$  as  $SK = h(K_1A) = h(K_1K_2G)$ . It is hard to compute  $h(K_1B) = h(K_2A) = h(K_1K_2G)$  due to the difficulty of the ECCDH problem. Further,  $A$ ,  $B$

cannot be computed due to the difficulty of the ECDLP. Thus, the probability of an adversary  $A$  winning this game through an eavesdropping attack does not increase by game  $G_0$ . Then,  $G_0$  and  $G_1$  have the same probability, so we obtain:

$$Pr[Succ_0] = Pr[Succ_1] \quad (6.2)$$

- **Game  $G_2$ :** This game is an extension of  $G_1$  and  $G_2$  is simulated by *Send* and *Hash* oracle along with *Execute* ( $\Pi^t, \Pi^u, \Pi^v$ ) and *Test* oracles. It is an active attack modeled by adversary  $A$  by sending fabricated login request messages to the home network. Adversary repeatedly generates hash queries to obtain collisions. The login request message  $M_{MF} = \{A, M_1, M_2, T_1\}$  is associated with random number  $K_1$  and time stamp  $T_1$ . Further,  $A = K_1G$  cannot be computed due to the difficulty of the of ECDLP. So adversary cannot obtain a collision hence cannot generate valid login request message  $M_{MF}$ . Using the birthday paradox (Boyko et al. 2000), we obtain,

$$|Pr[Succ_1] - Pr[Succ_2]| \leq \frac{q_h^2}{2|Hash|} \quad (6.3)$$

- **Game  $G_3$ :** The *CorruptMD* oracle is simulated by this game and a lost/stolen mobile device attack is launched. Adversary  $A$  can attempt a dictionary attack using the information from a mobile device and can attempt to obtain a password  $PW_i$  and biometric key  $BIO_i$ . A strong biohashing function is used in the suggested protocol. Therefore, the probability that  $A$  can guess the biometric key  $BIO_i$  is approximately  $\frac{1}{2^l}$  (Wazid et al. 2016). Since the number of wrong passwords input is controlled by the system we obtain the following:

$$|Pr[Succ_2] - Pr[Succ_3]| \leq \frac{q_{send}}{2^l|D|} \quad (6.4)$$

- **Game  $G_4$ :** In this game, the adversary tries to acquire the session key  $SK$  through eavesdropping the broadcasted messages namely;  $M_{MF} = \{A, M_1, M_2, T_1\}$ ,  $M_{FH} = \{ID_F, M_{MF}, M_3, B, T_2\}$  and  $M_{HF} = \{M_4, M_5, T_3\}$  and  $M_{FM} = \{B, M_5, M_6, T_4\}$ . Here  $A$  cannot compute  $SK = h(K_1K_2G)$  from known values  $A = K_1G$  and  $B = K_2G$  due to unsolvability of the ECCDHP. Further, no information about  $K_1$  and  $K_2$  can be obtained from  $M_2, M_3, M_4$  and  $M_5$  due to irreversibility of one way hash function  $h(\cdot)$ . Thus, we obtain,

$$|Pr[Succ_3] - Pr[Succ_4]| \leq Adv^{ECCDHP}(t) \quad (6.5)$$

All session keys are random and independent and the  $c$  value is not exposed to Adversary. Therefore, it is clear that



guess  $ID_i$  and  $PW_i$  to be  $ID_i^*$  and  $PW_i^*$  respectively and computes  $h(ID_i), H(BIO_i^*), x_i^* = B_i \oplus H(BIO_i^*), MP_i^* = h(h(ID_i^*) || PW_i^* || x_i^*)$ , and may get a pair  $(ID_i^*, PW_i^*)$  such that  $MP_i \neq MP_i^*$ . However, the size of the password dictionary and identity dictionary (Wang and Wang 2016) are sufficiently large and once the number of login failures exceeds the threshold value, the mobile device will be suspended and the attack fails.

### 7.3. Mobile user impersonation attacks

If an adversary wants to impersonate a mobile user  $MU$  he/she has to deceive  $FN$  and  $HN$  by producing the valid messages  $M_{MF} = \{A, M_1, M_2, T_1\}$  and  $M_{MF'} = \{M_7, T_5\}$ . An adversary  $A$  cannot calculate  $M_{MF}$  as he/she cannot compute  $K_1Q$  from known values  $A = K_1G$  and  $Q = xG$  due to unsolvability of the ECCDHP. Subsequently valid  $M_2$  cannot be generated. Similarly  $A$  cannot compute  $SK = h(K_1K_2G)$  from known values  $A = K_1G$  and  $B = K_2G$  due to unsolvability of the ECCDHP. So, a valid  $M_7$  cannot be generated. Therefore, the proposed scheme could withstand mobile user impersonation attacks.

### 7.4. Foreign network impersonation attacks

If an adversary  $A$  wants to impersonate a foreign network  $FN$  to deceive  $HN$  by producing the valid message  $M_{FH} = \{ID_F, M_{MF}, M_3, B, T_2, \}$  and  $M_{FM} = \{B, M_5, M_6, T_4\}$ .  $A$  cannot produce a valid  $M_3$ , as he/she do not know  $K_{FH}$ , hence adversary cannot impersonate as  $FN$ . Also,  $A$  cannot compute  $SK = h(K_1K_2G)$  from known values  $A = K_1G$  and  $B = K_2G$  due to the unsolvability of the ECCDHP. So valid  $M_6$  cannot be generated. Therefore, the proposed scheme could withstand foreign network impersonation attacks.

### 7.5. Home network impersonation attacks

If an adversary  $A$  wants to impersonate a home network  $HN$  he/she has to deceive  $MU$  and  $FN$  by producing valid messages  $M_4$  and  $M_5$  but  $A$  cannot produce valid  $M_4$  or  $M_5$  due to the unsolvability of ECCDHP, hence adversary cannot impersonate as  $HA$

### 7.6. Replay attacks

If an adversary replays an old login request message  $M_{MF} = \{A, M_1, M_2, T_1\}$ , then the foreign network can detect a replay attack by checking the freshness of the time stamp  $T_1$ . If the adversary changes the timestamp to the current timestamp then the home agent can detect the attack by comparing the received  $M_2$  with  $M_2^* = h(xA || M_1 || S_i || T_1)$ . But the



adversary cannot generate  $M_2$  due to the unsolvability of ECCDHP. Therefore, the proposed scheme could withstand replay attacks.

### 7.7. Session key security

In the proposed scheme, only  $MU$ ,  $FN$  can compute  $SK = h(K_1K_2G)$  after mutual authentication. If an adversary wants to compute an established session key he/she has to know  $K_1$ ,  $K_2$ . The adversary could obtain  $A = K_1G$  and  $B = K_2G$  from the previously transmitted messages but cannot obtain  $K_1$  or  $K_2$  because of the unsolvability of the ECDLP. Hence, the proposed scheme could provide the property of session key security.

### 7.8. Perfect forward secrecy

If an adversary has recorded the previously transmitted messages he/she still cannot compute a previously established session key  $SK = h(K_1K_2G)$  because in the proposed scheme, the session key is not dependent on the home agent's secret key  $x$ . As demonstrated in Section 7.7, the session key is dependent on the random numbers  $n_m$  and  $n_f$  and without knowing them (or one of them), the adversary cannot compute previously computed session keys  $SK$ . Therefore, the proposed scheme could provide the property of perfect forward secrecy.

## 8. Performance analysis

The present section will perform comparisons of the computational cost as well as communication cost of the proposed scheme with the state-of-the-art scheme, namely Zhao et al. (2014), Zhang et al. (2015), Wu et al. (2017) and Lee et al. (2018) schemes in the following subsections:

### 8.1. Computational costs comparisons

For the comparisons of the computational costs, the following cryptographic operations are considered: the hash function  $T_h$ , the symmetric en/decryption  $T_s$ , the modular exponent operation  $T_m$ , the ECC based encryption/decryption operation  $T_e$  and elliptic curve multiplication  $T_p$ . The authors (Xu and Wu 2015) measured the approximate execution time of each cryptographic operation using the CPU: Intel(R) Core(TM)2T6570 2.1 GHz, Memory:4G OS:Win7 32-bit, Software: Visual C 2008,MIRACL C/C Library,Security level: 160-bit point in  $F_p$ , 1024-bit in a cyclic group, AES and SHA1.The experiment results of various operation are given in Table 5. In the comparison results, only login and authentication phase are displayed, as the registration phase and password change phase take place once, and a user can change his/

her password independently. Table 6 shows the comparative computational costs of various schemes. The execution time of the proposed scheme is 36.7721 ms, while the execution time of the schemes of Lee et al, Zhao et al., Zhang et al. and Wu et al. are 0.2614 ms, 81.800 ms, 37.939 ms and 6.9232 ms respectively. Though Lee et al. and Wu et al. scheme have lower computational costs compared to the proposed scheme, they are not secure. From Table 6 we can conclude that the proposed scheme is more efficient than related schemes.

## 8.2. Communication costs comparisons

For the communication cost comparisons, we assume in accordance with (Reddy et al. 2016; Kumari et al. 2015) that the lengths of the identity, random number, and timestamp are 128 bits, 64 bits, and 32 bits, respectively. The hash function and the symmetric-key encryption produce 160 bits and 256 bits, respectively. For the asymmetric key encryption, the modular prime operation and the scalar multiplication operation on the elliptic curve produces 1024 bits and 320 bits, respectively. Table 7 shows the comparative communications costs of the login and authentication phases of the various schemes. The communications costs of the proposed scheme is

**Table 5.** Notations and execution time of cryptographic operations.

Notation	Description and Execution time(ms) (Xu and Wu 2015)
$T_h$	Time complexity of performing a hash function operation $\approx 0.0004$ ms
$T_s$	Time complexity of performing a symmetric encryption/decryption operation $\approx 0.1303$ ms
$T_e$	Time complexity of performing a ECC based encryption/decryption operation $\approx 1.6003$ ms,
$T_m$	Time complexity of performing an exponentiation operation $\approx 1.8269$ ms
$T_p$	Time complexity of performing an elliptic curve point multiplication $\approx 7.3529$ ms

**Table 6.** Computational costs comparisons.

Schemes	Total	Time(ms)
Lee et al. (2018)	$20T_h + 2T_s$	0.2614
Zhao et al. (2014)	$15T_h + 7T_s + 11T_p$	81.800
Zhang et al. (2015)	$20T_h + 4T_s + 5T_p$	37.939
Wu et al. (2017)	$20T_h + 4T_s + 4T_e$	6.9232
Proposed scheme	$19T_h + 5T_p$	36.7721

**Table 7.** Communication costs comparisons.

Schemes	communication cost
Lee et al. (2018)	2976 bits
Zhao et al. (2014)	4032 bits
Zhang et al. (2015)	2944 bits
Wu et al. (2017)	3936 bits
Proposed scheme	2880 bits

2880 bits, while that of other schemes namely: Lee et al, Zhao et al., Zhang et al. and Wu et al. are 2976 bits, 4032 bits, 2944 bits and 3936 bits respectively. Therefore, from Table 7 we can conclude that the proposed scheme is a more practical option for the ubiquitous network environment.

## 9. Conclusion

In this paper, we analyzed a recently proposed secure authentication and key agreement scheme for roaming service with user anonymity by Lee et al. (Lee et al. 2018). We demonstrated that Lee et al. scheme has the following security and design flaws: off-line dictionary attack, replay attack and de-synchronization attack. The scheme is also vulnerable to key control attack and has incorrect XOR calculations. Moreover, we proposed an improved scheme to resolve the security and design flaws in Lee et al. scheme by using biometric data. The security of the proposed scheme is given in the random oracle model. Furthermore, informal analysis is also conducted to demonstrate that the proposed protocol meets the various security requirements and we also conducted comparisons in terms of the computational and communication cost to show the suitability of the proposed protocol for roaming in ubiquitous networks.

## About the authors

*Shaheena Khatoon* received the B.Sc., M.Sc. and MPhil degree in Mathematics from Pt. Ravishankar Shukla University, Raipur, Chhattisgarh, India in 2005, 2007 and 2009. She joined School of Studies in Mathematics, Pt. Ravishankar Shukla University, Raipur, India for her research work. Her field of interest are public key cryptography, information security and applied mathematics.

*Balwant Singh Thakur* is Professor and head at School of Studies in Mathematics, Pt. Ravishankar Shukla University Raipur, Chhattisgarh, India. His field of interest are Non Linear Operator Theory and Public Key Cryptography. He and his research scholars are recently working on many branches of public key cryptography.

## Funding

This work was supported by the Department of Science and Technology (DST), Government of India under Women Scientist Scheme A (WOS-A) No. SR/WOS-A/PM-10/2018(G).

## ORCID

Shaheena Khatoon  <http://orcid.org/0000-0001-6663-870X>

## References

- Abdalla, M., P. A. Fouque, and D. Pointcheval. 2005. *Password-based authenticated key exchange in the three-party setting*, 65–84. Berlin, Heidelberg: International Workshop on Public Key Cryptography.
- Arshad, H., and A. Rasoolzadegan. 2017. A secure authentication and key agreement scheme for roaming service with user anonymity. *International Journal of Communication Systems* 30 (18):e3361. doi:10.1002/dac.3361.
- Bellovin, S. M., and M. Merritt. 1992. Encrypted key exchange: Password-based protocols secure against dictionary attacks. Research in Security and Privacy, In: Proceedings IEEE Computer Society Symposium, pp. 72–84.
- Boyko, V., P. MacKenzie, and S. Patel. 2000. Provably secure password-authenticated key exchange using Diffie-Hellman. In International Conference on the Theory and Applications of Cryptographic Techniques, pp. 156–171.
- Chaudhry, S. A., A. Albeshri, N. Xiong, C. Lee, and T. Shon. 2017. A privacy preserving authentication scheme for roaming in ubiquitous networks. *Cluster Computing* 20 (2): 1223–36. doi:10.1007/s10586-017-0783-x.
- Chen, C., D. He, S. Chan, J. Bu, Y. Gao, and R. Fan. 2011. Lightweight and provably secure user authentication with anonymity for the global mobility network. *International Journal of Communication Systems* 24 (3):347–62. doi:10.1002/dac.1158.
- Dolev, D., and A. Yao. 1983. On the security of public key protocols. *IEEE Transactions on Information Theory* 29 (2):198–208. doi:10.1109/TIT.1983.1056650.
- Eisenbarth, T., T. Kasper, A. Moradi, C. Paar, M. Salmasizadeh, and M. T. Shalmani. 2008. On the power of power analysis in the real world: A complete break of the keeloq code hopping scheme. In: Annual International Cryptology Conference, pp. 203–220.
- Farash, M. S., S. A. Chaudhry, M. Heydari, S. Sadough, S. Mohammad, S. Kumari, and M. K. Khan. 2017. A lightweight anonymous authentication scheme for consumer roaming in ubiquitous networks with provable security. *International Journal of Communication Systems* (4):30. doi:10.1002/dac.3019.
- Gope, P., and T. Hwang. 2015. Enhanced secure mutual authentication and key agreement scheme preserving user anonymity in global mobile networks. *Wireless Personal Communications* 82 (4):2231–45. doi:10.1007/s11277-015-2344-z.
- Hankerson, D., A. Menezes, and S. Vanstone. 2004. *Guide to elliptic curve cryptography*. Berlin: Springer.
- He, D., and D. Wang. 2015. Robust biometrics-based authentication scheme for multiserver environment. *IEEE Systems Journal* 9 (3):816–23. doi:10.1109/JSYST.2014.2301517.
- He, D., S. Chan, C. Chen, J. Bu, and R. Fan. 2011. Design and validation of an efficient authentication scheme with anonymity for roaming service in global mobility networks. *Wireless Personal Communications* 61 (2):465–76. doi:10.1007/s11277-010-0033-5.
- He, D., S. Zeadally, N. Kumar, and W. Wu. 2016. Efficient and anonymous mobile user authentication protocol using self-certified public key cryptography for multi-server architectures. *IEEE Transactions on Information Forensics and Security* 11 (9):2052–64. doi:10.1109/TIFS.2016.2573746.
- Ignatenko, T., and F. M. Willems. 2009. Biometric systems: Privacy and secrecy aspects. *IEEE Transactions on Information Forensics and Security* 4 (4):956–73. doi:10.1109/TIFS.2009.2033228.

- Jiang, Q., J. Ma, G. Li, and L. Yang. 2013. An enhanced authentication scheme with privacy preservation for roaming service in global mobility networks. *Wireless Personal Communications* 68 (4):1477–91. doi:10.1007/s11277-012-0535-4.
- Jiang, Q., S. Zeadally, J. Ma, and D. He. 2017. Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks. *IEEE Access* 5: 3376–92. doi:10.1109/ACCESS.2017.2673239.
- Jung, J., D. Kang, D. Lee, and D. Won. 2017. An improved and secure anonymous biometric-based user authentication with key agreement scheme for the integrated EPR information system. *PLoS One* 12 (1) doi:10.1371/journal.pone.0169414.
- Karuppiah, M., S. Kumari, A. K. Das, X. Li, F. Wu, and S. Basu. 2016. A secure lightweight authentication scheme with user anonymity for roaming service in ubiquitous networks. *Security and Communication Networks* 9 (17):4192–209. doi:10.1002/sec.1598.
- Kumari, S., M. K. Khan, and M. Atiquzzaman. 2015. User authentication schemes for wireless sensor networks: A review. *Ad Hoc Networks* 27:159–94. doi:10.1016/j.adhoc.2014.11.018.
- Kumari, S., M.K. Khan, X. Li, and F. Wu. 2016. Design of a user anonymous password authentication scheme without smart card. *International Journal of Communication Systems* 29 (3):441–58. doi:10.1002/dac.2853.
- Kumari, S., X. Li, F. Wu, A.K. Das, V. Odelu, and M.K. Khan. 2016. A user anonymous mutual authentication protocol. *KSII Transaction and Internet Information System* 10 (9): 4103–19.
- Lee, C. C., M. S. Hwang, and I. E. Liao. 2006. Security enhancement on a new authentication scheme with anonymity for wireless environments. *IEEE Transactions on Industrial Electronics* 53 (5):1683–7. doi:10.1109/TIE.2006.881998.
- Lee, C.C., C.T. Chen, P.H. Wu, and T.Y. Chen. 2013. Three-factor control protocol based on elliptic curve cryptosystem for universal serial bus mass storage devices. *IET Computers & Digital Techniques* 7 (1):48–56. doi:10.1049/iet-cdt.2012.0073.
- Lee, H., D. Lee, J. Moon, J. Jung, D. Kang, and H. Kim. 2018. An improved anonymous authentication scheme for roaming in ubiquitous networks. *PLoS One* 13 (3): e0193366. doi:10.1371/journal.pone.0193366.
- Lee, T. F. 2015. Provably secure anonymous single-sign-on authentication mechanisms using extended Chebyshev chaotic maps for distributed computer networks. *IEEE Systems Journal* 9 (3):805–815. doi:10.1109/JSYST.2015.2471095.
- Mun, H., K. Han, Y. S. Lee, C. Y. Yeun, and H. H. Choi. 2012. Enhanced secure anonymous authentication scheme for roaming service in global mobility networks. *Mathematical and Computer Modelling* 55 (1-2):214–22. doi:10.1016/j.mcm.2011.04.036.
- Odelu, V., A. K. Das, S. Kumari, X. Huang, and M. Wazid. 2017. Provably secure authenticated key agreement scheme for distributed mobile cloud computing services. *Future Generation Computer Systems* 68:74–88. doi:10.1016/j.future.2016.09.009.
- Reddy, A. G., A. K. Das, V. Odelu, and K. Y. Yoo. 2016. An enhanced biometric based authentication with key-agreement protocol for multi-server architecture based on elliptic curve cryptography. *PLoS One* 11 (5):e0154308. doi:10.1371/journal.pone.0154308.
- Wang, C., and G. Xu. 2017. Cryptanalysis of three password-based remote user authentication schemes with non-tamper-resistant smart card. *Security and Communication Networks* 2017:1–14. doi:10.1155/2017/1619741.
- Wang, C., D. Wang, G. Xu, and Y. Guo. 2017. A lightweight password-based authentication protocol using smart card. *International Journal of Communication Systems*
- Wang, D., and P. Wang. 2016. Two birds with one stone: Two-factor authentication with security beyond conventional bound. *IEEE Transactions on Dependable and Secure Computing* 99:1–22.

- Wang, D., D. He, P. Wang, and C. Chu. 2015. Anonymous two-factor authentication in distributed systems: Certain goals are beyond attainment. *IEEE Transactions on Dependable and Secure Computing* 12 (4):428–42. doi:[10.1109/TDSC.2014.2355850](https://doi.org/10.1109/TDSC.2014.2355850).
- Wang, D., H. Cheng, P. Wang, X. Huang, and G. Jian. 2017. Zipf's law in passwords. *IEEE Transactions on Information Forensics and Security* 12 (11):2776–91. doi:[10.1109/TIFS.2017.2721359](https://doi.org/10.1109/TIFS.2017.2721359).
- Wazid, M., A. K. Das, S. Kumari, X. Li, and F. Wu. 2016. Design of an efficient and provably secure anonymity preserving three-factor user authentication and key agreement scheme for TMIS. *Security and Communication Networks* 9 (13):1983–2001. doi:[10.1002/sec.1452](https://doi.org/10.1002/sec.1452).
- Wen, F., W. Susilo, and G. Yang. 2013. A secure and effective anonymous user authentication scheme for roaming service in global mobility networks. *Wireless Personal Communications* 73 (3):993–1004. doi:[10.1007/s11277-013-1243-4](https://doi.org/10.1007/s11277-013-1243-4).
- Wu, C. C., W. B. Lee, and W. J. Tsaur. 2008. A secure authentication scheme with anonymity for wireless communications. *IEEE Communications Letters* 12 (10):722–23.
- Wu, F., L. Xu, S. Kumari, X. Li, M. K. Khan, and A. K. Das. 2017. An enhanced mutual authentication and key agreement scheme for mobile user roaming service in global mobility networks. *Annals of Telecommunications* 72 (3-4):131–44. doi:[10.1007/s12243-016-0547-2](https://doi.org/10.1007/s12243-016-0547-2).
- Xie, Q., B. Hu, B. Bao, and X. Yu. 2014. Robust anonymous two-factor authentication scheme for roaming service in global mobility network. *Wireless Personal Communications* 74 (2):600–14. doi:[10.1007/s11277-013-1309-3](https://doi.org/10.1007/s11277-013-1309-3).
- Xu, L., and F. Wu. 2015. Cryptanalysis and improvement of a user authentication scheme preserving uniqueness and anonymity for connected health care. *Journal of Medical Systems* 39 (2):10. doi:[10.1007/s10916-014-0179-x](https://doi.org/10.1007/s10916-014-0179-x).
- Zhang, G., D. Fan, Y. Zhang, X. Li, and X. Liu. 2015. A privacy preserving authentication scheme for roaming services in global mobility networks. *Security and Communication Networks* 8 (16):2850–9. doi:[10.1002/sec.1209](https://doi.org/10.1002/sec.1209).
- Zhao, D., H. Peng, L. Li, and Y. Yang. 2014. A secure and effective anonymous authentication scheme for roaming service in global mobility networks. *Wireless Personal Communications* 78 (1):247–69. doi:[10.1007/s11277-014-1750-y](https://doi.org/10.1007/s11277-014-1750-y).
- Zhu, J., and J. Ma. 2004. A new authentication scheme with anonymity for wireless environments. *IEEE Transactions on Consumer Electronics* 50 (1):231–5.

# An Efficient and Secure, ID-based Authenticated, Asymmetric Group Key Agreement Protocol for Ubiquitous Pay-TV Networks

Shaheena Khatoon<sup>1</sup>, Sk Md Mizanur Rahman<sup>2</sup>, Raylin Tso<sup>3</sup>, Mohammed F. Alhamid<sup>4</sup>

<sup>1</sup> School of Studies in Mathematics, Pt. Ravishankar Shukla University, India

<sup>2</sup> Information and Communication Engineering Technology (ICET), Centennial College, Canada

<sup>3</sup> Department of Computer Science, National Chengchi University, Taiwan

<sup>4</sup> Department of Software Engineering, King Saud University, Saudi Arabia

shaheenataj.28@gmail.com, SRahman@centennialcollege.ca, raylin@cs.nccu.edu.tw, mohalhamid@ksu.edu.sa

## Abstract

Internet-of-Things (IoT) based applications are rapidly gaining popularity. Smart home is one of them; home security and safety, home automation, energy management and health surveillance are some applications of smart homes. Smart homes have enormous potential as well as enormous threat to security and privacy of the end users. Pay TV is considered as the likely entry points for IoT services into smart homes. Pay TV has evolved security techniques very similar to of IoT based smart homes services. Pay TV is an application of broadcast encryption schemes in which premium content is broadcasted only to subscribed users. The broadcaster needs assurance that only subscribed user can access premium content, so the program is encrypted with a group key shared among all subscribers. Thus, to share the key, Pay-TV systems require efficient and secure group key agreement (GKA). This research proposes an efficient and secure, dynamic, ID-based authenticated, asymmetric group key agreement (AAGKA) protocol for Pay-TV networks. Security is proved under the assumptions of the discrete logarithm problem (DLP) and decisional Diffie-Hellman problem (DDHP). Finally, comparison of the protocol with state-of-art protocols shows that the proposed protocol is highly efficient.

**Keywords:** Internet-of-Things (IoT), Authentication, Asymmetric group key agreement, Bilinear pairing, Pay-TV network

## 1 Introduction

Smart homes, an IoT based application is next big thing in the rapidly growing technology-based lifestyle. Pay -TV has much to offer to the fast-developing smart home era. Over the years, Pay-TV had gained trust among the customers with secure data management and determination without compromising the privacy of the subscribers. In order to avail the benefits of smart homes and IoT, consumers have to allow the

new technology to go deeper into their homes.

With established subscriber relationship, Pay-TV can enable IoT to manage smart homes with robustness and reliability and without any attack on their privacy.

Group key agreement (GKA) protocols provide a secure and robust approach to establishing group session keys for public networks and hence aim to provide secure communication over an insecure network. Wu et al. [20], introduced the concept of the asymmetric group key agreement (AGKA) protocol, in which all group members compute a common secret group key and only group members can broadcast secret messages to the group. In asymmetric protocols, unlike in symmetric protocols, all group members compute a common group encryption key (GEK) and hold different group decryption keys (GDGs).

The authenticated asymmetric protocol proposed here has the following advantages: (1) messages can also be broadcasted by any non-registered member in the group (using the GEK); (2) asymmetric protocols use short signatures to achieve mutual authentication; and (3) the protocol complements dynamic networks by maintaining backward and forward secrecy. Thus, an authenticated, asymmetric group key agreement (AAGKA) protocol preserves benefits of both the GKA protocol and broadcast encryption.

In a Pay-TV system, broadcasters generate revenue by charging subscribers for viewing programs. Thus, broadcasters need a mechanism so that only the paid subscribers can view the program. We present only a brief discussion here of the specific requirements of Pay-TV systems, but greater detail may be found in [7-8, 11, 13]. A Pay-TV system is asymmetric with respect to computational and communication capabilities between the broadcaster and the subscribers. Since the broadcaster has greater computational capabilities than the subscribers, a GKA protocol for Pay-TV should place greater computational and communication load on the broadcaster than on the subscribers.

Further, a key agreement protocol for Pay-TV must

\*Corresponding Author: Shaheena Khatoon; E-mail: shaheenataj.28@gmail.com

be contributive; that is, each user in the group must equally contribute to the computation of the group decryption key, so that no user gets an undue computational advantage over another. Also, since Pay-TV is a dynamic system, with subscribers frequently joining or leaving the group, the rekeying mechanism should be efficient and secure. Additionally, the key agreement protocol must provide both forward and backward secrecy, so that joining or leaving subscribers can obtain no knowledge of any previously or newly established group decryption key. **A typical model for Pay-TV.** Broadcasters have a database storing keys, link values, and other relevant

information. Broadcasters have enough resources to undertake greater computational and communications load than subscribers. Broadcasters perform initial setup, generating the necessary public parameters, distributing them, and storing them securely. Meanwhile, each subscriber has a set-top box with a smart card that performs the necessary cryptographic operations. The set-top box makes registration and subscription requests to the broadcaster, receives encrypted content, and decrypts the content to make it available to the subscriber. Figure 1 illustrates a typical model for a Pay-TV communications and broadcasting network.

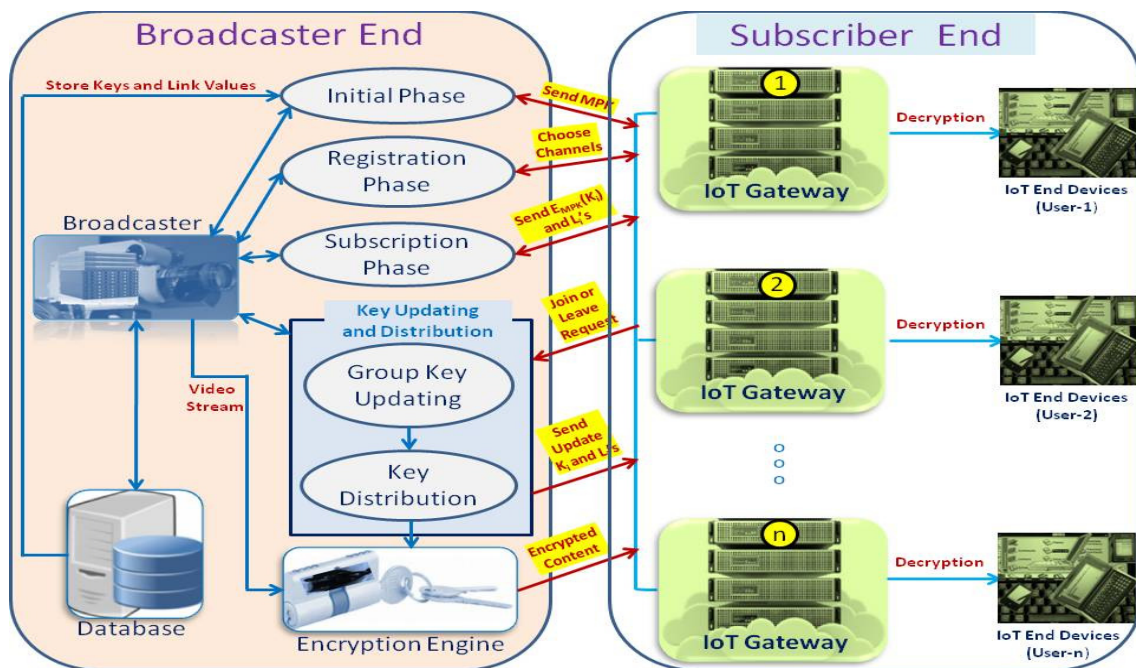


Figure 1. A typical communication model for Pay-TV system network

**Organization of the Paper.** The next section summarizes existing research in the same domain. In Section 3 describes the preliminaries of the cryptographic primitives to enable better understanding of the proposed protocol. The proposed protocol is detailed in Section 4. Section 5 describes the contributions of the subscribers in a model Pay-TV network and demonstrates the correctness of the proposed protocol. A detailed security analysis of the suggested protocol is presented in Section 6 while Section 7 analyzes the performance with respect to the computational and communications costs of the protocol. Finally, Section 8 concludes.

## 2 Related Works

There is an increasing interest to incorporate the IoT-based smart home service using Pay TVs. The genesis of IoT can be dated back in the year 1982, [22] when a coke vending machine was connected through internet. However, M. Weiser [24] gave a contemporary vision of IoT in the year 1991. Later in

year 1999, B. Joy [19] demonstrated device to device communication. In the year 2009, K. Ashton [1] first coined the term “Internet of Things”. But still there is no universally accepted definition of IoT, different group define it in different way. Concisely, IoT can be define as a system of interconnected physical objects, to exchange and collect data over the internet. Since its inception, IoT aims to improve one’s comfort and efficiency, by enabling cooperation among smart objects [12]. Further, Gubbi et al. [12] estimates that about 50 billion objects will be connected through IoT by 2020. So, the security challenges involved with IoT should be addressed at the design level.

Effective security practices, especially mutual authentication and key agreement schemes are needed to protect anonymity and privacy of the users. Fiat et al. [10] formalized the definition and paradigm of broadcasting encryption schemes. Since then, many schemes have been proposed for secure cryptographic broadcasting, with the most prominent among them being [5, 14-15, 18, 21]. However, these broadcasting encryption schemes do allow a sender to broadcast any



content to a group of receivers but do not provide a key management mechanism, as security of these schemes basically trusts upon a key server for generation as well as distribution of encrypted keys. Since the trusted server can read all the communicated keys, it represents a threat to the security of the scheme.

Furthermore, schemes such as [14, 18] do not provide forward secrecy, hence making them poorly suited for Pay-TV. Some authentication schemes were suggested for Pay-TV in [7, 11], but these only authenticate the user to the group without providing a key exchange mechanism. Group key agreement protocols seem to offer solutions to the problems discussed above. Existing, group key agreement protocols assume pre-determined group members and once all these members participate in the protocol then only a secure channel for broadcasting is established. Since Pay-TV model is highly dynamic, traditional GKA protocol seem not applicable to it. Hence, Kim et al. [14] and Kumar et al. [16] offered group key agreement protocols for Pay-TV, but both are symmetric, meaning they provide only a key agreement mechanism without having a broadcast-encryption ability. Hence, an asymmetric, group key agreement protocol seems to offer a better solution for key management and broadcasting of premium content in Pay-TV applications.

Some asymmetric group key agreement exist in literature like, [26-29]. But as pointed by [27], Zhang et al.'s [26] scheme requires an identity-based signature to assure the security of the protocol, and it only provides partial forward secrecy (PFS). Ermi et al. [9] demonstrated that [27] is mainly suitable for small group communication like instant messaging applications [17], conference communication applications similarly Li and Zhang's [29] protocol is suitable for instant messaging applications, such as Messenger, We-chat and Whats App, whereas Zhang's protocol works well in a vehicular ad hoc networks (VANETS). But, none of the above research considers the issues with Pay-TV in IoT infrastructure. So, the present paper proposes an efficient, two-round, authenticated, asymmetric group key agreement (AAGKA) protocol specifically for Pay-TV that fulfills the above-discussed requirements in IoT infrastructure. The suggested protocol is simple and efficient, minimizing subscribers' computational cost by shifting the burden to the broadcaster.

### 3 Preliminaries

The following section gives a widely accepted definition of bilinear pairing and also defines discrete logarithm problem (DLP) and decision Diffie-Hellman Problem (DDHP).

**Definition 3.1 (Bilinear Pairing).** Suppose,  $\langle G_1, + \rangle$  be acyclic additive group and  $\langle G_2, \cdot \rangle$  be a cyclic multiplicative group and the order of both the group is

a large prime  $p$ . A bilinear pairing  $e$  is a map defined by  $e: G_1 \times G_1 \rightarrow G_2$  and it has the following properties:

(1) **Bilinear:** According to this property, for given  $(R, S) \in G_1, e(aR, bS) = e(R, S)^{ab}$ , where  $a, b \in Z_p^*$ .

(2) **Non-degenerate:** According to this property, there exists  $(R, S) \in G_1$ , such that  $e(R, S) \neq 1$  where 1 is the identity of  $G_2$ .

(3) **Computable:** This property assures, that there exist an algorithm which can efficiently compute  $e(R, S)$  for all  $(R, S) \in G_1$ .

Two pairings used extensively for cryptography are the Weil pairing and its modifications and the Tate pairing. A full description of these pairings may be found in [2-4, 6].

**Discrete logarithm problem (DLP).** According to this problem, for given  $(R, S) \in G$ , it is computationally infeasible to find an integer  $n \in Z_p^*$ , such that  $S = nR$ .

Note, that discrete logarithm problem (DLP) is hard in both  $G_1$  and  $G_2$ .

**Decision Diffie-Hellman Problem (DDHP).** According to this problem, for given  $(P, aP, bP, cP)$ . Where  $a, b, c \in Z_p^*$ . It is computationally infeasible to decide whether  $c = ab \pmod p$ .

### 4 Proposed Group Key Agreement Protocol

This section presents an ID-based authenticated, asymmetric group key agreement (AAGKA) protocol suitable for Pay-TV. The following notations are used throughout for better understanding of the proposed protocol.

- $e$ : Denotes the bilinear map,  $e: G_1 \times G_1 \rightarrow G_2$ .
- $s$ : Denotes the master private key,  $s \in Z_p^*$ .
- $P$ : Denotes a generator of  $G_1$ .
- $P_{pub}$ : Denotes the system public key,  $P_{pub} = sP$ .
- $H_0$ : Denotes a hash function,  $H_0: \{0,1\}^* \rightarrow \{0,1\}^*$ .
- $H_1$ : Denotes a hash function,  $H_1: \{0,1\}^* \rightarrow Z_p^*$ .
- $U_i$ : Denotes the subscriber to Pay-TV,  $1 \leq i \leq n-1$ .
- $U_n$ : Denotes the broadcaster of Pay-TV.
- $ID_i$ : Denotes the identity of  $U_i$ .
- $PK_i$ : Denotes the long-term public key of a participant  $U_i, PK_i = H_0(ID_i) = Q_i$ .
- $SK_i$ : Denotes the long-term private key of a participant  $U_i, SK_i = sH_0(ID_i) = sQ_i$ .
- GEK: Denotes the group encryption key.
- GDK: Denotes the group decryption key.

Let  $U = \{U_1, U_2, \dots, U_n\}$  be the set of users in the AAGKA protocol, where  $U_i \in U, (1 \leq i \leq n-1)$  are the subscribers and  $U_n$  is the broadcaster. Each has the unique identity  $ID_i, (1 \leq i \leq n)$ . The protocol is executed in three phases: (1) the AAGKA phase, (2) the subscriber leaving phase (SLP) and (3) subscriber joining phase (SJP).

**(1) AAGKA phase.**

**(a) Setup:** With the security parameter  $k \in Z$ , the trusted key generator center (KGC) generates a set of system parameters as follow

- KGC executes  $k$  to generate a large prime  $p$ , cyclic groups  $G_1$  and  $G_2$ , where  $G_1$  is additive and  $G_2$  is multiplicative group, both the groups have same order  $p$  and pairing  $e$  which maps element of  $G_1 \times G_1$  to  $G_2$
- KGC randomly selects  $s \in Z_p^*$ , and computes system public key  $P_{pub} = sP$ , where  $s$  is the master private key (MPK).

**(b) Authenticated Key Exchange**

**Round 1:** Each subscriber  $U_i \in U, (1 \leq i \leq n-1)$  randomly selects two numbers  $m_i, r_i \in Z_p^*$  and computes

$$R_i = r_i P, M_i = m_i PK_n P_{pub} \text{ and } T_i = \left( \frac{m_i + SK_i}{r_i} \right) P \text{ and}$$

sends the tuple  $(U_i, R_i, M_i, T_i)$  to the broadcasting node  $U_n$ .

**Note:** Each subscriber can pre-compute these  $(R_i, M_i, T_i)$  off-line, reducing the computational burden.

**Round 2:** The broadcaster verifies the equation  $e(R_i, T_i) = e(P, SK_n^{-1} M_i + PK_i P_{pub})$  for all  $1 \leq i \leq n-1$ .

If the equation holds,  $U_n$  is assured that  $(U_i, R_i, M_i, T_i)$  has been sent by each  $U_i$ . Then, the broadcaster randomly selects two numbers  $m_n, r_n \in Z_p^*$ , computing

$$R_n = r_n P, T_n = \left( \frac{m_n + SK_n}{r_n} \right) P, PK = \sum_{i=1}^{n-1} PK_i \quad RT = \prod_{i=1}^{n-1} e(R_i, T_i),$$

$Q_1 = RT^{m_n^2}, Q_2 = m_n PK P_{pub}$  and  $X_i = SK_n^{-1} m_n M_i$ . Next the broadcaster computes the group encryption key and decryption key  $GEK = (Q_1, Q_2), GDK = e(f_n, \sum_{i=1}^{n-1} X_i)$  and  $f_n = m_n P$ . Finally, the broadcaster broadcasts  $(U_n, X_1, X_2, \dots, X_{n-1}, R_n, T_n, Q_1, Q_2)$  to each  $U_i$ .

**(c) Common Group Key Computation:** Each  $U_i$  verifies the equation  $e(R_n, T_n) = e(P, M_i^{-1} X_i + PK_n P_{pub})$ . If the equation holds, each  $U_i$  is assured that the message has been broadcasted by  $U_n$ . Each  $U_i$  then

computes,  $GDK = e(f_j, \sum_{j=1}^{n-1} X_j) = e(m_n P, \sum_{j=1}^{n-1} X_j)$   $GEK = (Q_1, Q_2), f_j = X_i m_i^{-1}$ .

If equation  $e(Q_2, f_i) GDK = Q_1$  the GEK and GDK keys are correct.

**(d) Encryption:** Any user  $U_i, (1 \leq i \leq n)$  encrypts plain text  $m$  as follows: randomly selects  $t \in Z_p^*$ , and computes  $\delta = tP, \eta = m \oplus H_1(Q_1 e(P, f_j)^{-1})^t$ . The ciphertext is  $c = (\delta, \eta)$ .

**(e) Decryption:** Any valid user can decrypt message  $m = \eta \oplus H_1(e(\delta, GDK))$ .

**(2) Subscriber Leave Phase (SLP)**

Let the set of subscribers  $\{U_{j+1}, U_{j+2}, \dots, U_{n-1}\}$  decide to leave the group  $U$ . Then,  $U_n$  updates the group to  $U' = \{U_i, \dots, U_{i-1}, U_n\}$  and executes the SLP phase in the following way:

**Round 1:**  $U_n$  randomly selects two numbers  $m'_n, r'_n \in Z_p^*$

and computes  $R'_n = r'_n P \quad T'_n = \left( \frac{m'_n + SK_n}{r'_n} \right) P, \quad PK' =$

$$\sum_{1 \leq j \leq n-1, j \neq i} PK_j, \quad RT' = \sum_{1 \leq j \leq n-1, j \neq i} e(R_j, T_j), \quad Q'_1 =$$

$(RT')^{m_n'^2}, \quad Q'_2 = m'_n PK' P_{pub}$  and  $X'_j = SK_n^{-1} m'_n M_j$ . Next

the broadcaster computes the group encryption key  $GEK' = (Q'_1, Q'_2), \quad f'_n = m'_n P,$  and decryption key

$GDK' = e(f'_n, \sum_{1 \leq j \leq n-1, j \neq i} X'_j)$ . Finally, the broadcaster

broadcasts  $(U_n, X'_1, X'_2, \dots, X'_{i-1}, X'_{i+1}, R'_n, T'_n, Q'_1, Q'_2)$  to each  $U'_i$

**Round 2:** Common Group Key Computation: Each  $U_j, (1 \leq j \leq n-1, j \neq i)$ , verifies the equation  $e(R'_n, T'_n) =$

$e(P, M_j^{-1} X'_j + PK_n P_{pub})$ . If the equation holds, each

$U_j$  is assured that the message has been broadcasted by  $U_n$ . Each  $U_j$  then computes  $GEK' = (Q'_1, Q'_2), f'_j = X'_j M_j^{-1}$

and  $GDK' = e(f'_j, \sum_{1 \leq j \leq n-1, j \neq i} X'_j) = e(m'_n P, \sum_{1 \leq j \leq n-1, j \neq i} X'_j)$ . If

$e(P, f'_j) GDK' = Q'_1$ , GEK and GDK keys are correct.

**(2) Subscriber join phase (SJP).**

Let the set of subscribers  $\{U_{n+1}, U_{n+2}, \dots, U_l\}$  decide to join the group  $U$ . Then,  $U_n$  updates the group to  $U'' = \{U_i, \dots, U_n, U_{n+1}, \dots, U_l\}$  and executes the SJP phase in the following way:

**Round 1:** Each  $U_k = (n+1 \leq k \leq l)$  register its identity with  $U_n$  randomly selects two numbers  $m_k, r_k \in Z_p^*$  and computes  $R_k = r_k P, M_k = m_k PK_n P_{pub}$  and  $T_k =$

$\left(\frac{m_k + SK_k}{r_k}\right)P$  sending the tuple  $(U_k, R_k, M_k, T_k)$  to the broadcasting node  $U_n$ .

**Note:** In this case, nodes can also pre-compute  $(R_k, M_k, T_k)$  and store the tuple on their memory cards.

**Round 2:** The broadcaster verifies the equation  $e(R_k, T_k) = e(P, SK_n^{-1}M_k + PK_k P_{pub})$  for all  $n+1 \leq k \leq l$ .

If the equation holds,  $U_n$  is assured that  $(U_k, R_k, M_k, T_k)$  has been sent by each  $U_k$ . Then, the broadcaster randomly selects two numbers  $m_n, r_n \in Z_p^*$ , computing

$$R_n'' = r_n''P, \quad T_n'' = \left(\frac{m_n'' + SK_n''}{r_n''}\right)P, \quad PK_n'' = \sum_{k=n+1}^l PK_k, \quad RT_n'' =$$

$$\prod_{k=n+1}^l e(R_k T_k), \quad Q_1'' = (RT_n'' + RT_n'')^{m_n''^2} \quad \text{and} \quad Q_2'' = m_n''(PK_n'' + PK_n'')P_{pub},$$

and  $X_i'' = SK_n^{-1}m_n''M_k, (1 \leq k \leq l, l \neq n)$ . Next the broadcaster computes the group encryption key and

decryption key  $GEK'' = (Q_1'', Q_2''), GDK'' = e(f_n'', \sum_{i=1, i \neq n}^l X_i)$

and  $f_n'' = m_n''P$ . Finally, the broadcaster broadcasts  $(U_n, X_1'', \dots, X_{n-1}'', X_{n+1}'', \dots, X_n'', R_n'', T_n'', Q_1'', Q_2'')$  to each joining node  $U_k (n+1 \leq k \leq l)$

**Common group key computation.** Each  $U_k (n+1 \leq k \leq l)$  verifies the Equation  $e(R_n'', T_n'') = e(P, M_k^{-1}X_k + PK_n P_{pub})$ .

If the equation holds, each  $U_k$  is assured that the message has been broadcasted by  $U_n$ .

Then each  $U_k$  computes  $GDK'' = e(f_j'', \sum_{i=1, i \neq n}^l X_i)$

$$= e(m_n''P, \sum_{i=1, i \neq n}^l X_i) \quad GEK'' = (Q_1'', Q_2''), \quad f_j'' = X_i M_i^{-1}.$$

If equation  $e(Q_2'', f_j'')GDK'' = Q_1''$  the GEK and GDK keys are correct.

## 5 Contributiveness and Correctness of the Proposed Protocol

The present section will demonstrate that the suggested protocol is correct and satisfies the property of contributiveness.

**Theorem 5.1 (Contributiveness)** In the proposed protocol, an identical contributory group encryption (GEK) and group decryption (GDK) keys are established by all the nodes, and each node's contribution is included in the construction of the group key.

**Proof 5.1:** We note that,  $GEK = (Q_1, Q_2) = (m_n PKP_{pub}, RT^{m_n^2}) = (m_n \sum_{i=1}^{n-1} PK_i P_{pub}, RT^{m_n^2})$ . In the

above equation, each  $PK_i$  (each user's public key) is used in the construction of the GEK. This proves that each node's contribution is included in the construction

of the GEK. Further,  $\sum_{j=1}^{n-1} X_j = SK_n^{-1}m_n M_i = m_n m_j P$

and  $f_j = X_j m_j^{-1}$ , from which  $GDK = e(f_j, \sum_{j=1}^{n-1} X_j)$

$= e(m_n P, \sum_{j=1}^{n-1} m_n m_j P)$ . From this equation, we can

observe that GDK contains  $m_i, (1 \leq i \leq n)$ , the secret number of all nodes. This proves that each node's contribution is included in the construction of the GDK.

**Theorem 5.2 (Correctness):** Each user  $U_i, (1 \leq i \leq n)$  computes the identical group decryption key GDK.

**Proof 5.2:** The group decryption key can be computed

$$GDK = e(f_j, \sum_{j=1}^{n-1} X_j)$$

$$\begin{aligned} \text{as follows:} \quad &= e(m_n P, \sum_{j=1}^{n-1} m_n m_j P) \\ &= e(m_n P, m_n (m_1 + m_2 + \dots + m_{(n-1)}))P \\ &= e(P, P)^{(m_1 + m_2 + \dots + m_{(n-1)})m_n^2} \end{aligned}$$

observing the above derivation it can be concluded that each user  $U_i, (1 \leq i \leq n)$  can compute the identical group decryption key GDK.

**Theorem 5.3 (Correctness):** The verification equations that are used in the proposed protocol are correct i.e.,

$$\begin{aligned} e(R_i, T_i) &= e(P, SK_n^{-1}M_i + PK_i P_{pub}), (1 \leq i \leq n-1), \\ e(R_n, T_n) &= e(P, M_i^{-1}X_i + PK_n P_{pub}), (1 \leq i \leq n-1), \\ e(Q_2, f_j)GDK &= Q_1, (1 \leq j \leq n-1). \end{aligned}$$

**Proof 5.3:** By the definition of bi-linear pairing,

$$e(R_i, T_i) = e(r_i P, \left(\frac{m_i + SK_i}{r_i}\right)P) = e(P, P)^{(m_i + SK_i)}$$

and

$$\begin{aligned} e(R_i, T_i) &= e(P, SK_n^{-1}M_i + PK_i P_{pub}), (1 \leq i \leq n-1), \\ &= e(P, s^{-1}Q_i^{-1}m_i PK_n P_{pub} + PK_i P_{pub}) \\ &= e(P, s^{-1}Q_i^{-1}m_i PK_n sP + PK_i sP) \\ &= e(P, P)^{(m_i + SK_i)} \end{aligned}$$

This derivation establishes the equation,  $e(R_i, T_i) =$

$$e(P, SK_n^{-1}M_i + PK_iP_{pub}).$$

In the similar way we can show,  $e(R_n, T_n) = e(P, M_i^{-1}X_i + PK_nP_{pub})$ .

Lastly, we will show,  $e(Q_2, f_j)GDK = Q_1, (1 \leq j \leq n-1)$ .

$$\begin{aligned} Q_2 &= m_n PKP_{pub} \\ &= m_n \sum_{i=1}^{n-1} PK_i sP \\ &= m_n P \sum_{i=1}^{n-1} SP K_i \\ &= m_n P \sum_{i=1}^{n-1} SK_i \end{aligned}$$

So, by the property of bi-linearity we have,

$$\begin{aligned} &e(Q_2, f_j)GDK \\ &= e\left(m_n P \sum_{i=1}^{n-1} SK_i, m_n P\right) e(P, P)^{(m_1+m_2+\dots+m_{(n-1)})m_n^2}, \\ &= e(P, P)^{\sum_{i=1}^{n-1} SK_i m_n^2} e(P, P)^{\sum_{i=1}^{n-1} m_i m_n^2}, \\ &= e(P, P)^{\sum_{i=1}^{n-1} (SK_i + m_i) m_n^2} \end{aligned}$$

and

$$\begin{aligned} Q_1 &= RT^{m_n^2} \\ &= \left[ \prod_{i=1}^{n-1} (R_i, T_i) \right]^{m_n^2}, \\ &= \left[ \prod_{i=1}^{n-1} e(r_i P, \left(\frac{m_i + SK_i}{r_i}\right)P) \right]^{m_n^2}, \\ &= \left[ \prod_{i=1}^{n-1} (P, P)^{\sum_{i=1}^{n-1} SK_i + m_i} \right]^{m_n^2}, \\ &= e(P, P)^{\sum_{i=1}^{n-1} (SK_i + m_i) m_n^2} \end{aligned}$$

Thus, all the verification equations are correct.

## 6 Security Analysis

The present section, shows that the suggested protocol is secure under the assumptions of DLP and DDHP.

**Theorem 6.1:** Under the DDHP assumption, the proposed protocol is secure. This means, no adversary can get the group decryption key (GDK) by eavesdropping the public parameters and messages broadcasted over the public channel.

**Proof 6.1:** Let adversary Adv try to construct the group decryption key (GDK) by eavesdropping on public parameters and messages broadcasted over the public channel. Adv cannot do so, as  $(M_j, X_j, GDK = e(f_j, \sum X_j))$  and  $(M_j, X_j, GDK = e(\beta, \sum X_j))$  for  $(1 \leq j \leq n-1)$  are computationally indistinguishable where  $\beta \in G_1$  is a random value.

Adversary Adv uses the algorithm A to construct  $A'$  (another algorithm) to differentiate between  $(aP, abP, bP)$  and  $(aP, abP, \beta P)$  where  $\beta \in G_1$  is a random value and  $a, b \in Z_p^*$ .

Let  $M_1 \in aP$ , and  $X_1 \in abP$ . Then  $A'$  randomly selects  $\lambda_1, \dots, \lambda_{n-1}$  and calculates  $M_1, \dots, M_{n-1}$  as below:

$$\begin{aligned} M_2 &= \lambda_1 P, X_2 = \lambda_1 M_1; \\ M_3 &= \lambda_2 P, X_3 = \lambda_2 M_2; \\ &\vdots \\ M_{n-1} &= \lambda_{n-2} P, X_{n-1} = \lambda_{n-2} M_1; \end{aligned}$$

in this way,  $A'$  constructs all  $(M_j, X_j), (1 \leq j \leq n-1)$ , calculating the group decryption key,  $GDK = e(\beta, \sum X_j)$ . It then calls A with this value. If  $GDK = e(\beta, \sum X_j)$  means that  $\beta = bP$ , adversary Adv can differentiate between  $(aP, abP, bP)$  and  $(aP, abP, \beta P)$  which contradicts to the DDHP assumption. Therefore, the suggested protocol is secure under the DDHP assumption.

**Theorem 6.2:** The suggested protocol provides forward secrecy under the DLP assumption. That is, newly joined members cannot obtain previously established group decryption keys.

**Proof 6.2:** To prove the theorem, we show that newly joined members  $U_k, (m-1 \leq k \leq l)$  cannot obtain a previously established group decryption key,  $GDK = e(X_i m_i^{-1}, \sum X_i), (1 \leq i \leq n-l)$ .

Because of the DLP assumption, the newly joined member  $U_k$  cannot obtain the ephemeral secret  $m_i$  from the broadcasted message  $M_i = m_i PK_n P_{pub}$  for  $(1 \leq i \leq n-l)$ , nor, similarly, can they get the ephemeral secret  $m_n$  from  $X_i$ . Hence,  $U_k$  cannot construct the previously established group decryption key.

**Theorem 6.3:** The proposed protocol provides backward secrecy under the DLP assumption. That is, members who leave the group can get no knowledge of any newly established group decryption keys.

**Proof 6.3:** Let the members  $\{U_{j+1}, \dots, U_{n-1}\}$  decide to leave the group. The remaining members then compute the new group decryption key GDK' (as described in the member leaving phase). However, the new ephemeral secret  $m'_n$  is not known to leaving members,

nor can it be derived from public parameters or the broadcasted message  $T'_n = \left( \frac{m'_n + SK_n}{r'_n} \right) P$  or  $X'_j = SK_n^{-1} m'_n M_j$ , due to the DLP assumption. Hence, leaving members cannot construct the newly established group decryption key, which proves the theorem.

### 7 Performance Evaluation and Comparison

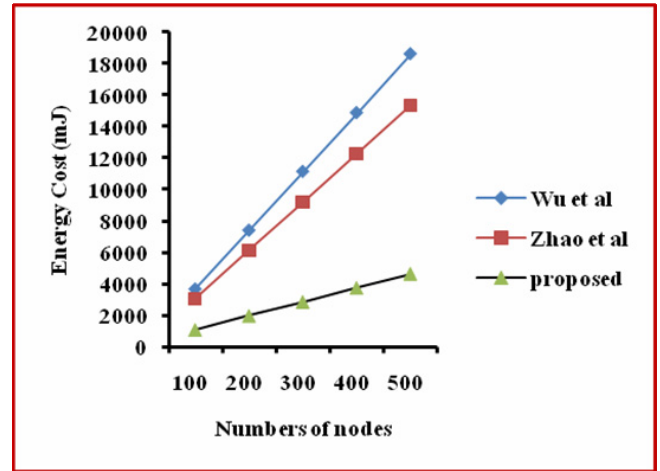
In this section, we evaluate the performance of the proposed protocol and compare it with the protocols of Wu et al. [20] and Zhao et al. [25]. For a more realistic comparison and evaluation, we used the data given in [23]. According to [23], a133-MHz Strong ARM microprocessor was used. Table 1 summarizes the energy costs used to evaluate the performance of the protocols, on the other hand Table 2 compares the efficiency of the protocols. Figure 2 and Figure 3 compare the computational and communication costs, respectively. From Table 2 and Figure 2 and Figure 3, we conclude that the proposed protocol is more efficient in terms of computational and communication resources than the other protocols.

**Table 1.** Comparison table considering energy consumption

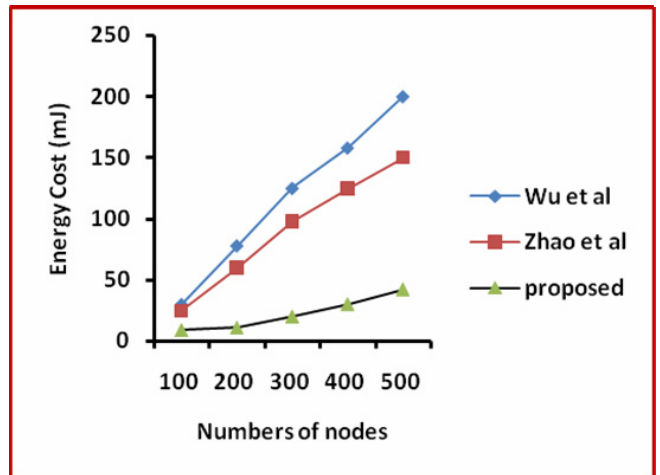
Operation	Energy costs/mJ
Cost of computation for a modular exponentiation (E)	9.1
Cost of computation for a scalar multiplication (M)	8.8
Cost of computation for a Tate pairing (T)	47.0
Sign. Gen. by elliptic curve digital signature algorithm (Sign)	8.8
Sign. Gen. by elliptic curve digital signature verify algorithm (Ver)	10.9
Cost of computation for transmitting a bit	0.00066
Cost of computation for receiving a bit	0.00031

**Table 2.** Comparison table considering efficiency

	Wu et al. [20]	Zhao et al. [25]	Proposed
Round	1	3	2
Forward secrecy	No	Yes	Yes
Contributory GKA	Yes	Yes	Yes
Dynamic	No	Yes	Yes
Computational cost of each subscriber	(n-1) Sign+ (n-1)Ver+ 2nM	3Sign+2nVe r+(n-1) M+4E	5T+nM
Computational cost of the broadcaster	-	-	E+(3n+2) T+(2n+2)M
Transmission cost of each subscriber	n G	(2n + 7) G	(n + 8) G
Transmission cost of the broadcaster	-	-	(n + 3) G  +  U



**Figure 2.** Comparison of computational cost



**Figure 3.** Comparison of communication cost

### 8 Conclusion

Pay TV has evolved security techniques very similar to those required by the IoT based smart homes services. So, the Pay TV are considered as the likely entry points for IoT services into smart homes. Over the years Pay TV has gained thrust among the subscribers, this trust is the biggest opportunity for Pay TV operators for extending their offering with IoT enabled smart home services. Hence the present paper, propose an ID-based authenticated, asymmetric group key agreement (AAGKA) protocol for Pay TV. The group members negotiate a common group encryption key (GEK) and compute a different group decryption key (GDK). So, any broadcaster of a secret message to the group need not join the group. Instead, such a broadcaster can share a secret key with the group members through a GKA protocol. Further, we have shown that the proposed protocol is secure under the DLP and DDHP assumptions in bilinear pairings. The proposed asymmetric protocol was also analyzed to be secure and efficient compared to existing protocols. Furthermore, it is contributory, which is a requirement

for Pay-TV networks.

## Acknowledgments

The authors are grateful to the Deanship of Scientific Research, King Saud University for funding through Vice Deanship of Scientific Research Chairs; Smart technologies; and by the Department of Science and Technology (DST), Government of India under Women Scientist Scheme A (WOS-A) No. under Grant no SR/WOS-A/PM-10/2018(G).

## References

- [1] K. Ashton, That Internet of Things, *RFID Journal*, Vol. 22, No. 7, pp. 97-114, June, 2009.
- [2] D. Boneh, B. Lynn, H. Shacham, Short Signatures from the Weil Pairing, *International Conference on the Theory and Application of Cryptology and Information Security*, Gold Coast, Australia, 2001, pp. 514-532.
- [3] P. Barreto, H. Kim, B. Lynn, M. Scott, Efficient Algorithms for Pairing-based Cryptosystems, *Annual International Cryptology Conference*, Santa Barbara, USA, 2002, pp. 354-368.
- [4] D. Boneh, M. Franklin, Identity-based Encryption from the Weil Pairing, *SIAM Journal on Computing*, Vol. 32, No. 3, pp. 586-615, August, 2003.
- [5] D. Boneh, C. Gentry, B. Waters, Collusion Resistant Broadcast Encryption with Short Cipher texts and Private Keys, *Annual International Cryptology Conference*, Santa Barbara, USA, 2005, pp. 258-275.
- [6] L. Chen, Z. Cheng, N. P. Smart, Identity-based Key Agreement Protocols from Pairings, *International Journal of Information Security*, Vol. 6, No. 4, pp. 213-241, July, 2007.
- [7] T. H. Chen, Y. C. Chen, W. K. Shih, H. W. Wei, An Efficient Anonymous Authentication Protocol for Mobile Pay-TV, *Journal of Network and Computer Applications*, Vol. 34, No. 4, pp. 1131-1137, July, 2011.
- [8] K. Y. Chou, Y. R. Chen, W. Tzeng, An Efficient and Secure Group Key Management Scheme Supporting Frequent Key Updates on Pay-TV Systems, *Network Operations and Management Symposium*, Taipei, Taiwan, 2011, pp. 1-8.
- [9] O. Ermiş, S. Bahtiyar, E. Anarim, M. Ufuk Caglayan, A Comparative Study on the Scalability of Dynamic Group Key Agreement Protocols, *Conference on Availability, Reliability and Security*, Reggio Calabria, Italy, 2017, pp. 306-310.
- [10] A. Fiat, M. Naor, Broadcast Encryption, *Annual International Cryptology Conference*, Santa Barbara, USA, 1993, pp. 480-491.
- [11] M. S. Farash, M. A. Attari, A Provably Secure and Efficient Authentication Scheme for Access Control in Mobile Pay-TV Systems, *Multimedia Tools and Applications*, Vol. 75, No. 1, pp. 405-424, January, 2016.
- [12] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of Things (IoT): A vision, Architectural Elements, and Future Directions, *Future Generation Computer Systems*, Vol. 29, No. 7, pp. 1645-1660, September, 2013.
- [13] H. Kim, J. Nam, S. Kim, D. Won, Secure and Efficient ID-based Group Key Agreement Fitted for Pay-TV, *Pacific-Rim Conference on Multimedia*, Jeju Island, Korea, 2005, pp. 117-128.
- [14] C. Kim, Y. Hwang, P. Lee, Practical Pay-TV Scheme Using Traitor Tracing Scheme for Multiple Channels, *International Workshop on Information Security Applications*, Jeju Island, Korea, 2004, pp. 264-277.
- [15] F. Kanazawa, N. Ohkawa, H. Doi, T. Okamoto, E. Okamoto, Broadcast Encryption with Sender Authentication and Its Duality, *International Conference on Convergence Information Technology*, Gyeongju, South Korea, 2007, pp. 793-798.
- [16] A. Kumar, S. Tripathi, P. Jaiswal, Design of Efficient ID-based Group Key Agreement Protocol Suited for Pay-TV Application, *International Conference on Advances in Computing, Communications and Informatics*, Kochi, India, 2015, pp. 1940-1944.
- [17] J. Wang, Y. Miao, P. Zhou, M. S. Hossain, Sk M. M. Rahman, A Software Defined Network Routing in Wireless Multihop Network, *Journal of Network and Computer*, Vol. 85, pp. 76-83, May, 2017.
- [18] Y. Mu, V. Varadharajan, Robust and Secure Broadcasting, *International Conference on Cryptology*, Chennai, India, 2001, pp. 223-231.
- [19] J. Pontin, *ETC: Bill Joy's Six Webs*, <https://www.technologyreview.com/2005/09/29/230292/etc-bill-joys-six-webs/>, 2005.
- [20] Q. Wu, Y. Mu, W. Susilo, B. Qin, J. Domingo-Ferrer, Asymmetric Group Key Agreement, *International Conference on the Theory and Applications of Cryptographic Techniques*, Cologne, Germany, 2009, pp. 153-170.
- [21] D. H. Phan, D. Pointcheval, V. C. Trinh, Multi-channel broadcast encryption, *8th ACM SIGSAC Symposium on Information, Computer and Communications Security*, Hangzhou, China, 2013, pp. 277-286.
- [22] The Only Coke Machine on the Internet, Carnegie Mellon University, School of Computer Science.
- [23] C. H. Tan, J. C. M. Teo, Energy-efficient ID-based Group Key Agreement Protocols for Wireless Networks, *20th International Parallel and Distributed Processing Symposium*, Rhodes Island, Greece, 2006, pp. 1-8.
- [24] M. Weiser, The Computer for the 21st Century, *Scientific American*, Vol. 265, No. 3, pp. 94-105, September, 1991.
- [25] X. Zhao, F. Zhang, H. Tian, Dynamic Asymmetric Group Key Agreement for Ad Hoc Networks, *Ad Hoc Networks*, Vol. 9, No. 5, pp. 928-939, July, 2011.
- [26] L. Zhang, Q. Wu, B. Qin, J. Domingo-Ferrer, Provably Secure One-round Identity-based Authenticated Asymmetric Group Key Agreement Protocol, *Information Sciences*, Vol. 181, No. 19, pp. 4318-4329, October, 2011.
- [27] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, Z. Dong, Round-efficient and Sender-unrestricted Dynamic Group Key Agreement Protocol for Secure Group Communications, *IEEE Transactions on Information Forensics and Security*, Vol. 10, No. 11, pp. 2352-2364, November, 2015.

- [28] L. Zhang, OTIBAAGKA: A New Security Tool for Cryptographic Mix-Zone Establishment in Vehicular Ad Hoc Networks, *IEEE Transactions on Information Forensics and Security*, Vol. 12, No. 12, pp. 2998-3010, December, 2017.
- [29] J. Li, L. Zhang, Sender Dynamic, Non-Repudiable, Privacy-Preserving and Strong Secure Group Communication Protocol, *Information Sciences*, Vol. 414, pp. 187-202, November, 2017.

## Biographies



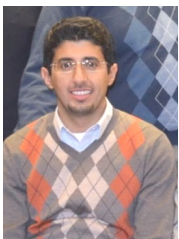
**Shaheena Khatoon** is a full-time research scholar at Pt. Ravishankar Shukla University, India. She received the B.Sc., M.Sc. and MPhil degree in Mathematics from the same university in 2005, 2007 and 2009 respectively. She was awarded the gold medal for securing highest marks in the M.Sc. program. Her research interests are public key cryptography, information security and applied mathematics.



**Sk Md Mizanur Rahman** is a full-time professor in Centennial College. He has published around hundred peer reviewed journals and conference research articles and an industrial patent on cryptographic key generation and protection. Dr. Rahman's main research focuses on cryptography, software and network security, machine learning in information security.



**Raylin Tso** is a Professor at the Department of Computer Science, National Chengchi University, Taiwan. He received his Ph.D. degree from Tsukuba University, Japan. His research interests include cryptography, privacy preserving technologies, and blockchain. He is also the Editor-in-Chief of the International Journal of Information and Computer Security.



**Mohammed F. Alhamid** received his Ph.D. degree in computer science from the University of Ottawa, Canada. He is currently an Assistant Professor with the Software Engineering Department, King Saud University, Riyadh, Saudi Arabia. His research interests include Artificial Inteliginet and Machine Learning.

## Research Article

# Edge Theoretic Extended Contractions and Their Applications

R. Rajagopalan <sup>1</sup>, Ekta Tamrakar,<sup>2</sup> Fahad. S. Alshammari <sup>1</sup>, H. K. Pathak,<sup>2</sup>  
and Reny George <sup>1,3</sup>

<sup>1</sup>Department of Mathematics, College of Science and Humanities at Al-Kharj, Prince Sattam Bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia

<sup>2</sup>School of Studies in Mathematics, Pt. Ravishankar Shukla University, Raipur 492010, India

<sup>3</sup>PG Department of Mathematics and Computer Science, St. Thomas College, Bhilai, Chhattisgarh State, India

Correspondence should be addressed to R. Rajagopalan; r.gopalan@psau.edu.sa and Reny George; renygeorge02@yahoo.com

Received 13 September 2021; Revised 15 October 2021; Accepted 18 October 2021; Published 9 November 2021

Academic Editor: Huseyin Isik

Copyright © 2021 R. Rajagopalan et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Edge theoretic extended contractions are introduced and coincidence point theorems and common fixed-point theorems are proved for such contraction mappings in a metric space endowed with a graph. As further applications, we have proved the existence of a solution of a nonlinear integral equation of Volterra type and given a suitable example in support of our result.

## 1. Introduction and Preliminaries

The celebrated Banach contraction principle is a motivation for many fixed-point theorems. It guarantees the existence and uniqueness of solution of various equations arising in mathematics. The initial generalizations of Banach's result came up in the form of Kannan's contraction, Chatterjea's contraction, Reich's contraction, Ćirić's contraction, Hardy-Roger's contraction, and Ćirić's quasicontraction. Among these, Ćirić's quasicontraction is the most general form in the sense that any mapping which does not satisfy Ćirić's quasicontraction does not satisfy any of the previously mentioned contractions. Further, these results have been widely investigated and many interesting applications have been found by many authors (see [1–7]).  $F$ -contraction and fixed-point theorem for  $F$ -contraction mappings were introduced by Wardowski [8] as a generalisation of the Banach contraction principle.

**Definition 1** (see [8]). Consider the collection of functions  $F : (0, \infty) \rightarrow \mathbb{R}$  satisfying the following:

- (F<sub>1</sub>)  $F$  is strictly increasing
- (F<sub>2</sub>) If  $\{\alpha_n\} \subset (0, \infty)$  is a sequence, then  $\lim_{n \rightarrow \infty} \alpha_n = 0$  iff  $\lim_{n \rightarrow \infty} F(\alpha_n) = -\infty$
- (F<sub>2</sub>) There exists  $k \in (0, 1)$  such that  $\lim_{\gamma \rightarrow 0^+} \gamma^k F(\gamma) = 0$

An operator  $T : X^i, d_i \rightarrow X^i$  is an  $\mathcal{F}$ -contraction if we can find  $\tau > 0$  such that

$$\forall x^i, y^i \in X^i, d_i(Tx^i, Ty^i) > 0 \implies \tau + F(d_i(Tx^i, Ty^i)) \leq F(d_i(x^i, y^i)). \quad (1)$$

Later, the concept of  $F$ -weak contraction and ordered  $F$ -contractions was introduced by Wardowski and Van Dung [9] and Durmaz et al. [10], respectively. In 2016, Sawangsup et al. [11] extended the  $F$ -contraction using a relation theoretic approach which was later generalised by Imdad et al. [12] and Alfaqih et al. [13]. Espinola and Kirk [14] introduced graph theory in fixed-point theory, and Jachymski [15] continued this idea by using different views thereby introducing the  $G$ -contraction and proved fixed-point theorem for a  $G$ -contraction mapping. These ideas were further extended and generalised by [16–24].

It is interesting to note that all these contraction conditions ensure the existence of a unique fixed point or common fixed point of the mappings under consideration. However, it is observed that a mapping which possesses nonunique fixed points does not satisfy the above contractions, for if  $x^i$  and  $y^i$  are any two fixed points of a self-map  $T^i$  of a metric space  $(X^i, d^i)$ , then



$$\begin{aligned}
d^i(T^i x^j, T^i y^j) &= d^i(x^j, y^j) \\
&= \max \left\{ d^i(x^j, y^j), d^i(x^j, T^i x^j), d^i(y^j, T^i y^j), \frac{d^i(x^j, T^i y^j) + d^i(y^j, T^i x^j)}{2} \right\}, \\
d^i(T^i x^j, T^i y^j) &= d^i(x^j, y^j) \\
&= \max \left\{ d^i(x^j, y^j), d^i(x^j, T^i x^j), d^i(y^j, T^i y^j), d^i(x^j, T^i y^j), d^i(y^j, T^i x^j) \right\},
\end{aligned} \tag{2}$$

and thus, we see that  $T^i$  does not satisfy Ćirić's quasicontraction, Wardowski's  $F$ -contraction, and Wardowski and Van Dung's  $F$ -weak contraction. Thus, these contraction conditions cannot be used to prove the existence of nonunique fixed points of a function defined in a metric space. On the other hand, many equations obtained by modeling various problems of engineering and science need not necessarily have a unique solution. Thus, it becomes meaningful to obtain extended forms of above contractions which will ensure the existence of nonunique fixed points of self-maps defined in a metric space.

Motivated by this fact, in this paper, we have introduced extended  $\mathcal{FW}$ -contraction (Jungck-Wardowski contraction), extended  $\mathcal{CW}$ -contraction (Ćirić-Wardowski contraction), and extended  $\mathcal{CQ}$ -contraction (Ćirić-Wardowski quasicontraction) and established fixed-point theorems which will ensure the existence of nonunique fixed points of a self-map and coincidence points of a pair of self-maps, respectively, in a metric space endowed with a graph. As an application of our result, we have also proven the existence of solution of a nonlinear integral equation of Volterra type.

Throughout this paper, we consider the metric space  $(X^j, d_j)$  to be endowed with the graph  $G = (V(G), E(G))$ ,  $V(G) = X^j$ , and  $\Delta \subseteq E(G)$ ;  $\Delta = \{(x^j, x^j) : x^j \in X^j\}$ .

**Definition 2** (see [15]). A sequence  $\{x_n^j\} \subseteq X^j$  is edge-preserving if  $(x_n^j, x_{n+1}^j) \in E(G)$  for all  $n \in \mathbb{N}_0$ .

**Definition 3.** Let  $g : X^j \rightarrow X^j$ . A sequence  $\{x_n^j\} \subseteq X^j$  is  $g$ -edge-preserving if  $(gx_n^j, gx_{n+1}^j) \in E(G)$  for all  $n \in \mathbb{N}_0$ .

**Definition 4.**  $T : X^j \rightarrow X^j$  is edge-preserving if  $(x^j, y^j) \in E(G)$  implies  $(Tx^j, Ty^j) \in E(G)$ .

**Definition 5.**  $T, g : X^j \rightarrow X^j$  is  $g$ -edge-preserving if for all  $x^j, y^j \in X$ ,  $(gx^j, gy^j) \in E(G)$  implies  $(Tx^j, Ty^j) \in E(G)$ .

**Definition 6** (see [15]).  $(X^j, d_j)$  is edge-complete if every edge-preserving Cauchy sequence in  $X^j$  converges to some point in  $X^j$ .

**Definition 7** (see [15]).  $T : X^j \rightarrow X^j$  is edge-continuous at  $x^j$  if  $\{x_n^j\} \rightarrow x^j$  implies  $\{Tx_n^j\} \rightarrow Tx^j$  for any edge-preserving sequence  $\{x_n^j\} \subseteq X^j$ . If  $T$  is edge-continuous at all  $x^j \in X^j$ , then  $T$  is an edge-continuous mapping.

**Definition 8.** Let  $T, g : X^j \rightarrow X^j$  and  $x^j \in X^j$ . We say that  $T$  is  $g$ -edge continuous at  $x^j$  if  $\{gx_n^j\} \rightarrow gx^j$  implies  $\{Tx_n^j\}$

$\rightarrow Tx^j$  for any edge-preserving sequence  $\{x_n^j\} \subseteq X^j$ . If  $T$  is  $g$ -edge continuous at all  $x^j \in X^j$ , then  $T$  is an  $g$ -edge continuous mapping.

**Definition 9.**  $(T, g)$  is edge-compatible if and only if for any sequence  $T$  and  $g$  edge-preserving sequence  $\{x_n^j\} \subseteq X$ ,  $\lim_{n \rightarrow \infty} gx_n^j = \lim_{n \rightarrow \infty} Tx_n^j = x \in X^j$  implies  $\lim_{n \rightarrow \infty} d_j(gTx_n^j, Tgx_n^j) = 0$ .

We will use the following lemmas taken from [25, 26]:

**Lemma 10.** (see [25]). Let  $M$  be a nonempty set and  $g : M \rightarrow M$ . Then, there exists a subset  $S \subseteq M$  such that  $g(S) = g(M)$  and  $g : S \rightarrow S$  is one-one.

**Lemma 11** (see [26]). Let  $\{x_n^j\}$  be a sequence in metric space  $(X^j, d_j)$  such that  $\lim_{n \rightarrow +\infty} d_j(x_n^j, x_{n+1}^j) = 0$ . If  $\{x_n^j\}$  is not Cauchy in  $(X^j, d_j)$ , then there exist  $\xi > 0$  and sequences  $\{n_k\}$  and  $\{p_k\}$  in  $\mathbb{N}$  such that  $n_k > p_k > k$ , and the sequences

$$\begin{aligned}
&\left\{ d_j(x_{n_k}^j, x_{p_k}^j) \right\}, \left\{ d_j(x_{n_k+1}^j, x_{p_k}^j) \right\}, \left\{ d_j(x_{n_k}^j, x_{p_k-1}^j) \right\}, \\
&\left\{ d_j(x_{n_k+1}^j, x_{p_k-1}^j) \right\}, \left\{ d_j(x_{n_k+1}^j, x_{p_k+1}^j) \right\},
\end{aligned} \tag{3}$$

tend to be  $\xi^+$ , as  $k \rightarrow +\infty$ .

## 2. Edge Theoretic Extended Contractions

Let  $\mathbb{F}$  be the collection of all nondecreasing continuous functions  $\mathcal{F} : (0, \infty) \rightarrow \mathbb{R}$ .

**Example 1.** Some examples of function belonging to the class  $\mathbb{F}$  are

$$\begin{aligned}
\mathcal{F}(y) &= y^2, \\
\mathcal{F}(y) &= \ln y, \\
\mathcal{F}(y) &= y - \frac{1}{y}, \\
\mathcal{F}(y) &= \ln \left( \frac{y}{3} + \sin y \right).
\end{aligned} \tag{4}$$

Let  $A \subset [0, \infty)$  and  $\Xi$  be the collection of all continuous functions  $\xi : A \times A \rightarrow [0, \infty)$  satisfying the following:

- (i)  $\alpha = 0$  or  $\beta = 0$  implies  $\xi(\alpha, \beta) = 0$
- (ii)  $\alpha > 0$  and  $\beta > 0$  implies  $\xi(\alpha, \beta) > 0$

$$\sup_{\alpha, \beta \in A} \xi(\alpha, \beta) = \zeta > 0. \tag{5}$$

Some examples of function  $\xi$  are as follows:

**Example 2.**

- (i)  $\xi(\alpha, \beta) = k.\alpha\beta$ , for some  $k > 0$
- (ii)  $\xi(\alpha, \beta) = \min \{\alpha, \beta\}$
- (iii)  $\xi(\alpha, \beta) = \alpha/(1 + \ln \beta)$
- (iv)  $\xi(\alpha, \beta) = (\alpha + \beta)/(1 + \ln (\alpha\beta))$
- (v)  $\xi(\alpha, \beta) = \alpha\beta(\alpha + \beta)$
- (vi)  $\xi(\alpha, \beta) = \alpha\beta/(1 + \alpha\beta)$
- (vii)  $\xi(\alpha, \beta) = \ln (1 + K.\min \{\alpha, \beta\})$

Let  $\Theta$  be the family of all functions  $\theta : [0, \infty) \rightarrow R$  which satisfy the following conditions:

- $(\theta_1)\theta$  is strictly increasing
- $(\theta_2)\theta(t) = 0$  iff  $t = 0$
- $(\theta_3)\sup_{t>0}\theta(t) = \lambda$  for some  $\lambda > 0$

Example 3. Some examples of elements of  $\Theta$  are

$$\begin{aligned} \theta(t) &= \frac{t}{1+t}, \\ \theta(t) &= \ln \left( 1 + \frac{t}{1+t} \right), \\ \theta(t) &= \frac{t}{1 + \ln(1+t)}. \end{aligned} \tag{6}$$

Definition 12. A pair of mappings  $T, g : X^j \rightarrow X^j$  is an  $\xi$ -extended  $\mathcal{FW}$ -contraction pair if we can find  $\tau > 0, F \in \mathcal{F}, \xi \in \Xi$ , and  $L \geq 0$  such that for all  $x^j, y^j \in X^j$ ,

$$\begin{aligned} d_j(Tx^j, Ty^j) > 0 &\implies \tau + F(d_j(Tx^j, Ty^j)) \\ &\leq \mathcal{F}(d_j(gx^j, gy^j)) + L\xi(d_j(gy^j, Tx^j), d_j(gx^j, Ty^j)), \end{aligned} \tag{7}$$

Definition 13. A pair of mappings  $T, g : X^j \rightarrow X^j$  is an  $\xi$ -extended  $\mathcal{EW}$ -contraction pair if we can find  $\tau > 0, F \in \mathcal{F}, \xi \in \Xi$ , and  $L \geq 0$  such that for all  $x^j, y^j \in X^j$ ,

$$\begin{aligned} d_j(Tx^j, Ty^j) > 0 &\implies \tau + F(d_j(Tx^j, Ty^j)) \\ &\leq \mathcal{F}(M^j(x^j, y^j)) + L\xi(d_j(gy^j, Tx^j), d_j(gx^j, Ty^j)), \end{aligned} \tag{8}$$

where

$$M^j(x^j, y^j) = \max \left\{ d_j(gx^j, gy^j), d_j(gx^j, Tx^j), d_j(gy^j, Ty^j), \frac{d_j(gx^j, Ty^j) + d_j(gy^j, Tx^j)}{2} \right\}. \tag{9}$$

Definition 14. A pair of mappings  $T, g : X^j \rightarrow X^j$  is an  $\xi$ -extended  $\mathcal{EQ}$ -contraction pair provided that there is a  $\tau > 0, F \in \mathcal{F}, \xi \in \Xi$ , and  $L \geq 0$  such that for all  $x^j, y^j \in X^j$ ,

$$\begin{aligned} d_j(Tx^j, Ty^j) > 0 &\implies \tau + F(d_j(Tx^j, Ty^j)) \\ &\leq \mathcal{F}(M^*(x^j, y^j)) + L\xi(d_j(gy^j, Tx^j), d_j(gx^j, Ty^j)), \end{aligned} \tag{10}$$

where

$$\begin{aligned} M^*(x^j, y^j) &= \max \{ d_j(gx^j, gy^j), d_j(gx^j, Tx^j), d_j \\ &\cdot (gy^j, Ty^j), d_j(gx^j, Ty^j), d_j(gy^j, Tx^j) \}. \end{aligned} \tag{11}$$

Definition 15. In Definitions 12, 13, and 14, if conditions (7), (8), and (10) are satisfied only for all  $x^j, y^j \in X^j$  with  $(x^j, y^j) \in E(G)$ , then the pair  $(T, g)$  is an  $\xi$ -extended  $\mathcal{FW}$ -edge contraction,  $\xi$ -extended  $\mathcal{EW}$ -edge contraction, and  $\xi$ -extended  $\mathcal{EQ}$ -edge contraction, respectively.

Definition 16.  $T, g : X^j \rightarrow X^j$  is a  $\theta$ -extended  $\mathcal{FW}$ -edge contraction if we can find  $\tau > 0, F \in \mathcal{F}$ , and  $\theta \in \Theta$  such that for all  $x^j, y^j \in X^j$  with  $(gx^j, gy^j) \in E(G)$ ,

$$\begin{aligned} d_j(Tx^j, Ty^j) > 0 &\implies \tau + F(d_j(Tx^j, Ty^j)) \\ &\leq \mathcal{F}(d_j(gx^j, gy^j)) + L\theta(d_j(gy^j, Tx^j)). \end{aligned} \tag{12}$$

Definition 17. A pair of mappings  $T, g : X^j \rightarrow X^j$  is a  $\theta$ -extended  $\mathcal{EW}$ -edge contraction if we can find  $\tau > 0, F \in \mathcal{F}$ , and  $\theta \in \Theta$  such that

$$\begin{aligned} d_j(Tx^j, Ty^j) > 0 &\implies \tau + F(d_j(Tx^j, Ty^j)) \\ &\leq \mathcal{F}(M^j(x^j, y^j)) + L\theta(d_j(gy^j, Tx^j)), \end{aligned} \tag{13}$$

for all  $x^j, y^j \in X^j$  with  $(gx^j, gy^j) \in E(G)$  and  $M^j(x^j, y^j)$ , is as in (9).

If  $g = I$  in the above definitions, then  $T$  is an  $\xi$ -extended  $F$ -contraction mapping,  $\xi$ -extended  $\mathcal{EW}$ -contraction mapping,  $\theta$ -extended  $\mathcal{FW}$ -edge contraction mapping, and  $\theta$ -extended  $\mathcal{EW}$ -edge contraction mapping, respectively.

Property (\*). The space  $(X^j, d_j)$  is said to have property(\*) if for any edge-preserving sequence  $\{x_n^j\} \in X$  such that  $\{x_n^j\} \rightarrow x$ ; there exists a subsequence  $\{x_{n_k}^j\}$  of  $\{x_n^j\}$  such that  $(x_{n_k}^j, x) \in E(G)|_X$  for all  $k \in \mathbb{N}_0$

*Example 4.* Let  $X = [0, 1] \cup \{2\}$ ,  $d_j(x^i, y^j) = |x^i - y^j|$ , and  $Tx^i = x^{i^4}/8$  for all  $x^i \in X$ . Then, at  $x^i = 0$  and  $y^j = 2$ ,  $T$  does not satisfy the conditions of Ciric's quasicontraction, Wardowski's  $F$ -contraction, and Wardowski and Van Dung's  $F$ -weak contraction. However,  $T$  is an  $\xi$ -extended  $F$ -contraction with  $\tau = \ln(2)$ , as shown below:

Let  $F : (0, \infty) \rightarrow \mathbb{R}$  be defined by

$$F(t) = \ln(t), \quad (14)$$

and  $\xi(\alpha, \beta) = \ln(1 + K \cdot \min\{\alpha, \beta\})$ .

*Case 1.*  $x^i, y^j \in [0, 1]$ . Clearly,

$$\begin{aligned} d_j(Tx^i, Ty^j) &= \frac{1}{8} \left| x^{i^4} - y^{j^4} \right| \leq \frac{1}{8} \left| x^i - y^j \right| \left( |x^i + y^j| |x^{i^2} + y^{j^2}| \right) \\ &\leq \frac{1}{4} \left| x^i - y^j \right| \left( |x^i + y^j| \right) < \frac{1}{2} \left| x^i - y^j \right| \leq \frac{1}{2} d_j(x^i, y^j). \end{aligned} \quad (15)$$

Then, we have  $\ln(d_j(Tx^i, Ty^j)) < \ln(1/2 d_j(x^i, y^j))$  or

$$\ln 2 + \ln(d_j(Tx^i, Ty^j)) < \ln(d_j(x^i, y^j)) + L\xi(d_j(gy^j, Tx^i), d_j(gx^i, Ty^j)). \quad (16)$$

*Case 2.*  $x^i \in [0, 1]$  and  $y^j = 2$ . Note that in this case,  $d_j(x^i, y^j) \geq 1$ .

$$\begin{aligned} d_j(Tx^i, Ty^j) &= \left| \frac{x^{i^4}}{8} - 2 \right| \leq \frac{1}{2} + 2 \min \left\{ |x^i - 2|, \left| 2 - \frac{x^{i^4}}{8} \right| \right\} \\ &\Rightarrow d_j(Tx^i, Ty^j) \\ &\leq \frac{1}{2} d_j(x^i, y^j) \left( 1 + 8 \min \left\{ |x^i - 2|, \left| 2 - \frac{x^{i^4}}{8} \right| \right\} \right) \\ &\Rightarrow \ln(d_j(Tx^i, Ty^j)) \\ &\leq -\ln 2 + \ln(d_j(x^i, y^j)) + \ln \left( 1 + 8 \min \left\{ |x^i - 2|, \left| 2 - \frac{x^{i^4}}{8} \right| \right\} \right) \\ &\Rightarrow \ln 2 + \ln(d_j(Tx^i, Ty^j)) \\ &\leq \ln(d_j(x^i, y^j)) + \ln \left( 1 + 8 \min \left\{ |x^i - 2|, \left| 2 - \frac{x^{i^4}}{8} \right| \right\} \right) \\ &\Rightarrow \ln 2 + F(d_j(Tx^i, Ty^j)) \\ &\leq F(d_j(x^i, y^j)) + \xi(1 + 8 \min \{d_j(x^i, y^j), d_j(y^j, Tx^i)\}). \end{aligned} \quad (17)$$

*Example 5.* Let  $X^j = [0, \infty)$ ,  $d_j(x^j, y^j) = |x^j - y^j|$ ,  $E(G) = \{(n, n), (n, n+1) : n = 0, 1, 2, 3, \dots\}$ , and  $T, g : X^j \rightarrow X^j$  be given by

$$\begin{aligned} Tx^j &= \begin{cases} 0, & \text{if } 0 \leq x^j \leq 1, \\ x^j - 1, & \text{if } x^j \geq 1, \end{cases} \\ gx^j &= x^j + (n+1 - x^j)(x^j - n), \quad \text{whenever } n \leq x^j \leq n+1. \end{aligned} \quad (18)$$

Let  $F : (0, \infty) \rightarrow \mathbb{R}$  be defined by

$$F(t) = t - \frac{1}{t}, \quad (19)$$

and  $\theta \in \Theta$  be defined by  $\theta(t) = t/(t+1)$ . Then,

$$\begin{aligned} \tau + F(d_j(T(n), T(n+1))) &\leq F(d_j(g(n), g(n+1))) \\ &\quad + L\theta(d_j(g(n+1), T(n))) \\ &\Rightarrow \tau + F(d_j(n-1, n)) \leq F(d_j(n, n+1)) \\ &\quad + L\theta(d_j(n+1, n-1)) \\ &\Rightarrow \tau \leq F(1) - F(1) + L\theta(2) \Rightarrow \tau \leq L\theta(2). \end{aligned} \quad (20)$$

Hence, for any  $0 < \tau < 2/3$  and  $L = 1$ , (13) is satisfied and thus  $(T, g)$  is a  $\theta$ -extended  $\mathcal{W}\mathcal{F}$ -edge contraction and  $\theta$ -extended  $\mathcal{W}\mathcal{C}$ -edge contraction. However, the pair  $(T, g)$  is neither an  $\xi$ -extended  $\mathcal{F}\mathcal{W}$ -edge contraction pair nor an  $\xi$ -extended  $\mathcal{C}\mathcal{W}$ -contraction pair. If we take  $g$  to be the identity mapping, then  $T$  is a  $\theta$ -extended  $\mathcal{F}\mathcal{W}$ -edge contraction mapping and  $\theta$ -extended  $\mathcal{C}\mathcal{W}$ -edge contraction mapping. However, again  $T$  is none of Wardowski's  $F$ -contraction, Wardowski and Van Dung's  $F$ -weak contraction, and Ciric's quasicontraction.

### 3. Main Results

We start by proving the following main theorems:

**Theorem 18.** Suppose  $(X^j, d_j)$  be endowed with a graph  $G$  satisfying transitivity property, and the following conditions hold for  $T, g : X^j \rightarrow X^j$ .

- (a)  $(gx_0^j, Tx_0^j) \in E(G)$  for some  $x_0^j \in X^j$
- (b)  $T$  is  $g$ -edge preserving
- (c)  $(T, g)$  is an  $\theta$ -extended  $\mathcal{C}\mathcal{W}$ -edge contraction pair of mappings
- (d)  $(d_1)$  There exists an edge-complete subset  $M^j$  of  $X^j$  for which  $T(X^j) \subseteq M^j \subseteq g(X^j)$
- (d<sub>2</sub>) One of the following conditions holds:

- (i)  $T$  is  $g$ -edge continuous
- (ii)  $T$  and  $g$  are continuous
- (iii)  $E(G)|_{X^j}$  satisfies property(\*)

Then, the pair  $(T, g)$  has a coincidence point.

*Proof.* In view of the assumption (a), we have  $(gx_0^j, Tx_0^j) \in E(G)$ . If  $Tx_0^j = gx_0^j$ , then  $x_0$  is a coincidence point of  $(T, g)$ , i.e.,  $\text{Coin}(T, g) \neq \emptyset$ , and there is nothing to prove. Assume

that  $Tx_0^j \neq gx_0^j$ ; then, since  $T(X^j) \subseteq g(X^j)$ , there exists  $x_1^j \in X^j$  such that  $gx_1^j = Tx_0^j$ .  $\square$

Similarly, there is  $x_2^j \in X^j$  such that  $gx_2^j = Tx_1^j$  with  $(gx_1^j, gx_2^j) \in E(G)$  and consequently  $(Tx_0^j, Tx_1^j) \in E(G)$ . Inductively, one can construct a sequence  $\{x_n^j\} \subseteq X^j$  such that

$$gx_{n+1}^j = Tx_n^j, \text{ for all } n \in \mathbb{N}_0, \tag{21}$$

with

$$(gx_n^j, gx_{n+1}^j) \in E(G) \text{ for all } n \in \mathbb{N}_0, \tag{22}$$

and consequently, as  $T$  is  $g$ -edge preserving,

$$(Tx_n^j, Tx_{n+1}^j) \in E(G). \tag{23}$$

Now, if  $Tx_{n_0}^j = Tx_{n_0}^j$  for some  $n_0 \in \mathbb{N}_0$ , then  $x_{n_0}$  is a coincidence point  $(T, g)$  and we are done. Assume that  $Tx_n^j \neq Tx_{n+1}^j$ , for all  $n \in \mathbb{N}_0$ . On using (21), (22), (23), and condition (c), we have

$$\begin{aligned} \tau + F(d(gx_n^j, gx_{n+1}^j)) &= \tau + F(d(Tx_{n-1}^j, Tx_n^j)) \\ &\leq F(M(x_{n-1}^j, x_n^j)) + L\theta(d(gx_n^j, Tx_{n-1}^j)). \end{aligned} \tag{24}$$

Now,

$$\begin{aligned} M(x_{n-1}^j, x_n^j) &= \max \left\{ d_j(gx_{n-1}^j, gx_n^j), d_j(gx_{n-1}^j, Tx_{n-1}^j), d_j(gx_n^j, Tx_n^j), \frac{d_j(gx_{n-1}^j, Tx_n^j) + d_j(gx_n^j, Tx_{n-1}^j)}{2} \right\} \\ &= \max \left\{ d_j(gx_{n-1}^j, gx_n^j), d_j(gx_n^j, gx_{n+1}^j) \right\}, \end{aligned}$$

$$\theta(d(gx_n^j, Tx_{n-1}^j)) = \theta(d(gx_n^j, gx_n^j)) = 0. \tag{25}$$

Thus, we get

$$\tau + F(d(gx_n^j, gx_{n+1}^j)) \leq F(\max \{d_j(gx_{n-1}^j, gx_n^j), d_j(gx_n^j, gx_{n+1}^j)\}), \tag{26}$$

i.e.,

$$F(d(gx_n^j, gx_{n+1}^j)) < \tau + F(d(gx_n^j, gx_{n+1}^j)) \leq F(d(gx_{n-1}^j, gx_n^j)). \tag{27}$$

Since  $F$  is nondecreasing, we get  $d(gx_n^j, gx_{n+1}^j) < d(gx_{n-1}^j, gx_n^j)$ . This further means that  $d_j(x_n^j, x_{n+1}^j) \rightarrow \delta \geq 0$  as  $n \rightarrow +\infty$ . If  $\delta > 0$ , we obtain from (27) that

$$F(\delta +) \leq \tau + F(\delta +) \leq F(\delta +), \tag{28}$$

which is a contradiction. Hence,  $\lim_{n \rightarrow +\infty} d_j(x_n^j, x_{n+1}^j) = 0$ . Suppose the sequence  $\{gx_n^j\}$  is not a Cauchy sequence. By Lemma 11, there exist  $\xi > 0$  and sequences  $\{n_k\}$  and  $\{p_k\}$  in  $\mathbb{N}$  such that  $n_k > p_k > k$ , such that the sequences  $d_j(x_{n_k}^j, x_{p_k}^j)$  and  $d_j(x_{n_k+1}^j, x_{p_k+1}^j)$  tend to be  $\xi^+$ , as  $k \rightarrow +\infty$ . By (27) we get

$$\tau + F(\xi^+ +) \leq F(\xi^+ +), \tag{29}$$

which is a contradiction. So sequence  $\{gx_n^j\}$  is a Cauchy sequence.

By (21) and (22),  $\{gx_n^j\}$  is an edge-preserving Cauchy sequence in  $T(X^j) \subset M^j$ , and since  $M^j$  is edge-complete, there exists  $y^j \in M^j$  such that  $\{gx_n^j\} \rightarrow y^j$ . As  $M^j \subseteq g(X^j)$ , there exists  $u^j \in X^j$  such that  $y^j = gu^j$ . Hence, on using (21), we obtain

$$\lim_{n \rightarrow \infty} gx_n^j = \lim_{n \rightarrow \infty} Tx_n^j = gu^j. \tag{30}$$

Now, suppose condition  $(d_2(i))$  is true. Using (22) and (30), we obtain

$$\lim_{n \rightarrow \infty} Tx_n^j = Tu^j. \tag{31}$$

By (30) and (31), we have

$$Tu^j = gu^j. \tag{32}$$

Suppose condition  $(d_2(ii))$  is true. By Lemma 10, there is  $S \subseteq X^j$  for which  $g(S) = g(X^j)$  and  $g : S \rightarrow S$  is one-one. Consider the function  $f : g(S) \rightarrow g(X^j)$  given by

$$f(gs) = Ts \text{ (} gs \in g(S), s \in S \text{)}. \tag{33}$$

As  $g : S \rightarrow X^j$  is one-one and  $T(X^j) \subseteq g(X^j)$ ,  $f$  is well-

defined. Since  $T$  and  $g$  are continuous,  $f$  is also continuous by condition  $(d_1)$  of the hypothesis  $T(X^j) \subseteq M^j \subseteq g(S)$ . Thus, we have  $\{x_n^j\} \subseteq S$  and  $u^j \in S$ . Therefore,

$$Tu^j = f(gu^j) = f\left(\lim_{n \rightarrow \infty} gx_n^j\right) = \lim_{n \rightarrow \infty} f(gx_n^j) = \lim_{n \rightarrow \infty} Tx_n^j = gu^j. \quad (34)$$

Suppose condition  $(d_2(\text{iii}))$  is true; that is,  $E(G)|_{X^j}$  satisfied Property $(*)$ . Since  $\{gx_n^j\} \subseteq X$ , it follows that  $\{g x_n^j\}$  is  $E(G)|_{X^j}$ -preserving (due to (22)) and  $\{gx_n^j\} \rightarrow gu^j$  (by (30)) and so we have a subsequence  $\{gx_{n_k}^j\} \subseteq \{g x_n^j\}$  such that

$$\left(gx_{n_k}^j, gu^j\right) \in E(G)|_X, \quad \text{for all } k \in \mathbb{N}_0. \quad (35)$$

Using (35) and condition  $(b)$  of the hypothesis, we have

$$\left(Tx_{n_k}^j, Tu^j\right) \in E(G)|_{X^j} \subseteq S, \quad \text{for all } k \in \mathbb{N}_0. \quad (36)$$

Now, let  $P^j = \{k \in \mathbb{N} : Tx_{n_k}^j = Tu^j\}$ .

If  $P^j$  is finite, then  $\{Tx_{n_k}^j\}$  has a subsequence  $\{Tx_{n_{k_i}}^j\}$  such that  $Tx_{n_{k_i}}^j \neq Tu^j$  for all  $i \in \mathbb{N}$ . Also,  $(gx_{n_{k_i}}^j, gu^j) \in E(G)|_X \subseteq E(G)$ . Thus, we have

$$\begin{aligned} \tau + F\left(d\left(Tx_{n_{k_i}}^j, Tu^j\right)\right) &\leq F\left(M\left(x_{n_{k_i}}^j, u^j\right)\right) + L\theta\left(d\left(gu^j, Tx_{n_{k_i}}^j\right)\right), \\ M\left(x_{n_{k_i}}^j, u^j\right) &= \max \left\{ d_j\left(gx_{n_{k_i}}^j, gu^j\right), d_j\left(gx_{n_{k_i}}^j, Tx_{n_{k_i}}^j\right), d_j\left(gu^j, Tu^j\right), \frac{d_j\left(gx_{n_{k_i}}^j, Tu^j\right) + d_j\left(gu^j, Tgx_{n_{k_i}}^j\right)}{2} \right\}. \end{aligned} \quad (37)$$

Letting  $i \rightarrow \infty$ , we obtain  $M(x_{n_{k_i}}^j, u^j) = d_j(gu^j, Tu^j)$  and  $\theta(d(gu^j, Tx_{n_{k_i}}^j)) = 0$ . Thus, we get

$$\tau + F(d_j(gu^j, Tu^j)) \leq F(d(gu^j, Tu^j)), \quad (38)$$

which is a contradiction. Hence,  $P^j$  is not finite. Thus,  $P^j$  is infinite and so  $\{Tx_{n_k}^j\}$  has a subsequence  $\{Tx_{n_{k_i}}^j\}$  such that  $Tx_{n_{k_i}}^j = Tu^j$  for all  $i \in \mathbb{N}$ . Thus,  $\lim_{i \rightarrow \infty} Tx_{n_{k_i}}^j = Tu^j$ . As  $\lim_{n \rightarrow \infty} Tx_n^j = gu^j$  (by (30)), we get  $Tu^j = gu^j$ .

**Theorem 19.** *If, in addition to hypothesis (a) - (d) of Theorem 18, we assume the following:*

(i) For all  $u^j, v^j \in \text{Coin}(T, g)$ ,

$$\begin{aligned} d_j(Tu^j, Tv^j) > 0 &\implies \tau + F(d_j(Tu^j, Tv^j)) \\ &\leq \mathcal{F}(M^j(u^j, v^j)) + L\theta(d_j(gu^j, Tu^j)), \end{aligned} \quad (39)$$

(ii) One of  $T$  or  $g$  is one-one

(iii)  $T$  and  $g$  are weakly compatible

then  $(T, g)$  has a unique common fixed point.

*Proof.* In view of Theorem 18, the set  $\text{Coin}(T, g)$  is non-empty. Let  $u^j, v^j \in \text{Coin}(T, g)$ . If  $d_j(Tu^j, Tv^j) = 0$ , then we

have  $Tu^j = gv^j = gv^j = Tv^j$ , and hence,  $u^j = v^j$  as one of  $T$  and  $g$  is one-one. Otherwise, using condition (39), we obtain

$$\begin{aligned} \tau + F(d(Tu^j, Tv^j)) &\leq F(d(gu^j, gv^j)) + L\theta(d(gu^j, Tu^j)), \\ &= F(d(Tu^j, Tv^j)), \end{aligned} \quad (40)$$

which is a contradiction. So the coincidence point of  $T$  and  $g$  is unique.

Let  $w^j$  be the unique coincidence point of  $T$  and  $g$ , and let  $z^j \in X$  such that  $z^j = Tu^j = gu^j$ . As  $T$  and  $g$  are weakly compatible, we have  $Tz^j = Tgu^j = gTu^j = gz^j$ . Thus,  $z^j$  is a coincidence point of  $T$  and  $g$ . By the uniqueness of the coincidence point, we conclude  $w^j = z^j$ ; that is,  $u$  is a common fixed point of the pair  $(T, g)$  which is indeed unique. as the coincidence point of  $T$  and  $g$  is unique.  $\square$

*Remark 20.* If we replace condition  $(d)$  of Theorem 18 with the following alternate condition:

- $(d^*)(d_1^*)$  There exists a subset  $Y^j$  of  $X^j$  such that  $T(X^j) \subseteq g(X^j) \subseteq Y^j$  and  $Y^j$  is edge-complete
  - $(d_2^*)$   $(T, g)$  is an edge-compatible pair
  - $(d_3^*)$   $T$  and  $g$  are edge-continuous
- the conclusions of Theorems 18 and 19 still hold.

*Proof.* Clearly,  $\{gx_n^j\}$  is an edge-preserving Cauchy sequence in  $Y^j$ , and by edge-completeness of  $Y$ , we get  $v^j \in Y^j$  such that

$$\lim_{n \rightarrow \infty} g x_n^j = v^j, \tag{41}$$

and then, by (21), we have

$$\lim_{n \rightarrow \infty} T x_n^j = v^j. \tag{42}$$

Using the edge continuity of  $g$  and  $T$ , we also have

$$\lim_{n \rightarrow \infty} T(g x_n^j) = T\left(\lim_{n \rightarrow \infty} g x_n^j\right) = T v^j, \tag{43}$$

$$\lim_{n \rightarrow \infty} g(T x_n^j) = g\left(\lim_{n \rightarrow \infty} T x_n^j\right) = g v^j. \tag{44}$$

Then, by edge-compatibility of  $g$  and  $T$ , we get

$$\lim_{n \rightarrow \infty} d(g T x_n^j, T g x_n^j) = 0. \tag{45}$$

Finally from (44), (45), and (43), we get

$$d(g v^j, T v^j) = d\left(\lim_{n \rightarrow \infty} g T x_n^j, \lim_{n \rightarrow \infty} T g x_n^j\right) = \lim_{n \rightarrow \infty} d(g T x_n^j, T g x_n^j) = 0. \tag{46}$$

Hence,  $v^j$  is a coincidence point of the pair  $(T, g)$ .  $\square$

*Remark 21.* Since every  $\xi$ -extended contraction mapping is a  $\theta$ -extended contraction, the conclusions of Theorems 18 and 19 remain true for an edge theoretic  $\xi$ -extended  $\mathcal{C}\mathcal{W}$ -contraction pair of mappings also.

On setting  $g = I$  in Theorem 18, we deduce the following corresponding fixed-point result.

**Theorem 22.** *Let  $(M, d)$  be a metric space endowed with a directed graph  $G$  and  $T : M \rightarrow M$ . Assume that the following conditions are fulfilled:*

- (a) *There exists  $x_0 \in M$  such that  $(x_0, T x_0) \in E(G)$*
- (b)  *$T$  is edge-preserving*
- (c)  *$T$  is a  $\theta$ -extended  $\mathcal{C}\mathcal{W}$ -edge contraction mapping*
- (d) *( $d_1$ ) There exists a subset  $X$  of  $M$  such that  $T(M) \subseteq X$  and  $X$  is edge-complete*
- ( $d_2$ ) *One of the following conditions is satisfied:*
  - (i)  *$T$  is edge-continuous*
  - (ii)  *$E(G)|_X$  satisfies Property(\*)*

*Then,  $T$  has a fixed point.*

*Example 6.* Let  $\{X^j, d_j\}$ ,  $E(G)$ ,  $T$ , and  $g$  be as in Example 5. Then, we have the following:

- (1)  $(g0, T0) \in E(G)$
- (2)  $T$  is  $g$ -edge-preserving. In fact, we see that  $(g x^j, g y^j) \in E(G)$  implies either  $x^j = n, y^j = n$  or  $x^j = n, y^j = n$

+ 1. If  $n = 0$ , then  $(T0, T0) \in E(G)$  and  $(T0, T1) \in E(G)$ . If  $n = 1$ , then  $(T1, T1) \in E(G)$  and  $(T1, T2) \in E(G)$ . If  $n = k > 1$ , then  $(Tk, Tk) \in E(G)$  and  $(Tk, T(k+1)) = (k-1, k) \in E(G)$

(3)  $(T, g)$  is a  $\theta$ -extended  $\mathcal{C}\mathcal{W}$ -edge contraction mapping

(4)  $T(X^j) \subseteq g(X^j)$

(5)  $T$  is  $g$ -edge-continuous

Thus, all conditions of Theorem 18 are satisfied and 0 is a coincidence point of  $T$  and  $g$ . Moreover, we see that  $T$  and  $g$  satisfy conditions (i), (ii) ( $g$  is one-one), and (iii) of Theorem 19, and 0 is the unique common fixed point of  $T$  and  $g$ .

*Remark 23* (an open problem). Prove Theorems 18, 19, and 22 for  $\xi$ -extended  $\mathcal{C}\mathcal{Q}\mathcal{W}$ -contraction mappings.

### 4. Application to Nonlinear Integral Equations

Consider the Banach space  $M = C([0, 1], R)$  of all continuous functions  $x : [0, 1] \rightarrow R$  equipped with norm

$$\|x\| = \max_{s \in [0,1]} |x(s)|. \tag{47}$$

Define a metric  $d_j$  on  $M$  by  $d_j(x^j, y^j) = \|x^j - y^j\|$  for all  $x^j, y^j \in M$ . Then,  $(M, d_j)$  is a complete metric space.

In this section, we show the applicability of Theorem 19 by investigating the existence and uniqueness of a solution for the following nonlinear integral equation of Volterra type:

$$x^j(s) = \int_0^{\mu(s)} K(s, v, (x^j)(\eta(v))) dv + \int_0^{\sigma(s)} J(s, v, (x^j)(\zeta(v))) dv + f(s), s \in [0, 1], \tag{48}$$

where  $K, J : [0, 1] \times [0, 1] \times R \rightarrow R$ ,  $f : [0, 1] \rightarrow R$ , and  $\mu, \sigma, \eta, \zeta : [0, 1] \rightarrow [0, 1]$ .

**Definition 24.** A lower solution for (48) is a function  $x \in M$  such that

$$x^j(s) \leq \int_0^{\mu(s)} K(s, v, (x^j)(\eta(v))) dv + \int_0^{\sigma(s)} J(s, v, (x^j)(\zeta(v))) dv + f(s), s \in [0, 1]. \tag{49}$$

**Definition 25.** An upper solution for (48) is a function  $x \in M$  such that

$$x^j(s) \geq \int_0^{\mu(s)} K(s, v, (x^j)(\eta(v))) dv + \int_0^{\sigma(s)} J(s, v, (x^j)(\zeta(v))) dv + f(s), s \in [0, 1]. \tag{50}$$

Consider the operator  $T : M \rightarrow M$  defined by

$$\begin{aligned} T(x^j(s)) &= \int_0^{\mu(s)} K(s, v, (x^j)(\eta(v))) dv \\ &\quad + \int_0^{\sigma(s)} J(s, v, (x^j)(\zeta(v))) dv + f(s), \text{ for all } x \in M. \end{aligned} \quad (51)$$

Then,  $x^j$  is a fixed point of the operator  $T$  if and only if it is a solution of the integral equation (48).

Let

$$\begin{aligned} M^\circ(x^j, y^j) &= \max \left\{ |x^j - y^j|, |x^j - T(x^j(s))|, |y^j - T(y^j(s))|, \frac{|x^j - T(y^j(s))| + |y^j - T(x^j(s))|}{2} \right\}, \\ \|M^\circ(x^j, y^j)\| &= \max \left\{ \|x^j - y^j\|, \|x^j - T(x^j(s))\|, \|y^j - T(y^j(s))\|, \frac{\|x^j - T(y^j(s))\| + \|y^j - T(x^j(s))\|}{2} \right\}. \end{aligned} \quad (52)$$

**Theorem 26.** Assume that  $K$  and  $J$  are nondecreasing in the third variable,  $\mu(t) + \sigma(t) \leq 1$  for all  $t \in [0, 1]$ , and the following conditions hold:

There exists  $\tau > 0$  such that

$$\begin{aligned} |K(s, v, gx^j) - K(s, v, gy^j)| &\leq \frac{M^\circ(x^j, y^j)}{\|M^\circ(x^j, y^j)\| \{ \tau - ((L\|y^j - T(x^j(s))\|)/(1 + \|y^j - T(x^j(s))\|)) \} + 1}, \\ |J(s, v, gx^j) - J(s, v, gy^j)| &\leq \frac{M^\circ(x^j, y^j)}{\|M^\circ(x^j, y^j)\| \{ \tau - L\|y^j - T(x^j(s))\|/1 + \|y^j - T(x^j(s))\| \} + 1}, \end{aligned} \quad (53)$$

for all  $s, v \in [0, 1]$ ,  $x^j, y^j \in M$  with  $x^j(s) \leq y^j(s)$  and  $L \geq 0$ . If (48) has a lower solution, e.g.,  $x^j_0(s)$ , then a solution exists for the integral equation (48).

which shows that  $(Tx^j, Ty^j) \in E(G)$ . Thus,  $T$  is edge-preserving. Now, for all  $(x^j, y^j) \in E(G)$  and  $s \in [0, 1]$ , we have

*Proof.* Consider the graph  $G$  in  $M$ , with edges  $E(G)$  given by

$$E(G) = \{ (x^j, y^j) \in M \times M : x^j(s) \leq y^j(s) \}. \quad (54)$$

For any  $(x^j, y^j) \in E(G)$ , we have (for all  $s \in [0, 1]$ )

$$\begin{aligned} T(x^j(s)) &= \int_0^{\mu(s)} K(s, v, (x^j)(\eta(v))) dv \\ &\quad + \int_0^{\sigma(s)} J(s, v, (x^j)(\zeta(v))) dv + f(s) \\ &\leq \int_0^{\mu(s)} K(s, v, (y^j)(\eta(v))) dv \\ &\quad + \int_0^{\sigma(s)} J(s, v, (y^j)(\zeta(v))) dv + f(s) \\ &= T(y^j(s)), \end{aligned} \quad (55)$$

$$\begin{aligned} |T(x^j(s)) - T(y^j(s))| &\leq \int_0^s |(K(s, v, (x^j)(\eta(v))) \\ &\quad - K(s, v, (y^j)(\eta(v))))| dv + \int_0^s |(J(s, v, (x^j)(\zeta(v))) - J(s, v, (y^j)(\zeta(v))))| dv \\ &\leq \int_0^{\mu(s)} \frac{M^\circ(x^j, y^j)}{M^\circ(x^j, y^j) \{ \tau - (L\|y^j - T(x^j(s))\|/(1 + \|y^j - T(x^j(s))\|)) \} + 1} dv \\ &\quad + \int_0^{\sigma(s)} \frac{M^\circ(x^j, y^j)}{M^\circ(x^j, y^j) \{ \tau - (L\|y^j - T(x^j(s))\|/(1 + \|y^j - T(x^j(s))\|)) \} + 1} dv \\ &\leq \int_0^{\mu(s)} \frac{\max_{s \in [0, 1]} M^\circ(x^j, y^j)}{\|M^\circ(x^j, y^j)\| \{ \tau - (L\|y^j - T(x^j(s))\|/(1 + \|y^j - T(x^j(s))\|)) \} + 1} dv \\ &\quad + \int_0^{\sigma(s)} \frac{\max_{s \in [0, 1]} M^\circ(x^j, y^j)}{M^\circ(x^j, y^j) \{ \tau - (L\|y^j - T(x^j(s))\|/(1 + \|y^j - T(x^j(s))\|)) \} + 1} dv \\ &\leq \frac{\|M^\circ(x^j, y^j)\|}{\|M^\circ(x^j, y^j)\| \{ \tau - (L\|y^j - T(x^j(s))\|/(1 + \|y^j - T(x^j(s))\|)) \} + 1} \int_0^{\mu(s)} dv \\ &\quad + \frac{\|M^\circ(x^j, y^j)\|}{M^\circ(x^j, y^j) \{ \tau - (L\|y^j - T(x^j(s))\|/(1 + \|y^j - T(x^j(s))\|)) \} + 1} \int_0^{\sigma(s)} dv \\ &= \frac{\|M^\circ(x^j, y^j)\|}{M^\circ(x^j, y^j) \{ \tau - (L\|y^j - T(x^j(s))\|/(1 + \|y^j - T(x^j(s))\|)) \} + 1} (\mu(s) + \sigma(s)) \\ &\leq \frac{\|M^\circ(x^j, y^j)\|}{M^\circ(x^j, y^j) \{ \tau - (L\|y^j - T(x^j(s))\|/(1 + \|y^j - T(x^j(s))\|)) \} + 1}. \end{aligned} \quad (56)$$

Taking the supremum, we get

$$\|T(x) - T(y)\| \leq \frac{\|M^\circ(x^j, y^j)\|}{M^\circ(x^j, y^j)\{\tau - (L\|y^j - T(x^j(s))\|/(1 + |y^j - T(x^j(s))))\} + 1}, \tag{57}$$

or

$$\tau + \frac{1}{\|M^\circ(x^j, y^j)\|} \leq \frac{1}{\|T(x) - T(y)\|} + \frac{L\|y^j - T(x^j(s))\|}{1 + |y^j - T(x^j(s))|}, \tag{58}$$

or

$$\tau - \frac{1}{\|T(x) - T(y)\|} \leq \frac{-1}{\|M^\circ(x^j, y^j)\|} + \frac{L\|y^j - T(x^j(s))\|}{1 + |y^j - T(x^j(s))|}. \tag{59}$$

That is,

$$\tau - \frac{1}{d_j(Tx^j, Ty^j)} \leq \frac{-1}{\|M^j(x^j, y^j)\|} + \frac{L d_j(y^j, Tx^j(s))}{1 + d_j(y^j, Tx^j(s))}. \tag{60}$$

Thus, inequality (13) is satisfied with  $F(\alpha) = -1/\alpha$  and  $\theta(\beta) = \beta/(1 + \beta)$ , so that  $\lambda = \sup_{t>0} \theta(t) = 1$ . Also, by Definition 24, we have  $(x^j_0, Tx^j_0) \in E(G)$ . Therefore, all the assumptions of Theorem 22 are satisfied, and thus, problem (48) has a solution.  $\square$

**Theorem 27.** Assume that  $K$  is nonincreasing in the third variable and there exists  $\tau > 0$  such that

$$|K(s, v, gx^j) - K(s, v, gy^j)| \leq \frac{|gx^j - gy^j|}{\tau \|gx^j - gy^j\| + 1}, \tag{61}$$

for all  $s, v \in [0, 1]$  and  $x, y \in M$ . Then, the existence of an upper solution of the integral equation (48) ensures the existence of a solution of (48).

*Proof.* Define set  $E(G)$  of edges on  $M$  by

$$E(G) = \{(x, y) \in M \times M : x(s) \geq y(s)\}. \tag{62}$$

Now, following the steps of the proof of Theorem 26 with an analogous procedure, one can check that all the hypotheses of Theorem 22 are validated, and thus, Theorem 22 ensures the existence of a unique solution of the integral equation (48).  $\square$

We now furnish a numerical example to validate the hypothesis of Theorem 27.

*Example 7.* Consider the function  $x \in M$  defined by  $x(s) = s^2, s \in [0, 1]$ . We show that this function is an upper solution in  $M$  for the following integral equation:

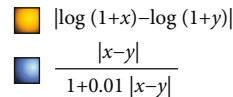
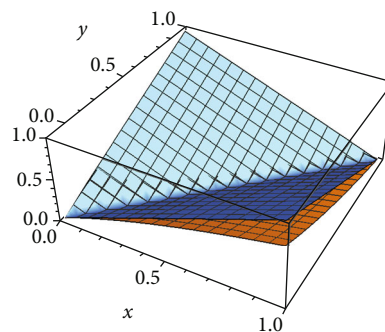


FIGURE 1: Inequality in (66).

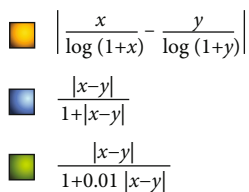
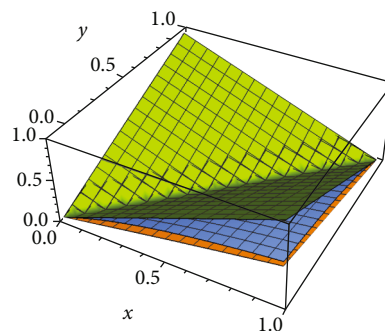


FIGURE 2: Inequality in (67).

$$x(s) = -\frac{1}{2}s + 2s^2 + \arctan\left(\frac{1}{2}s\right) - 3 \arctan\left(\frac{1}{2}s^2\right) - \frac{1}{2}s^2 \ln\left(1 + \frac{1}{4}s^4\right) + \int_0^{s^2/2} \ln(1+x(v))dv + \int_0^{s^2/2} \frac{x(v)}{1+x(v)}dv, \quad s \in [0, 1]. \tag{63}$$

Finally, we see that  $x_u(s) = s^2 - \arctan(s^2/2)$  is the unique solution of (63).

*Proof.* Define the operator  $T : M \rightarrow M$  as

$$Tx(s) = -\frac{1}{2}s + 2s^2 + \arctan\left(\frac{1}{2}s\right) - 3 \arctan\left(\frac{1}{2}s^2\right) - \frac{1}{2}s^2 \ln\left(1 + \frac{1}{4}s^4\right) + \int_0^{s^2/2} \ln(1+x(v))dv + \int_0^{s^2/2} \frac{x(v)}{1+x(v)}dv, \quad s \in [0, 1]. \tag{64}$$



Now, set  $K(s, v, x(v)) = \ln(1 + x(v))$ ,  $J(s, v, x(v)) = x(v)/(1 + x(v))$ ,  $\mu(s) = (1/2)s^2$ ,  $\sigma(s) = (1/2)s$ ,  $f(s) = -(1/2)s + 2s^2 + \arctan((1/2)s) - 3 \arctan((1/2)s^2) - (1/2)s^2 \ln(1 + (1/4)s^4)$ , and  $\tau \leq 0.01$ . We observe the following:

(i) Both the functions  $K(s, v, x(v)) = \ln(1 + x(v))$  and  $J(s, v, x(v)) = x(v)/(1 + x(v))$  are nondecreasing in the third variable

(ii) By actual computation, we have

$$\int_0^{s^2/2} \ln(1 + x(v)) dv = -s^2 + 2 \arctan\left(\frac{1}{2}s^2\right) + \frac{1}{2}s^2 \ln\left(1 + \frac{1}{4}s^4\right), \quad s \in [0, 1],$$

$$\int_0^{s^2/2} \frac{x(v)}{1 + x(v)} dv = \frac{1}{2}s - \arctan\left(\frac{1}{2}s\right), \quad s \in [0, 1]. \quad (65)$$

(iii)  $s^2 \geq -(1/2)s + 2s^2 + \arctan((1/2)s) - 3 \arctan((1/2)s^2) - (1/2)s^2 \ln(1 + (1/4)s^4) + \int_0^{s^2/2} \ln(1 + x(v)) dv + \int_0^{s^2/2} x(v)/(1 + x(v)) dv$ ,  $s \in [0, 1]$  so that  $x(s) = s^2$  is an upper solution for (63)

(iv) The following inequalities hold true for all  $x, y \in [0, 1]$  (see Figures 1 and 2):

$$|\ln(1 + x) - \ln(1 + y)| \leq \frac{|x - y|}{1 + 0.01|x - y|}, \quad (66)$$

$$\left| \frac{x}{1 + x} - \frac{y}{1 + y} \right| \leq \frac{|x - y|}{1 + |x - y|} \leq \frac{|x - y|}{1 + 0.01|x - y|}. \quad (67)$$

□

Furthermore, using the nondecreasing function  $s \mapsto s/(1 + 0.01s)$ , we have

$$\begin{aligned} |\ln(1 + x) - \ln(1 + y)| &\leq \frac{|x - y|}{1 + 0.01|x - y|} \\ &\leq \frac{\max_{s \in [0, 1]} |x - y|}{1 + 0.01 \max_{s \in [0, 1]} |x - y|} \\ &= \frac{\|x - y\|}{1 + 0.01\|x - y\|}. \end{aligned} \quad (68)$$

Similarly, for all  $x, y \in [0, 1]$ , we have

$$\left| \frac{x}{1 + x} - \frac{y}{1 + y} \right| \leq \frac{\|x - y\|}{1 + 0.01\|x - y\|}. \quad (69)$$

Hence, all the conditions of Theorem 27 are satisfied. It is evident that the integral equation (63) has a unique solution  $x_u \in M$  defined by  $x_u(s) = s^2 - \arctan(s^2/2)$ .

## Data Availability

No data were used to support this study.

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## References

- [1] D. Boyd and J. S. W. Wong, "On nonlinear contractions," *Proceedings of American Mathematical Society*, vol. 20, no. 2, pp. 458–464, 1969.
- [2] L. B. Ćirić, "A generalization of Banach's contraction principle," *Proceedings of American Mathematical Society*, vol. 45, no. 2, pp. 267–273, 1974.
- [3] R. Gubran, M. Imdad, I. A. Khan, and W. M. Alfaqih, "Order-theoretic common fixed point results for F-contractions," *Bulletin of Mathematical Analysis and Applications*, vol. 10, no. 1, pp. 80–88, 2018.
- [4] J. J. Nieto and R. López, "Contractive mapping theorems in partially ordered sets and applications to ordinary differential equations," *Order*, vol. 22, no. 3, pp. 223–239, 2005.
- [5] H. Piri and P. Kumam, "Some fixed point theorems concerning F-contraction in complete metric spaces," *Fixed Point Theory and Applications*, vol. 2014, no. 1, 2014.
- [6] A. C. M. Ran and M. C. B. Reurings, "A fixed point theorem in partially ordered sets and some applications to matrix equations," *Proceedings of the American Mathematical Society*, vol. 132, pp. 1435–1443, 2004.
- [7] S. B. Nadler, "Multi-valued contraction mappings," *Pacific Journal of Mathematics*, vol. 30, no. 2, pp. 475–488, 1969.
- [8] D. Wardowski, "Fixed points of a new type of contractive mappings in complete metric spaces," *Fixed Point Theory and Applications*, vol. 94, 6 pages, 2012.
- [9] D. Wardowski and N. Van Dung, "Fixed points of F-weak contractions on complete metric spaces," *Demonstratio Mathematica*, vol. 47, no. 1, pp. 146–155, 2014.
- [10] G. Durmaz, G. Minak, and I. Altun, "Fixed points of ordered F-contractions," *Hacettepe Journal of Mathematics and Statistics*, vol. 1, no. 45, pp. 15–21, 2016.
- [11] S. Sawangsup, W. Sawangsup, A. Francisco, and R. L. De Heirro, "Fixed point theorems for  $F_{\frac{R}{\mathfrak{g}}}$ -contractions with applications to solution of nonlinear matrix equations," *Journal of Fixed Point Theory and Applications*, vol. 19, no. 3, pp. 1711–1725, 2017.
- [12] M. Imdad, Q. Khan, W. M. Alfaqih, and R. Gubran, "A relation theoretic (F, R)-contraction principle with applications to matrix equations," *Bulletin of Mathematical Analysis and Applications*, vol. 10, no. 1, pp. 1–12, 2018.
- [13] W. M. Alfaqih, M. Imdad, R. Gubran, and I. A. Khan, "Relation-theoretic coincidence and common fixed point results under  $(F, R)_{\mathfrak{g}}$ -contractions with an application," *Fixed Point Theory and Applications*, vol. 12, 18 pages, 2019.
- [14] R. Espinola and W. A. Kirk, "Fixed point theorems in R-trees with applications to graph theory," *Topology and its Applications*, vol. 153, no. 7, pp. 1046–1055, 2006.
- [15] J. Jachymski, "The contraction principle for mappings on a metric space with a graph," *Proceedings of the American Mathematical Society*, vol. 136, no. 4, pp. 1359–1373, 2008.

- [16] W. M. Alfaqih, R. Gubran, and M. Imdad, "Coincidence and common fixed point results under generalized  $(A, S)_f$ -contractions," *Filomat*, vol. 32, no. 7, pp. 2651–2666, 2018.
- [17] R. Batra and S. Vashistha, "Fixed points of an F-contraction on metric spaces with a graph," *International Journal of Computer Mathematics*, vol. 91, no. 12, pp. 2483–2490, 2014.
- [18] I. Beg, A. R. Butt, and S. Radojevic, "The contraction principle for set valued mappings on a metric space with a graph," *Computers & Mathematics with Applications*, vol. 60, no. 5, pp. 1214–1219, 2010.
- [19] F. Bojor, "Fixed point of  $\varphi$ -contraction in metric spaces endowed with a graph," *Annals of the University of Craiova-Mathematics and Computer Science Series*, vol. 37, no. 4, pp. 85–92, 2010.
- [20] F. Bojor, "Fixed point theorems for Reich type contractions on metric spaces with a graph," *Nonlinear Analysis*, vol. 75, no. 9, pp. 3895–3901, 2012.
- [21] F. Bojor, "Fixed points of Kannan mappings in metric spaces endowed with a graph," *Versita*, vol. 20, no. 1, pp. 31–40, 2012.
- [22] C. Chifu and G. Petrusel, "New results on coupled fixed point theory in metric spaces endowed with a directed graph," *Fixed Point Theory and Applications*, vol. 151, 11 pages, 2014.
- [23] G. Prasad, R. C. Dimri, and A. Bartwal, "Coincidence theorems in new generalized metric spaces under locally g-transitive binary relation," *Journal of the Indian Mathematical Society*, vol. 85, no. 3-4, pp. 396–410, 2018.
- [24] G. Prasad, "Fixed points of Kannan contractive mappings in relational metric spaces," *The Journal of Analysis*, vol. 29, no. 3, pp. 669–684, 2021.
- [25] R. H. Haghi, S. Rezapour, and N. Shahzad, "Fixed points of G-type quasi-contractions on graphs," *Abstract and Applied Analysis*, vol. 2013, Article ID 167530, 5 pages, 2013.
- [26] S. Aleksić, Z. Mitrovic, and S. T. Radenovic, "Picard sequences in b-metric spaces," *Fixed Point Theory*, vol. 21, no. 1, pp. 35–46, 2020.

# Picard-Mann hybrid iteration process for nonexpansive semigroup in CAT(0) spaces

Dipti Thakur

School of Studies in Mathematics  
Pt.Ravishankar Shukla University  
Raipur - 492010 (C.G.), India  
dipti.thakur15@gmail.com

## ABSTRACT

*In this paper, consider Picard-Mann hybrid iteration process for nonexpansive semigroups in CAT(0) spaces. Then, prove strong and  $\Delta$ -convergence theorems for such iterative process in CAT(0) spaces. The results obtained in this paper extend and improve some recent known results.*

**Keywords:** Fixed point, Nonexpansive semigroup,  $\Delta$ -convergence, CAT(0) space.

**2000 Mathematics Subject Classification:** 47H09, 47H10.

## 1 Introduction

Fixed point theory in CAT(0) spaces was first studied by Kirk (Kirk, 2003). Since then the fixed point theory for nonexpansive mappings in CAT(0) spaces has been rapidly developed and many of papers have appeared (Dhompongsa, Kirk and Panyanak, 2007; Dhompongsa and Panyanak, 2008; Kirk, 2004; Kirk and Panyanak, 2008). It is worth mentioning that fixed point theorems in CAT(0) spaces (specially in R-trees) can be applied to graph theory, biology, and computer science (Bartolini, Ciaccia and Patella, 2002; Bestvina, 2002; Bridson and Haefliger, 1999; Espínola and Kirk, 2006; Kirk, 2004; Park, 2010).

Let  $(X, d)$  be a metric space,  $D$  a closed convex subset of  $X$  and  $S : D \rightarrow D$  a mapping. If  $d(Sx, Sy) \leq d(x, y)$ , for all  $x, y \in D$ , then  $S$  is nonexpansive on  $D$ . We denote the set of all fixed points of  $S$  by  $F(S)$ , i.e.,  $F(S) = \{x \in X : Sx = x\}$ .

A family  $\mathcal{S} := \{S(s) : 0 \leq s < \infty\}$  of mappings on a closed convex subset  $D$  of a CAT(0) space  $X$  is called a nonexpansive semigroup if it satisfies the following conditions:

- (i) for each  $t \geq 0$ ,  $S(t)$  is a nonexpansive mapping on  $D$ ;
- (ii)  $S(0)x = x$  for all  $x \in D$ ;
- (iii)  $S(s + t) = S(s) \circ S(t)$  for all  $s, t \geq 0$ ;

(iv) for all  $x \in D$ ,  $s \rightarrow S(s)x$  is continuous.

We use  $F(\mathcal{S})$  to denote the common fixed point set of the semigroup  $\mathcal{S}$ , i.e.,  $F(\mathcal{S}) = \{x \in D : S(s)x = x, \forall s \geq 0\}$ .

The Mann iterative process (Mann, 1953) is defined in a CAT(0) space by

$$x_{n+1} = \alpha_n x_n \oplus (1 - \alpha_n) Sx_n, \quad \forall n \geq 0$$

where  $\{\alpha_n\}$  is a sequence in  $[0, 1]$ . Li et al. (Li and Yip, 2012) proved the convergence results of implicit Mann iteration processes with bounded perturbations for approximating a common fixed point of nonexpansive semigroup in CAT(0) spaces.

The Ishikawa iterative sequence (Ishikawa, 1974) is defined by

$$\begin{aligned} y_n &= \alpha_n x_n \oplus (1 - \alpha_n) Sx_n \\ x_{n+1} &= \beta_n x_n \oplus (1 - \beta_n) Sy_n, \end{aligned}$$

for all  $n \geq 0$  where  $\{\alpha_n\}$  and  $\{\beta_n\}$  are sequences in  $[0, 1]$ . In 2013 Liu et al. (Liu, Chen, Li and Xiao, 2013) proved the convergence result of the implicit Ishikawa iteration processes for approximating a common fixed point of nonexpansive semigroup in CAT(0) spaces.

In 2003, Suzuki (Suzuki, 2003) introduced an iterative process  $\{x_n\}$  for nonexpansive semigroup on  $D$ , where  $D$  is a compact and convex subset of a Banach space  $X$  defined by  $x_1 \in D$  and

$$x_{n+1} = \lambda S(t_n)x_n + (1 - \lambda)x_n$$

where  $\lambda \in (0, 1)$  and  $\{t_n\} \subset [0, \infty)$ . Then the author proved that  $\{x_n\}$  converges strongly to a common fixed point of  $\{S(t) : t \geq 0\}$ . Recently Cho et al. (Cho, Ćirić and Wang, 2011) generalized the result of Suzuki for CAT(0) spaces.

In 2013, Khan (Khan, 2013) introduced the following Picard-Mann hybrid iterative process for a nonexpansive mappings in Banach space and claimed that this process is independent of Picard and Mann iterative process, the convergence process is faster than Picard and Mann iteration process. For any initial point  $x_1 \in D$ ,

$$\begin{cases} y_n = (1 - \alpha_n)x_n + \alpha_n Sx_n, \\ x_{n+1} = Sy_n, \end{cases} \quad (1.1)$$

where  $\{\alpha_n\}$  is a real sequence in  $(0, 1)$ .

In this paper, we introduce Picard-Mann hybrid iteration process for nonexpansive semigroups in CAT(0) spaces, and then prove strong and  $\Delta$  - convergence theorems for such iterative process in CAT(0) spaces. Moreover, we present a convergence theorem for a sequence of nonexpansive mappings in CAT(0) spaces. Our results generalized some recent known results.

## 2 Preliminaries

Throughout in this paper, we denote by  $\mathbb{N}$  the set of positive integers and by  $\mathbb{R}$  the set of real numbers. Refer to (Bridson and Haefliger, 1999) for the some definitions. suppose  $(X, d)$  be a metric space,  $x, y \in X$  and  $[0, l] \subset \mathbb{R}$ . A map  $c : [0, l] \rightarrow X$  is said to be a geodesic path joining

the point  $x$  to  $y$  such that  $c(0) = x$ ,  $c(l) = y$ , with  $d(c(t), c(t')) = |t - t'|$  for all  $t, t' \in [0, l]$ . In short, we use a geodesic from  $x$  to  $y$  instead of a geodesic path joining  $x$  to  $y$ . Notice that if  $c$  is an isometry, then  $d(x, y) = l$ . The image of  $c$  is called a geodesic (or metric) segment joining  $x$  and  $y$ . If it is unique, this geodesic segment is denoted by  $[x, y]$ . A metric space  $(X, d)$  is said to be a geodesic space if every two points of  $X$  are joined by a geodesic. Moreover  $X$  is said to be uniquely geodesic if there is exactly one geodesic joining  $x$  and  $y$  for each  $x, y \in X$ . A subset  $Y \subseteq X$  is said to be convex if  $Y$  includes every geodesic segment joining any two of its points.

In a geodesic metric space  $(X, d)$ , geodesic triangle  $\Delta(x_1, x_2, x_3)$  consists of three points  $x_1, x_2, x_3$  in  $X$  (the vertices of  $\Delta$ ) and a geodesic segment between each pair of vertices (the edges of  $\Delta$ ). A triangle  $\overline{\Delta}(x_1, x_2, x_3) := \Delta(\bar{x}_1, \bar{x}_2, \bar{x}_3)$  in the Euclidean plane  $\mathbb{E}^2$ , is said to be a comparison triangle for the geodesic triangle  $\Delta(x_1, x_2, x_3)$  in  $(X, d)$  such that  $d_{\mathbb{E}^2}(\bar{x}_i, \bar{x}_j) = d(x_i, x_j)$  for  $i, j \in \{1, 2, 3\}$ .

Comparison Axiom (Bridson and Haefliger, 1999): Let  $\Delta$  be a geodesic triangle in  $X$  and let  $\overline{\Delta}$  be a comparison triangle for  $\Delta$  in a geodesic metric space  $(X, d)$ . Then we say that  $\Delta$  satisfy the  $CAT(0)$  inequality if for all  $x, y \in \Delta$  and all comparison points  $\bar{x}, \bar{y} \in \overline{\Delta}$ ,

$$d(x, y) \leq d_{\mathbb{E}^2}(\bar{x}, \bar{y}).$$

A geodesic metric space is called a  $CAT(0)$  space (Bridson and Haefliger, 1999) if all geodesic triangles of appropriate size satisfy the comparison axiom.

We refer following results from Dhompongsa and Panyanak (Dhompongsa and Panyanak, 2008).

**Definition 2.1.** (Dhompongsa and Panyanak, 2008) For any  $x, y \in X$  and  $t \in [0, 1]$ , there exists a unique point  $z \in [x, y]$  such that

$$d(x, z) = td(x, y), \quad d(y, z) = (1 - t)d(x, y). \tag{2.1}$$

Notation  $(1 - t)x \oplus ty$  is used for the unique point  $z$  satisfying (2.1)

We also denote by  $[x, y]$  the geodesic segment joining from  $x$  to  $y$ , that is,  $[x, y] = \{(1 - t)x \oplus ty : t \in [0, 1]\}$  (Bridson and Haefliger, 1999).

A subset  $D$  of  $CAT(0)$  space  $X$  is said to be convex if  $[x, y] \subset D$  for all  $x, y \in D$ .

**Definition 2.2.** (Dhompongsa, Kirk and Sims, 2006) Let  $\{x_n\}$  be a bounded sequence in a  $CAT(0)$  space  $X$ . For  $x \in X$ , we set

$$r(x, \{x_n\}) = \limsup_{n \rightarrow \infty} d(x, x_n).$$

The asymptotic radius  $r(\{x_n\})$  of  $\{x_n\}$  is given by

$$r(\{x_n\}) = \inf\{r(x, \{x_n\}) : x \in X\}.$$

The asymptotic center  $A(\{x_n\})$  of  $\{x_n\}$  is the set

$$A(\{x_n\}) = \{x \in X : r(x, \{x_n\}) = r(\{x_n\})\}.$$

In a  $CAT(0)$  space,  $A(\{x_n\})$  consists of exactly one point (Dhompongsa et al., 2006, Proposition 7).

**Definition 2.3.** (Kirk and Panyanak, 2008) A sequence  $\{x_n\}$  in  $X$  is said to  $\Delta$ -converge to  $p \in X$  if  $p$  is the unique asymptotic center of  $\{u_n\}$  for every subsequence  $\{u_n\}$  of  $\{x_n\}$ .

In this case, we write  $\Delta\text{-}\lim x_n = p$  and call  $p$  the  $\Delta$ -limit of  $\{x_n\}$ .

The following lemmas plays an important role in our paper

**Lemma 2.4.** (Kirk and Panyanak, 2008) Every bounded sequence in a complete  $CAT(0)$  space has a  $\Delta$ -convergent subsequence.

**Lemma 2.5.** (Dhompongsa et al., 2007) If  $D$  is a closed convex subset of a complete  $CAT(0)$  space and if  $\{x_n\}$  is a bounded sequence in  $D$ , then the asymptotic center of  $\{x_n\}$  is in  $D$ .

**Lemma 2.6.** (Dhompongsa and Panyanak, 2008) If  $\{x_n\}$  is a bounded sequence in complete  $CAT(0)$  space  $X$  with  $A(\{x_n\}) = \{x\}$  and  $\{u_n\}$  is a subsequence of  $\{x_n\}$  with  $A(\{u_n\}) = \{u\}$  and the sequence  $\{d(x_n; u)\}$  converges, then  $x = u$ .

**Lemma 2.7.** (Dhompongsa and Panyanak, 2008) Let  $X$  be a  $CAT(0)$  space. Then for all  $x, y, z \in X$  and all  $t \in [0, 1]$  we have

- (i)  $d((1-t)x \oplus ty, z) \leq (1-t)d(x, z) + td(y, z),$
- (ii)  $d((1-t)x \oplus ty, z)^2 \leq (1-t)d(x, z)^2 + td(y, z)^2 - t(1-t)d(x, y)^2.$

**Lemma 2.8.** (Dhompongsa and Panyanak, 2008) Let  $D$  be a nonempty closed convex subset of a complete  $CAT(0)$  space  $X$ , and  $S : D \rightarrow D$  be a nonexpansive mapping. If  $\{x_n\}$  is a sequence in  $D$  such that  $\lim_{n \rightarrow \infty} d(x_n, Sx_n) = 0$  and  $\Delta\text{-}\lim_{n \rightarrow \infty} x_n = v$ , then  $v = Sv$ .

### 3 Main Result

In this section we present some strong and  $\Delta$ -convergent theorems of Picard-Mann hybrid iteration process for nonexpansive semigroups in a  $CAT(0)$  space.

**Theorem 3.1.** Let  $D$  be a nonempty closed convex subset of a complete  $CAT(0)$  space  $X$ . Let  $S := \{S(t) : t \geq 0\}$  be nonexpansive semigroups. Assume that  $\mathcal{F} = F(S)$  Let  $\{x_n\}$  be sequence generated by (1.1), where  $\{\alpha_n\}$  and  $\{t_n\}$  satisfy the following conditions:

- (i)  $\{\alpha_n\} \in [a, b] \subset (0, 1)$
- (ii)  $t_n > 0, \liminf_{n \rightarrow \infty} t_n = 0, \limsup_{n \rightarrow \infty} t_n > 0, \lim_{n \rightarrow \infty} (t_{n+1} - t_n) = 0.$

Then for  $t > 0$  we have  $\lim_{n \rightarrow \infty} d(x_n, S(t)x_n) = 0$  and  $\lim_{n \rightarrow \infty} d(x_n, p)$  exists for all  $p \in \mathcal{F}$ .

*Proof.* Let  $p \in \mathcal{F}$ , then by using Lemma 2.7(i) we have,

$$\begin{aligned}
 d(y_n, p) &= d((1 - \alpha_n)x_n \oplus \alpha_n S(t_n)x_n, p) & (3.1) \\
 &\leq (1 - \alpha_n)d(x_n, p) + \alpha_n d(S(t_n)x_n, p) \\
 &\leq (1 - \alpha_n)d(x_n, p) + \alpha_n d(x_n, p) \\
 &= d(x_n, p)
 \end{aligned}$$

and

$$\begin{aligned} d(x_{n+1}, p) &= d(S(t_n)y_n, p) \\ &\leq d(y_n, p) \\ &\leq d(x_n, p) \end{aligned} \tag{3.2}$$

Hence  $\lim_{n \rightarrow \infty} d(x_n, p)$  exists, and therefore  $\{x_n\}$  is bounded. Also by Lemma 2.7(ii) we have,

$$\begin{aligned} d(y_n, p)^2 &= d((1 - \alpha_n)x_n \oplus \alpha_n S(t_n)x_n, p)^2 \\ &\leq (1 - \alpha_n)d(x_n, p)^2 + \alpha_n d(S(t_n)x_n, p)^2 - \alpha_n(1 - \alpha_n)d(x_n, S(t_n)x_n)^2 \\ &\leq (1 - \alpha_n)d(x_n, p)^2 + \alpha_n d(x_n, p)^2 - \alpha_n(1 - \alpha_n)d(x_n, S(t_n)x_n)^2 \\ &= d(x_n, p)^2 - \alpha_n(1 - \alpha_n)d(x_n, S(t_n)x_n)^2. \end{aligned} \tag{3.3}$$

$$\begin{aligned} d(x_{n+1}, p)^2 &= d(S(t_n)y_n, p)^2 \\ &\leq d(y_n, p)^2 \\ &\leq d(x_n, p)^2 - \alpha_n(1 - \alpha_n)d(x_n, S(t_n)x_n)^2. \end{aligned} \tag{3.4}$$

Thus we have,

$$a(1 - b)d(x_n - S(t_n)x_n)^2 \leq \alpha_n(1 - \alpha_n)d(x_n, S(t_n)x_n)^2 \leq d(x_n, p)^2 - d(x_{n+1}, p)^2,$$

since  $\lim_{n \rightarrow \infty} d(x_n, p)$  exists, by taking Limit in above inequality we obtain that

$$\lim_{n \rightarrow \infty} d(x_n, S(t_n)x_n) = 0.$$

Now we show that for a fixed  $t > 0$

$$\lim_{n \rightarrow \infty} d(x_n, S(t)x_n) = 0.$$

With the same proof, we only show that  $\lim_{n \rightarrow \infty} d(x_n, S(t)x_n) = 0$ , without loss of generality, as in (Saejung, 2008) we can assume that

$$\lim_{n \rightarrow \infty} t_n = \lim_{n \rightarrow \infty} \frac{d(x_n, S(t_n)x_n)}{t_n} = 0.$$

$$\begin{aligned} d(x_n; S(t)x_n) &\leq \sum_{k=0}^{[\frac{t}{t_n}] - 1} d(S((k+1)t_n)x_n, S(kt_n)x_n) + d(S([\frac{t}{t_n}]t_n)x_n, S(t)x_n) \\ &\leq [\frac{t}{t_n}]d(S(t_n)x_n, x_n) + d(S(t - [\frac{t}{t_n}]t_n)x_n, x_n) \\ &\leq \frac{t}{t_n}d(S(t_n)x_n, x_n) + \max\{d(S(s)x_n; x_n) : 0 \leq s \leq t_n\}, \end{aligned}$$

Now by continuity of the mapping  $t \rightarrow S(t)x, x \in D$  and  $\lim_{n \rightarrow \infty} d(x_n, S(t_n)x_n) = 0$ , we obtain that  $\lim_{n \rightarrow \infty} d(x_n, S(t)x_n) = 0$ .

□

**Theorem 3.2.** Let  $D$  be a nonempty closed convex subset of a complete CAT(0) space  $X$ . Let  $S := \{S(t) : t \geq 0\}$  be nonexpansive semigroups. Assume that  $\mathcal{F} = F(S) \neq \emptyset$ . Let  $\{x_n\}$  be sequence generated by (1.1), where  $\{\alpha_n\}$  and  $\{t_n\}$  satisfy the following conditions:

- (i)  $\{\alpha_n\} \in [a, b] \subset (0, 1)$
- (ii)  $t_n > 0, \liminf_{n \rightarrow \infty} t_n = 0, \limsup_{n \rightarrow \infty} t_n > 0, \lim_{n \rightarrow \infty} (t_{n+1} - t_n) = 0$ .

Then the sequence  $\{x_n\}$ ,  $\Delta$ -converges to an element of  $\mathcal{F}$ .

*Proof.* It follows from Theorem 3.1 that

$$\lim_{n \rightarrow \infty} d(S(t)x_n, x_n) = 0$$

for each  $t > 0$ . Next steps of the proof as same as (Eslamian and Dhompongsa, 2013).

Now we let  $W_w(x_n) := \cup A(\{u_n\})$  where the union is taken over all subsequences  $\{u_n\}$  of  $\{x_n\}$ . We claim that  $W_w(x_n) \subset \mathcal{F}$ . Let  $u \in W_w(x_n)$ , then there exists a subsequence  $\{u_n\}$  of  $\{x_n\}$  such that  $A(\{u_n\}) = \{u\}$ . By Lemmas 2.4 and Lemmas 2.5 there exists a subsequence  $\{v_n\}$  of  $\{u_n\}$  such that  $\Delta - \lim_n v_n = v \in D$ . We show that  $v \in \mathcal{F}$ , indeed

$$\begin{aligned} d(v_n, S(t)v) &\leq d(v_n, S(t)v_n) + d(S(t)v_n, S(t)v) \\ &\leq d(v_n, S(t)v_n) + d(v_n, v), \end{aligned}$$

hence

$$\limsup_{n \rightarrow \infty} d(v_n, S(t)v) = \limsup_{n \rightarrow \infty} d(v_n, v).$$

By uniqueness of the asymptotic center we obtain that  $S(t)v = v$  for all  $t > 0$  and hence  $v \in \mathcal{F}(S)$  and hence  $v \in \mathcal{F}$ . By Theorem 3.1 the limit  $\lim_{n \rightarrow \infty} d(x_n, v)$  exists. Hence by Lemma 2.6,  $u = v \in \mathcal{F}$ . This shows that  $W_w(x_n) \subset \mathcal{F}$ . Next we show that  $W_w(x_n)$  consists of exactly one point. Let  $\{u_n\}$  be a subsequence of  $\{x_n\}$  with  $A(\{u_n\}) = \{u\}$  and let  $A(\{x_n\}) = \{x\}$ . Since  $u \in W_w(x_n) \subset \mathcal{F}$  and  $d(x_n, v)$  converges, by Lemma 2.6 we have  $x = u$ . □

**Theorem 3.3.** Let  $D$  be a nonempty compact convex subset of a complete CAT(0) space  $X$ . Let  $S := \{S(t) : t \geq 0\}$  be nonexpansive semigroups. Assume that  $\mathcal{F} = F(S) \neq \emptyset$ . Let  $\{x_n\}$  be sequence generated by (1.1), where  $\{\alpha_n\}$  and  $\{t_n\}$  satisfy the following conditions:

- (i)  $\{\alpha_n\} \in [a, b] \subset (0, 1)$
- (ii)  $t_n > 0, \liminf_{n \rightarrow \infty} t_n = 0, \limsup_{n \rightarrow \infty} t_n > 0, \lim_{n \rightarrow \infty} (t_{n+1} - t_n) = 0$ .

Then the sequence  $\{x_n\}$ , converges strongly to an element of  $\mathcal{F}$ .



*Proof.* It follows from Theorem 3.1 that

$$\lim_{n \rightarrow \infty} d(S(t)x_n, x_n) = 0$$

for each  $t > 0$ . By compactness of  $C$ , there exists a subsequence  $\{x_{n_i}\}$  of  $\{x_n\}$  such that  $x_{n_i} \rightarrow w$ . We shall show that  $w \in \mathcal{F}$ , indeed for all  $t > 0$  we have

$$\begin{aligned} d(w, S(t)w) &\leq d(w, x_{n_i}) + d(x_{n_i}, S(t)x_{n_i}) + d(S(t)x_{n_i}, S(t)w) \\ &\leq 2d(w, x_{n_i}) + d(x_{n_i}, S(t)x_{n_i}) \rightarrow 0 \quad \text{as } n \rightarrow \infty \end{aligned}$$

hence we have  $w = S(t)w$ , i.e.,  $w \in \mathcal{F}(S)$  and hence  $w \in \mathcal{F}$ . Since  $\lim_{n \rightarrow \infty} d(x_n, w)$  exists, we obtain the result.  $\square$

*Definition 3.4.* (Schu, 1991) Let  $D$  be a nonempty closed convex subset of a CAT(0) space  $X$  and  $S_n : D \rightarrow D$ , where  $n \in \mathbb{N}$ . Then the family  $\{S_n\}$  is called uniformly asymptotically regular on  $S$ , if for all  $i \in \mathbb{N}$  and any bounded subset  $K$  of  $D$  we have

$$\lim_{n \rightarrow \infty} \sup_{x \in K} d(S_i(S_n x), S_n x) = 0$$

*Theorem 3.5.* Let  $S$  be a nonempty closed convex subset of a complete CAT(0) space  $X$ . Let  $S_n : D \rightarrow D$  be uniformly asymptotically regular and nonexpansive mappings such that  $\mathcal{F} = \bigcap_{n=1}^{\infty} F(S_n) \neq \emptyset$ . Let  $\{x_n\}$  be sequence generated by (1.1), where  $\{\alpha_n\} \in [a, b] \subset (0, 1)$ . Then the sequence  $\{x_n\}$ ,  $\Delta$ -converges to an element of  $\mathcal{F}$ .

*Proof.* Let  $p \in \mathcal{F}$ . Then by Lemma 2.7(i) we have

$$\begin{aligned} d(y_n, p) &= d((1 - \alpha_n)x_n \oplus \alpha_n S_n x_n, p) \\ &\leq (1 - \alpha_n)d(x_n, p) + \alpha_n d(S_n x_n, p) \\ &\leq (1 - \alpha_n)d(x_n, p) + \alpha_n d(x_n, p) \\ &= d(x_n, p) \end{aligned} \tag{3.5}$$

and

$$\begin{aligned} d(x_{n+1}, p) &= d(S_n y_n, p) \\ &\leq d(y_n, p) \\ &\leq d(x_n, p) \end{aligned} \tag{3.6}$$

Hence we have  $d(x_{n+1}, p) \leq d(x_n, p)$ , this gives that the limit  $\lim_{n \rightarrow \infty} d(x_n, p)$  exists. Applying Lemma 2.7(ii) we have

$$\begin{aligned} d(y_n, p)^2 &= d((1 - \alpha_n)x_n \oplus \alpha_n S_n x_n, p)^2 \\ &\leq (1 - \alpha_n)d(x_n, p)^2 + \alpha_n d(S_n x_n, p)^2 - \alpha_n(1 - \alpha_n)d(x_n, S_n x_n)^2 \\ &\leq (1 - \alpha_n)d(x_n, p)^2 + \alpha_n d(x_n, p)^2 - \alpha_n(1 - \alpha_n)d(x_n, S_n x_n)^2 \\ &= d(x_n, p)^2 - \alpha_n(1 - \alpha_n)d(x_n, S_n x_n)^2. \end{aligned} \tag{3.7}$$

$$\begin{aligned}
 d(x_{n+1}, p)^2 &= d(S_n y_n, p)^2 \\
 &\leq d(y_n, p)^2 \\
 &\leq d(x_n, p)^2 - \alpha_n(1 - \alpha_n)d(x_n, S_n x_n)^2.
 \end{aligned}
 \tag{3.8}$$

So,

$$\begin{aligned}
 \sum_{n=1}^{\infty} a(1 - b)d(x_n - S(t_n)x_n)^2 &\leq \sum_{n=1}^{\infty} \alpha_n(1 - \alpha_n)d(x_n, S(t_n)x_n)^2 \\
 &\leq \sum_{n=1}^{\infty} d(x_n, p)^2 - d(x_{n+1}, p)^2, < d(x_1, p)^2 < \infty,
 \end{aligned}$$

this follows that

$$\lim_{n \rightarrow \infty} d(x_n, S_n x_n) = 0.$$

Also we have

$$\begin{aligned}
 d(x_{n+1}, x_n) &\leq d(x_{n+1}, S_n x_n) + d(S_n x_n, x_n) \\
 &= d(S_n y_n, S_n x_n) + d(S_n x_n, x_n) \\
 &\leq d(y_n, x_n) + d(S_n x_n, x_n) \\
 &= d((1 - \alpha_n)x_n \oplus \alpha_n S_n x_n, x_n) + d(S_n x_n, x_n) \\
 &\leq (1 - \alpha_n)d(x_n, x_n) + \alpha_n d(S_n x_n, x_n) + d(S_n x_n, x_n) \\
 &\rightarrow 0 \quad \text{as } n \rightarrow \infty,
 \end{aligned}
 \tag{3.9}$$

and therefore

$$d(x_{n+1}, S_n x_n) \leq d(x_{n+1}, x_n) + d(x_n, S_n x_n) \rightarrow 0.$$

Now, by our assumption, for each  $i \in \mathbb{N}$  we have

$$\begin{aligned}
 d(x_{n+1}, S_i x_{n+1}) &\leq d(x_{n+1}, S_n x_n) + d(S_n x_n, S_i(S_n x_n)) + d(S_i(S_n x_n), S_i x_{n+1}) \\
 &\leq 2d(x_{n+1}, S_n x_n) + \sup_{u \in \{x_n\}} d(S_n u, S_i(S_n u)) \rightarrow 0 \text{ as } n \rightarrow \infty.
 \end{aligned}$$

Next steps of the proof as same as (Eslamian and Dhompangsa, 2013).

We let  $W_w(x_n) := \bigcup A(\{u_n\})$  where the union is taken over all subsequences  $\{u_n\}$  of  $\{x_n\}$ . We claim that  $W_w(x_n) \subset \mathcal{F}$ . Let  $u \in W_w(x_n)$ , then there exists a subsequence  $\{u_n\}$  of  $\{x_n\}$  such that  $A(\{u_n\}) = \{u\}$ . By Lemmas 2.4 and Lemmas 2.5 there exists a subsequence  $\{v_n\}$  of  $\{u_n\}$  such that  $\Delta - \lim_n v_n = v \in C$ . By Lemma 2.8 we have  $v \in \mathcal{F}$ , and hence the limit  $\lim_{n \rightarrow \infty} d(x_n, v)$  exists. Hence by Lemma 2.6,  $u = v \in \mathcal{F}$ . This shows that  $W_w(x_n) \subset \mathcal{F}$ . Next we show that  $W_w(x_n)$  consists of exactly one point. Let  $\{u_n\}$  be a subsequence of  $\{x_n\}$  with  $A(\{u_n\}) = \{u\}$  and let  $A(\{x_n\}) = \{x\}$ . Since  $u \in W_w(x_n) \subset \mathcal{F}$  and  $d(x_n, v)$  converges, by Lemma 2.6 we have  $x = u$ . □

## References

- Bartolini, I., Ciaccia, P. and Patella, M. 2002. String matching with metric trees using an approximate distance, *International Symposium on String Processing and Information Retrieval*, Springer, pp. 271–283.
- Bestvina, M. 2002.  $\mathbb{R}$ -trees in topology, geometry, and group theory, *Handbook of geometric topology*, North-Holland, Amsterdam, pp. 55–91.
- Bridson, M. R. and Haefliger, A. 1999. *Metric spaces of non-positive curvature*, Vol. 319 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*, Springer-Verlag, Berlin.  
**URL:** <https://doi.org/10.1007/978-3-662-12494-9>
- Cho, Y. J., Ćirić, L. and Wang, S.-h. 2011. Convergence theorems for nonexpansive semigroups in  $CAT(0)$  spaces, *Nonlinear Anal.* **74**(17): 6050–6059.  
**URL:** <https://doi.org/10.1016/j.na.2011.05.082>
- Dhompongsa, S., Kirk, W. A. and Panyanak, B. 2007. Nonexpansive set-valued mappings in metric and Banach spaces, *J. Nonlinear Convex Anal.* **8**(1): 35–45.
- Dhompongsa, S., Kirk, W. A. and Sims, B. 2006. Fixed points of uniformly Lipschitzian mappings, *Nonlinear Anal.* **65**(4): 762–772.  
**URL:** <https://doi.org/10.1016/j.na.2005.09.044>
- Dhompongsa, S. and Panyanak, B. 2008. On  $\Delta$ -convergence theorems in  $CAT(0)$  spaces, *Comput. Math. Appl.* **56**(10): 2572–2579.  
**URL:** <https://doi.org/10.1016/j.camwa.2008.05.036>
- Eslamian, M. and Dhompongsa, S. 2013. Modified Ishikawa iteration process for two nonexpansive semigroups in  $CAT(0)$  spaces, *Politehn. Univ. Bucharest Sci. Bull. Ser. A Appl. Math. Phys.* **75**(1): 99–106.
- Espínola, R. and Kirk, W. A. 2006. Fixed point theorems in  $\mathbb{R}$ -trees with applications to graph theory, *Topology Appl.* **153**(7): 1046–1055.  
**URL:** <https://doi.org/10.1016/j.topol.2005.03.001>
- Ishikawa, S. 1974. Fixed points by a new iteration method, *Proc. Amer. Math. Soc.* **44**: 147–150.  
**URL:** <https://doi.org/10.2307/2039245>
- Khan, S. H. 2013. A Picard-Mann hybrid iterative process, *Fixed Point Theory Appl.* pp. 2013:69, 10.  
**URL:** <https://doi.org/10.1186/1687-1812-2013-69>
- Kirk, W. A. 2003. Geodesic geometry and fixed point theory, *Seminar of Mathematical Analysis (Malaga/Seville, 2002/2003)*, Vol. 64 of *Colecc. Abierta*, Univ. Sevilla Secr. Publ., Seville, pp. 195–225.

- Kirk, W. A. 2004. Fixed point theorems in  $CAT(0)$  spaces and  $\mathbb{R}$ -trees, *Fixed Point Theory Appl.* (4): 309–316.  
**URL:** <https://doi.org/10.1155/S1687182004406081>
- Kirk, W. A. and Panyanak, B. 2008. A concept of convergence in geodesic spaces, *Nonlinear Anal.* **68**(12): 3689–3696.  
**URL:** <https://doi.org/10.1016/j.na.2007.04.011>
- Li, X.-s. and Yip, T.-l. 2012. Implicit Mann approximation with perturbations for nonexpansive semigroups in  $CAT(0)$  spaces, *Fixed Point Theory Appl.* pp. 2012:145, 13.  
**URL:** <https://doi.org/10.1186/1687-1812-2012-145>
- Liu, Z.-b., Chen, Y.-s., Li, X.-s. and Xiao, Y.-b. 2013. Implicit Ishikawa approximation methods for nonexpansive semigroups in  $CAT(0)$  spaces, *Abstr. Appl. Anal.* pp. Art. ID 503198, 8.  
**URL:** <https://doi.org/10.1155/2013/503198>
- Mann, W. R. 1953. Mean value methods in iteration, *Proc. Amer. Math. Soc.* **4**: 506–510.  
**URL:** <https://doi.org/10.2307/2032162>
- Park, S. 2010. The KKM principle in abstract convex spaces: equivalent formulations and applications, *Nonlinear Anal.* **73**(4): 1028–1042.  
**URL:** <https://doi.org/10.1016/j.na.2010.04.029>
- Saejung, S. 2008. Strong convergence theorems for nonexpansive semigroups without Bochner integrals, *Fixed Point Theory Appl.* pp. Art. ID 745010, 7.  
**URL:** <https://doi.org/10.1155/2010/806837>
- Schu, J. 1991. Approximation of fixed points of asymptotically nonexpansive mappings, *Proc. Amer. Math. Soc.* **112**(1): 143–151.  
**URL:** <https://doi.org/10.2307/2048491>
- Suzuki, T. 2003. On strong convergence to common fixed points of nonexpansive semigroups in Hilbert spaces, *Proc. Amer. Math. Soc.* **131**(7): 2133–2136.  
**URL:** <https://doi.org/10.1090/S0002-9939-02-06844-2>



# An improved user authentication and key agreement scheme for roaming service in ubiquitous network

Shaheena Khatoon<sup>1</sup> · Te-Yu Chen<sup>2</sup> · Cheng-Chi Lee<sup>3,4</sup>

Received: 6 December 2020 / Accepted: 26 October 2021 / Published online: 7 January 2022  
© Institut Mines-Télécom and Springer Nature Switzerland AG 2021

## Abstract

Up till now, numerous authentication and key agreement schemes have been proposed for ubiquitous networks. Recently, Arshad and Rasoolzadegan also proposed an authentication and key agreement scheme for ubiquitous network with user anonymity. However, we determined that Arshad and Rasoolzadegan's scheme has the following flaws: (1) the login phase is inefficient, which may lead to server resource exhaustion attacks; (2) the password change phase is inefficient and not user-friendly; and (3) the revocation phase arisen when the mobile device is lost and the re-register phase is absent. Therefore, we propose an improved scheme that successfully removes all of the previous mentioned flaws existing in Arshad and Rasoolzadegan's protocol by using the biometric based authentication. Formal analysis of the proposed scheme is conducted using the random oracle model, and heuristic analysis is also conducted to demonstrate that the proposed scheme fulfills all of the security requirements. In addition, the proposed scheme is validated by the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool. Moreover, computational and communication cost comparisons indicate that our improved scheme is more suitable for ubiquitous networks.

**Keywords** Ubiquitous networks · Mutual authentication · Key agreement · Random oracle · AVISPA

## 1 Introduction

Ubiquitous networks enable any mobile user (MU) to remotely access the data and resources of the foreign

network (FN) via the home network (HN). A MU registers himself/herself with his/her HN. When the MU moves away from the region in which his/her HN can provide service, he/she should contact the FN to request for the resources. The MU sends a request to the FN; then, the FN forwards it to the HN for authentication of the MU. After authenticating the MU, the HN accordingly sends the result back to the FN. Then, the FN decides to accept or decline the request on the basis of the result received from the HN. Once the HN has authenticated the MU, a session key is established between FN and MU to ensure secure communication in the future. In addition to mutual authentication, the privacy and intractability of the user's identity are also critical issues in ubiquitous networks. Elliptic curve cryptography (ECC), RSA, hash function, chaotic map, XOR, and concatenation operation are some commonly used cryptographic tools to design secure mutual authentication and key agreement schemes. Given its shorter key length, the ECC equipped with 160 bits key length is faster and more efficient than the RSA equipped with 1024 bits key length. Hash functions and chaotic maps are equivalent in terms of security. However, the hash function is more desirable than the chaotic map because of its lower computation cost.

---

✉ Cheng-Chi Lee  
cclee@mail.fju.edu.tw

Shaheena Khatoon  
shaheenataj.28@gmail.com

Te-Yu Chen  
chendy@mail.ntin.edu.tw

- <sup>1</sup> School of Studies in Mathematics, Pt.Ravishankar Shukla University, Raipur, 492010 (C.G.), India
- <sup>2</sup> Center of General Education, National Tainan Junior College of Nursing, Tainan, Taiwan
- <sup>3</sup> Department of Library and Information Science, Research and Development Center for Physical Education, Health, and Information Technology, Fu Jen Catholic University, New Taipei City, 24205, Taiwan
- <sup>4</sup> Department of Computer Science and Information Engineering, Asia University, Wufeng Shiang, Taichung, 41354, Taiwan

In recent years, numerous authentication and key agreement schemes have been proposed to provide robust security in an open network. Moreover, two-factor and key agreement schemes have been proposed to strengthen the security. The password and smart card are the most commonly adopted in two-factor authentication schemes. However, some flaws have been identified in these two-factor authentication schemes. A weak password can be easily broken by simple dictionary attacks [6, 41]. Meanwhile, a smart card can be misappropriated and subjected to differential power attack. Consequently, biometric-based user authentication protocols are introduced. The biometric-based scheme is considered as a better and more reliable alternative to the password-based authentication scheme because of the following reasons: biometric information from irises, fingerprints, and palm prints (1) is unique and cannot be forged, (2) cannot be guessed, and (3) cannot be lost or stolen. However, biometric information is prone to various noises during the acquisition process and the reproduction of actual biometric is generally difficult. Furthermore, if biometric information is leaked, then serious privacy problems will occur [18]. Bio-hash function and fuzzy extractor [20, 29, 37] are two commonly used techniques to address these kinds of problems. These techniques extract and translate biometric information into a random value.

## 2 Related work

To facilitate roaming services in ubiquitous networks, numerous mutual authentication and key agreement schemes exist in the literature. In 2004, Zhu and Ma [47] first proposed an anonymous authentication and key agreement scheme for ubiquitous networks. However, in 2006, Lee et al. [24] demonstrated that Zhu and Ma's scheme [47] does not provide mutual authentication and perfect backward secrecy and is unable to resist forgery attack. Consequently, they proposed an improved scheme to overcome the security issues of Zhu and Ma's scheme [47]. However, in 2008, Wu et al. [34] showed that the schemes of Zhu and Ma [47] and Lee et al. [24] fail to preserve user anonymity. They also showed that the scheme of Lee et al. [24] does not provide perfect backward secrecy. Additionally, Wu et al. [34] presented an improved scheme. All of the above schemes are password-based. The primitive cryptographic operations, such as symmetric encryption/decryption, hash, xor, and concatenation, are generally used in these schemes.

In 2012, Mun et al. [27] analyzed the scheme of Wu et al. [34] and determined that it does not provide perfect forward secrecy and user anonymity. Consequently, they proposed an improved authentication scheme. In 2014, the scheme of Mun et al. was proven to be vulnerable to a number of attacks by Zhao et al. [45]. Zhao et al. indicated that

the scheme of Mun et al. [27] is prone to impersonation attack, insider attack and fails to achieve user anonymity. Accordingly, they proposed a new authentication scheme to remedy these weaknesses. Elliptic curve cryptography is further adopted in both of [27] and [45].

In 2011, Chen et al. [8] proposed an authentication scheme for ubiquitous networks. However, Xie et al. [42] showed that the scheme of Chen et al. [8] fails to achieve session key security and user privacy in 2014. In 2011, He et al. [15] also proposed a password-based authentication scheme for ubiquitous networks. Nevertheless in 2013, Jiang et al. [19] reported that various security flaws, such as server-spoofing, off-line password-guessing, privileged-insider and replay attacks exist in He et al.'s scheme [15]. They presented an improved scheme to remedy these flaws accordingly. However, in 2103, Wen et al. [35] showed that the scheme of Jiang et al. [19] is not secure. Wen et al. [35] illustrated that the scheme of Jiang et al. [19] cannot achieve forward secrecy and suffers from many kinds of attacks, such as denial-of-service (DOS) attack, stolen verifier attack, server-spoofing attack, and replay attack. They also proposed an improved scheme which was independently analyzed by Farash et al. [12] and Gope and Hwang [13]. They examined the scheme of Wen et al. [35] and determined that it is prone to off-line password-guessing attacks. In 2015, Farash et al. [12] and Gope and Hwang [13] presented their improved schemes, respectively. In addition to the frequently used cryptographic operations, the quadratic residues are launched to design the schemes of [13, 19, 35].

In 2016, Karuppiyah et al. [21] analyzed the scheme of Farash et al. [12] and found its vulnerability against off-line password-guessing and replay attacks. Moreover, the scheme of Farash et al. [12] fails to provide user anonymity, session key security, and perfect forward secrecy. Karuppiyah et al. [21] proposed an improved scheme which was analyzed by Arshad and Rasoolzadegan [2] in 2017. They showed that the scheme of Karuppiyah et al. [21] cannot resist the off-line password-guessing attack and fails to provide perfect forward secrecy. In 2017, Farash et al.'s scheme [12] was also analyzed by Wu et al. [39] and Chaudhry et al. [9]. They showed that the scheme of Farash et al. [12] can reveal the session key and secret parameters of the mobile node, which leads to mobile node impersonation attack, and cannot facilitate user anonymity. In 2017, Gope and Hwang's scheme [13] was also analyzed by Wu et al. [39].

In 2017, Xie et al. [43] proposed an authentication scheme for ubiquitous network using chaotic maps. However, Ostad-Sharif et al. [33] found that Xie et al. scheme [43] is vulnerable to the known session specific information attack and proposed an improved scheme in 2019. In 2018, Lee et al. [17] showed that the scheme of Chaudhry et al. [9] is not secure against user impersonation

**Table 1** The flaws of the related protocols

Major attack/ flaw	Suspected protocol
Lack of perfect backward secrecy	Zhu and Ma [47]
Lack of mutual authentication	Zhu and Ma [47]
Lack of user anonymity	Zhu and Ma [47], Lee et al. [24], Wu et al. [34], Chen et al. [8], Mun et al. [27], Farash et al. [12], Wu et al. [39]
Lack of perfect forward secrecy	Lee et al. [24], Jiang et al. [19], Karuppiah et al. [21], Wu et al. [39]
Forgery attack	Zhu and Ma [47]
Session key disclosure attack	Chen et al. [8]
Server-spoofing attack	He et al. [15], Jiang et al. [19]
Offline password-guessing attack	He et al. [15], Wen at al. [35], Karuppiah et al. [21]
Insider attack	He et al. [15], Mun et al. [27]
Replay attack	He et al. [15], Jiang et al. [19]
Impersonation attack	Mun et al. [27], Farash et al. [12], Chaudhry et al. [9]
DoS attack	Jiang et al. [19]
Stolen verifier attack	Jiang et al. [19]

attack and stolen mobile device attack. Furthermore, the scheme of Chaudhry et al. [9] has incorrect login-input detection and password change phase and does not have the revocation phase. Both schemes of [39] and [17] are

designed by the help of the elliptic curve cryptography. In 2019, Lu et al. [26] found some weaknesses in Gope and Hwang’s scheme [13] and proposed an ECC based user authentication scheme. In 2020, Alzahrani et al. [3] showed that Lu et al.’s scheme [26] is vulnerable to stolen verifier and traceability attacks and proposed an improved scheme based on ECC. In the same year, Khatoun and Thakur [32] demonstrated that Lee et al.’s scheme [17] is vulnerable to off-line dictionary attack and replay attack and proposed an improved scheme

Table 1 provides a summary of the flaws of the previously mentioned schemes. Cryptographic operations used to design the previous schemes are also briefly reviewed in Table 2.

### 2.1 Motivation and contributions

Arshad and Rasoolzadegan [2] proposed an authentication and key agreement scheme for roaming service with user anonymity in a ubiquitous network in 2017. They also conducted a formal security analysis of the proposed scheme using Burrows-Abadi-Needham (BAN) logic [5] and proved that it is secure against various known attacks and is more efficient than the existing schemes. However, we found that Arshad and Rasoolzadegan’s scheme has the following flaws: (1) the login phase is inefficient, which may lead to server resource exhaustion attacks; (2) the password change phase is inefficient and not

**Table 2** Cryptographic operations used in the related schemes

Protocol	OP1	OP2	OP3	OP4	OP5	OP6	OP7	OP8
Zhu and Ma [47]	✓	✓	✓	✓	–	–	–	–
Lee et al. [24]	✓	✓	✓	✓	–	–	–	–
Wu et al. [34]	✓	✓	✓	✓	–	–	–	–
Mun et al. [27]	✓	✓	✓	–	–	–	–	✓
Zhao et al. [45]	✓	✓	✓	✓	–	–	–	✓
Chen et al. [8]	✓	✓	✓	✓	–	–	–	–
Xie et al. [42]	✓	✓	✓	✓	✓	–	–	–
He et al. [15]	✓	✓	✓	–	–	–	–	–
Jiang et al. [19]	✓	✓	✓	–	–	✓	✓	–
Wen at al. [35]	✓	✓	✓	–	✓	✓	✓	–
Farash et al. [12]	✓	✓	✓	✓	–	–	–	–
Gope and Hwang [13]	✓	✓	✓	✓	–	✓	✓	–
Karuppiah et al. [21]	✓	✓	✓	✓	✓	–	–	–
Wu et al. [39]	✓	✓	✓	✓	–	–	–	✓
Chaudhry et al. [9]	✓	✓	✓	✓	–	–	–	–
Lee at al. [17]	✓	✓	✓	✓	–	–	–	✓
OP1: String concatenation				OP2: Xor				
OP3: Hash				OP4: Symmetric encryption/decryption				
OP5: Modular exponentiation				OP6: Modular squaring				
OP7: Square root computation				OP8: Elliptic curve point multiplication				

user-friendly; and (3) the revocation phase arisen from mobile devices are lost and the re-register phase are absent. Therefore, we propose an improved scheme that successfully removes all of the previously mentioned flaws existing in Arshad and Rasoolzadegan's protocol by using biometric-based authentication. The security of the proposed scheme is analyzed using the random oracle model and the formal security verification is completed through AVISPA tool. Heuristic analysis is also conducted. Moreover, the proposed scheme achieves comparatively better performance by comparing with the other existing schemes.

The remainder of this paper is organized as follows: The preliminaries are given in Section 3. This section also briefly introduces a typical model of a ubiquitous network and the capabilities of an adversary. Arshad and Rasoolzadegan's scheme is analyzed in Section 4. The improved scheme is proposed in Section 5. Formal security and heuristic analyses of the improved scheme are demonstrated in Sections 6 and 7 respectively. Formal security verification through AVISPA simulation is performed in Section 8. The performance analysis and comparisons are illustrated in Sections 9. Finally, Section 10 concludes this paper.

### 3 Preliminaries

This section defines two computationally hard problems and briefly discusses a typical model of a ubiquitous network and its security requirements and adversary capabilities.

### 3.1 Computationally hard problems

Given  $p$  and  $q$  two large primes,  $F_p$  is the prime field of order  $p$ ,  $E/F_p$  is an elliptic curve defined over  $F_p$ ;  $E/F_p$  equipped with the usual addition on the elliptic curve is a group. Let  $G$  be a subgroup of  $E/F_p$  of order  $q$ . Let  $P$  be a generator of  $G$ . We recall the following two problems [48–50]:

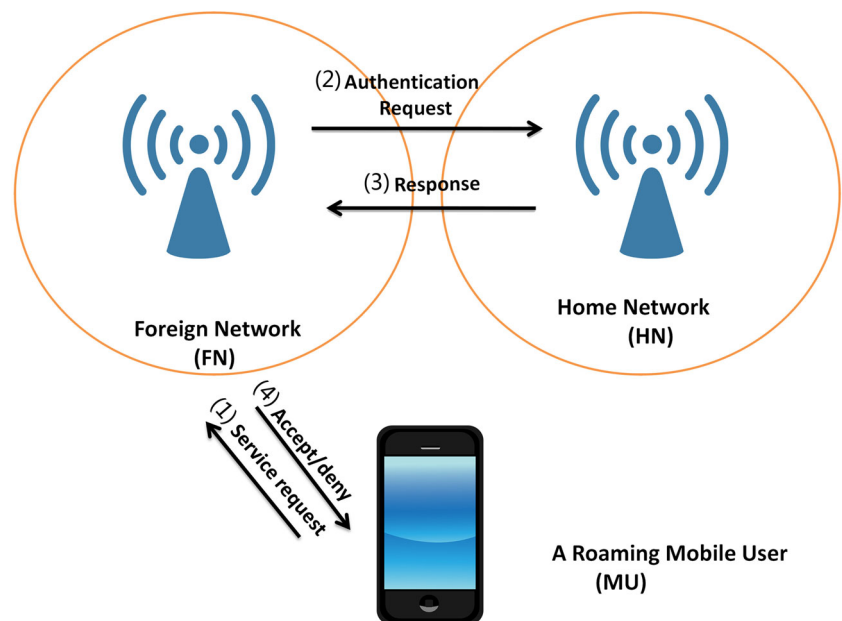
- Elliptic curve discrete logarithm problem (ECDLP): Given a point  $Q$  in  $G$ , find an integer  $a \in Z_p^*$  such that  $Q = aP$ .
- Elliptic curve computational Diffie-Hellman problem (ECCDHP): Given two points  $(aQ, bQ)$  in  $G$ , compute  $abQ$  in  $G$ .

Generally, ECDLP and ECCDHP are assumed to be intractable. That is, no algorithm can be used to solve ECDLP and ECCDHP in polynomial time.

### 3.2 Typical model of the ubiquitous network

Ubiquitous networks provide roaming services to the **MU**, while he/she roams from one place to another [19]. In a ubiquitous network, the **MU** obtains access to the remote services provided by the **FN**, which achieves prior agreement with the **HN**, while he/she roams outside the **HN**. Mutual authentication and session key security can be achieved by the **MU** and **FN** with the support of the **HN**.

**Fig. 1** A typical model for a ubiquitous network





The scenario is depicted in Fig. 1. The mutual authentication process can be briefly described as follows:

1. The **MU** requests permission from the **FN** to access the services.
2. The **FN** sends a request to the **HN** to authenticate the **MU**.
3. After receiving the request from the **FN**, the **HN** checks whether the **MU** is a registered user or not and sends back the result to the **FN**.
4. The **MU**'s request is either denied or accepted by the **FN** in accordance with the response of the **HN**.

### 3.3 Security requirements

The security requirements of a ubiquitous network are elaborated as follows:

- Mutual authentication: Mutual authentication enables two parties to mutually authenticate each other in the scheme. In the ubiquitous network, the mutual authentication between **FN** and **MU** is facilitated by the **HN**.
- User anonymity: This property refers to the protection of the identity of the user, which is necessary in a distributed system like a ubiquitous network. The user's anonymity is protected to prevent the **FN** or any adversary from determining the user's identity. Moreover, the location of the user should also remain anonymous.
- Key agreement: The **FN** and **MU** must agree upon a common session key for further secure communication.
- User-friendly: A user-friendly scheme allows the **MU** to pick any password of his/her choice and to change it locally whenever he/she requires [38]. Moreover, the user can revoke the card in case the card is stolen, lost, or misplaced and can reregister to the system again.
- The proposed scheme should be able to resist all known attacks.

### 3.4 Adversary capabilities

The following are the capabilities of an adversary  $A$ :

- The communication channel is under full control of an adversary, i.e., the adversary  $A$  can modify, intercept, delete, and resend any legitimate message [10, 11, 22, 23].
- The adversary  $A$  can enumerate all of the items in  $D_{pw} \times D_{id}$  in polynomial time, where  $D_{pw}$  and  $D_{id}$  denote the password and identity spaces, respectively [36, 46].

- All of the public parameters are known to  $A$ , including the user's biometrics [16, 46].

## 4 Weaknesses of Arshad and Rasoolzadegan's protocol

### 4.1 A brief review of Arshad and Rasoolzadegan's protocol

This section provides a brief review of Arshad and Rasoolzadegan's protocol. The protocol consists of the following three phases: registration, login and authentication, and password change phases. Table 3 lists the various notations used in illustrating Arshad and Rasoolzadegan's protocol.

1. **Registration phase:** The registration phase is executed between **MU** and **HN**. It is a one-time process in which any **MU** registers his/her identity with the **HN**. The registration phase between **MU** and **HN** can be described as follows:
  - (a) The **MU** selects  $\{ID_M, PW_M, b\}$ , where  $b$  is a random number of his/her choice.
  - (b) The **MU** computes  $MPW_M = h(ID_M || PW_M || b)$ .
  - (c) The **MU** sends registration request  $\{ID_M, MPW_M\}$  to the **HN**.
  - (d) Upon receiving  $\{ID_M, MPW_M\}$ , the **HN** checks whether  $ID_M$  is the same as that of another registered **MU** or not. If it is, then the **HN** requests the **MU** to select another identity.

**Table 3** Notations used in Arshad and Rasoolzadegan's protocol

Notations	Description
<b>MU</b>	The mobile user.
<b>FN</b>	The foreign network.
<b>HN</b>	The home network
$ID_M, PW_M$	The mobile user's identity and password.
$K_H$	The secret key of <b>HN</b> .
$K_{FH}$	The secret key pre-shared between <b>HN</b> and <b>FN</b> .
$T_1, T_2$	Time stamps.
$P$	A base point of an elliptic curve.
$h(\cdot)$	A secure cryptographic hash function.
$E_k(\cdot)/D_k(\cdot)$	Symmetric encryption/decryption using the key $k$ .
$  $	Concatenation operation.
$\oplus$	XOR operation.

- (e) Otherwise, the **HN** selects a random number  $c$  and computes  
 $A_M = h(ID_M || K_H)$ ,  
 $B_M = A_M \oplus MPW_M$ , and  
 $DID_M = E_{K_H}(ID_M || c)$ .
- (f) The **HN** securely sends  $\{DID_M, B_M, E, P, n, h(\cdot), E_K(\cdot), D_K(\cdot)\}$  to the **MU**.
- (g) The **MU** stores the received values  $\{DID_M, B_M, E, P, n, h(\cdot), E_K(\cdot), D_K(\cdot)\}$  along with  $b$  on his/her mobile device.

2. **Login and authentication phase:** The **MU** and **HN** mutually authenticate each other and agree upon a common session key in the following manner:

- (a) The **MU** inputs his/her  $ID_M$  and  $PW_M$ . Then, the **MU**'s device computes the following:  
 $MPW_M = h(ID_M || PW_M || b)$ ,  
 $A_M = B_M \oplus MPW_M$ ,  
 $N_M = n_M P$ , where  $n_M$  is randomly selected by the device,  
 $MV_{MH} = h(A_M || N_M || ID_F || ID_M || T_1)$ , where  $T_1$  is the present time stamp.  
 The **MU** sends  $M_1 = \{DID_M, MV_{MH}, N_M, T_1\}$  to the **FN**.
- (b) After receiving  $M_1$ , the **FN** first checks the freshness of  $T_1$  and then computes the following:  
 $N_F = n_F P$ , where  $n_F$  is randomly selected by the **FN**,  
 $MV_{FH} = h(M_1 || N_F || ID_F || T_2 || K_{FH})$ , where  $T_2$  is the present time stamp and  $K_{FH}$  is a secret key shared between **FN** and **HN**.  
 Then, the **FN** sends a message  $M_2 = \{ID_F, M_1, N_F, MV_{FH}, T_2\}$  to the **HN**.
- (c) Upon receiving  $M_2$ , the **HN** first checks the freshness of  $T_2$  and then computes  $MV_{FH}^*$  as  
 $MV_{FH}^* = h(M_1 || N_F || ID_F || T_2 || K_{FH})$ .  
 The **HN** tests whether  $MV_{FH}^*$  is equal to  $MV_{FH}$  included in  $M_2$ . If they are not equal, then the **HN** rejects the request. Otherwise, the **HN** decrypts  $DID_M$  as  
 $D_{K_H}(DID_M) = (ID_M || c)$ ,  
 and searches  $ID_M$  in its database. If the identity does not exist in the database, then the **HN** aborts this session. Otherwise, the **HN** computes the following:  
 $A_M = h(ID_M || K_H)$ ,  
 $MV_{MH}^* = h(A_M || N_M || ID_F || ID_M || T_1)$ .  
 Then the **HN** tests  
 $MV_{MH}^* = MV_{MH}$ .

If the equality does not hold, then the **HN** rejects the request.

Otherwise, the **HN** randomly selects  $c^{New}$  and computes the following:

$$DID_M^{New} = E_{K_H}(ID_M || c^{New}),$$

$$MV_{HM} = h(A_M || ID_F || N_F || ID_M || N_M || DID_M^{New}),$$

$$K_{HM} = h(N_M || ID_F || A_M || ID_M || N_F),$$

$$M_{HM} = E_{K_{HM}}(DID_M^{New}),$$

$$MV_{HF} = h(ID_F || MV_{FH} || K_{FH} || M_{HM} || MV_{HM} || N_F || N_M).$$

Then **HN** sends  $M_3 = \{MV_{HF}, M_{HM}, MV_{HM}\}$  to the **FN**.

- (d) After receiving  $M_3$ , the **FN** computes  
 $MV_{HF}^* = h(ID_F || MV_{FH} || K_{FH} || M_{HM} || MV_{HM} || N_F || N_M)$ .  
 Then, the **FN** tests  
 $MV_{HF}^* = MV_{HF}$ .  
 If the equation does not hold, then the **FN** rejects the request. Otherwise, the **FN** computes the following:  
 $SK = h(n_F N_M) = h(n_F n_M P)$ ,  
 $MV_{FM} = h(M_{HM} || MV_{HM} || SK || N_F)$ .  
 Then, the **FN** sends  $M_4 = \{M_{HM}, MV_{HM}, N_F, MV_{FM}\}$  to the **MU**.
- (e) Upon receiving  $M_4$ , the **MU** computes  
 $K_{HM} = h(N_M || ID_F || A_M || ID_M || N_F)$ ,  
 and decrypts  $M_{HM}$  as  
 $D_{K_{HM}}(M_{HM}) = (DID_M^{New})$ .  
 Then, the **MU** computes  
 $MV_{HM}^* = h(A_M || ID_F || N_F || ID_M || N_M || DID_M^{New})$   
 and tests whether  $MV_{HM}^*$  is equal to  $MV_{HM}$ . If they are not equal, then the **MU** rejects the request. Otherwise, the **MU** computes the following:  
 $SK = h(n_M N_F) = h(n_M n_F P)$ ,  
 $MV_{FM}^* = h(M_{HM} || MV_{HM} || SK || N_F)$ .  
 Then, the **MU** tests the equality of  $MV_{FM}^*$  and  $MV_{FM}$ . If the equality does not hold, then the **MU** rejects the request. Otherwise, the **MU** completes the authentication on the **FN**. Then, the **MU** computes  
 $MV_{MF} = h(N_M || M_{HM} || MV_{HM} || SK)$ ,  
 and replaces  $DID_M$  with  $DID_M^{New}$  in his/her mobile device, and finally sends  $M_5 = \{MV_{MF}\}$  to the **FN**.
- (f) After receiving  $M_5$ , the **FN** computes  
 $MV_{MF}^* = h(N_M || M_{HM} || MV_{HM} || SK)$ ,  
 and verifies whether  $MV_{MF}^*$  is equal to  $MV_{MF}$ . If they are not equal, then the **FN** rejects the request. Otherwise, the **FN** authenticates the **MU** and accepts his/her request.

3. **Password change phase:** This phase enables the **MU** to change his/her current password  $PW_M$  to a new password  $PW_M^{New}$ .

(a) The **MU** inputs his/her identity  $ID_M$  and sends a request message  $\{DID_M, CPW_M, T_1\}$  to the **HN** by computing the following:

$$MPW_M = h(ID_M || PW_M || b),$$

$$A_M = B_M \oplus MPW_M,$$

$$CPW_M = h(ID_M || A_M || DID_M || T_1),$$

where  $T_1$  is the current time stamp.

(b) After receiving the request, the **HN** checks the freshness of  $T_1$ . If it is fresh, then the **HN** decrypts  $DID_M$  as

$$D_{K_H}(DID_M) = (ID_M || c).$$

The **HN** confirms whether  $ID_M$  is a registered user or not by searching its database. If it is a registered user, then the **HN** computes the following:

$$A_M = h(ID_M || K_H),$$

$$CPW_M^* = h(ID_M || A_M || DID_M || T_1).$$

Then, the **HN** verifies whether  $CPW_M^*$  is equal to  $CPW_M$  or not. If they are not equal, then the **HN** rejects the request. Otherwise, the **HN** selects a new random number  $c^{New}$  and computes the following:

$$DID_M^{New} = E_{K_H}(ID_M || c^{New}),$$

$$VPW_H = h(ID_M || CPW_M || DID_M || A_M || DID_M^{New} || \text{ACCEPT} || T_2),$$

where  $T_2$  is the current time stamp,

$$K_{HM} = h(ID_M || T_2 || CPW_M || A_M || DID_M),$$

$$CPW_H = E_{K_{HM}}(DID_M^{New}, VPW_H, \text{ACCEPT}).$$

Then, the **HN** sends the message  $\{CPW_H, T_2\}$  to the **MU**.

(c) Upon receiving the message  $\{CPW_H, T_2\}$ , the **MU** checks the freshness of  $T_2$ . If it is not fresh, then the **MU** stops the process. Otherwise, the **MU** computes

$$K_{HM} = h(ID_M || T_2 || CPW_M || A_M || DID_M),$$

and decrypts  $CPW_H$  as

$$D_{K_{HM}}(CPW_H) = (DID_M^{New}, VPW_H, \text{ACCEPT}).$$

Then, the **MU** computes

$$VPW_H^* = h(ID_M || CPW_M || DID_M || A_M || DID_M^{New} || \text{ACCEPT} || T_2).$$

The **MU** verifies whether  $VPW_H^*$  is equal to  $VPW_H$  or not. If the equality does not hold, then the **MU** terminates the session. Otherwise, the **MU** computes

$$MPW_M^{New} = h(ID_M || PW_M^{New} || b) \text{ and}$$

$$B_M^{New} = B_M \oplus MPW_M \oplus MPW_M^{New}$$

$$= A_M \oplus MPW_M \oplus MPW_M \oplus MPW_M^{New}$$

$$= A_M \oplus MPW_M^{New}.$$

Finally, the **MU** replaces  $B_M$  and  $DID_M$  with  $B_M^{New}$  and  $DID_M^{New}$ , respectively.

## 4.2 Security flaws in Arshad and Rasoolzadegan’s protocol

### 4.2.1 Server resource exhaustion attack

We determined that Arshad and Rasoolzadegan’s protocol is prone to the server resource exhaustion attack due to its inefficient login and authentication phase. According to their scheme, as soon as the **MU** inputs his/her  $ID_M$  and  $PW_M$  into the mobile device, the device directly computes  $M_1$  (the login request message) without verifying the correctness of the parameters entered by the **MU**. If an incorrect identity or password is provided by the user either intentionally or accidentally, then the mobile device computes the incorrect  $M_1$  and sends it to the **FN**. Subsequently, the **FN** forwards it in the form of  $M_2$  to the **HN**. Then, the **HN** checks the correctness of  $ID_M$  and  $PW_M$  to decide whether to accept or reject the login request accordingly. Therefore, the **HN** is responsible for checking the correctness of  $ID_M$  and  $PW_M$ , but not the mobile device. This operation wastes the **HN**’s valuable resources including its memory and CPU cycles. In this circumstance it causes unnecessary burden on the **HN** and may lead to the server resource exhaustion attack. In a satisfied password-based authentication scheme, the mobile device should check the correctness of the entered  $ID_M$  and  $PW_M$  before the login message is sent for further authentication. In the following cases, we elaborate on this problem in Arshad and Rasoolzadegan’s protocol.

*Case 1* This case will discuss the problem encountered in Arshad and Rasoolzadegan’s login and authentication phases when a wrong identity  $ID_M^{wrong}$  is inserted by the **MU** instead of the correct identity  $ID_M$ .

Step 1 The **MU** enters the wrong identity  $ID_M^{wrong}$  and the correct password  $PW_M$ . The device randomly selects  $n_M$  and computes

$$MPW_M^{wrong} = h(ID_M^{wrong} || PW_M || b),$$

$$A_M^{wrong} = B_M \oplus MPW_M^{wrong},$$

$$N_M = n_M P, \text{ and}$$

$$MV_{MH}^{wrong} = h(A_M^{wrong} || N_M || ID_F || ID_M^{wrong} || T_1).$$

Then, the **MU** sends  $\{DID_M, MV_{MH}^{wrong}, N_M, T_1\}$  to the **FN**.

Step 2 The **FN** sends the message  $M_2 = \{ID_F, M_1, N_F, MV_{FH}, T_2\}$  to the **HN**. Upon receiving  $M_2$ , the **HN** first authenticates the **FN**. The **HN** subsequently

authenticates the **MU** by performing the following process. The **HN** obtains  $ID_M$  by decrypting  $DID_M$  as

$$D_{K_H}(DID_M) = (ID_M || c).$$

Then, the **HN** computes

$$A_M = h(ID_M || K_H) \text{ and}$$

$$MV_{MH}^* = h(A_M || N_M || ID_F || ID_M || T_1).$$

Finally, the **HN** authenticates the **MU** by verifying whether  $MV_{MH}^*$  is equal to  $MV_{MH}^{wrong}$  or not. Obviously, the **HN** would reject the login request because  $MV_{MH}^*$  is not equal to  $MV_{MH}^{wrong}$ . However, the **HN** has wasted a considerable amount of computational cost on authenticating the **FN** and **MU**. Moreover, the **MU** should be notified if a wrong identity or password is entered in input.

**Case 2** This case will discuss the problem encountered in Arshad and Rasoolzadegan's login and authentication phases when a wrong password  $PW_M^{wrong}$  is inserted by the **MU** instead of the correct password  $PW_M$ .

**Step 1** The **MU** enters the incorrect password  $PW_M^{wrong}$  and the correct identity  $ID_M$ . The device randomly selects  $n_M$  and computes

$$MPW_M^{wrong} = h(ID_M || PW_M^{wrong} || b),$$

$$A_M^{wrong} = B_M \oplus MPW_M^{wrong}, N_M = n_M P,$$

$$MV_{MH}^{wrong} = h(A_M^{wrong} || N_M || ID_F || ID_M || T_1).$$

Then, the **MU** sends  $\{DID_M, MV_{MH}^{wrong}, N_M, T_1\}$  to the **FN**.

**Step 2** The **FN** sends the message  $M_2 = \{ID_F, M_1, N_F, MV_{FH}, T_2\}$  to the **HN**. Upon receiving  $M_2$ , the **HN** first authenticates the **FN**. The **HN** subsequently authenticates the **MU** by performing the following process. The **HN** obtains  $ID_M$  by decrypting  $DID_M$  as

$$D_{K_H}(DID_M) = (ID_M || c).$$

Then, the **HN** computes

$$A_M = h(ID_M || K_H),$$

$$MV_{MH}^* = h(A_M || N_M || ID_F || ID_M || T_1).$$

Finally, the **HN** authenticates the **MU** by verifying whether  $MV_{MH}^*$  is equal to  $MV_{MH}^{wrong}$  or not. Obviously, the **HN** would reject the login request because  $MV_{MH}^*$  is not equal to  $MV_{MH}^{wrong}$ . Similar to that in Case 1, the **HN** has wasted a considerable amount of computational cost on authenticating the **FN** and the **MU** when the **HN** detects this problem.

In the previously presented cases, if the **MU** is a legitimate user, then the **HN** rejects his/her request because of the unsatisfied verification caused by his/her mistyping. By contrast, a malicious user can burden the **HN** by inputting fake parameters. All of these will subsequently lead to a server resource exhaustion attack. Thus, we conclude

that the mobile device should perform an efficient and robust authentication process to verify the login identity and password before the **FN** and **HN** could execute further authentication.

#### 4.2.2 Password change phase is inefficient and unfriendly

The password change phase of Arshad and Rasoolzadegan's protocol is inefficient and not user-friendly. Their protocol requires two rounds of secure communication for each password change, which is costly and difficult to achieve in the real-world environment. Furthermore, periodic change of password is necessary for security reasons. Therefore, the mobile device should be able to change the password by itself without any intervention of the **HN**.

#### 4.2.3 Absence of lost/stolen mobile device revocation Phase

The revocation phase is required to ensure adequate security of the end user in any smart-card-based authentication scheme. However, Arshad and Rasoolzadegan's protocol does not provide a revocation phase for a lost/stolen device. The revocation phase is always recommended in the design of any authentication scheme so that the lost/stolen device can be blocked by the user to prevent any misuse of the smart card, as well as the request for a new smart card. Usually, smart cards are non-temper resistant, i.e., if an adversary steals/picks the smart card of any legitimate user, then the adversary can obtain information from the card by performing offline analysis, can derive the valid password of the user, and can impersonate the legal user with the help of the guessed password and the stolen/lost smart card. Thus, the lost/stolen smart card revocation phase is a desirable phase in any authentication scheme.

## 5 The proposed scheme

This section elaborates the improved scheme, which consists of the registration, login and authentication, password change, revocation, and reregister phases. The proposed scheme can resist various known attacks and provide necessary security attributes. The scheme is improved from the following aspects:

- A public key algorithm is used to resist the offline dictionary attack. The verification parameter between **MU** and the **HN** consists of a "challenge"  $N_M, N'_M$ . The adversary  $A$  who intends to start an offline dictionary attack has to know the dynamic key  $n_m$ , which exists apart from the static values stored in the mobile device. Thus, the offline dictionary attack cannot be launched in the proposed scheme.

**Table 4** Notations used in the proposed scheme

Notations	Description
<b>MU<sub>i</sub></b>	Mobile user <i>i</i> .
<b>FN</b>	Foreign network.
<b>HN</b>	Home network.
<i>ID<sub>i</sub>, PW<sub>i</sub>, BIO<sub>i</sub></i>	<b>MU<sub>i</sub></b> 's identity, password, and biometric information.
<i>x</i>	The private key of <b>HN</b> .
<i>K<sub>FH</sub></i>	The secret key pre-shared between <b>HN</b> and <b>FN</b> .
<i>h(·)</i>	A cryptographic secure hash function.
<i>T<sub>i</sub>, T<sub>f</sub>, T<sub>h</sub></i>	Time stamps of <b>MU<sub>i</sub></b> , <b>FN</b> and <b>HN</b> .
<i>Gen(BIO<sub>i</sub>)</i>	The part of fuzzy extractor which outputs <i>R<sub>i</sub></i> (biometric key) and <i>P<sub>i</sub></i> (helper string).
<i>Rep(BIO<sub>i</sub>, P<sub>i</sub>)</i>	The part of fuzzy extractor which outputs <i>R<sub>i</sub></i> (biometric key) in <i>Gen(BIO<sub>i</sub>)</i> .
→	Represents the network which is insecure.
⇒	Represents the network which is secure.
	Concatenation operation.
⊕	XOR operation.

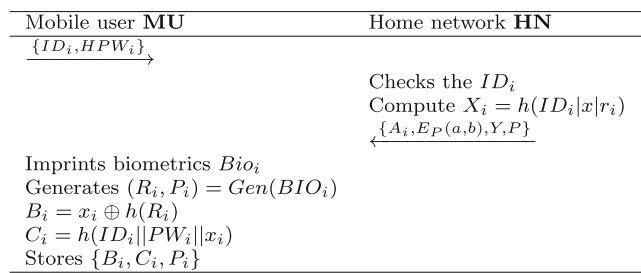
- The proposed scheme also uses “List” and “fuzzy-verifiers” to resist the on-line dictionary attack [38, 40].
- The proposed scheme protects user anonymity by deploying a dynamic identity technique via a public key algorithm.

Table 4 lists the various notations used in the proposed scheme.

### 5.1 Registration phase

Figure 2 illustrates the registration phase. A mobile user **MU<sub>i</sub>** registers with an **HN** in the following manner:

1. **MU<sub>i</sub> ⇒ HN**: {*ID<sub>i</sub>, HPW<sub>i</sub>*}.  
 $HPW_i = h(PW_i || x_i)$ , where *x<sub>i</sub>* is a random number generated by the mobile device.



**Fig. 2** Registration phase

2. **HN ⇒ MU<sub>i</sub>**: {*A<sub>i</sub>, Y, P*}.  
 Upon receiving the registration request, the **HN** checks whether *ID<sub>i</sub>* exists in its database or not. If it exists, then the **HN** requests the user to select another *ID<sub>i</sub>*. Otherwise, the **HN** computes  $X_i = h(ID_i || x || r_i)$ , where *r<sub>i</sub>* is a random number generated by **HN**,  
 $A_i = X_i \oplus HPW_i$ , and  
 $Y = xP$ .  
 The **HN** also records (*ID<sub>i</sub>, r<sub>i</sub>, List*) in its database. Notably, *List* counts the number of fail login attempts of an **MU** and its initial value is assigned as NULL. If the value of *List* exceeds the threshold value, then the mobile device will be suspended until the user reregisters.
3. Upon receiving the message from the **HN**, **MU<sub>i</sub>** imprints his/her biometrics *BIO<sub>i</sub>* and generates  $(R_i, P_i) = Gen(BIO_i)$ ,  
 $B_i = x_i \oplus h(R_i)$ , and  
 $C_i = h(ID_i || PW_i || x_i)$ .  
 Finally, **MU<sub>i</sub>** stores {*A<sub>i</sub>, P, h(·), B<sub>i</sub>, C<sub>i</sub>, P<sub>i</sub>, Y*} in the mobile device.

### 5.2 Login and authentication phase

This phase enables the **FN** to authenticate the login request of **MU<sub>i</sub>** and negotiate a session key with the help of the **HN**. Here, *K<sub>FH</sub>* is the secret key pre-shared between **HN** and **FN**. Figure 3 briefly summarizes the login and authentication phase.

1. **MU<sub>i</sub> → FN**:  $M_1 = \{DID_i, N_M, M_{MH}, T_i\}$ .  
**MU<sub>i</sub>** inputs *ID<sub>i</sub>, PW<sub>i</sub>*, and *BIO<sub>i</sub>*. Then, the mobile device computes the following:  
 $R_i^* = Rep(BIO_i, P_i)$ ,  
 $x_i^* = B_i \oplus h(R_i^*)$ , and  
 $C_i^* = h(ID_i || PW_i || x_i^*)$ .  
 If  $C_i \neq C_i^*$ , then the device aborts the process. Otherwise, the device randomly generates a number  $n_m \in Z_p^*$  and computes the following:  
 $N_M = n_m P$ ,  
 $N'_M = n_m Y$ ,  
 $X_i^* = A_i \oplus HPW_i^*$ ,  $k_i = h(X_i^* || T_i)$ ,  
 $DID_i = ID_i \oplus h(N_M || N'_M)$ , and  
 $M_{MH} = h(X_i^* || N_M || N'_M || k_i || T_i)$ .  
 Then, the mobile device sends the login request  $M_1 = \{DID_i, N_M, M_{MH}, T_i\}$  to the **FN**.
2. **FN → HN**:  $M_2 = \{ID_F, N_F, N_M, M_1, M_{FH}, T_i, T_f\}$ .  
 The **FN** first checks the freshness of *T<sub>i</sub>* and then randomly generates a number  $n_f \in Z_p^*$  and computes the following:  
 $N_F = n_f P$ ,

**Fig. 3** Login and authentication phase

Mobile user <b>MU</b>	Foreign network <b>FN</b>	Home network <b>HN</b>
Enters $ID_i, PW_i, BIO_i$ Verifies $C_i \neq C_i^*$ Computes $N_M = n_m P$ $N'_M = n_m Y$ $X_i^* = A_i \oplus HPW_i^*$ $k_i = h(X_i^*    T_i)$ $DID_i = ID_i \oplus h(N_M    N'_M)$ $M_{MH} = h(X_i^*    N_M    N'_M    k_i    T_i)$ $(M_1 = \{DID_i, N_M, M_{MH}, T_i\})$	Checks $T_i$ Computes $N_F = n_f P$ $M_{FH} = h(M_1    ID_F    N_F    T_f    K_{FH})$ $(M_2, T_h)$	Checks $T_h$ Verifies $M_{FH}^* \neq M_{FH}$ Search $(ID_i, r_i, List)$ Verifies $M_{MH}^* \neq M_{MH}$ Sets $List = List + 1$ Computes $X'_f, M, M_{HF}, M_{HM}$ $(M_3 = \{M_1, M_{HM}, M_{HF}, T_h\})$
Check freshness of $t_h$ , Verifies $M_{HM}^* = M_{HM}$ , Computes: $SK = h(N_M    N_F    n_f N_M)$ , Verifies $M_{FM}^* = M_{FM}$ , Computes $M_{MF}$ $(M_5 = \{M_{MF}, t_m\})$	Check $T_h$ Verifies $M_{HF}^* = M_{HF}$ Computes: $SK = h(N_M    N_F    n_f N_M)$ $M_{FM} = h(M_{HM}    M_{HF}    SK    N_F)$ . $(M_4, t_h)$ ,	
	Check $T_m$ , Verifies $M_{MF}^* = M_{MF}$ , If valid accepts the request	

$$M_{FH} = h(M_1 || ID_F || N_F || T_f || K_{FH}).$$

The **FN** forwards the message  $M_2 = \{ID_F, N_F, M_1, M_{FH}, T_i, T_f\}$  to the **HN**.

- HN** → **FN**:  $M_3 = \{M_1, M_{HM}, M_{HF}, T_h\}$ .

The **HN** first verifies the freshness of  $T_f$  and then authenticates the **FN** by calculating  $M_{FH}^* = h(M_1 || ID_F || N_F || T_f || K_{FH})$  and comparing whether the calculated  $M_{FH}^*$  is equal to  $M_{FH}$  or not. If  $M_{FH}^* \neq M_{FH}$ , the **HN** denies the request. Otherwise, it computes the following:

$$N_M^* = x N_M,$$

$$ID_i = DID \oplus h(N_M || N'_M).$$

The **HN** searches  $ID_i, r_i, List$  in the database. If the value of  $List$  is greater than the threshold value, then the **HN** aborts the process. Otherwise, the **HN** computes the following:

$$X_i^* = h(ID_i' || x || r_i'), k_i^* = h(X_i^* || T_i),$$

$$M_{MH}^* = h(X_i^* || N_M || N'_M || k_i^* || T_i).$$

Then, the **HN** verifies the equality of the computed  $M_{MH}^*$  and the received  $M_{MH}$  in  $M_1$ . If  $M_{MH}^* \neq M_{MH}$ , then the **HN** denies the request and sets  $List = List + 1$ . Otherwise, it computes the following:

$$X'_f = h(ID_F || K_{FH}),$$

$$M = h(X'_f) \oplus h(k_i^*),$$

$$M_{HF} = h(X'_f || N_M || N_F || h(k_i^*) || ID_f || T_h),$$

$$M_{HM} = h(X'_f || N_M || N_F || h(k_i^*) || ID_i || T_h).$$

The **HN** transmits  $M_3 = \{M_1, M_{HM}, M_{HF}, T_h\}$  to the **FN**.

- FN** → **MU**:  $M_4 = \{T_h, T_f, N_F, M_{FM}, M_{HM}, M_{HF}\}$ . Upon receiving the message  $M_3$ , the **FN** first checks the freshness of  $T_h$  and then computes the following:

$$X_f^* = h(ID_F || K_{FA}), h(k_i^*) = M \oplus h(X_f^*),$$

$$M_{HF}^* = h(X_f^* || N_M || N_F || h(k_i^*) || ID_f || T_h).$$

Then, the **FN** verifies whether the calculated  $M_{HF}^*$  is equal to the received  $M_{HF}$ . If  $M_{HF}^* \neq M_{HF}$ , then

the **FN** rejects the request. Otherwise, the **FN** computes the following:

$$SK = h(N_M || N_F || n_f N_M),$$

$$M_{FM} = h(M_{HM} || M_{HF} || SK || N_F).$$

Then, the **FN** sends  $\mathbf{MU}_i$  the message  $M_4 = \{T_h, T_f, N_F, M_{FM}, M_{HM}, M_{HF}\}$

5.  $\mathbf{MU}_i \rightarrow \mathbf{FN}: M_5\{M_{MF}, T_m\}$ .

Upon receiving the message  $M_4$ ,  $\mathbf{MU}_i$  checks the freshness of  $T_h$  and computes

$$M_{HM}^* = h(X_i^* || N_M || N_F || h(k_i) || ID_i || T_h).$$

Then, the  $\mathbf{MU}_i$  verifies the calculated  $M_{HM}^*$  and the received  $M_{HM}$ . If  $M_{HM}^* \neq M_{HM}$ , then the **HN** rejects the request. Otherwise,  $\mathbf{MU}_i$  computes the following:

$$SK = h(N_M || N_F || n_m N_F),$$

$$M_{FM}^* = h(M_{HM} || M_{HF} || SK || N_F).$$

Then,  $\mathbf{MU}_i$  verifies the calculated  $M_{FM}^*$  and the received  $M_{FM}$ . If  $M_{FM}^* \neq M_{FM}$ , then  $\mathbf{MU}_i$  aborts the process. Otherwise,  $\mathbf{MU}_i$  calculates

$$M_{MF} = h(M_{HM} || M_{HF} || SK || N_M || T_m),$$

where  $T_m$  is the current time stamp, and sends the message  $M_5 = \{M_{MF}, T_m\}$  to the **FN**.

6. Upon receiving the message  $M_5$ , the **FN** first checks the freshness of  $T_m$  and then computes

$$M_{MF}^* = h(M_{HM} || M_{HF} || SK || N_M || T_m).$$

The **FN** compares  $M_{MF}^*$  with the received  $M_{MF}$ . If  $M_{MF}^* \neq M_{MF}$ , then the **FN** rejects the request. Otherwise, the **FN** authenticates  $\mathbf{MU}_i$  and accepts his/her request to access its network service.

### 5.3 Password change phase

The password change phase is illustrated in Fig. 4. Any **MU** can independently change his/her password for security reasons without the help of the **HN** by performing the following steps:

1.  $\mathbf{MU}_i$  inputs  $ID_i$ ,  $PW_i$ , and a new password  $PW_i^{new}$ .
2. The mobile device computes the following:

$$R_i^* = Rep(BIO_i, P_i),$$

$$x_i^* = B_i \oplus h(R_i^*),$$

$$C_i^* = h(ID_i || PW_i || x_i^*).$$

If  $C_i \neq C_i^*$ , then the mobile device rejects the request.

Otherwise, the mobile device computes the following:

$$A_i^{new} = h(PW_i^{new} || x_i^*) \oplus A_i \oplus h(PW_i || x_i^*),$$

$$C_i^{new} = h(ID_i || PW_i^{new} || x_i^*).$$

Finally, the mobile device replaces  $A_i, C_i$  with  $A_i^{new}, C_i^{new}$ .

### 5.4 Revocation phase

Any **MU** can protect his/her account from being misused by revoking the device if he/she detects that his/her mobile device is breached.

1.  $\mathbf{MU}_i$  completes the authentication process in accordance with the steps previously described in this section.
2.  $\mathbf{MU}_i \rightarrow \mathbf{HN}: \{DID_i, X_i, M_{MH}, T_i, \text{revoke-request}\}$ . Here,  $DID_i, X_i, M_{MH}$  are calculated by the mobile device, as previously described in this section.
3. Upon receiving the revocation request from  $\mathbf{MU}_i$ , the **HN** first authenticates  $\mathbf{MU}_i$ . If  $\mathbf{MU}_i$  is a legal user, then the **HN** sets  $List$  to be greater than the threshold value and revokes the mobile device. From then on, nobody can login to the network with the device until  $\mathbf{MU}_i$  reregisters himself/herself. Otherwise, the **HN** rejects the request.

### 5.5 Reregister phase

After revoking a mobile device, a user can reregister by performing the following steps:

1.  $\mathbf{MU}_i \rightarrow \mathbf{HN}: \{ID_i, HPW_i, \text{re-register}\}$ .
2. First, the **HN** searches for  $ID_i$  in its database. If the value of  $List$  is greater than or equal to the threshold value, then the **HN** confirms that the card is revoked. Then, the user reregisters in accordance with the steps in Section 5.1.

Fig. 4 Password change phase

Mobile user <b>MU</b>	Mobile device
Enters $ID_i, PW_i, PW_i^{new}$	Computes $R_i^* = Rep(BIO_i, P_i)$ $HPW_i^* = h(PW_i    R_i^*)$ $B_i^* = h(h(HPW_i^*) \oplus h(ID_i) \oplus h(P_i)) \text{mod } n_0$ $x_m = B_i \oplus h(R_i)$ $C_i = h(ID_i    PW_i    x_i^*)$ Verifies $C_i \neq C_i$ Computes $A_i^{new} = h(x_m    PW_i^{new}) \oplus A_i \oplus h(x_m    PW_i)$ , $C_i^{new} = h(ID_i    PW_i^{new}    x_m)$ , Replaces $A_i, C_i$ with $A_i^{new}, C_i^{new}$ .

## 6 Formal security analysis using the random oracle model

The formal security analysis of the proposed scheme using the real-or-random (ROR) model proposed by Abdalls et al. [1] is elaborated in this section.

- Instance:  $\prod_H^t$ ,  $\prod_F^u$  and  $\prod_{MU_i}^v$  are the instance  $t$  of **HN**, instance  $u$  of **FN**, and instance  $v$  of **MU<sub>i</sub>**, respectively. These instances are called oracles.
- Session identifier (SID): The SID is simply a concatenation of all of the messages sent and received by the oracles.
- Open oracle: If an oracle  $\prod_H^t$  reveals the accepted session key in any state, then the oracle is considered opened in that state.
- Fresh oracle: An unopened and uncorrupted oracle is a fresh oracle.
- Partner oracle: If two oracles,  $\prod_H^t$  and  $\prod_F^u$ , possess the same SID, then they are called partner oracles.
- Adversary: In the ROR model, the adversary  $A$  has the capability to control all communications and can input the following queries:
  - Execute( $\prod^t$ ,  $\prod^u$ ): Any adversary  $A$  can launch the eavesdropping attack by sending this query. Thus, the adversary  $A$  can obtain the messages communicated between honest participants.
  - Send( $\prod^t$ ,  $m$ ): This query is an active attack, in which the adversary  $A$  records the response received by communicating a message  $m$  to an instance  $\prod^t$  participating in the game.
  - CorruptMD( $\prod_{MU_i}^v$ ): This query is used by the adversary  $A$  to retrieve the parameters accumulated in the stolen/lost mobile device.
  - Test( $\prod^t$ ): The semantic security of the session key  $SK$  is modeled by the query and follows the indistinguishability of the ROR model [1]. This query enables the adversary  $A$  to input the test query to any fresh oracle at any instant of time. The experiment begins with the flipping of a fair unbiased coin  $c$ . If the answer is 1, then the output is a randomly selected session key. Otherwise, the output is the agreed session key of the test oracle.
- Semantic security of the session key: In the ROR model, the adversary  $A$  challenges the experiment to differentiate between the real session key  $SK$  of the instance and the randomly selected session key. The adversary  $A$  can execute a number of Test queries to either the user or the server instance. The result of the Test query must be

consistent with respect to random bit  $c$ . At the end of the experiment, the adversary  $A$  returns a bit  $c'$ . If  $c' = c$ , then this game is won by the adversary  $A$ . This event is denoted as  $Succ$ . The advantage of breaching the security of the protocol is  $Adv_P^{ake} = 2|Pr[Succ] - 1|$ . Therefore, if  $Adv_P^{ake} \leq \eta$ , for any sufficiently small  $\eta > 0$ , then the protocol  $P$  is considered to be a secure protocol in the ROR sense.

- Random oracle: Notably, the one-way hash function  $h(\cdot)$  is modeled as a Hash oracle by all of the players and the adversary  $A$ .

The difference lemma [25] is described here and will be used in the formal security proof.

**Lemma 1** (Difference lemma) *Let  $Succ_1$ ,  $Succ_2$ , and  $Succ_3$  denote the events defined in some probability distribution. Let  $Succ_1 \wedge \sim Succ_3 \iff Succ_2 \wedge \sim Succ_3$ . Then, we derive the following expression:*

$$|Pr[Succ_1] - Pr[Succ_2]| \leq Pr[Succ_3].$$

The following theorem will establish the semantic security of the session key.

**Theorem 1** *Let any adversary  $A$  operate within polynomial time  $t$  for the proposed scheme  $P$  in a random oracle. Assume that  $D$  represents a uniformly distributed password dictionary and  $l$  denotes the bit size of the biometrics key  $BI O_i$ . The probability of  $P$ 's session key being breached by the adversary  $A$  can be expressed as follows:*

$$Adv_P^{ake} \leq \frac{q_h^2}{|Hash|} + \frac{q_{send}}{2^l \cdot |D|} + 2Adv^{ECDLP}(t),$$

where  $q_h$ ,  $|Hash|$ ,  $q_{send}$ ,  $|D|$ , and  $Adv^{ECDLP}(t)$  denote the number of hash queries, range space of the one-way hash function, number of send queries, size of  $D$ , and the advantage of the adversary  $A$  in breaching the ECDLP, respectively.

*Proof* We begin by defining a sequence of game  $G_i$ ,  $0 \leq i \leq 4$ . Here,  $Succ_i$  represents the success of the adversary  $A$  in guessing the bit  $c$  in the game  $G_i$ . The proposed scheme runs from game  $G_0$  to game  $G_4$ , and the conclusion of the proof will show that the adversary  $A$  has a negligible advantage in breaching the session key security of the proposed scheme  $P$ .

- **Game  $G_0$** : This game is a real attack by the adversary against protocol  $P$  in the random oracle. The bit  $c$  is selected at the commencement of this game. In accordance to the definition,

$$Adv_P^{ake}(A) = 2Pr[Succ_0] - 1 \quad (1)$$



- **Game  $G_1$ :** This game simulates an eavesdropping attack of the adversary  $A$  using the Execute oracles ( $\Pi^u, \Pi^v$ ). The attacker also queries the Test oracle and checks whether the result is a real session key  $SK$  or some other random value. The session key  $SK$  is computed by the FN and the mobile user  $MU_i$  as  $SK = h(N_M || N_F || n_f N_M)$  and  $SK = h(N_M || N_F || n_m N_F)$ , respectively. However, computing  $n_f N_M = n_m N_F = n_f n_m P$  is difficult because of the complexity of the ECCDHP. Furthermore,  $N_M$  and  $N_F$  cannot be computed because of the complexity of the ECDLP. Thus, the probability of the adversary  $A$  winning this game through an eavesdropping attack does not increase. Then,  $G_0$  and  $G_1$  have the same probability. Thus, we derive the following expression:

$$Pr[Succ_0] = Pr[Succ_1] \tag{2}$$

- **Game  $G_2$ :** This game is an extension of  $G_1$ .  $G_2$  is simulated by the Send and Hash oracles along with the Execute ( $\Pi^t, \Pi^u, \Pi^v$ ) and Test oracles. It is an active attack modeled by the adversary  $A$  by sending fabricated messages to deceive the authenticated participants. The adversary  $A$  repeatedly generates hash queries to obtain collisions. The login request message  $M_1 = \{DID_i, N_M, M_{MH}, T_i\}$  is associated with the random number  $n_m$ , and the time stamp. Furthermore,  $N_M$  and  $n_m P$  cannot be computed because of the complexity of the ECDLP. Therefore, the messages are guaranteed to be random. Hence, no collision will be achieved by querying the Send oracle. Using the birthday paradox [7], we derive the following expression:

$$|Pr[Succ_1] = Pr[Succ_2]| \leq \frac{q_h^2}{2|Hash|} \tag{3}$$

- **Game  $G_3$ :** The CorruptMD oracle is simulated by this game. The adversary  $A$  can attempt to perform a dictionary attack using the parameters accumulated in the mobile device to acquire the password  $PW_i$  and biometric information  $BIO_i$ . However, a strong fuzzy extractor is used in the proposed protocol. Therefore, the probability that biometric information  $BIO_i$  can be guessed is approximately  $\frac{1}{2^l}$  [37]. Furthermore,  $List$  counts the number of failed login attempts. Thus, we derive the following expression:

$$|Pr[Succ_2] = Pr[Succ_3]| \leq \frac{q_{send}}{2^l |D|} \tag{4}$$

- **Game  $G_4$ :** In this game, an adversary tries to acquire the session key  $SK$  through eavesdropping of the login request message  $M_1 = \{DID_i, N_M, M_{MH}, T_i\}$ .  $M_1$  is associated with the random numbers  $n_m$  and the time stamp. Furthermore,  $N_M = n_m P$  cannot be computed

because of the complexity of the ECDLP. Thus, we derive the following expression:

$$|Pr[Succ_3] = Pr[Succ_4]| \leq Adv^{ECDLP}(t) \tag{5}$$

All session keys are random and independent, and the value of  $c$  is not exposed to any adversary. Therefore, it is clear that

$$Pr[Succ_4] = \frac{1}{2} \tag{6}$$

Combining the previously presented equations and Lemma 1, the desired result can be derived as follows:

$$Adv_p^{ake} \leq \frac{q_h^2}{|Hash|} + \frac{q_{send}}{2^l |D|} + 2Adv^{ECDLP}(t).$$

□

## 7 Heuristic analysis of the proposed scheme

A heuristic analysis of the proposed scheme is presented in this section. The analysis shows that this scheme meets all of the desirable security requirements. Notably, an adversary cannot derive  $n_m, n_f$  from  $N_M = n_m P, N_F = n_f P$  because of the complexity of the ECDLP [14]. Table 5 provides a brief comparison of the security requirements of the proposed scheme and several related schemes.

### 7.1 Server resource exhaustion attack

A server resource exhaustion attack is an attempt to waste resources including the memory and CPU cycles in the server. In our proposed scheme, the mobile device first verifies the authenticity of  $MU_i$  during the login and authentication phase. As soon as  $MU_i$  inputs  $ID_i, PW_i$ , and  $BIO_i$ , the mobile device computes  $C_i^* = h(ID_i || PW_i || x_i^*)$  and verifies whether  $C_i$  is equal to  $C_i^*$  or not. It is obvious that if  $MU_i$  provides incorrect identity or incorrect password or both by mistake, or any adversary tries to access a stolen mobile device, the mobile device will detect this mistake immediately. Hence, the mobile device is responsible for detecting this type of error instead of HN. Therefore, the proposed protocol provides fast error detection mechanism which reduces the burden on the HN and prevents the server resource exhaustion attack subsequently.

### 7.2 User anonymity and untraceability

In the proposed scheme, the original identity  $ID_i$  is not sent publicly but concealed in  $DID_i$ , which changes with  $N'_M$  in every session. An adversary has to compute  $N'_M$  to obtain  $ID_i$ , which is equivalent to solving the ECCDHP. Moreover, no algorithm can solve it in polynomial time.

**Table 5** Comparison of the security requirements

Schemes	$P_1$	$P_2$	$P_3$	$P_4$	$P_5$	$P_6$	$P_7$	$P_8$	$P_9$	$P_{10}$	$P_{11}$	$P_{12}$
Arshad and Rasoolzadegan [2]	o	o	o	o	o	o	o	×	×	o	×	×
Chaudhry et al. [9]	×	o	×	o	o	×	o	×	×	o	×	×
Farash et al. [12]	×	o	×	×	o	×	×	×	×	×	×	×
Gope and Hwang [13]	o	o	×	o	o	o	o	o	o	×	×	×
The proposed scheme	o	o	o	o	o	o	o	o	o	o	o	o

o: satisfaction, ×: non-satisfaction,

- $P_1$  : mobile user anonymity,
- $P_2$  : untraceability of the user,
- $P_3$  : resistance to stolen/lost mobile device attack,
- $P_4$  : mutual authentication,
- $P_5$  : session key agreement,
- $P_6$  : resistance to impersonation attack,
- $P_7$  : resistance to replay attack,
- $P_8$  : efficient login phase,
- $P_9$  : user-friendly password change,
- $P_{10}$  : perfect forward secrecy,
- $P_{11}$  :resistance to synchronization attack,
- $P_{12}$  : provision of the revocation phase.

```

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%ROLE OF MOBILE USER MU%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
role role_M(M, F, HN: agent, Kmh:symmetric_key, H: hsah_func, SND, RCV:channel(dy))
played_by M
def=
local
    State: nat,
    IDi, PWi, X,Xi, HPWi,S, Ri, Ai, Yi, P, BIOi, Bi, Ci, Ki, nm, nf: text
    const sp1, sp2, sp3, mu_fn_nm, fn_hn_nf: protocol_id
init State := 0
transition
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Receive User Registration Phase %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
1. State=0 ^ RCV(start)=|>
    State':=1 ^ X':=new() ^ HPW':=H(PWi.X') ^ SND({IDi,HPWi}_Kmh)
        ^ secret(PWi,{M})
        ^ secret(IDi, {M, HN})
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Receive registration reply from HA securely %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
2. State:= 2 ^ RCV({H(IDi.S.Ri), xor(H(IDi.S.Ri)).HPWi').S.P}_Kmh)
    State':= 4 ^ Bi:= xor(xi.H(Ri))
        ^ Ci:=h(IDi.PWi.Xi)
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% authentication and SK establishment %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
    ^ nm':=new()
    ^ NM':=Mul(nm'.P)
    ^ NM1':= Mul(nm'.Y)
    ^ Xi*':=xor(Ai, HPWi')
    ^ ki':=h(Xi*.Ti)
    ^ DIDi':=xor(IDi, h(NM'.NM1'))
    ^ Mmh':= h(Xi*'.NM'.NM1'.ki.Ti)
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Send message to FN via open network%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
    ^ SND(DIDI'.NM.Mmh'.Ti)
    ^ witness(M, mu_fn_nm, NM')
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Receive registration reply from HA securely %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
3. State = 4 ^ RCV{NF, MFM, MHM, MHF, Th, Tf}=|.
    State'=6 ^ SK':=H(NM.NF.Mul(nm,NF))
        ^ MFM':=H(MHM,MHF,SK'.NM'.Tm)
        ^ SND(MFM'.Tm)
        ^ request(F,M, fn_hn_nf, NF')
endrole
    
```

**Fig. 5** Mobile user MU’s role specification in HLSPL

Consequently, the proposed scheme provides both user anonymity and untraceability.

### 7.3 MU impersonation attacks

To impersonate an **MU**, the attacker *A* has to produce the valid login request  $M_1 = \{DID_i, N_M, M_{MH}, T_i\}$  and  $M_5 = \{M_{MF}, t_m\}$ , where  $M_{MH} = h(X_i^* || N_M || N'_M || k_i || T_i)$  and  $M_{MF} = h(M_{HM} || M_{HF} || SK || N_M)$ . The adversary *A* cannot calculate  $M_{MF}$  because he/she has to compute  $N'_M$  which is equivalent to solving the ECCDHP. In addition, the adversary *A* can try replaying a previous message  $M_1 = \{DID_i, N_M, M_{MH}, T_i\}$  within the expected valid time interval. However, the adversary *A* knows nothing about the random number  $n_m$ . Thus, the adversary *A* cannot derive  $M_{MF}$  because he/she will not be able to compute  $n_m n_f P$ . Hence, the valid message  $M_5 = \{M_{MF}, t_m\}$  cannot be produced by the adversary *A*. Therefore, the improved scheme could successfully resist **MU** impersonation attacks.

### 7.4 FN impersonation attacks

To impersonate an **FN**, the attacker *A* has to deceive the **MU** and **HN**. To convince the **HN**, the adversary *A*

should produce a valid message  $M_2 = \{ID_F, N_F, N_M, M_1, M_{FH}, T_i, T_f\}$ . On the other hand, the adversary *A* should produce a valid message  $M_4 = \{T_h, t_f, N_F, M_{FM}, M_{HM}\}$  to convince the **MU**. However, the adversary *A* cannot produce the valid message  $M_2$  because he/she does not know  $K_{FH}$ . Hence, the adversary *A* cannot impersonate the **FN** to cheat the **HN**. The adversary *A* will also not be able to compute  $n_m n_f P$  because he/she knows nothing about the random number  $n_f$ . Hence, the adversary *A* cannot obtain a qualified  $M_{FM}$  and cannot produce a valid  $M_4$  subsequently. Therefore, the adversary *A* cannot impersonate the **FN** to cheat the **MU**.

### 7.5 HN impersonation attacks

To impersonate an **HN**, the attacker *A* has to generate a valid message  $M_3 = \{M_1, M_{HM}, M_{HF}, T_h\}$  to deceive the **MU** and **FN**. The **FN** authenticates the **HN** by verifying the validity of  $M_{HF} = h(X'_f || N_M || N_F || h(k_i^*) || ID_f || T_h)$ . The adversary *A* cannot produce a valid  $M_{HF}$  because he/she does not know  $K_{FH}$ . The **MU** authenticates the **HN** by verifying the validity of  $M_{HM} = h(X_i^* || N_M || N_F || h(k_i^*) || ID_i || T_h)$ . Moreover, the adversary *A* cannot produce a valid  $M_{HM}$  because he/she cannot derive  $X_i^* =$

```

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
role role_M(M, F, HN: agent, Kmh:symmetric_key, H: hsah_func, SND, RCV:channel(dy))
played_by M
def=
local
    State: nat,
    IDi, PWi, X,Xi, HPWi,S, Ri, Ai, Yi, P, BIOi, Bi, Ci, Ki, nm, nf, xF': text
    const sp1, sp2, sp3, mu_fn_nm, fn_hn_nf: protocol_id
init State := 0
transition
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% receive registration request from MU %%%%%%%%%
1. State=0 ^ RCV(start)=|> State':1 ^ X':new() ^ HPWi'=H(PWi.X') ^ SND({IDi, HPWi}_Kmh)
   ^ secret (PWi, {M})
   ^ secret(S,{H}) ^ secret(IDi,{M,H})
   Snd({H(IDi.S.R)}, xor(H{IDi.S.Ri}), HPWi'), Mul(S,P)}_Kmh
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% receive message from FN %%%%%%%%%
2. State:= 3 ^ nf':new()
   ^ NF':= Mul(nf'.P)
   ^ MFH':= H(M1, IDf.NF'.Tf.KFH)
   ^ RCV(IDf, NF'.M1.MFH'.Ti.Tf) =|.
   State' := 6 ^ secret(KFH, sp4{H,F})
   ^ Xf':= H(IDd.KHF)
   ^ M':= xor{H(Xf').H(h(ki'))}
   ^ MHF':=H(Xf'.NM'.NF'.H(ki')).IDi.Th)
   ^ MHM':=H(Xi'.NM'.NF'.H(ki')).IDi.Th)
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% HN send to FN via open network %%%%%%%%%
   ^ Snd(M'.MGF'.Th)
   ^ request(F, M, fn_hn_nf, NF')
endrole
    
```

Fig. 6 Foreign network FN’s role specification in HLSPL

$h(ID_i' || x || r_i')$  in which the secret key  $x$  of the **HN** is included and is unknown to the adversary  $A$ . Consequently, the proposed scheme can resist the **HN** impersonation attacks.

## 7.6 Replay attacks

In the replay attack, the adversary  $A$  sends a previously eavesdropped login request message  $M_1 = \{DID_i, N_M, M_{MH}, T_i\}$ , which will be detected by the **FN** during checking of the freshness of  $T_i$ . The adversary  $A$  intends to replace the time stamp  $T_i$  with the current time stamp. However, the adversary  $A$  cannot generate a valid  $M_{MH} = h(X_i^* || N_M || N_M' || K_i || T_i)$ . This attempt will be detected by the **HN** when comparing the received  $M_{MH}$  with the computed  $M_{MH}^* = h(X_i^* || N_M || N_M' || K_i^* || T_i)$ . On the other hand, the adversary  $A$  sends a previously eavesdropped login request message  $M_1 = \{DID_i, N_M, M_{MH}, T_i\}$  within the valid time interval. However, the adversary  $A$  neither knows the random number  $n_m$  nor can compute  $n_m n_f P$ . Hence, he/she cannot compute  $M_{MF}$ . Therefore, a valid  $M_5 = \{M_{MF}, T_m\}$  cannot be produced by the adversary  $A$  subsequently. Hence, the improved scheme could successfully resist the replay attacks.

## 7.7 Session key security

In the proposed scheme, only  $MU_i$  and **FN** can compute  $SK = h(N_M || N_F || n_m n_f P)$  after mutual authentication. If the adversary  $A$  wants to compute an established session key, then he/she has to obtain  $n_m$  and  $n_f$  to compute  $n_m n_f P$ . The adversary  $A$  could obtain  $N_M = n_m P$  and  $N_F = n_f P$  from the previously transmitted messages but cannot obtain  $n_m$  or  $n_f$  because of the unsolvability of the ECDLP. Hence, the improved scheme could successfully ensure the session key security.

## 7.8 Perfect forward secrecy

Assume that the previously transmitted messages ( $M_1, M_2, M_3, M_4, M_5$ ) are recorded by the adversary  $A$ , he/she still cannot compute any previously established session key  $SK = h(N_M || N_F || n_m n_f P)$  because he/she knows nothing about  $n_m$  and  $n_f$ . Furthermore,  $n_m$  and  $n_f$  change during each login. Therefore, a broken session key would not affect any other session key. Hence, the improved scheme successfully provides the perfect forward secrecy.

```

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%ROLE OF HN %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
role role_M(M, F, HN: agent, Kmh:symmetric_key, H: hsah_func, SND, RCV:channel(dy))
played_by M
def=
local
    State: nat,
    IDi, PWi, X,Xi, HPWi,S, Ri, Ai, Yi, P, BIOi, Bi, Ci, Ki, nm, nf, xf': text
    const sp1, sp2, sp3, mu_fn_nm, fn_hn_nf: protocol_id
init State := 0
transition
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Receive message from MU via open network %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
1. State=0 ^ RCV(DIDi', NM', Mmh', Ti) = | >
   State:= 1 ^ \secret(IDi, sp1, {M, HN})
           ^ \secret(KFH, sp4, {HN, F})
           ^ \nf:=new()
           ^ \NF':=Mul(nf.P)
           ^ \MFH':=h(M1.IDf.NF'.Tf.KFH)
           ^ \SND(IDf.NF', M1, MFH'.Ti, Tf)
           ^ \witness(H, F, h_f_nf, NF')
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Receive message from HN via open network %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
2. State:= 2 ^ RCV(M'.MHF'.MHM', Th) = | >
   State:= 3 ^ \XF':=H(IDf.KFA)
           ^ \H(ki'):=xor(H(XF'.M))
           ^ \SK:=H(NM'.NF'.Mul(nf'.NM'))
           ^ \MFM'=H(MHM'.MHF'.SK.NF')
           ^ \SND(NF'.MFM'.MHM'.MHF'.Th, Tf)
           ^ \witness(H, F, h_f_nf, NF')
3. State:= 3 ^ RCV(MFM', Tm) = | >
   State:= 5 ^ request(M, F, fn_hn_nm, NM')

endrole

```

Fig. 7 Home network HN's role specification in HLSPL

```

%%Role for the session
role session(M, F, HN: agent,
             Kmh:symmetric_key,
             H: hsah_func, SND, RCV:channel(dy))
def=
    local S1, S2, S3, R1, R2, R3 : channel(dy)
composition
mobileuser(M,F,H, Kmh, H, Mul, S1,R1)
/\homenetwork(M, F,H,Kmh H,Mul,S2,R2)
/\foreignnetwork(M, F,H,H,Mul,S3,R3)
endrole
role environment()
def=
const M, H,F: agent
Kmh : symmetric_key
IDm, IDf, IDh:text
M_f_x, f_h_y :protocol_id
SP1, SP2, SP3, SP4 : protocol_id
Intruder_knowledge=(m,h,f, ID_f)
Composition
session(m,f,h,Kmh,H)
/\ session(i,f,h,Kmh,H)
/\ session(m,i,h,Kmh,H)
/\ session(m,f,i,Kmh,H)
endrole
gole
secrecy_of SP1, SP2, Sp3, SP4
authentication_on fn_hn_nf
authentication_on mu_fn_nm
endrole
environment()
    
```

Fig. 8 Session and environments role specification in HLSPL

## 8 Formal security verification through AVISPA simulation

AVISPA is an automated software tool for the formal verification of security-sensitive protocols and applications [4]. It implements the Dolev-Yao (DY) threat model and verifies whether a scheme can resist replay and man-in-the-middle attacks. A protocol that has to be verified is written in High Level Protocol Specification Language (HLPSL) [28]. HLPSL is translated into the intermediate format (IF) with help of a translator known as HLPSL2IF. The IF is interpreted by using one of the following backends:

1. On-the-fly Model-Checker (OFMC)
2. Constraint-Logic-based Attack Searcher (CL-AtSe)
3. SAT-based Model-Checker (SATMC) and
4. Tree Automata based on Automatic Approximations for the Analysis of Security Protocols (TA4SP).

Among these, OFMC and CL-AtSe are most widely accepted, and we evaluate the proposed scheme under these backends to formally verify its resistance to the man-in-the-middle and replay attacks. The proposed scheme is implemented in HLSPL. The necessary roles for the mobile user **MU**, the foreign network **FN**, and the home network

```

%OFMC
SUMMARY
SAFE
DETAILS

BOUNDED_NUMBER_OF_SESSIONSPROTOCOLS

/home/span/span/testsuite/results/protocol.if
GOAL
    as_specified
BACKEND
    OFMC
COMMENTS
STATISTICS
parseTime: 0.00s
searchTime: 0.22s
visitedNodes: 48 nodes
depth:16 plies
    
```

Fig. 9 The simulation results using the OFMC backend

```

SUMMARY
SAFE

DETAILS
BOUNDED_NUMBER_OF_SESSIONSTYPED_MODEL

PROTOCOL
/home/span/span/testsuite/results/myprotocol

GOAL
    As specified

BACKEND
    CL-AtSe

STATISTICS

Analysed: 63 states
Reachable: 28 states
Transiation: 0.04 seconds
Computation: 0.93 seconds
    
```

Fig. 10 The simulation results using the CL-AtSe backend

**Table 6** Notations and execution times of cryptographic operations

Notation	Description and Execution time(ms) [44]
$T_h$	Execution time of a hash function $\approx 0.5$ ms
$T_S$	Execution time of a symmetric encryption/decryption $\approx 8.7$ ms
$T_M$	Execution time of a modular exponentiation $\approx 522$ ms
$T_P$	Execution time of an elliptic curve point multiplication $\approx 63.075$ ms
$T_A$	Execution time of an elliptic curve point addition $\approx 0.025$ ms

**HN** for the different phases of the proposed scheme are defined respectively in Figs. 5, 6, and 7. We have also specified the roles for the session, goal, and environment in Fig. 8 as per the HLPSSL specification.

Finally, we simulate the proposed scheme using the SPAN, the Security Protocol ANimator for AVISPA tool [4]. Figures 9 and 10 presents the simulation results under the widely-used OFMC and CL-AtSe backends. The simulation results clearly demonstrate that the proposed scheme is secure against the man-in-the-middle attack and the replay attack.

### 9 Performance analysis

The performance of the proposed scheme is analyzed in this section. The performance evaluation focuses on the computational and communication costs. We compare the proposed scheme with the related schemes proposed by Arshad and Rasoolzadegan [2], Chaudhry et al. [9], Farash et al. [12], Gope and Hwang [13], Alzahrani et al. [3], and Lu et al. [26] in the following sections.

### 9.1 Computational cost comparisons

The computational costs are compared in terms of the number of cryptographic operations performed. Table 6 shows the cryptographic operations and their approximate execution times as taken by [2].

Table 7 shows the comparative computational costs of the related schemes. Only the computational cost of the login and authentication phase is considered. The registration and password change phases are not considered because these phases do not occur frequently. The execution time of the proposed scheme is 264.8 ms, which surpasses that of all of the related schemes in terms of the computational cost except Chaudhry et al. and Farash et al. scheme. However, their schemes are not secure.

### 9.2 Communication cost comparisons

For the communication cost comparisons, we assume that the length of an identity is 128 bits, the length of a random number is 128 bits, the length of a hashed value is 128 bits, the length of a time stamp is 32 bits, and the length of a key in the symmetric encryption is 256 bits according to [30, 31]. Furthermore, the length of a scalar multiplication in elliptic curve is 320 bits and the length of a modular operation is 1024 bits. Table 8 shows the comparative communication costs of the various schemes. The communication costs of the proposed scheme is 2176 bits. The communication cost of the proposed scheme is slightly greater than that of Chaudhry et al. [9] and Farash et al. [12] scheme. However, their schemes are not secure. Also, the communication cost of **MIU** in the proposed scheme is 736 bits. Based on the comprehensive considerations from the efficiency and security attributes, we assert that the proposed scheme makes a better tradeoff and is more suitable to ubiquitous networks.

**Table 7** Computational cost comparisons

Schemes	HN	FA	HA	Total
Arshad and Rasoolzadegan [2]	$2T_P + T_S + 7T_H$	$2T_P + 5T_H$	$6T_H$	$18T_H + 4T_S + 4T_P$ $\approx 296.1$ ms
Chaudhry et al. [9]	$5T_H$	$1T_H + 2T_S$	$4T_H + 3T_S$	$10T_H + 5T_S \approx 48.5$ ms
Farash et al. [12]	$6T_H$	$T_H + 2T_S$	$5T_H + 2T_S$	$12T_H + 4T_S \approx 40.8$ ms
Gope and Hwang [13]	$4T_H + T_M$	$4T_H$	$4T_H + T_M$	$12T_H + 2T_M \approx 1050$ ms
Alzahrani et al. [3]	$9T_H + 5T_P + 2T_A$	$6T_H + 4T_P + 2T_A$	$8T_H + 5T_P + 3T_A$	$23T_H + 14T_P + 7T_A$ $\approx 894.725$ ms
Lu et al. [26]	$10T_H + 5T_P + 3T_A + 2T_S$	$6T_H + 4T_P + 2T_A$	$9T_H + 6T_P + 5T_A + T_S$	$25T_H + 15T_P + 10T_A + 4T_S$ $\approx 993.675$ ms
Proposed scheme	$10T_H + 2T_P$	$10T_H + T_P$	$10T_H + T_P$	$25T_H + 4T_P \approx 264.8$ ms

**Table 8** Communication cost comparisons

Schemes	Communication cost	
	MU	Total
Arshad and Rasoolzadegan [2]	736 bits	2432 bits
Chaudhry et al. [9]	736 bits	1824 bits
Farash et al. [12]	608 bits	1700 bits
Gope and Hwang [13]	1152 bits	3070 bits
Alzahrani et al. [3]	736 bits	3232 bits
Lu et al. [26]	736 bits	3296 bits
Proposed scheme	736 bits	2176 bits

## 10 Conclusions

In this study, we propose a secure and efficient authentication and key agreement scheme for a ubiquitous network. This enhanced scheme resolves all of the flaws existing in Arshad and Rasoolzadegan's scheme. Formal analysis of the proposed scheme is conducted using the random oracle model, the formal security verification is performed by AVISPA, and heuristic analysis is also conducted to demonstrate that the proposed scheme fulfills all of the security requirements. Comparisons of the computational and communication costs are also conducted to show the suitability of the proposed scheme for ubiquitous networks. Therefore, the proposed scheme not only eliminates vulnerabilities but also improves security and efficiency.

**Funding** This work is supported by the Department of Science and Technology (DST), Government of India under Women Scientist Scheme A (WOS-A) under Grant No. SR/WOS-A/PM-10/2018.

## References

1. Abdalla M, Fouque PA, Pointcheval D (2005) Password-based authenticated key exchange in the three-party setting. In: Vaudenay S (ed) *Public key cryptography - PKC 2005*. PKC 2005. Lecture Notes in Computer Science. Springer, Berlin, p 3386
2. Arshad H, Rasoolzadegan A (2017) A secure authentication and key agreement scheme for roaming service with user anonymity. *Int J Commun Syst* 30(18):e3361
3. Alzahrani BA, Chaudhry SA, Barnawi A, Al-Barakati A, Alsharif MH (2020) A privacy preserving authentication scheme for roaming in IoT-based wireless mobile networks. *Symmetry* 2020:287–305
4. AVISPA (2021) Automated validation of internet security protocols and applications. Available online: <http://www.avispa-project.org/>
5. Burrows M, Abadi M, Needham R (1990) A logic of authentication. *ACM Trans Comput Syst* 8(1):18–36
6. Bellare SM, Merritt M (1992) Encrypted key exchange: password-based protocols secure against dictionary attacks. In: *Proceedings 1992 IEEE computer society symposium on research in security and privacy*, Oakland, CA, USA, pp 72–84
7. Boyko V, MacKenzie P, Patel S (2000) Provably secure password-authenticated key exchange using Diffie-Hellman. In: Preneel B (ed) *Advances in cryptology — EUROCRYPT 2000*. Lecture Notes in Computer Science. Springer, Berlin, p 1807
8. Chen C, He D, Chan S, Bu J, Gao Y, Fan R (2011) Lightweight and provably secure user authentication with anonymity for the global mobility network. *Int J Commun Syst* 24(3):347–362
9. Chaudhry SA, Albeshri A, Xiong N, Lee C, Shon T (2017) A privacy preserving authentication scheme for roaming in ubiquitous networks. *Clust Comput* 20(2):1223–1236
10. Dolev D, Yao AC (2006) On the security of public key protocols. *IEEE Trans Inf Theory* 29(2):198–208
11. Eisenbarth T, Kasper T, Moradi A, Paar C, Salmasizadeh M, Shalmani MTM (2008) On the power of power analysis in the real world: a complete break of the keeloq code hopping scheme. In: Wagner D (ed) *Advances in cryptology - CRYPTO 2008*. Lecture notes in computer science. Springer, Berlin, p 5157
12. Farash MS, Chaudhry SA, Heydari M, Sadough S, Kumari S, Khan MK (2015) A lightweight anonymous authentication scheme for consumer roaming in ubiquitous networks with provable security. *Int J Commun Syst* 30(4):e3019
13. Gope P, Hwang T (2015) Enhanced secure mutual authentication and key agreement scheme preserving user anonymity in global mobile networks. *Wirel Pers Commun* 82(4):2231–2245
14. Hankerson D, Menezes AJ, Vanstone S (2004) *Guide to elliptic curve cryptography*. Springer, Berlin
15. He D, Chan S, Chen C, Bu J, Fan R (2011) Design and validation of an efficient authentication scheme with anonymity for roaming service in global mobility networks. *Wirel Pers Commun* 61(2):465–476
16. He D, Wang D (2015) Robust biometrics-based authentication scheme for multiserver environment. *IEEE Syst J* 9(3):816–823
17. Lee H, Lee D, Moon J, Jung J, Kang D, Kim H (2018) An improved anonymous authentication scheme for roaming in ubiquitous networks. *PLoS One* 13(3):e0193366
18. Ignatenko T, Willems FMJ (2009) Biometric systems: privacy and secrecy aspects. *IEEE Trans Inf Forensics Secur* 4(4):956–973
19. Jiang Q, Ma J, Li G, Yang L (2013) An enhanced authentication scheme with privacy preservation for roaming service in global mobility networks. *Wirel Pers Commun* 68(4):1477–1491
20. Jung J, Kang D, Lee D, Won D (2017) An improved and secure anonymous biometric-based user authentication with key agreement scheme for the integrated EPR information system. *PLoS One* 12(1):e0169414
21. Karupiah M, Kumari S, Das AK, Li X, Wu F, Basu S (2016) A secure lightweight authentication scheme with user anonymity for roaming service in ubiquitous networks. *Secur Commun Netw* 9(17):4192–4209
22. Kumari S, Khan MK, Li X, Wu F (2016) Design of a user anonymous password authentication scheme without smart card. *Int J Commun Syst* 29(3):441–458
23. Kumari S, Li X, Wu F, Das AK, Odelu V, Khan MK (2016) A user anonymous mutual authentication protocol. *KSII Trans Internet Inf Syst* 10(9):4508–4528
24. Lee CC, Hwang MS, Liao IE (2006) Security enhancement on a new authentication scheme with anonymity for wireless environments. *IEEE Trans Ind Electron* 53(5):1683–1687
25. Lee TF (2015) Provably secure anonymous single-sign-on authentication mechanisms using extended chebyshev chaotic maps for distributed computer networks. *IEEE Syst J* 12(2):1499–1505
26. Lu Y, Xu G, Li L, Yang Y (2019) Robust privacy-preserving mutual authenticated key agreement scheme in roaming service for global mobility networks. *IEEE Syst J* 13(2):1454–1465
27. Mun H, Han K, Lee YS, Yeun CY, Choi HH (2012) Enhanced secure anonymous authentication scheme for roaming service

- in global mobility networks. *Math Comput Model* 55(1-2):214–222
28. Oheimb VD (2005) The high-level protocol specification language HLPSL developed in the EU project AVISPA. In: *Proceedings of the 3rd APPSEM II (Applied Semantics II) Workshop (APPSEM'05)*, Germany
  29. Odelu V, Das AK, Kumari S, Huang X, Wazid M (2017) Provably secure authenticated key agreement scheme for distributed mobile cloud computing services. *Futur Gener Comput Syst* 68: 74–88
  30. Reddy AG, Das AK, Odelu V, Yoo KY (2016) An enhanced biometric based authentication with key-agreement protocol for multi-server architecture based on elliptic curve cryptography. *PLoS One* 11(5):e0154308
  31. Kumari S, Khan MK, Atiquzzaman M (2015) User authentication schemes for wireless sensor networks: a review. *Ad Hoc Netw* 27:159–194
  32. Khatoon S, Singh Thakur B (2020) Cryptanalysis and improvement of authentication scheme for roaming service in ubiquitous network. *Cryptologia* 44(4):315–340
  33. Ostad-Sharif A, Babamohammadi A, Abbasinezhad-Mood D, Nikooghadam M (2019) Efficient privacy-preserving authentication scheme for roaming consumer in global mobility networks. *Int J Commun Syst* 32(5):e3904
  34. Wu CC, Lee WB, Tsaur WJ (2008) A secure authentication scheme with anonymity for wireless communications. *IEEE Commun Lett* 12(10):722–723
  35. Wen F, Susilo W, Yang G (2013) A secure and effective anonymous user authentication scheme for roaming service in global mobility networks. *Wirel Pers Commun* 73(3):993–1004
  36. Wang D, He D, Wang P, Chu CH (2015) Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment. *IEEE Trans Depend Secur Comput* 12(4):428–442
  37. Wazid M, Das AK, Kumari S, Li X, Wu F (2016) Design of an efficient and provably secure anonymity preserving three-factor user authentication and key agreement scheme for TMIS. *Secur Commun Netw* 9(13):1983–2001
  38. Wang D, Wang P (2018) Two birds with one stone: two-factor authentication with security beyond conventional bound. *IEEE Trans Depend Secur Comput* 15(4):708–722
  39. Wu F, Xu L, Kumari S, Li X, Khan MK, Das AK (2017) An enhanced mutual authentication and key agreement scheme for mobile user roaming service in global mobility networks. *Ann Telecommun* 72(3-4):131–144
  40. Wang C, Xu G (2017) Cryptanalysis of three password-based remote user authentication schemes with non-tamper-resistant smart card. *Secur Commun Netw* 2017:e1619741
  41. Wang C, Wang D, Xu G, Guo Y (2017) A lightweight password-based authentication protocol using smart card. *Int J Commun Syst* 30(16):e3336
  42. Xie Q, Hu B, Tan X, Bao B, Yu X (2014) Robust anonymous two-factor authentication scheme for roaming service in global mobility network. *Wirel Pers Commun* 74(2):601–614
  43. Xie Q, Hu B, Tan X, Wong DS (2017) Chaotic maps-based strong anonymous authentication scheme for roaming services in global mobility networks. *Wirel Pers Commun* 96(4):5881–5896
  44. Xu L, Wu F (2015) Cryptanalysis and improvement of a user authentication scheme preserving uniqueness and anonymity for connected health care. *J Med Syst* 39(10)
  45. Zhao D, Peng H, Li L, Yang Y (2014) A secure and effective anonymous authentication scheme for roaming service in global mobility networks. *Wirel Pers Commun* 78(1):247–269
  46. Jiang Q, Zeadally S, Ma J, He D (2017) Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks. *IEEE Access* 5:3376–3392
  47. Zhu J, Ma J (2004) A new authentication scheme with anonymity for wireless environments. *IEEE Trans Consum Electron* 50(1): 231–235
  48. Koblitz N (1987) Elliptic curve cryptosystems. *Math Comput* 48(177):203–209
  49. Miller VS (1986) Use of elliptic curves in cryptography. In: Williams HC (ed) *Advances in Cryptology — CRYPTO '85 Proceedings*. CRYPTO 1985, Lecture Notes in Computer Science, 218, Springer, pp 417–426
  50. Blake I, Seroussi G, Smart N (1999) *Elliptic curves in cryptography* (London mathematical society lecture note series). Cambridge University Press, Cambridge

**Publisher's note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.



## NUMERICAL RECKONING OF FIXED POINTS FOR GENERALIZED NONEXPANSIVE MAPPINGS IN CAT(0) SPACES WITH APPLICATIONS

Manoj Kumar<sup>1</sup>, Hemant Kumar Pathak<sup>2</sup>

*In this paper, we propose an iterative process for the reckoning of a fixed point of a mapping endowed with the (E) property in the setting of CAT(0) spaces. Results on strong and  $\Delta$ -convergence for this algorithm are stated and proved. Numerical examples are provided, regarding the behavior of this method from different point of views. Several relevant theorems in the existing literature have been generalized and improved.*

**Keywords:** Iterative algorithm; condition (E); fixed points;  $\Delta$ -convergence; strong convergence; CAT(0) space.

**MSC2020:** 47H09, 47H10, 58C3.

### 1. Introduction

Various nonlinear equations can be transformed in fixed point problems, a fact which allows determining their solutions by means of iterative processes. After Picard [21] introduced his famous iterative algorithm, Mann [17] developed this idea further. Ishikawa [11] stated a two step algorithm for the determination of a fixed point for a suitable class of operators, by means of two auxiliary sequences of real numbers from  $[0, 1]$ . Agrawal *et al.* [2] introduced another two step method based on two sequences, which satisfy a condition defined by means of a divergent series, for nearly asymptotically nonexpansive mappings. Noor [19] developed a three step iterative scheme in order to solve a class of variational inequalities by means of a fixed point approach. Sintunavarat et al [27] introduced a new three step iteration scheme for approximating fixed points of the nonlinear self mappings on a normed linear spaces satisfying Berinde contractive condition. Sahu et al. [24] developed an S-iteration technique for finding common fixed points for nonself quasi-nonexpansive mappings in the framework of a uniformly convex Banach space. Suzuki [28] proved convergence theorems for an algorithm designed for mappings endowed with the property (C), which is obviously fulfilled by nonexpansive mappings. These results have been developed further by Pant and Shukla [20], to the class of generalized  $\alpha$ -nonexpansive mappings. Extending more, the operators which fulfill the condition (E) were introduced by García-Falset *et al.* [9], and fixed point properties have been proved by means of almost fixed point sequences. Basarir and Sahin [3] performed a study of the S-iteration method in the framework of CAT(0) spaces, for a class of generalized nonexpansive mappings. The same geometric setting has been used by Dhompongsa and Panyanak [8] or by Khan and Abbas [12] in order to develop  $\Delta$ -convergence theorems for various algorithms. Garodia and Uddin [10] stated the counterpart of the Thakur *et al.* [29] scheme in the setting of CAT(0) spaces, for Suzuki generalized nonexpansive mappings. Nanjaras *et al.* [18] developed a Mann type iterative

<sup>1</sup>Research scholar, School of Studies in Mathematics, Pt. Ravishankar Shukla University, Raipur (C.G.) 492010, India, e-mail: manojyadav4567@gmail.com

<sup>2</sup>Professor, School of Studies in Mathematics, Pt. Ravishankar Shukla University, Raipur (C.G.) 492010, India, e-mail: hkpathak05@gmail.com

process regarding the reckoning of a fixed point associated with operators which satisfy the (C) conditions, on CAT(0) spaces.

The paper is organized as follows. Section 2 contains some concepts and properties needed in the sequel. Section 3 refers to convergence properties regarding an iterative scheme introduced here in the framework of CAT(0) spaces and meaningful numerical examples.

## 2. Preliminaries

Throughout this paper  $\mathbb{N} = \{1, 2, 3, \dots\}$  denotes the set of natural numbers, and  $\mathcal{F}(\mathcal{T}) = \{x \in C : \mathcal{T}x = x\}$  is the set of all fixed points of a mapping  $\mathcal{T} : C \rightarrow C$  where  $C$  is a convex subset of a linear space  $X$ .

Iterative procedures for the reckoning of a fixed point of a mapping endowed with suitable properties have been developed extensively.

In 1890, Picard [21] introduced his renowned iteration by  $x_{n+1} = \mathcal{T}x_n$ ,  $n \in \mathbb{N}$ .

Sixty three years later, Mann [17] imposed his iteration method on Banach spaces, as follows

$$x_{n+1} = (1 - \alpha_n)x_n + \alpha_n\mathcal{T}x_n, \quad n \in \mathbb{N}.$$

where  $\{\alpha_n\} \subset (0, 1)$  and  $\sum_{n=1}^{\infty} \alpha_n(1 - \alpha_n) = \infty$ , (see also [23]).

In 1974, Ishikawa [11] made the debut of several step iteration processes, for the reckoning of fixed points associated with Lipschitzian pseudo-contractive mappings in the setting of Hilbert spaces. For  $\{\alpha_n\}$ ,  $\{\beta_n\}$  sequences of numbers from  $(0, 1)$ , he defined

$$x_{n+1} = (1 - \alpha_n)x_n + \alpha_n\mathcal{T}((1 - \beta_n)x_n + \beta_n\mathcal{T}x_n), \quad n \in \mathbb{N}.$$

The Noor [19] iteration method appeared in 2000, related to a strongly monotone operator variational inequality on Hilbert spaces, and consists of

$$x_{n+1} = (1 - \alpha_n)x_n + \alpha_n\mathcal{T}((1 - \beta_n)x_n + \beta_n\mathcal{T}((1 - \gamma_n)x_n + \gamma_n\mathcal{T}x_n)), \quad n \in \mathbb{N}. \quad (1)$$

where  $\{\alpha_n\}$ ,  $\{\beta_n\}$ , and  $\{\gamma_n\}$  are sequences of numbers from  $(0, 1)$ .

In 2014, Abbas and Nazir [1] defined their iteration method for nonexpansive operators on uniformly convex Banach spaces, as follows

$$x_{n+1} = \alpha_n\mathcal{T}((1 - \beta_n)\mathcal{T}x_n + \beta_n\mathcal{T}((1 - \gamma_n)x_n + \gamma_n\mathcal{T}x_n)) + (1 - \alpha_n)\mathcal{T}((1 - \gamma_n)x_n + \gamma_n\mathcal{T}x_n), \quad n \in \mathbb{N}. \quad (2)$$

where  $\{\alpha_n\}$ ,  $\{\beta_n\}$ , and  $\{\gamma_n\}$  are sequences of numbers from  $(0, 1)$ .

In 2014, Thakur *et al.* [30] stated their iteration method TTP14 for the class of nonexpansive mappings, on the framework of Banach spaces, by

$$x_{n+1} = (1 - \alpha_n)\mathcal{T}x_n + \alpha_n\mathcal{T}((1 - \beta_n)((1 - \gamma_n)x_n + \gamma_n\mathcal{T}x_n) + \beta_n\mathcal{T}((1 - \gamma_n)x_n + \gamma_n\mathcal{T}x_n)), \quad n \in \mathbb{N}. \quad (3)$$

where  $\{\alpha_n\}$ ,  $\{\beta_n\}$ , and  $\{\gamma_n\}$  are sequences of numbers from  $(0, 1)$ .

The numerical process TTP16, was introduced by Thakur *et al.* [29] for nonexpansive mappings, on on uniformly convex Banach spaces, as follows:

$$x_{n+1} = (1 - \alpha_n)\mathcal{T}((1 - \gamma_n)x_n + \gamma_n\mathcal{T}x_n) + \alpha_n\mathcal{T}((1 - \beta_n)((1 - \gamma_n)x_n + \gamma_n\mathcal{T}x_n) + \beta_n\mathcal{T}((1 - \gamma_n)x_n + \gamma_n\mathcal{T}x_n)), \quad n \in \mathbb{N}. \quad (4)$$

where  $\{\alpha_n\}$ ,  $\{\beta_n\}$ ,  $\{\gamma_n\}$  are in  $(0, 1)$ .

In 2019, Garodia *et al.* [10] studied convergence behaviour of this algorithm in the setting of CAT(0) spaces, for generalized nonexpansive mappings.

In 2019, Piri *et al.* [22] introduced a new iterative scheme to approximate a fixed point of generalized  $\alpha$ -nonexpansive mappings in Banach spaces, as below.

$$\begin{cases} x_1 = x \in C, \\ x_{n+1} = (1 - \alpha_n)\mathcal{T}(\mathcal{T}((1 - \beta)x_n + \beta\mathcal{T}x_n)) + \alpha_n\mathcal{T}(\mathcal{T}(\mathcal{T}((1 - \beta)x_n + \beta\mathcal{T}x_n))) \quad n \in \mathbb{N}. \end{cases}$$

where  $\{\alpha_n\}, \{\beta_n\}, \{\gamma_n\}$  are in  $(0, 1)$ .

In order to develop our new results, we need to recall some classes of mappings whose properties will be used in the sequel.

**Definition 2.1.** Suppose  $K$  is a nonempty, closed, and convex subset of uniformly convex Banach space  $(X, \|\cdot\|)$ . A mapping  $\mathcal{T}: K \rightarrow K$  is said to be

- nonexpansive, if  $\|\mathcal{T}x - \mathcal{T}y\| \leq \|x - y\|$ , for all  $x, y \in K$ .
- quasi-nonexpansive, if  $\mathcal{T}$  possesses fixed points and  $\|\mathcal{T}x - p\| \leq \|x - p\|$ , for all  $x \in K$ , and any  $p \in \mathcal{F}(\mathcal{T})$ .

In 2011, García Falset *et. al.* [9] introduced the class of the mappings endowed with the  $(E)$  property, as follows.

**Definition 2.2.** Let  $(X, \|\cdot\|)$  be a Banach space, and  $S$  a nonempty subset of  $X$ . A mapping  $\mathcal{T}: S \rightarrow S$  satisfies the  $(E_\mu)$  condition on the set  $S$  if there can be found a real number  $\mu \geq 1$  so that

$$\|x - \mathcal{T}y\| \leq \mu\|x - \mathcal{T}x\| + \|x - y\|,$$

for all  $x, y \in S$ .

Moreover, it is said that  $\mathcal{T}$  accomplishes the condition  $(E)$  if there exists  $\mu \geq 1$  such that  $\mathcal{T}$  fulfills the condition  $(E_\mu)$ .

This class of operators entails those endowed with the  $(C)$  property (so all nonexpansive mappings satisfy the condition  $(E)$ ), but also other types of mappings, as proved in [9]. In the same paper, it is proved that a mapping endowed with the  $(E)$  property and has a fixed point is quasinonexpansive. Note that this condition can be easily formulated in the framework of metric spaces.

Motivated by above, in this paper we introduce a three-step iteration process with a single set of parameters,

$$\begin{cases} x_1 = x \in K \\ x_{n+1} = \mathcal{T}(\mathcal{T}(\mathcal{T}((1 - \alpha_n)x_n + \alpha_n\mathcal{T}x_n))), \quad n \in \mathbb{N}. \end{cases} \tag{5}$$

where  $\{\alpha_n\}$  is in  $(0, 1)$ .

The aim of this paper is to study the convergence of this iteration process (5) for mappings which fulfill the condition  $(E)$  in the framework of CAT(0) spaces. This setting has been considered here due to the fact that the non-positive curvature of Riemannian geometry, can be here presented in a wider sense, in this setting. Moreover, because of the absence of a natural linear and convex structure, many problems cannot be studied in usual metric spaces. Therefore we are aiming our study to those CAT(0) spaces, which are both Hilbert spaces as well as Banach spaces

Let us now recall some basics definitions, propositions and lemmas on CAT(0) spaces which shall be used in the next sections.

Let  $(X, d)$  be a metric space. A geodesic map is an isometric map  $f: I \rightarrow X$  on a convex subset  $I \subseteq \mathbb{R}$  to  $X$ , where the real line  $\mathbb{R}$  is endowed with the Euclidean distance. The map  $f$  is called a geodesic segment (respectively ray, line) if  $I$  is a closed interval (respectively  $I$  is a half-line,  $I = \mathbb{R}$ ).

A geodesic metric space is a metric space  $(X, d)$  in which any two points are joined by a geodesic segment.

**Example 2.1.** (i) The Euclidean space  $(\mathbb{R}^n, d_{Eucl})$  is a geodesic metric space.  
(ii) Any metric graph is a geodesic metric space.

Let  $(X, d)$  be a geodesic metric space. Given a triple  $(x, y, z) \in X^3$ , a Euclidean comparison triangle for  $(x, y, z)$  is a triple  $(\bar{x}, \bar{y}, \bar{z})$  of points from the Euclidean plane  $\mathbb{R}^2$

such that  $d(x, y) = d_{Eucl}(\bar{x}, \bar{y})$ ,  $d(y, z) = d_{Eucl}(\bar{y}, \bar{z})$  and  $d(z, x) = d_{Eucl}(\bar{z}, \bar{x})$ . Notice that any triple in  $X$  admits some Euclidean comparison triangle.

Intuitively, a geodesic metric  $(X, d)$  is a CAT(0) space if every geodesic triangle in  $X$  is at least as “thin” as its comparison triangle in the Euclidean plane.

**Definition 2.3.** Let  $\Delta$  be a geodesic triangle in the geodesic metric space  $(X, d)$  and let  $\bar{\Delta}$  be a comparison triangle for  $\Delta$ . Then  $\Delta$  is said to satisfy the CAT(0) inequality if for all  $x, y \in \Delta$  and all comparison points  $\bar{x}, \bar{y} \in \bar{\Delta}$ , the inequality  $d(x, y) \leq d_{\mathbb{R}^2}(\bar{x}, \bar{y})$  holds true.  $(X, d)$  is a CAT(0) space if the CAT(0) inequality is satisfied for any triangle from this space.

As examples of CAT(0) spaces, we enumerate the following.

**Example 2.2.** (i) The Euclidean space  $(\mathbb{R}^n, d_{Eucl})$  is a CAT(0) space, and so is any pre-Hilbert space.

(ii) A metric graph  $X$  is a CAT(0) space if and only if  $X$  is a tree.

Assume now that  $x, y_1, y_2$  are points in a CAT(0) space and  $y_0$  is the midpoint of the segment  $[y_1, y_2]$ . Then the CAT(0) inequality implies

$$d(x, y_0)^2 \leq \frac{1}{2}d(x, y_1)^2 + \frac{1}{2}d(x, y_2)^2 - \frac{1}{4}d(y_1, y_2)^2. \quad (CN)$$

This is the (CN) inequality of Bruhat and Tits [5]. In fact, a geodesic space is a CAT(0) space if and only if it satisfies the (CN) inequality.

In the following, we mention some interesting and useful properties of CAT(0) spaces.

**Lemma 2.1** ([8]). Let  $(X, d)$  be a CAT(0) space. Then

- (1)  $(X, d)$  is uniquely geodesic.
- (2) Let  $p, x, y$  be points of  $X$ ,  $\alpha \in [0, 1]$ ,  $m_1$  and  $m_2$  denote, respectively, the points from  $[p, x]$  and  $[p, y]$  satisfying  $d(p, m_1) = \alpha d(p, x)$  and  $d(p, m_2) = \alpha d(p, y)$ . Then the next statement is fulfilled

$$d(m_1, m_2) \leq \alpha d(x, y).$$

- (3) Let  $x, y \in X$ ,  $x \neq y$  and  $z, w \in [x, y]$  such that  $d(x, z) = d(x, w)$ . Then  $z = w$ .
- (4) Let  $x, y \in X$ . For each  $t \in [0, 1]$ , there exists a unique point  $z \in [x, y]$  such that

$$d(x, z) = td(x, y) \quad \text{and} \quad d(y, z) = (1-t)d(x, y). \quad (6)$$

- (5) For  $x, y, z \in X$  and  $t \in [0, 1]$ , the next inequality holds true

$$d((1-t)x \oplus ty, z) \leq (1-t)d(x, z) + td(y, z).$$

For the sake of convenience, from now on the notation  $(1-t)x \oplus ty$  will be used for the unique point  $z$  satisfying equalities (6).

Regarding the geometric properties, we recollect the ones which play a vital role in the development of our outcomes.

Let  $\{s_n\}$  be a bounded sequence in a CAT(0) space  $(X, d)$ . For  $s \in X$ , we set

$$r(s, \{s_n\}) = \limsup_{n \rightarrow \infty} d(s, s_n).$$

The asymptotic radius of  $\{s_n\}$  is given by

$$r(\{s_n\}) = \inf\{r(s, \{s_n\}) : s \in X\}.$$

The asymptotic center of  $\{s_n\}$  is the set

$$A(\{s_n\}) = \{s \in X : r(s, \{s_n\}) = r(\{s_n\})\}.$$

In 2006, Dhompongsa *et al.* [7] stated that, in the framework of CAT(0) spaces, the asymptotic center consists of exactly one point.

CAT(0) spaces feature an interesting type of convergence defined by means of asymptotic centers, namely the  $\Delta$ -convergence.

**Definition 2.4** ([14]). A sequence  $\{s_n\}$  in a CAT(0) space  $X$  is said to be  $\Delta$ -convergent to  $s \in X$  if the unique asymptotic center of  $\{u_n\}$  is  $s$ , for every subsequence  $\{u_n\}$  of  $\{s_n\}$ .

Such kind of convergence will be represented by  $\Delta - \lim_{n \rightarrow \infty} s_n = s$ , and read as  $s$  is the  $\Delta$ -limit of  $\{s_n\}$ .

We denote  $W_\Delta(\{s_n\}) = \bigcup A(\{u_n\})$ , where the union is considered over all subsequences  $\{u_n\}$  of  $\{s_n\}$ .

The following lemmas have been proved by Dhompongsa and Panyanak [8].

**Lemma 2.2.** Suppose  $X$  is a CAT(0) space. Then, for all  $x, y, z \in X$ , and  $t \in [0, 1]$ , the next inequality is fulfilled

$$d((1-t)x \oplus ty, z) \leq (1-t)d(x, z) + td(y, z).$$

**Lemma 2.3.** Suppose  $(X, d)$  is a CAT(0) space. Then the next statements hold true.

- 1) Every bounded sequence in  $X$  has a  $\Delta$ -convergent subsequence.
- 2) If  $K$  is a closed, and convex subset of  $X$  and if  $\{x_n\}$  is a bounded sequence in  $K$ , then the asymptotic center of  $\{x_n\}$  is an element of the set  $K$ .

**Lemma 2.4.** Suppose that  $\{s_n\}$  is a bounded sequence in a complete CAT(0) space so that  $A(\{s_n\}) = \{s\}$ , and  $\{u_n\}$  is a subsequence of  $\{s_n\}$ ,  $A(\{u_n\}) = \{u\}$ . If the sequence  $\{d(s_n, u)\}$  converges, then  $s = u$ .

The next lemma proved by Laowang and Panyanak [15] regards the behaviour of some sequences with adequate properties in CAT(0) spaces.

**Lemma 2.5.** Let  $(X, d)$  be a complete CAT(0) space and  $x \in X$ . Suppose  $\{t_n\}$  is a sequence in  $[b, c] \subset (0, 1)$  and  $\{u_n\}, \{v_n\}$  are sequences in  $X$  such that  $\limsup_{n \rightarrow \infty} d(u_n, u) \leq r$ ,  $\limsup_{n \rightarrow \infty} d(v_n, u) \leq r$  and  $\lim_{n \rightarrow \infty} d(t_n v_n \oplus (1 - t_n)u_n, x) = r$  hold for some  $r \geq 0$ . Then  $\lim_{n \rightarrow \infty} d(u_n, v_n) = 0$ .

Iteration (5) has its CAT(0) spaces version, as in the next lines.

Let  $K$  be a nonempty, closed, and convex subset of a complete CAT(0) space  $X$ , and  $\mathcal{T}: K \rightarrow K$  be a mapping. Let  $x_1 \in K$  be arbitrary, and the sequence  $\{x_n\}$  generated iteratively by

$$\begin{cases} x_1 = x \in K \\ x_{n+1} = \mathcal{T}\bar{x}_n, \\ \bar{x}_n = \mathcal{T}\tilde{x}_n, \\ \tilde{x}_n = \mathcal{T}((1 - \alpha_n)x_n \oplus \alpha_n \mathcal{T}x_n), \quad n \in \mathbb{N}. \end{cases} \tag{7}$$

where  $\alpha_n \in (0, 1)$ , for  $n \in \mathbb{N}$ .

Please note that Kirk [13] proved that any nonexpansive mapping defined on a bounded closed convex subset of a complete CAT(0) space has a fixed point.

### 3. $\Delta$ -Convergence and Strong Convergence Theorems

In the following, we will prove the strong and  $\Delta$ -convergence of this iteration process (7). Our results will be generalization of some results of Chanchal Garodia *et al.* [10], Khan and Abbas [12], and Piri *et al.* [22].

The next theorem provides conditions for the boundedness of the sequence generated by Algorithm (7).

**Theorem 3.1.** *Let  $K$  be a nonempty, closed, convex subset of a complete  $CAT(0)$  space  $X$ , and  $\mathcal{T}: K \rightarrow K$  be a mapping endowed with the property (E). Consider that  $\{x_n\} \subset K$  is defined by (7), where  $\{\alpha_n\}$  is in  $(0, 1)$  and  $\mathcal{F}(\mathcal{T}) \neq \emptyset$ . Then  $\{x_n\}$  is bounded and  $\lim_{n \rightarrow \infty} d(x_n, p)$  exists for all  $p \in \mathcal{F}(\mathcal{T})$ .*

*Proof.* Let  $p \in \mathcal{F}(\mathcal{T})$  be a fixed point of  $\mathcal{T}$ , which is a quasicontractive mapping. From (7) and using Lemma 2.2, we have, for any  $n \in \mathbb{N}$ ,

$$\begin{aligned} d(\tilde{x}_n, p) &= d(\mathcal{T}((1 - \alpha_n)x_n \oplus \alpha_n \mathcal{T}x_n), p) \\ &\leq d((1 - \alpha_n)x_n \oplus \alpha_n \mathcal{T}x_n, p) \\ &\leq (1 - \alpha_n)d(x_n, p) + \alpha_n d(\mathcal{T}x_n, p) \\ &\leq (1 - \alpha_n)d(x_n, p) + \alpha_n d(x_n, p) \\ &= d(x_n, p), \end{aligned} \tag{8}$$

and

$$d(\bar{x}_n, p) = d(\mathcal{T}\tilde{x}_n, p) \leq d(\tilde{x}_n, p) \leq d(x_n, p), \quad n \in \mathbb{N}. \tag{9}$$

Inequalities (8) and (9) imply

$$d(x_{n+1}, p) = d(\mathcal{T}\bar{x}_n, p) \leq d(\bar{x}_n, p) \leq d(x_n, p), \quad n \in \mathbb{N}.$$

Therefore,  $d(x_n, p)$  is bounded below and nonincreasing. Hence  $\lim_{n \rightarrow \infty} d(x_n, p)$  exists. The boundedness of the sequence  $\{x_n\}$  follows then easily.  $\square$

**Theorem 3.2.** *Let  $K$  be a nonempty, closed, and convex subset of a complete  $CAT(0)$  space  $(X, d)$ . Let  $\mathcal{T}: K \rightarrow K$  be a mapping which satisfies the condition (E) on  $K$ , such that  $\mathcal{F}(\mathcal{T}) \neq \emptyset$ , and  $\{x_n\}$  be defined by Algorithm (7), where  $\{\alpha_n\}$  is in  $(0, 1)$ . Then  $\lim_{n \rightarrow \infty} d(x_n, \mathcal{T}x_n) = 0$ .*

*Proof.* According to Theorem 3.1, the sequence  $\{d(x_n, p)\}$  is convergent. Assume that  $\lim_{n \rightarrow \infty} d(x_n, p) = l$ . Inequality (9) from Theorem 3.1 compels  $d(\bar{x}_n, p) \leq d(x_n, p)$ ,  $n \in \mathbb{N}$ , hence it follows that  $\limsup d(\bar{x}_n, p) \leq \lim d(x_n, p) = l$ . Therefore,

$$\limsup d(\bar{x}_n, p) \leq l. \tag{10}$$

Since  $T$  is a quasicontractive mapping, we have

$$\limsup d(\mathcal{T}x_n, p) \leq \lim d(x_n, p) = l. \tag{11}$$

Having in view inequality (9) from Theorem 3.1, we obtain  $d(x_{n+1}, p) = d(\mathcal{T}\bar{x}_n, p) \leq d(\bar{x}_n, p)$ , implying that  $\lim d(x_{n+1}, p) \leq \liminf d(\bar{x}_n, p)$ . Thus, we have

$$l \leq \liminf d(\bar{x}_n, p). \tag{12}$$

From relations (10) and (12), it follows that

$$\lim_{n \rightarrow \infty} d(\bar{x}_n, p) = l.$$

Moreover, the above mentioned inequality and relation (11) leads to

$$\begin{aligned} l &= \lim_{n \rightarrow \infty} d(\bar{x}_n, p) = \lim_{n \rightarrow \infty} d(\mathcal{T}\tilde{x}_n, p) \leq \liminf_{n \rightarrow \infty} d(\tilde{x}_n, p) \\ &\leq \liminf_{n \rightarrow \infty} d(\mathcal{T}((1 - \alpha_n)x_n \oplus \alpha_n \mathcal{T}x_n), p) \leq \liminf_{n \rightarrow \infty} d(((1 - \alpha_n)x_n \oplus \alpha_n \mathcal{T}x_n), p) \\ &\leq \liminf_{n \rightarrow \infty} ((1 - \alpha_n)d(x_n, p) + \alpha_n d(\mathcal{T}x_n, p)) \leq \limsup_{n \rightarrow \infty} ((1 - \alpha_n)d(x_n, p) + \alpha_n d(\mathcal{T}x_n, p)) \\ &\leq \limsup_{n \rightarrow \infty} ((1 - \alpha_n)d(x_n, p) + \alpha_n d(x_n, p)) = l. \end{aligned}$$

This implies that

$$\lim_{n \rightarrow \infty} ((1 - \alpha_n)d(x_n, p) + \alpha_n d(\mathcal{J}x_n, p)) = l.$$

Based on relation (11) and Lemma 2.5, we have drawn the conclusion that  $\lim_{n \rightarrow \infty} d(x_n, \mathcal{J}x_n) = 0$ , and the proof is completed.  $\square$

The next result refers to a  $\Delta$ -convergence property associated with the iterative method (7).

**Theorem 3.3.** *Let  $\mathcal{J}: K \rightarrow K$  be a mapping which fulfills the condition (E) on a nonempty, closed, and convex subset  $K$  of a complete CAT(0) space  $(X, d)$  such that the set of the fixed points of  $T$  is not empty. If  $\{x_n\}$  is a sequence defined by the iteration process (7), then  $\{x_n\}$  is  $\Delta$ -convergent to a fixed point of  $\mathcal{J}$ .*

*Proof.* From Theorem 3.1 and Theorem 3.2, it is clear that  $\lim_{n \rightarrow \infty} d(x_n, p)$  exists for each  $p \in \mathcal{F}(\mathcal{J})$ , the sequence  $\{x_n\}$  is bounded, and  $\lim_{n \rightarrow \infty} d(x_n, Tx_n) = 0$ . Let  $W_\Delta(\{x_n\}) = \bigcup A(\{u_n\})$ , where the reunion is taken over all subsequences  $\{u_n\}$  of  $\{x_n\}$ .

First we will show that  $W_\Delta(\{x_n\}) \subseteq \mathcal{F}(\mathcal{J})$ . Let  $u \in W_\Delta(\{x_n\})$ . Then, there exists a subsequence  $\{u_n\}$  of  $\{x_n\}$  such that  $A(\{u_n\}) = u$ . By Lemma 2.3 there exists a subsequence  $\{v_n\}$  of  $\{u_n\}$  such that  $\Delta - \lim_{n \rightarrow \infty} v_n = v$  and  $v \in K$ . Since  $\lim_{n \rightarrow \infty} d(\mathcal{J}x_n, x_n) = 0$  and  $\{v_n\}$  is a subsequence of  $\{x_n\}$ ,  $\lim_{n \rightarrow \infty} d(v_n, Tv_n) = 0$ . Since  $\mathcal{J}$  satisfies the condition (E), there exists  $\mu \geq 1$ , so that for all  $x, y \in K$ ,  $d(x, \mathcal{J}y) \leq \mu d(x, \mathcal{J}x) + d(x, y)$ . This inequality compels that

$$d(v_n, \mathcal{J}v) \leq \mu d(v_n, \mathcal{J}v_n) + d(v_n, v).$$

Taking lim sup in both sides of this relation, it follows that

$$\begin{aligned} \limsup_{n \rightarrow \infty} d(v_n, \mathcal{J}v) &\leq \limsup_{n \rightarrow \infty} (\mu d(v_n, \mathcal{J}v_n) + d(v_n, v)) \\ &\leq \mu \limsup_{n \rightarrow \infty} d(v_n, \mathcal{J}v_n) + \limsup_{n \rightarrow \infty} d(v_n, v) = \limsup_{n \rightarrow \infty} d(v_n, v). \end{aligned}$$

As  $\Delta - \lim_{n \rightarrow \infty} v_n = v$ , we get  $\limsup_{n \rightarrow \infty} d(v_n, v) \leq \limsup_{n \rightarrow \infty} d(v_n, \mathcal{J}v)$ , and hence

$$\limsup_{n \rightarrow \infty} d(v_n, v) = \limsup_{n \rightarrow \infty} d(v_n, \mathcal{J}v).$$

It follows that  $\mathcal{J}v = v$  i.e.  $v \in \mathcal{F}(\mathcal{J})$ .

Presume that  $u \neq v$ . By Theorem 3.1,  $\lim_{n \rightarrow \infty} d(x_n, v)$  exists as  $v \in \mathcal{F}(\mathcal{J})$ . We now claim that  $v = u$ . Then by the uniqueness property regarding the asymptotic centers, we have

$$\begin{aligned} \limsup_{n \rightarrow \infty} d(v_n, v) &< \limsup_{n \rightarrow \infty} d(v_n, u) \leq \limsup_{n \rightarrow \infty} d(u_n, u) \\ &< \limsup_{n \rightarrow \infty} d(u_n, v) = \limsup_{n \rightarrow \infty} d(x_n, v) = \limsup_{n \rightarrow \infty} d(v_n, v) \end{aligned}$$

which is a contradiction. Thus  $u = v$  and hence  $W_\Delta(\{x_n\}) \subseteq \mathcal{F}(\mathcal{J})$ .

To show that the sequence  $\{x_n\}$  is  $\Delta$ -convergent to a fixed point of  $T$ , we show that  $W_\Delta(\{x_n\})$  consists of exactly one point. In this respect, consider  $\{u_n\}$  a subsequence of  $\{x_n\}$ . By using Lemma 2.3, there can be found a subsequence  $\{v_n\}$  of  $\{u_n\}$  such that  $\Delta - \lim_{n \rightarrow \infty} v_n = v$  and  $v \in K$ . Let  $A(\{u_n\}) = \{u\}$  and  $A(\{x_n\}) = \{x\}$ . It has already been proved that  $u = v$  and  $v \in \mathcal{F}(\mathcal{J})$ . Since  $v \in \mathcal{F}(\mathcal{J})$ , by Theorem 3.1,  $\{d(x_n, v)\}$  is convergent. Lemma 2.4 leads to  $v = x$ . Therefore  $W_\Delta(\{x_n\}) = \{x\}$ . This completes the proof.  $\square$

Using Theorem 3.1 and Theorem 3.2, now we are in a position to prove a strong convergence result.

**Theorem 3.4.** Let  $\mathcal{T}: K \rightarrow K$  be a mapping endowed with the property (E), defined on a nonempty, closed, and convex subset  $K$  of a complete CAT(0) space  $(X, d)$ , which possesses at least one fixed point. Denote by  $\{x_n\}$  the sequence defined by the iteration process (7). Then  $\{x_n\}$  converges to a fixed point of  $T$  if and only if  $\liminf_{n \rightarrow \infty} d(x_n, \mathcal{F}(\mathcal{T})) = 0$ .

*Proof.* Presume first that the sequence  $\{x_n\}$  converges to a point  $p \in \mathcal{F}(\mathcal{T})$ . Then  $\lim_{n \rightarrow \infty} d(x_n, p) = 0$ , so  $\liminf_{n \rightarrow \infty} d(x_n, \mathcal{F}(\mathcal{T})) = 0$ , and the conclusion has been proved.

Conversely, suppose now that  $\liminf_{n \rightarrow \infty} d(x_n, \mathcal{F}(\mathcal{T})) = 0$ . According to Theorem 3.1,

$$d(x_{n+1}, p) \leq d(x_n, p), \quad \text{for all } p \in \mathcal{F}(\mathcal{T}).$$

Because  $d(x_{n+1}, \mathcal{F}(\mathcal{T})) = \inf_{q \in \mathcal{F}(\mathcal{T})} d(x_{n+1}, q) \leq d(x_{n+1}, p)$ , for all fixed points  $p$  of  $\mathcal{T}$ , it follows that  $d(x_{n+1}, \mathcal{F}(\mathcal{T})) \leq d(x_n, \mathcal{F}(\mathcal{T}))$ , and, as a consequence,  $\lim_{n \rightarrow \infty} d(x_n, \mathcal{F}(\mathcal{T}))$  exists. Having in view the hypothesis of the theorem, we get  $\lim_{n \rightarrow \infty} d(x_n, \mathcal{F}(\mathcal{T})) = 0$ .

Let us prove now that  $\{x_n\}$  is a Cauchy sequence in  $K$ . Consider  $\epsilon > 0$ . Since  $\lim_{n \rightarrow \infty} d(x_n, \mathcal{F}(\mathcal{T})) = 0$ , there exists  $n_0 \in \mathbb{N}$  such that  $d(x_n, \mathcal{F}(\mathcal{T})) < \frac{\epsilon}{4}$ , for all  $n \geq n_0$ . In particular,  $\inf\{d(x_{n_0}, p) : p \in \mathcal{F}(\mathcal{T})\} < \frac{\epsilon}{4}$ . Therefore, there exists  $p^* \in \mathcal{F}(\mathcal{T})$  such that  $d(x_{n_0}, p^*) < \frac{\epsilon}{2}$ . If  $m, n \geq n_0$ , it can be noticed that

$$d(x_{n+m}, x_n) < d(x_{n+m}, p^*) + d(p^*, x_n) \leq 2d(x_{n_0}, p^*) < 2 \frac{\epsilon}{2} = \epsilon.$$

Hence  $\{x_n\}$  is a Cauchy sequence in the closed subset  $K$  of a complete CAT(0) space. Let  $x \in K$  be its limit. As  $\lim_{n \rightarrow \infty} d(x_n, \mathcal{F}(\mathcal{T})) = 0$ , it follows that  $d(x, \mathcal{F}(\mathcal{T})) = 0$ . According to Chidume and Maruster [6], the set  $\mathcal{F}(\mathcal{T})$  is closed, which allows us to conclude that  $x \in \mathcal{F}(\mathcal{T})$ .  $\square$

Senter *et al.* [26] introduced the condition (A) as follows.

Let  $(B, \|\cdot\|)$  be a Banach space, and  $K \subseteq B$ . A mapping  $\mathcal{T}: K \rightarrow K$  is said to satisfy the condition (A) if there exists a nondecreasing function  $f: [0, \infty) \rightarrow [0, \infty)$  with  $f(0) = 0$ ,  $f(r) > 0$ , for all  $r \in (0, \infty)$  such that  $d(x, \mathcal{T}x) \geq f(d(x, \mathcal{F}(\mathcal{T})))$  for all  $x \in K$ .

A similar definition can be easily formulated in the framework of CAT(0) spaces.

**Theorem 3.5.** Let  $\mathcal{T}: K \rightarrow K$  be a mapping defined on a nonempty, closed, and convex subset  $K$  of a complete CAT(0) space  $X$ , endowed with the property (E), which satisfies the condition (A), such that  $\mathcal{F}(\mathcal{T})$  is not empty. If  $\{x_n\}$  is a sequence defined by Algorithm (7), then  $\{x_n\}$  converges strongly to a fixed point of  $\mathcal{T}$ .

*Proof.* By Theorem 3.1,  $\lim_{n \rightarrow \infty} d(x_n, p)$  exists for all  $p \in \mathcal{F}(\mathcal{T})$ . Since  $d(x_{n+1}, p) \leq d(x_n, p)$ ,  $n \in \mathbb{N}$ , it follows that

$$\inf_{q \in \mathcal{F}(\mathcal{T})} d(x_{n+1}, q) \leq d(x_n, p), \quad \text{for any } p \in \mathcal{F}(\mathcal{T}),$$

which yields  $d(x_{n+1}, \mathcal{F}(\mathcal{T})) \leq d(x_n, \mathcal{F}(\mathcal{T}))$ . This compels that the sequence  $\{d(x_n, \mathcal{F}(\mathcal{T}))\}$  is nonincreasing and bounded from below. It follows that the limit  $\lim_{n \rightarrow \infty} d(x_n, \mathcal{F}(\mathcal{T}))$  exists. Also, by Theorem 3.2,  $\lim_{n \rightarrow \infty} d(x_n, \mathcal{T}x_n) = 0$ .

Since the condition (A) is fulfilled,  $\lim_{n \rightarrow \infty} f(d(x_n, \mathcal{F}(\mathcal{T}))) \leq \lim_{n \rightarrow \infty} d(x_n, \mathcal{T}x_n) = 0$ . It follows that  $\lim_{n \rightarrow \infty} f(d(x_n, \mathcal{F}(\mathcal{T}))) = 0$ . Keeping in mind that  $f$  is a nondecreasing function satisfying  $f(0) = 0$ , and  $f(r) > 0$ , for all points  $r \in (0, \infty)$ , we obtain that  $\lim_{n \rightarrow \infty} d(x_n, \mathcal{F}(\mathcal{T})) = 0$ . Since all the conditions in Theorem 3.4 are satisfied, the sequence  $\{x_n\}$  converges strongly to a fixed point of  $\mathcal{T}$ .  $\square$



Recall that a complete simply connected Riemannian manifold of nonpositive sectional curvature is called a Hadamard manifold. For some fundamental definitions, properties and notations of Riemannian manifolds, one can refer to [4, 25]. We now continue our discussion with an example which regards a Hadamard manifold (all Hadamard manifolds are CAT(0) spaces), inspired by [16].

**Example 3.1.** Let  $\mathbb{E}^{3,1}$  be the Minkowski space  $\mathbb{R}^{3+1}$  endowed with the Lorentz inner product

$$\langle x, y \rangle = \sum_{k=1}^3 x^k y^k - x^4 y^4, \quad x = (x^k), y = (y^k) \in \mathbb{R}^{3+1}.$$

According to [4], p. 93, the set  $\mathbb{H}^3 = \{x \in \mathbb{E}^{3,1} : \langle x, x \rangle = -1, x^4 > 0\}$  can be organized as a Riemannian manifold. The corresponding distance is  $d: \mathbb{H}^3 \times \mathbb{H}^3 \rightarrow \mathbb{R}$ , where  $d(x, y)$  is the unique non-negative value for which  $\cosh d(x, y) = -\langle x, y \rangle$ .

Let  $x \in \mathbb{H}^3$  and a unit vector  $v$  from the tangent space  $\mathcal{T}_x \mathbb{H}^3$ . The corresponding geodesic is

$$\gamma: \mathbb{R} \rightarrow \mathbb{H}^3 \quad \gamma(t) = (\cosh t)x + (\sinh t)v,$$

while the exponential map is

$$\exp_x: \mathcal{T}_x \mathbb{H}^3 \rightarrow \mathbb{H}^3, \quad \exp_x(rv) = (\cosh r)x + (\sinh r)v, \quad r \in \mathbb{R}^+, x \in \mathbb{H}^3, v \in \mathcal{T}_x \mathbb{H}^3,$$

while its inverse is given by

$$\exp_x^{-1} y = r(x, y)V(x, y), \quad y \in \mathbb{H}^3,$$

where  $r(x, y) = \operatorname{arccosh}(-\langle x, y \rangle)$  and  $V(x, y) = \frac{y + \langle x, y \rangle x}{\sqrt{\langle x, y \rangle^2 - 1}}$ .

In the following, consider the nonexpansive mapping

$$\mathcal{T}: \mathbb{H}^3 \rightarrow \mathbb{H}^3, \quad \mathcal{T}x = (-x^1, -x^2, -x^3, x^4), \quad x = (x^k) \in \mathbb{H}^3,$$

with the unique fixed point  $(0, 0, 0, 1)$ .

As an initial value we considered  $x_0 = (1, 1, 1, 2)$ . We have considered  $\alpha_n = \frac{3}{5}$  in the scheme introduced here. Comparisons made with respect to the algorithms introduced by Abbas and Nazir [1], Noor [19], Thakur *et al.* [30] (TTP14), Thakur *et al.* [29] (TTP16), for the choice of all parameter sequences equal to  $\frac{3}{5}$ , are presented below. In the second column we have indicated the number of iteration at which an error smaller than  $10^{-9}$  is obtained.

Process	No. of iteration
TTP14	iteration#29
Noor	iteration #24
TTP16	iteration#10
Abbas	iteration # 9
Algorithm (7)	iteration #8

Now, we present an example of a mapping which fulfills the condition (E) and illustrates the convergence of the iteration process (7) with respect to different initial values.

**Example 3.2.** Let the set  $K = [0, \infty)$  be equipped with the usual norm  $|\cdot|$  and let

$$\mathcal{T}: K \rightarrow K, \quad \mathcal{T}(x) = \begin{cases} \frac{x}{2}, & \text{if } x > 2, \\ 0, & \text{otherwise.} \end{cases}$$

Piri [22] proved that the mapping  $\mathcal{T}$  does not satisfy the condition (C), but it is a generalized  $\alpha$ -nonexpansive mapping, so it fulfills the condition (E).

For  $\alpha_n = \frac{n}{n^2 + 1}$ , we obtain Table 1 and Figure 1 for different initial values.

TABLE 1. Comparison Table for Example 3.2

Steps	$x_1 = 10^1$	$x_1 = 10^2$	$x_1 = 10^3$	$x_1 = 1500$	$x_1 = 10^5$
0	10	100.0000	1000.0000	1500.0000	10000.0000
1	2.5000	25.0000	250.0000	375.0000	2500.0000
2	0.4688	4.6875	46.8750	70.3125	468.7500
3	0.0000	0.9375	9.3750	14.0625	93.7500
4	0.0000	0.0000	1.9922	2.9883	19.9219
5	0.0000	0.0000	0.0000	0.6592	4.3945
6	0.0000	0.0000	0.0000	0.0000	0.9929
7	0.0000	0.0000	0.0000	0.0000	0.0000

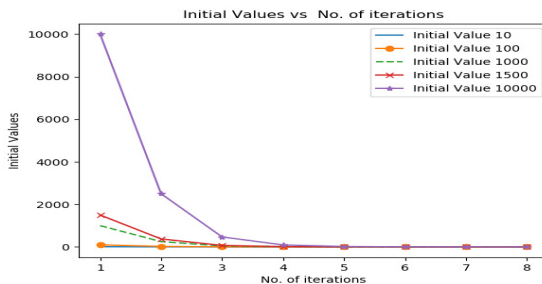


FIGURE 1. Convergence behavior of process (7) for Example 3.2 for various initial values

**Example 3.3.** Let  $K = [0, 1]$  which is a closed, and convex subset of the  $CAT(0)$  space  $X = \mathbb{R}$ , endowed with the usual metric. Define a mapping

$$\mathcal{T}: K \rightarrow K, \mathcal{T}x = \begin{cases} \frac{x}{2}, & \text{if } x \neq 1, \\ \frac{7}{11}, & \text{if } x = 1. \end{cases}$$

It is obvious that  $0 \in F(\mathcal{T})$ , and that  $\mathcal{T}$  fulfills the condition (E) for  $\mu = \frac{11}{8} > 1$ . The operator  $T$  does not satisfy the condition (C) of Suzuki. Indeed, if we consider  $x = \frac{4}{5}$  and  $y = 1$ , then

$$\frac{1}{2}|x - \mathcal{T}x| = \frac{1}{2} \left| \frac{4}{5} - \frac{2}{5} \right| = \frac{1}{5} = |x - y|.$$

On the other hand,

$$|\mathcal{T}x - \mathcal{T}y| = \left| \mathcal{T}\frac{4}{5} - \mathcal{T}1 \right| = \left| \frac{2}{5} - \frac{7}{11} \right| = \frac{13}{55} > \left| \frac{4}{5} - 1 \right| = |x - y|.$$

Thus,  $\mathcal{T}$  fails to satisfy condition (C). Furthermore, we have examined the influence of parameters  $\alpha_n, \beta_n$  and  $\gamma_n$ . For this we have considered various sets of parameters and present a study regarding the number of iterations required. Each iteration starts with a particular initial value and the respective number of iterations, average of the number of iterations for different initial points are given in Figure 2. We have examined the fastness and stability of different iterations relative to above mentioned set of parameters. The observations are given in Figure 2 and Figure 3. We have concluded that the new iteration process (7) not only converges faster than the known iterations but also is stable with respect to the parameters  $\alpha_n, \beta_n$  and  $\gamma_n$ . From Figure 2, we also observe that the average number of iterations of the new iteration process (7) is the smallest with respect to other processes.

We now discuss the influence of parameters  $\alpha_n, \beta_n, \gamma_n$  by considering the following five sets of parameters:

*Case 1.*  $\alpha_n = \sqrt{\frac{2n}{3n+5}}, \beta_n = \frac{1}{\sqrt{2n+9}}, \gamma_n = \frac{2n}{7n+9}$   
*Case 2.*  $\alpha_n = \frac{n}{n+2}, \beta_n = \frac{1}{\sqrt{n+5}}, \gamma_n = \frac{2n}{5n+3}$   
*Case 3.*  $\alpha_n = \frac{3n}{8n+4}, \beta_n = \frac{1}{n+4}, \gamma_n = \frac{n}{(5n+2)^2}$   
*Case 4.*  $\alpha_n = \frac{2n}{3n+2}, \beta_n = \frac{n}{\sqrt{49n^2+1}}, \gamma_n = \sqrt{\frac{2n}{(3n+5)}}$   
*Case 5.*  $\alpha_n = \frac{n}{n+1}, \beta_n = \frac{n}{n+5}, \gamma_n = \frac{n}{\sqrt{2n^2+9}}$ .

Comparison of various iteration processes for Example 3.3

Iterations		0.25					0.5					0.75					1					Iterations Average ↓				
Case	Ini. Value	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
Mann		70	59	167	88	55	71	60	171	90	55	72	60	171	91	56	73	61	174	92	57	71.5	60	171.2	90.2	56.2
Ishikawa		65	52	165	82	36	66	53	169	83	36	67	54	171	84	36	68	55	172	85	37	66.5	53.5	169.2	83.5	36.5
Noor		64	51	165	80	31	65	52	169	82	31	66	53	171	83	32	67	53	172	84	32	65.5	52.2	169.2	82.2	31.7
Abbas		29	27	39	30	23	29	27	39	30	23	29	28	40	50	23	36	28	41	31	24	29.5	27.5	39.7	30.5	23.5
TTP16		39	35	49	37	24	39	35	50	38	24	40	36	50	58	25	41	36	51	39	25	39.7	35.5	50	38	24.7
Piri		18	17	21	19	16	18	18	22	20	16	19	18	22	20	16	19	19	23	21	17	18.5	18	22	20	16.2
Alg. (7)		14	14	16	15	14	14	14	16	15	14	15	14	16	15	14	15	15	17	16	15	14.5	14.2	16.2	15.2	14.2

FIGURE 2. Table depicting Comparison of various iterations process under distinct parameters for Example 3.3

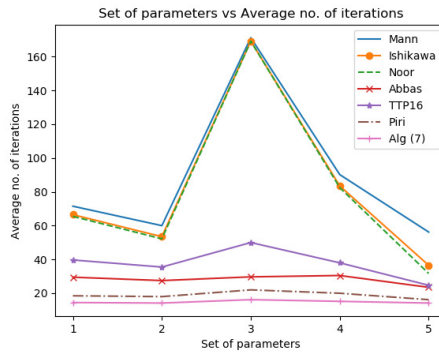


FIGURE 3. Average no. of iterations under distinct parameters for Example 3.3

#### 4. Conclusions

In this paper, we obtained some strong and  $\Delta$ -convergence results in CAT(0) space for a new iterative scheme for operators endowed with the (E) property. Our results extend and generalize many results in the literature. More precisely, Theorem 3.3, Theorem 3.4 and Theorem 3.5 extend Theorem 1, Theorem 2 and Theorem 3 of Khan and Abbas [12] in the sense that it provides a convergent scheme for approximating fixed points a class of mappings more general than that of nonexpansive mappings. Theorem 3.3, Theorem 3.4 and Theorem 3.5 generalize Theorem 3.1, Theorem 3.2 and Theorem 3.3 of Garodia and Uddin [10] proved for the TTP 14 [30] iteration scheme for generalized nonexpansive mappings.

#### REFERENCES

[1] M. Abbas and T. Nazir, A new faster iteration process applied to constrained minimization and feasibility problems, *Mat. Vesn.*, **66**(2004), 223-234.

- [2] *R.P. Agarwal, D. O'Regan, D. R. Sahu*, Iterative construction of fixed points of nearly asymptotically nonexpansive mappings, *J. Nonlinear Convex Anal.*, **8**(2007), 61-79.
- [3] *M. Basarir and A. Sahin*, On the strong and  $\Delta$ -convergence of S-iteration process for generalized nonexpansive mappings on CAT(0) space, *Thai J. Math.*, **12**(2014), 549-559.
- [4] *M. Bridson and A. Haefliger*, *Metric Spaces of Non-Positive Curvature*, Springer-Verlag, Berlin, Heidelberg, 1999.
- [5] *F. Bruhat and J. Tits* Groupes réductifs sur un corps local. I. Données radicielles valuées., *Inst. Hautes Études Sci. Publ. Math.*, **41**(1972), 5-251.
- [6] *C.E. Chidume, S. Măruşter*, Iterative methods for the computation of fixed points of demicontractive mappings, *J. Computational Appl. Math.*, **234**(2010), 861-882.
- [7] *S. Dhompongsa, W.A. Kirk and B. Sims*, Fixed points of uniformly Lipschitzian mappings, *Nonlinear Anal.*, **65**(2006), 762-772.
- [8] *S. Dhompongsa and B. Panyanak*, On  $\Delta$ -convergence theorems in CAT(0) spaces, *Comput. Math. Appl.*, **56**(2008), 2572-2579.
- [9] *J. García-Falset, E. Llorens-Fuster and T. Suzuki*, Fixed point theory for a class of generalized nonexpansive mappings, *J. Math. Anal. Appl.*, **375**(2011), 185-195.
- [10] *C. Garodia and I. Uddin*, Some convergence results for generalized nonexpansive mappings in CAT(0) space, *Commun. Korean Math. Soc.*, **34**(2019), 253-265.
- [11] *S. Ishikawa*, Fixed points by a new iteration method, *Proc. Amer. Math. Soc.*, **44**(1974), 147-150.
- [12] *S.H. Khan and M. Abbas*, Strong and  $\Delta$ -convergence of some iterative schemes in CAT(0) spaces, *Comput. Math. Appl.*, **61**(2011), 109-116.
- [13] *W. Kirk*, Geodesic geometry and fixed point theory, Seminar of Mathematical Analysis (Malaga/Seville, 2002/2003), in: *Colecc. Alberta, Univ. Sevilla Secr. Publ.*, Seville 64(2003), 195-225.
- [14] *W. Kirk and B. Panyanak*, A concept of convergence in geodesic spaces, *Nonlinear Anal.*, **68**(2008), 3689-3696.
- [15] *W. Laowang and B. Panyanak*, Approximating fixed points of nonexpansive nonself mappings in CAT(0) spaces, *Fixed Point Theory Appl.*, (2010), Art. ID 367274.
- [16] *C. Li, G. López and M. Martín-Márquez*, Iterative algorithms for nonexpansive mappings in Hadamard manifolds, *Taiwan. J. Math.*, **14**(2010), 541-559.
- [17] *W.R. Mann*, Mean value methods in iteration, *Proc. Am. Math. Soc.*, **4**(1953), 506-510.
- [18] *B. Nanjaras, B. Panyanak and W. Phuengrattana*, Fixed point theorems and convergence theorems for Suzuki-generalized nonexpansive mappings in CAT(0) spaces, *Nonlinear Anal. Hybrid Syst.*, **4**(2010), 25-31.
- [19] *M.A. Noor*, New approximation schemes for general variational inequalities, *J. Math. Anal. Appl.*, **251**(2000), 217-229.
- [20] *R. Pant and R. Shukla*, Approximating fixed point of generalized  $\alpha$ -nonexpansive mappings in Banach spaces, *Numer. Funct. Anal. Optim.*, **38**(2017), 248-266.
- [21] *E. Picard*, Mémoire sur la théorie des équations aux dérivées partielles et la méthode des approximations successives, *J. Math. Pures Appl.*, **6**(1890), 145-210.
- [22] *H. Piri, B. Daraby, S. Rahrovi and M. Ghasemi*, Approximating fixed points of generalized  $\alpha$ -nonexpansive mappings in Banach spaces by new faster iteration process, *Numer. Algorithms*, **81**(2019), 1129-1148.
- [23] *S. Reich*, Weak convergence theorems for nonexpansive mappings, *J. Math. Anal. Appl.*, **67**(1979), 274-276.
- [24] *D. R. Sahu, A. Pitea and M. Verma* A new iteration technique for nonlinear operators as concerns convex programming and feasibility problems, *Numerical Algorithms*, **83** (2020), 421-449
- [25] *T. Sakai* *Riemannian Geometry*, Translations of Mathematical Monographs 149, American Mathematical Society, Providence, RI, 1996.
- [26] *H.F. Senter and W.G. Dotson*, Approximating fixed points of nonexpansive mappings, *Proc. Amer. Math. Soc.*, **44**(1974), 375-380.
- [27] *W. Sintunavarat and A. Pitea*, On a new iteration scheme for numerical reckoning fixed points of Berinde mappings with convergence analysis, *J. Nonlinear Sci. Appl.* **9** (2016), 2553-2562.
- [28] *T. Suzuki*, Fixed point theorems and convergence theorems for some generalized nonexpansive mappings, *J. Math. Anal. Appl.*, **340**(2008), 1088-1095.
- [29] *B.S. Thakur, D. Thakur and Postolache*, M. A new iteration scheme for approximating fixed points of nonexpansive mappings, *Filomat*, **30**(2016), 2711-2720.
- [30] *D. Thakur, B.S. Thakur and M. Postolache*, New iteration scheme for numerical reckoning fixed points of nonexpansive mappings, *J. Ineq. Appl.*, (2014):328.