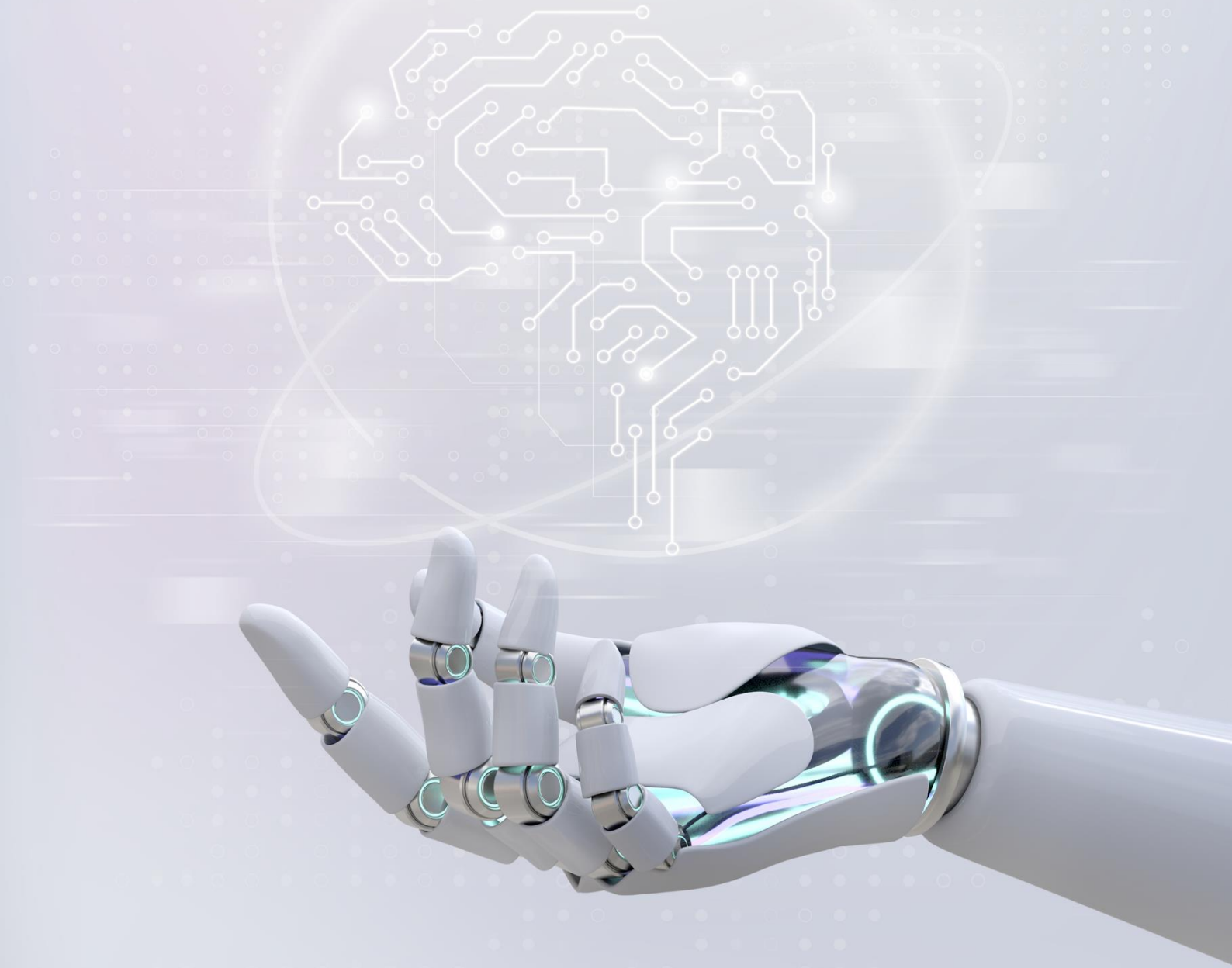
2ND INTERNATIONAL SYMPOSIUM ON SECURING NEXT-GENERATION SYSTEMS USING FUTURE ARTIFICIAL INTELLIGENCE TECHNOLOGIES (SNSFAIT-2023)

25th May 2023



CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

Editorial Board

Inquiries to
The Editor
SNSFAIT-2023 Symposium Souvenir
Maharaja Agrasen Institute of Technology,
Plot No 1 Rohini, Sector 22,
PSP Area, Delhi, 110086, India
Email: symposium.cse@mait.ac.in
Institute Website: www.mait.ac.in
Department Website: www.cse.mait.ac.in

Contents

Preface

We hereby are delighted to announce that Maharaja Agrasen Institute of Technology, Delhi, India in association with IEEE Communication Society Delhi Chapter has hosted the eagerly awaited and much coveted International Symposium on Securing Next-Generation Systems using Future Artificial Intelligence Technologies (SNSFAIT-2023) in Hybrid Mode. The second version of the symposium was able to attract a diverse range of engineering practitioners, academicians, scholars and industry delegates, with the reception of abstracts including more than 360 authors from different parts of the world. The committee of professionals dedicated towards the symposium is striving to achieve a high quality technical program with track on securing next-generation systems. Therefore, a lot of research is happening in the above-mentioned track and its related sub-areas. More than 90 full-length papers have been received, among which the contributions are focused on theoretical, computer simulation-based research, and laboratory-scale experiments. Amongst these manuscripts, 5 papers have been included in the CEUR workshop proceedings after a thorough two-stage review and editing process. All the manuscripts submitted to the SNSFAIT-2023 were peer-reviewed by at least two independent reviewers, who were provided with a detailed review proforma. The comments from the reviewers were communicated to the authors, who incorporated the suggestions in their revised manuscripts. The recommendations from two reviewers were taken into consideration while selecting a manuscript for inclusion in the proceedings. The exhaustiveness of the review process is evident, given the large number of articles received addressing a wide range of research areas. The stringent review process ensured that each published manuscript met the rigorous academic and scientific standards. It is an exalting experience to finally see these elite contributions materialize into a book volume as SNSFAIT-2023 proceedings by CEUR workshop proceedings entitled “International Symposium on Securing Next-Generation Systems using Future Artificial Intelligence Technologies”.

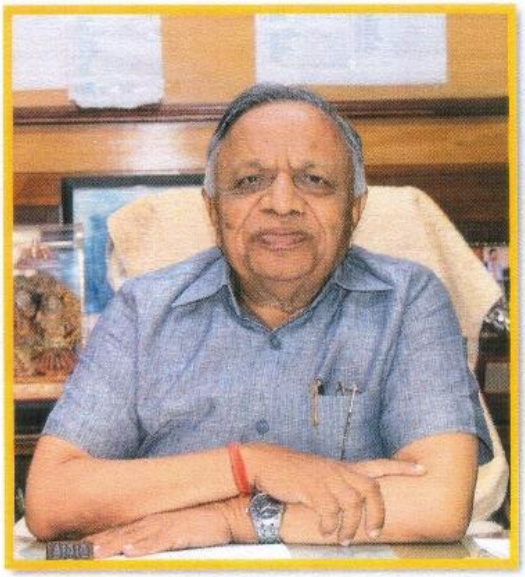
All the contributing authors owe thanks to the organizers of SNSFAIT-2023 for their interest and exceptional articles. We would also like to thank the authors of the papers for adhering to the time schedule and for incorporating the review comments. We wish to extend my heartfelt acknowledgment to the authors, peer-reviewers, committee members, and production staff whose diligent work put shape to the SNSFAIT-2023 proceedings. We especially want to thank our dedicated team of peer reviewers who volunteered for the arduous and tedious step of quality checking and critique on the submitted manuscripts. The management, faculties, administrative and support staff of the college has always been extending their services whenever needed, for which we remain thankful to them.

Lastly, we would like to thank CEUR workshop proceedings for accepting our proposal for publishing the SNSFAIT-2023 symposium proceedings.

Deepak Gupta, Namita Gupta
Organizers, SNSFAIT-2023

MATES
उद्यमेन हि सिध्यन्ति कार्याणि न मनोरथै :

MAHARAJA AGRASEN TECHNICAL EDUCATION SOCIETY



Dr. Nand Kishore Garg
Chief Patron

MESSAGE

It is a pleasure to know that the Department of Computer Science and Engineering, Maharaja Agrasen Institute of Technology, Delhi, India is organizing a "Second International Symposium on Securing Next-Generation Systems using Future Artificial Intelligence Technologies", SNSFAIT-2023, on 25th May 2023.

I am sure that the symposium will witness enthusiastic participation from across the globe, resulting in a productive partnership with the Institute to leverage the opportunities. It is sure to be a landmark event. Best wishes for the successful organization of the event.

I also congratulate Prof. Namita Gupta and her organizing team of SNSFAIT, 2023 for bringing out the souvenir on this occasion.

I wish them all the success in life.

03.05.2023

Dr. Nand Kishore Garg

Founder Chairman, MATES & Chancellor, MAU

MATES
उद्यमेन हि सिध्यन्ति कार्याणि न मनोरथै :

MAHARAJA AGRASEN TECHNICAL EDUCATION SOCIETY

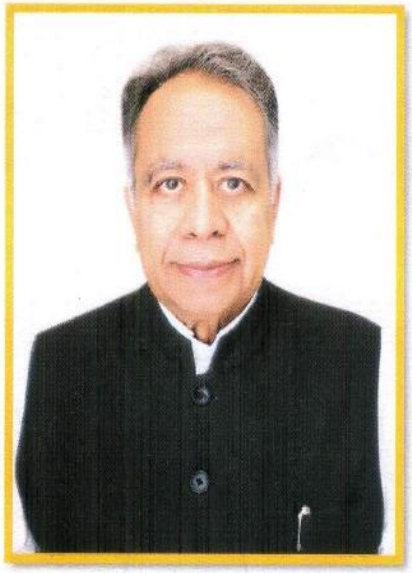
Founder & Chief Advisor
Dr. Nand Kishore Garg
Keshav Kunj,
7/41, West Punjabi Bagh
New Delhi-110026

Chairman
Vineet Kumar Gupta
Lohia Farm 1A OAK Drive
Chhattarpur Farm (DLF)
New Delhi-110074

Executive Chairman
S.P. Aggarwal
A-902, Bestech Park View Spa
Sector 47, Gurgaon-112018

General Secretary
T.R.Garg
BP-7 (West) Shalimar Bagh
Delhi-110088

Treasurer
Anand Gupta
4/5, Jaidev Park,
East Punjabi Bagh,
New Delhi-110026



Shree Vineet Kumar Lohia
Chief Patron

MESSAGE

I am gratified to know that the Department of Computer Science and Engineering, MAIT has taken the initiative to publish the Technical Magazine in the month of July 2022.

This is productive as well as a great platform for students, researchers, faculty members, and industry experts to disseminate achievements in research and developments in computer science and technology.

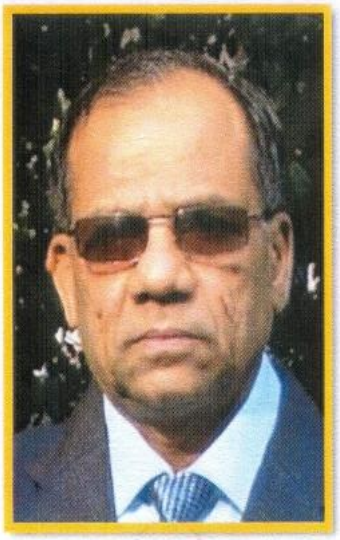
I acknowledge the efforts of Prof. (Dr.) Namita Gupta, HOD (CSE), the faculty members, and the students of the CSE department for their efforts in publishing the Technical Magazine.

I also applaud the coordination and efforts of the Editorial team to bring up the issue.

I wish them all a great success.

Sh. Vineet Kumar Lohia

Chairman, MATES



Prof. M L Goyal
Patron

MESSAGE

It gives me immense pleasure to know that the Department of Computer Science and Engineering, Maharaja Agrasen Institute of Technology, Delhi, India is organizing the "Second International Symposium on Securing Next-Generation Systems using Future Artificial Intelligence Technologies", SNSFAIT-2023, on 25th May 2023.

I give my heart-filled wishes to Prof. (Dr.) Namita Gupta and her team for the symposium. I am assured that we all will witness enthusiastic participation from across the globe. It is sure to be a landmark event. Best wishes for the successful organization of the event.

Prof. (Dr.) M.L. Goyal

Vice Chairman (Academics), MATES

MAHARAJA AGRASEN INSTITUTE OF TECHNOLOGY
MAIT
उद्यमेन हि सिध्यन्ति कार्याणि न मनोरथै :

MAHARAJA AGRASEN INSTITUTE OF TECHNOLOGY

(ISO 9001:2015 Certified)
APPROVED BY AICTE, MINISTRY OF HRD. GOVT OF INDIA
(AFFILIATED TO GURU GOBIND SINGH INDRAPRASTHA UNIVERSITY, DELHI)

Prof. (Dr.) Neelam Sharma
Patron

MESSAGE

Good Wishes to all,

I am extremely happy to know that the Department of Computer Science and Engineering, Maharaja Agrasen Institute of Technology, Delhi, India is organizing a "Second International Symposium on Securing Next-Generation Systems using Future Artificial Intelligence Technologies", SNSFAIT-2023, on 25th May 2023 after the grand success of first.

The Confluence of educationists, researchers, industry experts, students, and technocrats from various institutes and organizations on our campus will definitely create the right kind of vibrations.

I wish to express my sincere appreciation to the authors, presenters, reviewers, and committee members for their hard work, passion, and commitment to organizing an academic event of high quality. I would like to appreciate the quality of work done by the entire team. I congratulate all the authors who submitted papers and all the attendees. I wish the deliberations and the exchange of ideas will motivate all to excel in time to come.

I applaud Prof. (Dr.) Namita Gupta and her organizing team for organizing SNSFAIT- 2023. I wish them success.

Prof. (Dr.) Neelam Sharma
Director, MAIT

MAHARAJA AGRASEN CHOWK, SECTOR-22, ROHINI, DELHI- 110086
PHONES : 8448186931/35 TELEFAX:011-27582095 E-mail: mait@mait.ac.in www.mait.ac.in

MAHARAJA AGRASEN INSTITUTE OF TECHNOLOGY
MAIT
उद्यमेन हि सिध्यन्ति
कार्याणि न मनोरथै :

MAHARAJA AGRASEN INSTITUTE OF TECHNOLOGY

(ISO 9001:2015 Certified)
APPROVED BY AICTE, MINISTRY OF HRD. GOVT OF INDIA
(AFFILIATED TO GURU GOBIND SINGH INDRAPRASTHA UNIVERSITY, DELHI)

Prof. (Dr.) S. S. Deswal
Patron

MESSAGE

It is gratifying to know that the Department of Computer Science and Engineering, Maharaja Agrasen Institute of Technology, Delhi, India is organizing a "Second International Symposium on Securing Next-Generation Systems using Future Artificial Intelligence Technologies", SNSFAIT-2023, on 25th May 2023.

Organizing such an event at this point in time reinforces our objective of developing an environment for the exchange of ideas toward technological development. I wish the Symposium would able to deliberate on current smart cities challenges.

I extend my grateful wishes to Prof. (Dr.) Namita Gupta and her organizing team of SNSFAIT-2023 for making the Symposium a great success.

Prof. (Dr.) S.S. Deswal

Dean, MAIT

MAHARAJA AGRASEN CHOWK, SECTOR-22, ROHINI, DELHI- 110086
PHONES : 8448186931/35 TELEFAX:011-27582095 E-mail: mait@mait.ac.in www.mait.ac.in

MAHARAJA AGRASEN INSTITUTE OF TECHNOLOGY
MAIT
उद्यमेन हि सिध्यन्ति
कार्याणि न मनोरथै :

MAHARAJA AGRASEN INSTITUTE OF TECHNOLOGY

(ISO 9001:2015 Certified)
APPROVED BY AICTE, MINISTRY OF HRD. GOVT OF INDIA
(AFFILIATED TO GURU GOBIND SINGH INDRAPRASTHA UNIVERSITY, DELHI)

Prof. (Dr.) Namita Gupta
General Chair

MESSAGE

The members of the organizing committee and I are very proud to present the "International Symposium" under the theme of " Securing Next-Generation Systems using Future Artificial Intelligence Technologies " and welcome all participants to Maharaja Agrasen Institute of Technology, Delhi on 25th May 2023. The Symposium is organized by the Department of Computer Science and Engineering, MAIT in association with IEEE ComSoc Delhi Chapter.

The Symposium aimed to bring a deeper understanding of the recent advances in computing and communication technology that have enabled the development of networked systems that rely heavily on IoT and Edge technologies. However, the security and privacy of next-generation smart healthcare systems are significant challenges for the efficient adoption of connected healthcare. Future technologies such as Blockchain and Machine Learning (ML) are paving the way for system security solutions that will aid in effective adoption. The goal is to use blockchain technology for communication, data security, and trust management in an intelligent city IoT context.

We are extremely happy to host distinguished personalities from academics and industry as keynote speakers and invited expert talks. These talks along with the presentations of selected papers are expected to be a feast for the academics and research community.

The hard work and dedication of all the members of various organizing committees during the preparation for this Symposium are highly appreciated. Without them, the event would not have been possible. Thanks, and acknowledgment are due to the Management of Maharaja Agrasen Technical Education Society for giving us the opportunity to organize the Symposium. Special thanks to Dr. Nand Kishore Garg Sir, Prof. Neelam Sharma Mam, Prof. S S Deswal Sir, all Hods and CSE Department faculties, staff, and students for their support that makes it a success.

On behalf of the organizing committee, I thank IEEE ComSoc Delhi Chapter for sponsoring the Symposium and being our Financial Partner.

My personal respect goes out to all of you.

Prof. (Dr.) Namita Gupta
HoD, CSE, MAIT

MAHARAJA AGRASEN CHOWK, SECTOR-22, ROHINI, DELHI- 110086
PHONES : 8448186931/35 TELEFAX:011-27582095 E-mail: mait@mait.ac.in www.mait.ac.in

Profiles

Chief Patron(s)

Dr. N.K. Garg, Founder Chairman, Maharaja Agrasen Technical Education Society and Chancellor, Maharaja Agrasen University. Dr. N.K. Garg is a notable social worker and has many noble deeds attached to his name was MLA of Delhi from Trinagar constituency. He is a National Executive of Bhartiya Janta Party. He held prominent positions in renowned organizations.

Shri. Vineet Kumar Gupta, Chairman, Maharaja Agrasen Technical Education Society. He is a renowned businessman and industrialist. Being a businessman par excellence, his faith in engaging with the latest technical know-how from around the world has led to the success of all his industrial setups. Apart from being a renowned businessman and industrialist, philanthropy is very close to his heart, and he has devoted his life in trying to make the lives of the less fortunate better in all possible ways.

Patron(s)

Prof. (Dr.) M.L.Goyal, Vice Chairman Academics, MAIT. Dr. M.L. Goyal was given several appreciation and special contribution awards during his 31 years of service at CMC Limited. He was elected as the President of the Computer Society of India for two terms during 1994-96. He is a Fellow of Computer Society of India, the Institution of Engineers (India) and the Institution of Electronics & Telecommunication Engineers.

Prof. (Dr.) Neelam Sharma, Director, MAIT. Ph. D, M. Tech., B. Tech. She is awarded Ph.D. in Development of Fast VLSI RBSD Pipelined Arithmetic Logic Unit from UPTU Lucknow, 2006. Her Research Specialization is VLSI Technology, Digital Logic Design, Microprocessor & Microcontroller.

Prof. (Dr.) S S Deswal is currently working as Dean (Academic) at Maharaja Agrasen Institute of Technology. He is awarded Ph.D. from NIT, Kurukshetra with the Title, Studies on Ride through Capabilities for Adjustable Speed Drives. He is an active member of the International Association of Engineers, the International Association of Computer Science and Information Technology, Associate Member of the Institution of Engineers and IEEE.

Honorary Chair

Prof. Manu Malek has extensive experience in teaching, practicing, and research in communications and computer networking; and has held various academic positions in USA and overseas, as well as technical management positions at Telcordia Technologies and AT&T/Lucent Bell Labs. He was a Distinguished Member of Technical Staff at Lucent Bell Labs until 2001; then joined Stevens Institute of Technology as an Industry Professor of Computer Science and Telecom Management. He retired from Stevens in 2008. Dr. Malek is the author, co-author, or editor of seven books, and the author or co-author of more than fifty published technical papers in the areas of control systems, communication networks, computer communications, and network management. He is a Life Fellow of the IEEE, was an IEEE Millennium medalist for his contributions.

General Chair(s)

Prof. Namita Gupta is the Head of Computer Science and Engineering Department (an NBA accredited) at Maharaja Agrasen Institute of Technology, GGSIP University, Delhi, India. She has more than 21 years of teaching experience and has played an active role in research and project development. She has coordinated numerous National and International events and hackathons in the campus like Aakash Project, Smart India Hackathon (2017-2020), e-yantra. She is also President of MAIT IIC (Institute Innovation Cell). She has been awarded "Best Performance Award" in 2007 and "Long service Award" in 2017 by MAIT for her remarkable contribution. Her current research includes Data Mining, Databases and Machine Learning.

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

Symposium Organizing Committee Members

Chief Patron(s)

Dr. Nand Kishore Garg
Founder and Chief Advisor, MATES Chairman, Chancellor, MAU, Baddi, HP

Shri Vineet Kumar Lohia
MATES

Executive Committee

Shri. S P Aggarwal [IAS(Retd)]
Executive Chairman, MATES

Er. T.R Garg
(General Secretary-MATES)

Shri. Mohan Kumar Garg
Joint General secretary MATES

Shri. Gyanendra Shrivastava [IAS(Retd)]
Chief executive MATES

Shri. Rajnish Gupta
Secretory MATES

Shri. Anand Gupta
(Treasurer, MATES)

Patron(s)

Prof. (Dr.) M.L. Goyal
Vice Chairman, Academics, MATES

Prof. (Dr.) Neelam Sharma
Director, MAIT, Delhi

Prof. (Dr.) S.S. Deswal
Dean Academics, MAIT

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

Honorary Chair

Prof. Manu Malek,
Nokia Bell Labs, Stevens Institute of Technology,
New Jersey, USA

General Chair(s)

Prof. (Dr.) Namita Gupta
HOD (CSE), MAIT, Delhi

Symposium Chair(s)

Prof. Pravin Chandra,
Dean, USICT, GGSIPU, India

Mr. Prashant Chugh
(C-DOT, Chair,
IEEE ComSoc
Delhi Chapter)

Dr. Deepak Gupta
Assistant Professor (CSE)
MAIT, Delhi

Program Chair(s)

Prof. Amit Prakash Singh
(USICT, GGSIPU, Delhi)

Dr. Ashish Khanna
Associate Professor
(CSE, MAIT)

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

Technical Program Chair(s)

Prof. Oscar Castillo
(Tijuana Institute of Technology, Mexico)

Organizing Chair(s)

Mr. Ashish Sharma
Assistant Professor
(CSE, MAIT)

Mr. Yogesh Sharma
Assistant Professor
(CSE, MAIT)

Convener(s)

Dr. Sandeep Tayal
Assistant Professor
(CSE, MAIT)

Mr. Anupam Kumar
Assistant Professor
(CSE, MAIT)

Dr. Farzil Kidwai
Assistant Professor
(CSE, MAIT)

Co-Convener(s)

Mr. Alok Kumar Sharma
Assistant Professor
(CSE, MAIT)

Mr. Moolchand Sharma
Assistant Professor
(CSE, MAIT)

Ms. Ruchi Goel
Assistant Professor
(CSE, MAIT)

Ms. Savita Sharma
Assistant Professor
(CSE, MAIT)

Finance Chair

Mr. Yogesh Sharma
Assistant Professor
(CSE, MAIT)

Mr. Ajay Tiwari
Assistant Professor
(CSE, MAIT)

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

Publicity Chair

Ms. Zameer Fatima
Assistant Professor
(CSE, MAIT)

Ms. Savita Sharma
Assistant Professor
(CSE, MAIT)

Steering Committee

Prof. Rajveer Mittal
(HoD, EEE Dept., MAIT)

Prof. M L Sharma
(HoD, IT Dept.,MAIT)

Prof. Ved Nath Mathur
(HoD, MAE Dept., MAIT)

Prof. Sunil Kr Mathur
(HoD, ECE Dept., MAIT)

Prof. Chandra Prakash
(HoD, Applied Sciences Dept., MAIT)

Prof. Kusum Sharma
(Applied Sciences, MAIT)

Dr. Vaibhav Jain
(HoD, ME Dept., MAIT)

Dr. Amit Gupta
(HoD, MBA Dept., MAIMS)

Prof. Amita Goel
(HoD ITE Dept, MAIT)

Dr. Neeraj Garg
(HoD, AI & ML Dept, MAIT)

Dr. Pooja Gupta
(HoD CST Dept, MAIT)

Dr. Vinay Kr Saini
(HoD AI & DS Dept, MAIT)

Faculty coordinators

Dr. Sudha Narang
Associate Professor
(CSE, MAIT)

Dr. Ankita Gupta
Assistant Professor
(CSE, MAIT)

Ms. Deepti Gupta
Assistant Professor
(CSE, MAIT)

Mr. Saurabh Rastogi
Assistant Professor
(CSE, MAIT)

Ms. Kavita Saxena
Assistant Professor
(CSE, MAIT)

Ms. Prerna Sharma
Assistant Professor
(CSE, MAIT)

Ms. Shallu Juneja
Assistant Professor
(CSE, MAIT)

Ms. Garima Gupta
Assistant Professor
(CSE, MAIT)

Dr. Jyoti Kaushik
Assistant Professor
(CSE, MAIT)

Ms. Sakshi Jha
Assistant Professor
(CSE, MAIT)

Ms. Neetu Garg
Assistant Professor
(CSE, MAIT)

Ms. Karuna Middha
Assistant Professor
(CSE, MAIT)

Ms. Kajol Dahiya
Assistant Professor
(CSE, MAIT)

Ms. Mini Agarwal
Assistant Professor
(CSE, MAIT)

Dr. R.K. Choudhury
Associate Professor
(CSE, MAIT)

Ms. Divya Arora
Assistant Professor
(CSE, MAIT)

International Symposium on Securing Next-Generation Systems using Future Artificial Intelligence Technologies SNSFAIT – 2023

Organised by
Department of Computer Science & Engineering,
Maharaja Agrasen Institute of Technology, Delhi, India
in collaboration with
IEEE Communication Society Delhi Chapter
(25th May, 2023)

Symposium Schedule

Time	Program
10:30 am	**Registration & Networking High Tea** *Audi Lounge*
11:00 am	**Inauguration** **11:00am - 11:05am: Introduction of SNSFAIT - 2023** **11:05am - 11:10am: Prof. Namita Gupta, General Chair, SNSFAIT – 2023** **11:10am - 11:15am: Dr. Ashish Khanna, Program Chair, SNSFAIT – 2023; Secretary cum Treasurer, IEEE ComSoc Delhi Chapter** **11:15am - 11:20am: Prof. Neelam Sharma, Director MAIT, Patron, SNSFAIT - 2023** **11:20am - 11:30am: Dr. Nand Kishore Garg, Chief Advisor, MATES** *Venue: Mini Audi, MAIT Campus*
11:30 am	**Keynote address by Prof. Vivek Bohara, Head, Department of Electronics and Communication Engineering, IIIT-Delhi, Chair, IEEE ComSoc Delhi Chapter** *Venue: Mini Audi, MAIT Campus*
12:30 pm	**Vote of Thanks by Prof. S.S. Deswal, Dean (Academics), Patron, SNSFAIT - 2023** *Venue: Mini Audi, MAIT Campus*
12:40 pm	**Networking Lunch** *Venue: Basement, Block – 1*
1:30 pm	**Session – 01: Securing Next-Generation Systems using Future AI Technologies** **Session Chair(s):** **Dr. Vishal Gupta, Associate Professor, NSUT (East Campus)** **Dr. Pooja Gupta, Head (CST Department), MAIT-Delhi** **Dr. Ashish Khanna, CSE Department, MAIT-Delhi** *Venue: Lab No-114, Block-1*
3:30 pm	**Networking Tea** *Venue: Lab No-114, Block-1*
4:00 pm	**Valedictory Session** **Certificate Distribution** **Vote of Thanks by Dr. Deepak Gupta, Symposium Chair, SNSFAIT – 2023** *Venue: Lab No-114, Block-1*

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

Accepted Papers

2nd International Symposium
on
Securing Next-Generation Systems
using
Future Artificial Intelligence Technologies
SNSFAIT – 2023
25th May 2023
Organized By
Department of Computer Science & Engineering,
Maharaja Agrasen Institute of Technology, Delhi, India
in collaboration with
IEEE ComSoc Delhi Chapter

5G based Full-duplex Hybrid OCDMA-VLC system for secure IoT applications.

Meet Kumari

Chandigarh University, Mohali, Punjab, India

Abstract

In this work, a full-duplex hybrid visible light communication (VLC) and optical code division multiple access (OCDMA) for varied transmission range and data rate for different codes and light emitting diodes (LEDs) is analyzed respectively. The simulation results show that out of all codes random diagonal (RD) code offers high VLC transmission range of 70m in uplink and 55m in downlink at 10Gbps information rate than multi-diagonal as well as zero cross correlation codes. Also, high data rate of 90Gbps in uplink and 75Gbps in downlink can be obtained by employing red LED and RD code in the designed system over 10m VLC range. In addition, the comparison of the proposed work with other previous is presented to show its superiority.

Keywords [1]

Optical code division multiple access (OCDMA), internet of things (IoT), visible light communication (VLC), fifth generation (5G)

Introduction

The requirement for data intake of a mobile user improves continually. However in 2016, the information traffic was 7EB/month, the estimated information traffic for 21st centaury till now is supposed to be approximately 50EB. To manage such huge amount of data, latest and more effective techniques for data transmission must be evolved. The solution is to enhance a efficiency of spectral in recently downtrodden radio frequency bands. While even radio band is not suitable to cope with a spectrum crunch phenomenon. For this, visible light communication (VLC) permits an extended unlicensed spectrum bands which provides a high-speed transmission of data [1]. Also, VLC technology combines and complements with 5G and beyond this to meet the recent and next-generation high transmission rate as well as capacity utilization. Short distance communication within a campus, video monitoring and surveillance, disaster recovery, back-haul system etc. is some of the potential applications of VLC technology [2].

Proceedings of International Symposium on Securing Next-Generation Systems using Future Artificial Intelligence Technologies (SNSFAIT 2023), May XX-XX, 2023, Delhi, India
EMAIL: meetkumari08@yahoo.in(M. Kumari)
ORCID: 0000-0001-9975-1557

VLC has been regarded as a substitute to communicate huge sensing data generated by widespread internet of things (IoT) sensor nodes. These IoT smart sensors have capability to respond in the real world events in an rapid, automatic as well as enlightened way not only reveals new possibilities for handling critical or complex situations, but too allows a broad range of technologies operation to be optimized [3]. Various research work papers [4–6] focused on a VLC scenario.

Further, optical code division multiple access (OCDMA) is emerging as a promising solution that can offer quality of service in physical layer. OCDMA schemes are getting considerable attention due to its ability to behave asynchronously, improved capacity as well as privacy. Several OCDMA codes have been used to handle multimedia applications like random diagonal (RD) , zero cross correlation (ZCC), multi-diagonal (MD) etc. to cope with permitting large number of consumers to broadcasting high transmission rates adapted to various multimedia transmission [7]. Table 1 indicates the existing methodologies used in the previous work along with their pros as well as cons.

Table 1
Existing methodologies

Ref.	Year	System	Pros	Cons
[8]	2016	WDM-VLC	4.5m+20km	10Gbps
[9]	2020	WDM-VLC	2.3Tbps	1.5m
[5]	2021	wired/VLC	Range=10m+50km	Data rate=10/10Gbps
[10]	2022	wavelength division multiplexing (WDM)/VLC	50Gbps	12m

Previous recent work presents that, till now researchers have more focus on VLC system, but there is less work except [5], has been done on hybrid VLC-OCDMA system for IoT applications.

Thus in this paper a full-duplex hybrid VLC-OCDMA system using different OCDMA code on the basics of 5G for IoT applications has been reported. The novelty behind this work is to secure the IoT based VLC-OCDMA system using different OCDMA codes. It also enhances the transmission distance as well as data rate for various future based applications.

Main contributions of the proposed work:

- Design a full-duplex hybrid VLC-OCDMA system.
- Compare the designed system for different OCDMA codes like multi diagonal (MD), random diagonal (RD) and zero cross correlation (ZCC) codes.
- Identify the system performance for varied VLC link as well as transmission rate.

The work is organized as: Section 2 presents the proposed design of hybrid VLC-OCDMA system. Section 3 depicts the results and discussion. Lastly, conclusion is dawn in Section 4.

System design

The proposed hybrid VLC-OCDMA system is presented in Figure 1.

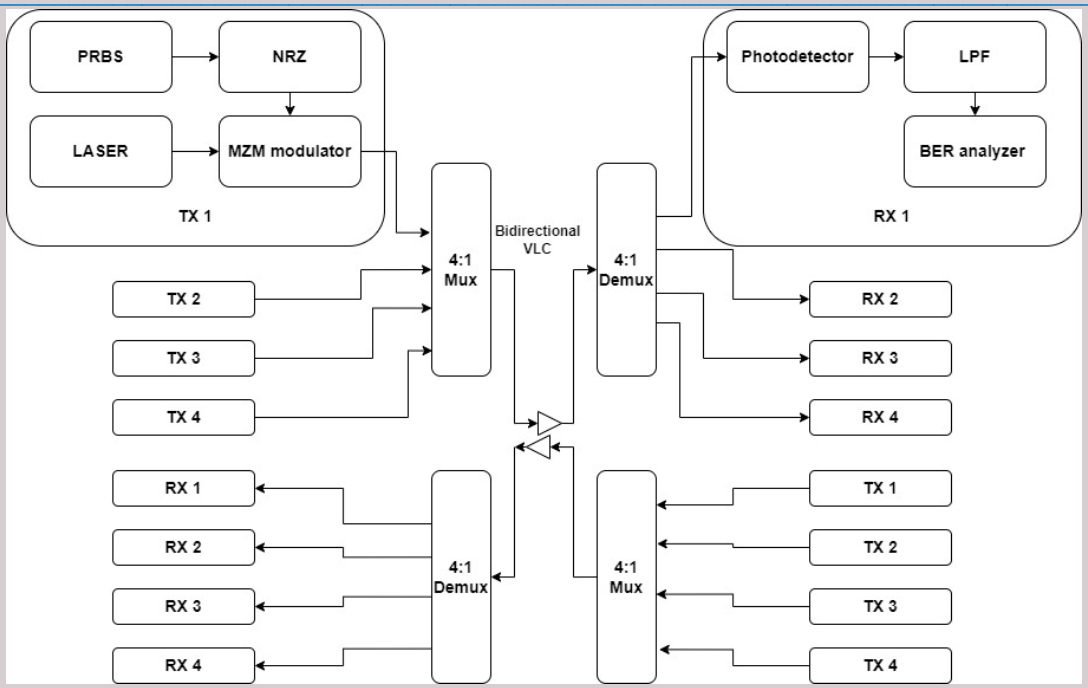


Figure 1: Block diagram of full-duplex hybrid VLC-OCDMA system

The proposed block diagram presents the full-duplex hybrid VLC-OCDMA system using RD, MD and ZCC codes for four users. It includes four downstream (DN) coded transmitters (TXs) and upstream (UP) coded TXs. For downlink transmission, each TX section consists of a series of pseudo random bit sequence generator with non return to zero data format to be modulated with incoming laser input signals via mach zehnder modulator. The code construction for three users RD, MD and ZCC code using three LEDs (red=640nm, white=625nm+514nm+450nm and violet=400nm) is reported below in Table 2.

Table 2
Code designs

Code	RD			MD			ZCC		
LED	U1	U2	U3	U1	U2	U3	U1	U2	U3
Red	0	0	1	1	0	0	1	0	0
White	0	1	0	0	1	0	0	1	0
Violet	1	0	0	0	0	1	1	0	0
Red	1	0	0	0	0	1	0	0	1
White	0	1	0	0	1	0	0	1	0
Violet	0	0	1	1	0	0	0	0	1

A 4:1 multiplexer is implemented at to multiplex the input wavelengths over bidirectional VLC channels. Likewise, a 1:4 de-multiplex is used at receiver to distribute the incoming wavelengths to different receivers. Each receiver consists of a photo detector for converting the optical energy to electrical. Low pass filter and BER analyzer are used to reduce the unwanted noise and to test the system performance respectively. The operation is performed for uplink transmission in the system.

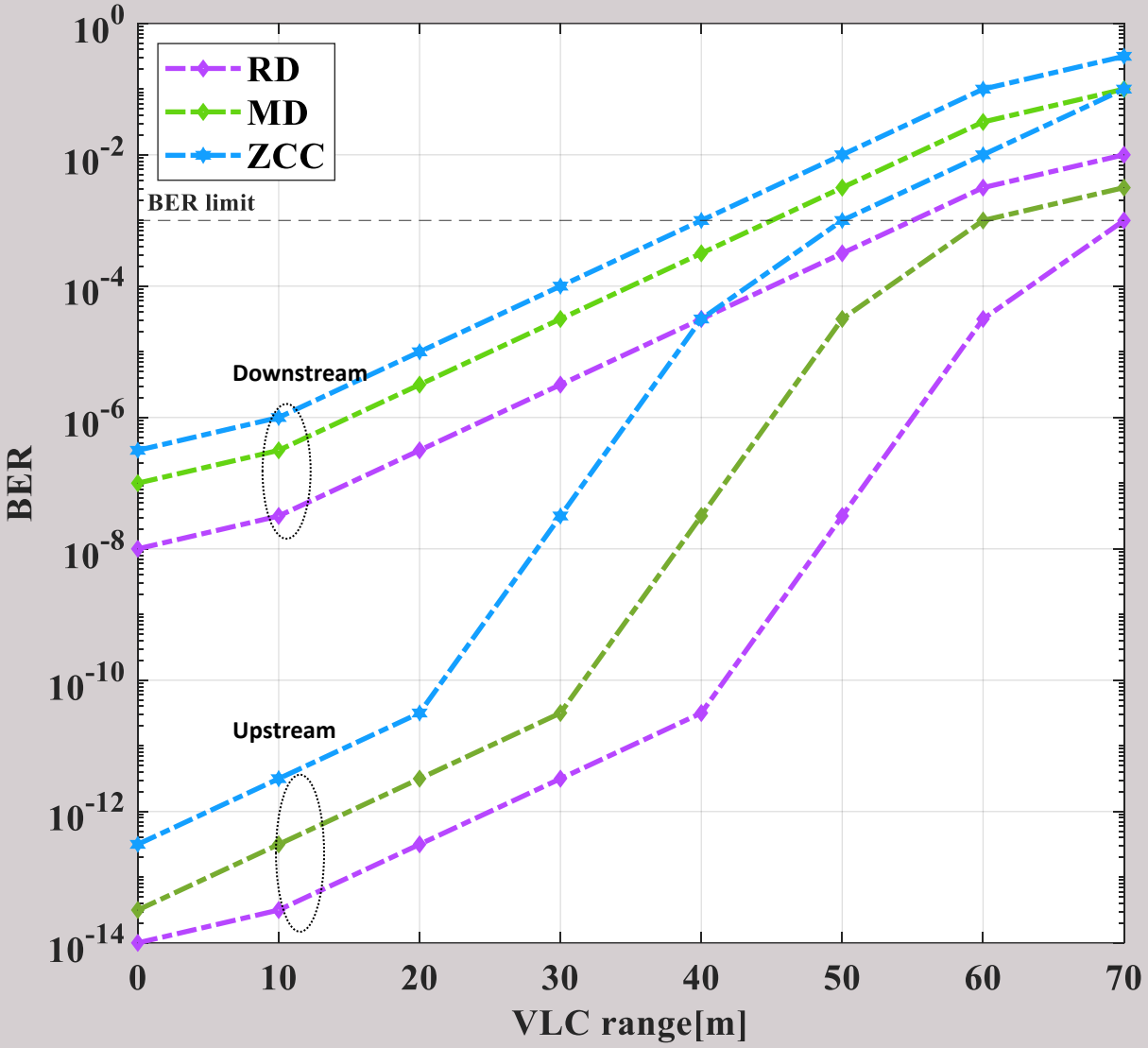
The parameters used in the proposed system are tabulated in Table 3.

Table 3
Parameters Used in OptiSystem simulation software

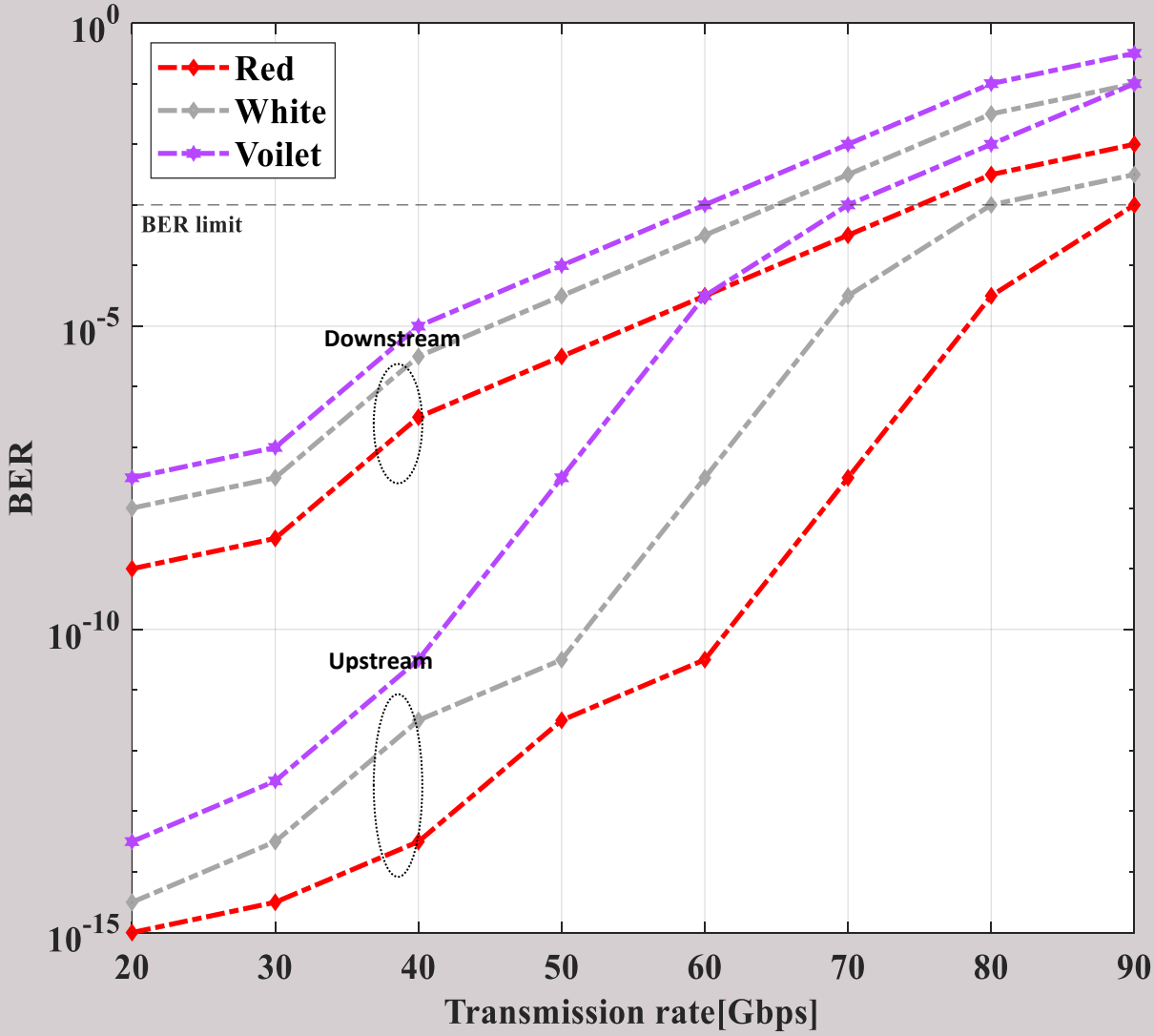
S. No.	Parameter	Value
1	Input power	10dBm
2	Transmission rate	20-90Gbps
3	Range	10-70m
4	Dark current	9nA
5	Responsitivity	1A/W
6	Thermal noise	10-22 W/Hz

Results and analysis

The proposed hybrid VLC-OCDMA system performance is measured under the influence of external interferences and noise in OptiSystem.


RD
MD
ZCC
BER limit
Downstream
Upstream
BER
VLC range[m]
10^{0}
10^{-2}
10^{-4}
10^{-6}
10^{-8}
10^{-10}
10^{-12}
10^{-14}
0
10
20
30
40
50
60
70

(a)



(b)

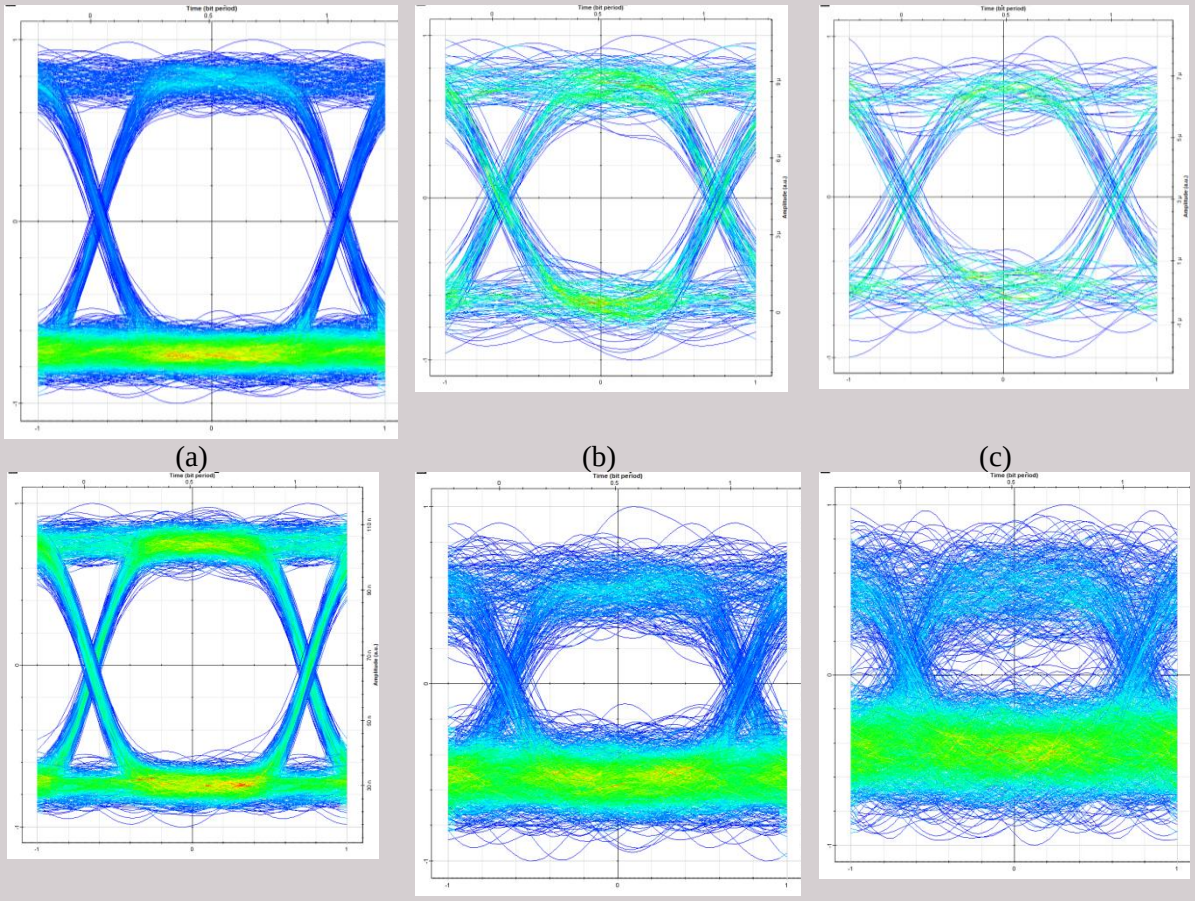
Figure 2: BER performance of proposed system for varied (a) VLC range employing different codes and (b) transmission rate for different LEDs using RD code

Figure 2(a) presents the BER performance of full-duplex VLC-OCDMA system employing RD, MD and ZCC codes for varied VLC range in both DN and UP transmission at 10/10Gbps data rate. It is seen that with increase transmission range, the performance of system degrades for various codes in both DN and UP directions. Also, RD code performs best compared to other codes in UP transmission as compared to DN transmission. The maximum achieved VLC range for RD, MD and ZCC code is 70, 60 and 50m in UP transmission, at 10^{-3} BER threshold. Also, the faithful VLC range for RD, MD and ZCC code is 55, 45 and 40m in DN transmission.

Figure 2(b) depicts the BER performance of full-duplex VLC-OCDMA system employing RD code for varied data rate in both DN and UP transmission over 10m range for different LEDs. It is noted that with increase transmission rate, the performance of system diminishes for various LEDs in both DN

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

and UP directions. Also, out of all codes, red LED shows best performance than white and violet LEDs in UP transmission as compared to DN. The highest obtained transmission rate for red, white and violet LED is 90, 80 and 70Gbps respectively, at BER threshold in UP transmission. Moreover, in DN transmission, the maximum transmission rate for red, white and violet LED is 75, 65 and 60Gbps respectively.

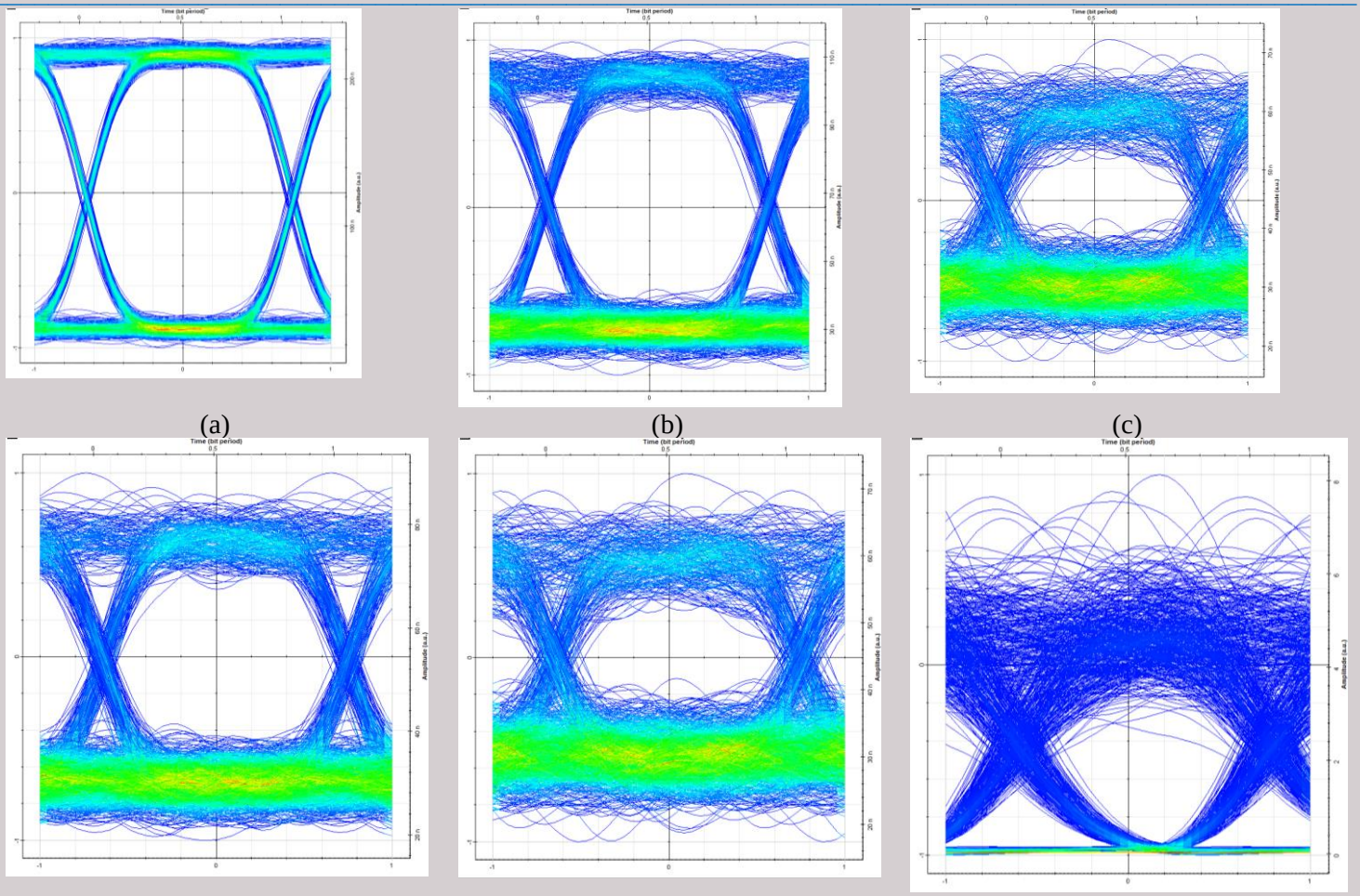


(a) (b) (c)

(d) (e) (f)

Figure 3: Eye patterns of the hybrid VLC-OCDMA system using RD code over (a)70m, (b)60m and (c)50m VLC range for UP; (d)70m, (e)60m and (f)50m VLC range for DN transmission

Figure 3(a)-3(f) illustrate that the eye patterns of the proposed system for different VLC range at 10Gbps data rate for UP and DN transmission. It is analysed that with increase in transmission range, eye patterns get disturbed causing decrease in system performance. Also UP transmission provides finer performance than DN.

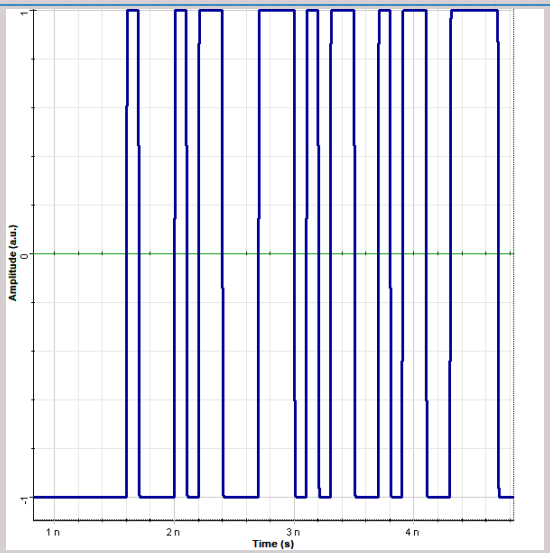


(a) (b) (c)

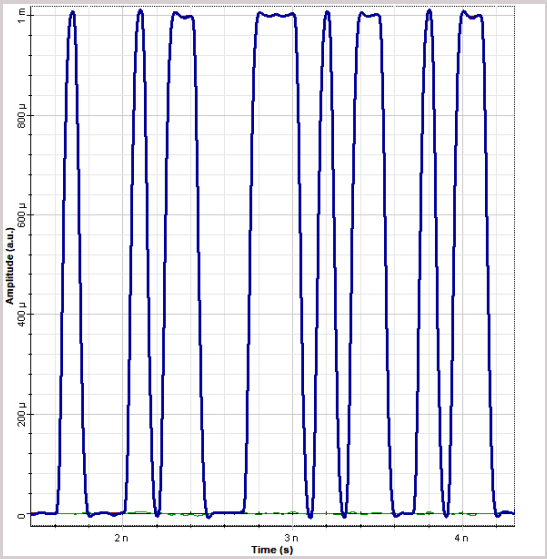
(d) (e) (f)

Figure 4: Eye patterns of the hybrid VLC-OCDMA system using RD code over (a)20Gbps, (b)60Gbps and (c)90Gbps VLC range for UP; (d)20Gbps, (e)60Gbps and (f)90Gbps VLC range for DN transmission

Figure 4(a)-4(f) illustrate that the eye patterns of the proposed system for different VLC traffic rate over 10m range for UP and DN transmission. It is observed that with increase in traffic rate, eye patterns get disturbed causing decrease in system performance. Also UP transmission provides finer performance than DN.



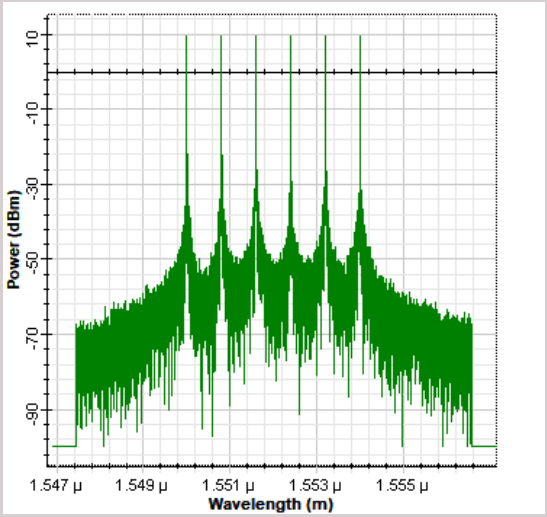
(a)



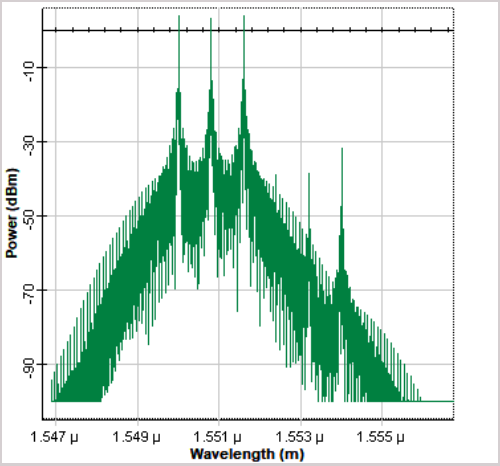
(b)

Figure 5: Measured spectra of the hybrid VLC-OCDMA system using RD code at (a) Tx and (b)Rx over 10m range at 10Gbps rate

Figure 5(a) as well as 5(b) report that the measured spectra of the proposed system at transmitter as well as receiver side.



(a)



(b)

Figure 6: Measured spectra of the hybrid VLC-OCDMA system using RD code at (a) Tx and (b) Rx over 10m range at 10Gbps rate.

Figure 6(a) as well as 6(b) report that the measured spectra of the proposed system at transmitter as well as receiver side. Table 4 presents the comparative system performance with other existing systems.

Table 3
Comparative system performance

Ref.	Max. VLC range (m)	Max. data rate (Gbps)
[12]	2	10
[13]	1.5	2.3
[14]	1.2	1.45
[15]	0.3	1.35
[16]	3	12.6
[17]	10	2.5
Proposed work	70	90

Tables 4 reports that for the proposed work faithful VLC range is 70m at symmetric 90Gbps data rate which is maximum than other existing works. However, this work has some limitations like external noise, large codes length, limited range and design complexity. In future more work need to be done on VLC-OCDMA system using LASER and optimum code to support the large no. of customers.

Conclusion

A full-duplex hybrid VLC-OCDMA using three different codes and three LEDs is presented. It is concluded that RD code presents finest performance with VLC range of 70m in uplink and 55m uplink direction than MD as well as ZCC code at BER threshold at 10Gbps. Also, the transmission rate can be extended upto 90Gbps and 75Gbps in uplink and downlink directions respectively, using RD code for red LED. Besides this, the proposed work shows better work than other previous works.

References

[1] Z. Becvar, R.G. Cheng, M. Charvat, P. Mach, Mobility management for D2D communication combining radio frequency and visible light communications bands, Wirel. Networks. 26 (2020) 5473–5484. https://doi.org/10.1007/s11276-020-02408-x.

[2] Anuranjana, S. Kaur, R. Goyal, S. Chaudhary, 1000 Gbps MDM-WDM FSO link employing DP-QPSK modulation scheme under the effect of fog, Optik (Stuttg). 257 (2022) 168809. https://doi.org/10.1016/j.ijleo.2022.168809.

[3] S.H. Chang, A Visible Light Communication Link Protection Mechanism for Smart Factory, in: Proc. - IEEE 29th Int. Conf. Adv. Inf. Netw. Appl. Work. WAINA 2015, 2015: pp. 733–737. https://doi.org/10.1109/WAINA.2015.41.

[4] M. Kumari, A. Sheetal, R. Sharma, Performance Analysis of a Full-Duplex TWDM-PON Using OFDM Modulation with Red LED Visible Light Communication System, Wirel. Pers. Commun. 119 (2021) 2539–2559. https://doi.org/10.1007/s11277-021-08343-0.

[5] M. Kumari, R. Sharma, A. Sheetal, A hybrid next-generation passive optical network and visible light communication for future hospital applications, Optik (Stuttg). 242 (2021) 166978. https://doi.org/10.1016/j.ijleo.2021.166978.

[6] M. Kumari, A. Sheetal, R. Sharma, Performance analysis of symmetrical and bidirectional 40 Gbps TWDM-PON employing m-QAM-OFDM modulation with multi-color LDs based VLC system, Opt. Quantum Electron. 53 (2021) 1–29. https://doi.org/10.1007/s11082-021-03108-2.

[7] M.H. Kakaee, S.I. Essa, T.H. Abd, S. Seyedzadeh, Dynamic quality of service differentiation using fi xed code weight in optical CDMA networks, Opt. Commun. 355 (2015) 342–351. https://doi.org/10.1016/j.optcom.2015.03.046.

[8] J. He, H. Dong, R. Deng, J. Shi, L. Chen, WDM-CAP-PON integration with VLLC system based on optical frequency comb, Opt. Commun. 374 (2016) 127–132. https://doi.org/10.1016/j.optcom.2016.04.059.

[9] L.Y. Wei, S.I. Chen, C.H. Yeh, Y. Liu, G.H. Chen, C.W. Peng, W.H. Gunawan, Y.H. Chang, P.C. Guo, C.W. Chow, 2.333-Tbit/s bi-directional optical mobile networks using optical wireless communication (OWC), Opt. Commun. 475 (2020) 126187. https://doi.org/10.1016/j.optcom.2020.126187.

[10] H.H. Lu, X.H. Huang, Y.T. Chen, P.S. Chang, Y.Y. Lin, T. Ko, C.X. Liu, WDM-VLLC and

White-Lighting Ring Networks with Optical Add-Drop Multiplexing Scheme, J. Light. Technol. 40 (2022) 4196–4205. https://doi.org/10.1109/JLT.2022.3162205.

[11] M. Kumari, R. Sharma, A. Sheetal, A hybrid next-generation passive optical network and visible light communication for future hospital applications, Optik (Stuttg). 242 (2021). https://doi.org/10.1016/j.ijleo.2021.166978.

[12] S. Selvendran, A. Sivanantha Raja, K. Esakki Muthu, A. Lakshmi, Certain Investigation on Visible Light Communication with OFDM Modulated White LED Using Optisystem Simulation, Wirel. Pers. Commun. 109 (2019) 1377–1394. https://doi.org/10.1007/s11277-019-06617-2.

[13] L.Y. Wei, S.I. Chen, C.H. Yeh, Y. Liu, G.H. Chen, C.W. Peng, W.H. Gunawan, Y.H. Chang, P.C. Guo, C.W. Chow, 2.333-Tbit/s bi-directional optical mobile networks using optical wireless communication (OWC), Opt. Commun. 475 (2020) 126187. https://doi.org/10.1016/j.optcom.2020.126187.

[14] J. Li, P. Zou, X. Ji, X. Guo, N. Chi, High-speed visible light communication utilizing monolithic integrated PIN array receiver, Opt. Commun. 494 (2021) 127027. https://doi.org/10.1016/j.optcom.2021.127027.

[15] Y. Wang, L. Tao, Y. Wang, N. Chi, High speed WDM VLC system based on multi-band CAP64 with weighted pre-equalization and modified CMMA based post-equalization, IEEE Commun. Lett. 18 (2014) 1719–1722. https://doi.org/10.1109/LCOMM.2014.2349990.

[16] P. Pesek, S. Zvanovec, P. Chvojka, Z. Ghassemlooy, P.A. Haigh, Demonstration of a hybrid FSO/VLC link for the last mile and last meter networks, IEEE Photonics J. 11 (2019) 1–7. https://doi.org/10.1109/JPHOT.2018.2886645.

[17] G.C. Mandal, R. Mukherjee, B. Das, A.S. Patra, A full-duplex WDM hybrid fiber-wired/fiber-wireless/fiber-VLC/fiber-IVLC transmission system based on a self-injection locked quantum dash laser and a RSOA, Opt. Commun. 427 (2018) 202–208. https://doi.org/10.1016/j.optcom.2018.06.048.

2nd International Symposium
on
Securing Next-Generation Systems
using
Future Artificial Intelligence Technologies
SNSFAIT – 2023
25th May 2023
Organized By
Department of Computer Science & Engineering,
Maharaja Agrasen Institute of Technology, Delhi, India
in collaboration with
IEEE ComSoc Delhi Chapter

A Biometric-Based Encryption Method for Secure Data Sharing in Cloud Environment

Gauraangi Praakash1, Pooja Khanna1, Sachin Kumar1, Pragya2

[1]*Amity University Uttar Pradesh, Lucknow Campus,*

[2]*MVD College, University of Lucknow, Lucknow.*

Abstract

When seen from the point of view of information collecting, distributed storage can very easily be converted into a decision-making approach. In a short amount of time, data storage evolves into a technique of preference. Since data is protected remotely rather than locally, consumers from both the home and the technical sphere are inclined to do so. If the dispersed storage is not completely confident, it means that users have "the possibility to incorporate knowledge about the online cloud." Regardless of whether customers find cloud-based information to be a major cause for concern, the fact remains that it can be a difficult problem, especially because we trade data on cloud servers. To address this issue in a competent and effective manner, the Revocable IBE conspires, and the primary refreshing technique are both already available. In addition, cloud architecture experience needs to be improved to enable the utilization of contemporary safe information structures in distributed computing. In this sense, a figure (or any encoded document) can contain a temporary amount of time. If the characteristics of the figurative content fit the configuration of the key, and if all possible occurrences are permitted to take place, then the figurative content must be decrypted. After a client has specified an end time, the information is permanently removed from the cloud server in a secure manner. The framework proposed is equipped with features such as unfailing viability for both PKG measures and client shared secret key size because of the utilization of the key updating service that is made available by the cloud server, further the time comparison establishes that proposed technique with GSP is more efficient as compared to without GSP. Results show that the proposed system with GSP reduces processing time by approximately 0.001 times.

Keywords [2]

Cloud Computing, Privacy Preservation, Bio-metric, Identity Based Encryption (IBE), Self-Destruction, Revocation.

Introduction

The most generally acknowledged example of distributed computing is the use of specialized properties or hardware that reside on re-bit computers as administration and is transferred on to the end user, with the internet being the most accepted example. Fame and significance are easily acquired by distributed

International Symposium on Securing Next-Generation Systems using Future Artificial Intelligence Technologies (SNSFAIT 2023), May XX-XX, 2023, Delhi, India
EMAIL: gauraangi.praakash@s.amity.edu(G. Praakash); pkhanna@lko.amity.edu(P.Khanna); skumar3@lko.amity.edu(S.Kumar), dr.pragya2011@gmail.com(Pragya)
ORCID: 0009-0008-3814-6247 (G. Praakash); 0000-0002-0043-1068 (P.Khanna); 0000-0003-2196-4573 (S.Kumar) ;0000-0002-5569-0307 (Pragya)

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

storage. To safely exchange information, the identity-based encoding strategy or the use of identity mixes is used [2]. A remarkable cornerstone of cryptography is Identity Based Encryption. It's a kind of transparent key encryption where customers are a key to the personality of a customer (e.g., the email address of a customer) because there are certain special specifics about it. To enter the general population criteria of this scheme, a sender must be able to encrypt a message using the contents measurement of the recipient's email address. The beneficiary collects her scrambling key from a specialist who can be trusted because he manufactures mystery keys for every client. It offers every conference an opportunity to enjoy the perceived character and an open key. The Private Key Generator is a trusting outsider's private key [13-15] The PKG key not only maintains the proportional ace private key but also disseminates an ace open key for the programmed to run. Every participant will be able to calculate an open key that is somewhat near to the personality ID if they enter the ace open key alongside the character respect given by the ace open key. The PKG, which utilizes the ace encryption key to render the private key for character ID, relates to the meeting that approved using the character ID to receive a coordinating private key. This allows the PKG to render the private key for personality ID. For security purposes, whether a client exits the meeting or acts poorly, he or she must be expelled from the gathering. This disavowed customer should then never have the right to get to and alter exchanged information again. A. Boldyreva, et al. [3] a revocable Identity Based Encryption scheme has been proposed, but it has the drawback of requiring calculation at a single level, i.e., an administrator or important individual from the organization. An estimation of outsourcing into IBE renunciation has been offered as a means of addressing this problem. Framework suggests a way for dumping all key era- related forms that must be completed between the key-issuing and key-refreshing processes. This would leave PKG and eligible clients with only a few straightforward activities to carry out locally. Another technique for the issuance of safe keys is suggested, and this one uses a half-breed private key for each customer. In addition, an AND gate is incorporated into the process of determining the key's age, and this gate is directed especially to the personality component and the time segment.

Similarly, in distributed computing, a stable information self-destructing system is proposed to increase distributed storage space. Each ciphertext in this structure is named with a time between value, so the private key is associated with a duration moment. The moment and the ciphertext will follow the key will be extracted if both the time characters and its related characters are present in the dictionary. In general, the owner has the authority to determine whether specific confidential data is valid for a given duration, i.e., whether it self-destructs at the end of a time span specified by the owner, or whether it cannot be released before a specific deadline.

RELATED WORK

The creator proposes a fully realistic encryption plot based on personalities in this paper [4] (IBE). In the arbitrary prophet display, the structure has chosen ciphertext defense, anticipating the Diffie-Hellman problem in a different computational form. The framework concentrates on logarithmic mapping linking the groups. Weil's fusion with elliptical curves is a consequence of this kind of principle. An alternative Concept of an open key encryption is introduced by the author in study presented in [3] called as Identity based encryption. It is more efficient and popular as it does not require the standard public key infrastructure for key management. Any environment, whether based on PKI or personality, must provide a way for customers to leave the system. Capable disavowal is a frequently discussed topic in the standard PKI environment.

On the other hand, there hasn't been much work done in the IBE environment to concentrate on the components of denial. When scrambling, the arrangement that is the most grounded demands that senders continue to employ eras and that collectors routinely update respective encryption information by meeting with a reliable specialist. In any event, this setup does not scale very well; when the number

of users increases, the function upon that main page becomes a bottleneck, and the configuration does not scale very well. We propose a conspiracy including the IBE that would considerably increase the suitability of key-refresh in favor of the stock that is placed in collection while continuing to retain the capability of supplying the customers.

Our structure has been shown to be secure, and it is derived from the ideas behind the information structure of the primitive and double trees used in the fuzzy IBE. The author of [5] focused on a variant of Identity-Based Encryption (IBE) that is referred to as Fuzzy Based Identity Encryption. Within the framework of Fuzzy IBE, a lifestyle is characterized by a collection of illustrative characteristics. A private key is used in a Fuzzy IBE arrangement to transcribe a figure material along with an identification for an identity, Providing, and only providing, that the characters are! In addition, according to the results of the partition measure known as "set cover," 0 and 0 are the same.

What precisely considers air conditioning number is a characteristic of a Fuzzy IBE plan referred to as its screw- up resistance. The usage of biometric identities, which will be permanently disrupted each time they are evaluated; the "mess up resistance property" of the Fuzzy IBE plan is simply what considers the air conditioning number as a factor. the utilization of biometric identities, which will invariably result in the production of some sort of disturbance each time that they are evaluated; the defect tolerance characteristic of a fuzzy IBE plan is precisely what takes into consideration air conditioning number [17-21]. The utilization of several types of biometric IDs as required in addition, we show how the Fuzzy-IBE algorithm can be used for "quality-based encryption," which is a concept that we define.

The creator tackles the dilemma of using untrusted (conceivably harmful) cryptographic accomplices in this paper [6]. Here, to ensure the privacy of the data outsourced over cloud, a structured mechanism has been proposed. In this model, the organized state of the will shapes the item for the accomplice, but as the contraption begins to depend on it, there is no synchronization correspondence with it. Not only does it offer a process for calculating adequacy and testing the potential of an outsourcing use, but it also provides a mechanism for measuring the adequacy. It also involves two simple stable outsourcing deals. It demonstrates how to outsource computed exponentiation, which is the technological limitation in most open encryption algorithms on computationally limited computers, in a secure manner. A computer will require O (n) special increases if it is to complete exponentiation frame bit types if it does not make use of outsourcing. Any exponentiation-based scheme in which the authentic contraption can employ two untrusted exponentiation programs as measurements, and with which use the Cramer-Shoup cryptographic algorithm and Schnor checks causes the pile to decrease to O (log2 n). Using an untrusted Cramer-Shoup encryption program, we achieve a comparable weight reduction for a simple going considered security for another CCA2-secure encryption arrangement.

As shown by the author in this paper [7], attribute-based encryption (ABE) is a promising cryptographic standard instrument for fine-grained access control. However, in current ABE schemes, the computational approach to online encryption often results in a one-sided life of access course of action, which translates into an obstacle to its use. In this article, a novel approach for outsourcing ABE encryption to a cloud organization provider is proposed to reduce the awkwardness of group computation. It makes use of an improved Map. Reduce cloud advancement by ensuring that at least one of the slave center points is visible from the master center point and, moreover. After outsourcing, the customer will experience an accurate numerical loss that is decreased from the initial loss of four exponentiations during the encryption process to a hazy four exponentiations. Another potential drawback of the change that is being suggested is that the customer may opt to encrypt each action.

The migration of data from a company's local servers to those hosted in the cloud can be accomplished with the help of cloud-based data clients. The result of this is that the consumer is relieved of the cost

of maintenance while also receiving data storage facilities of a high grade. The use of cloud storage creates a lot of privacy and safety concerns. Both the companies that supply cloud services and the servers that store data have some shortcomings. Concerns have been raised by the customer over the integrity of the data that has been uploaded to cloud storage. In this piece, the public key hash algorithm is utilized. In addition, for data dynamics, this makes it easier to do dynamic operations such as inserting new data, updating existing data, removing old data, and altering blocks.

The Merkle Hash Tree [8] is a tool that is utilized to help in the process of finding the position of each complex operation. A third-party examiner validates the accuracy of the user's data and attests to the reliability of the information that is kept on the cloud server. There is a significant reduction in the amount of computational and communication overhead. The defragmentation method is utilized to ascertain whether the file in question already resides on the cloud server before the user uploads it to the cloud storage location of their choice. This solution is robust and secure, even when faced with malicious server-launched replace attacks.

According to the author of this paper [9], ABE is an insight into future architecture that has mostly been associated with application fine-grained access control systems. However, as the numerical expense rises due to the multifaceted nature of the get-to recipe, ABE's high scheme over-head is being scrutinized. Since they have forced the figuring of assets, this problem has proven to be more genuine for portable de- indecencies. It demonstrates a general and capable approach for integrating a quality-based access management framework into ABE by introducing secure outsourcing strategies to achieve the aforementioned goal. More specifically, two cloud specialist co-ops (CSPs) have been created, namely the key age cloud specialist co-op (KG-CSP) and the decryption cloud specialist co-op (D-CSP), to handle outsourced key- issuing and unscrambling independently for the benefit of trait specialists and consumers.

In author in study [10], presented the automated formulation of cryptographic system for forward security. Mystery keys are refreshed on a regular basis; contact with a mystery key coordinating to a specific day and age does not allow a challenger in a forward-secure schedule to "kill" some previous period's strategy. Forward-secure advanced label plans, key-trade conventions, and symmetric-key plans have all seen developments. Under the definitive bilinear assumption of Diffie-Hellman, the primary building achieves security close to chosen plaintext attacks in the standard model. This structure is intuitive, and as the total number of eras grows, all parameters evolve in a logarithmic fashion.

IMPLEMENTATION DETAILS

With recent development in storage and technical advancements, cloud computing has stepped in as universal solution with features like colossal size data storage, bulky calculation, low-value benefit, and adaptable approach to get to the data. Concept is based on ide of virtualization. Virtualization is targeted to incorporate set of virtual assets or devices like storage gadget, server, organize or working system where the structure partitions the space into sectors to match the exact number of execution conditions that are required. Cloud computing is a powerful technique to for management of storage issues and insides of its administration, model suggested provides the data owner the capability to outsource and keep files saved at cloud platform. Number of organizations and subscribers have started employing cloud storage as reliable and easy to access source for facilitating data administration, processing, and storage, though concerns of security and privacy do exist. One of the primary concerns is whether the data stored in reliable manner and will not go missing in cloud facility.

Issues related whether organizations managing cloud facility meets data safety requirement of the client is a major concern. Concerns altogether make it vital and important to increase the confidence of data owners on cloud facility. Diversified models exist for securing and processing of data for public domain model and private domain model. Generally, with Private domain model, the owner of the data can establish the fidelity of the outsourced data that is being managed and stored at the cloud facility.

In this technique, the owner of the outsourced data is supposed to have expertise. One more major concern happens to be integrity and authenticity of the security mechanism taking care of steps related to accessing the data. Numerous methods exist for key generation, traditional mechanism employed for encryption is not enough for countering the attack techniques deployed by the unauthorized users and attackers. For aforementioned reasons an encryption technique based on user feature can be a efficient method for enhancing security. Technique offers a unique key based on a user feature; this technique can make the data access very secured but there is definitely there is scope for error if not security. Further an innovative solution could be to employ hybrid technique of a feature-based mechanism in tandem with user biometric data i.e. fingerprint, iris, face features etc. to improvise the system and secure the data access with unauthorized access nearly impossible. Employing to much in-between steps on the security concerns and including the resolution for the minutest detail may lead to the degradation in the efficiency of the system. Therefore, a balance is to be maintained for improving the security measures and efficiency acceptable. [22-25]

The proposed architecture and implementation details of the system has been discussed in this section. Following figure 1 shows the schematic representation of the proposed system.

A. System Overview

The client builds an account on the cloud and then logs in to frameworks using a correct username and password. User demands KU-CSP keys [1] after signing in. The client / proprietor uses the keys to scratch the documents and move them to the cloud server over a fixed period, all while being completely weightless. The remaining client is then sent to the KU-CSP, which creates a new key or refreshes the old ones in order to keep the device secure and passes the new keys to the client's key. The residual consumer is reshaped at this stage. When the predefined document cycle on the cloud server is complete, the report will be lost to the server and will no longer be available to clients. The computing space of the cloud system is expanded as a result of this. To overcome the disadvantage of the previous framework, the framework genius postures information self-destruction strategy. The literature review shows that the existing mechanism retains the data as it is over the cloud storage, even if it is no longer in use. It makes the users, remove the data manually to free the space. Thus increasing the workload of the user and simultaneously occupying the storage unnecessarily over the cloud storage. Thus, to overcome these issues from the existing system, our proposed system has the mechanism to automatically destroy the data once either the time duration to access the data is over or the data is no longer needed. We call this feature as self-data destruction mechanism. Here, the information is transmitted to the cloud server for a set period (for example, (2/2/2023-3/2/2023,). Here, in this example the data outsourced over cloud will be accessible to the authorized user only for the specified time frame of a day. Once the permissible time frame is over, the system will revoke the accessibility and destroy the data from the server. It will ensure the security of the data from unauthorized access also it will free the space from the server.

B. Data Self-Destructing Mechanism

A Self-Destructing Scheme known as key-strategy personality-based encryption collaborates with time-defined characteristics, which is based on the review that each identification thing can be linked to an arrangement of properties in suitable cloud application circumstances, and each attribute is linked to a

time interval detail, demonstrating that the encrypted data thing can be deciphered between those periods. Each user's key is linked to a get-to tree, and each leaf hub is linked to a period during which the data owner scrambles his or her information before distributing the device to customers. Since the get to tree's simple articulation can mean any desired information index for it, it can obtain fine- grained get to command at any time between each of the. The ciphertext cannot be decoded if the time moments are not within the predefined time intermediate, i.e., the ciphertext will be naturally lost and no one would be able to unscramble it due to the secure key closure. Along these lines, it is possible to achieve a secure self-pulverization of data with fine-grained control. The essential characteristics should satisfy the get to tree, where even the time span of each leaf in the key customers should have a place in the ciphertext with the coordinating characteristic, keeping in mind the goal of effectively unscrambling the ciphertext.

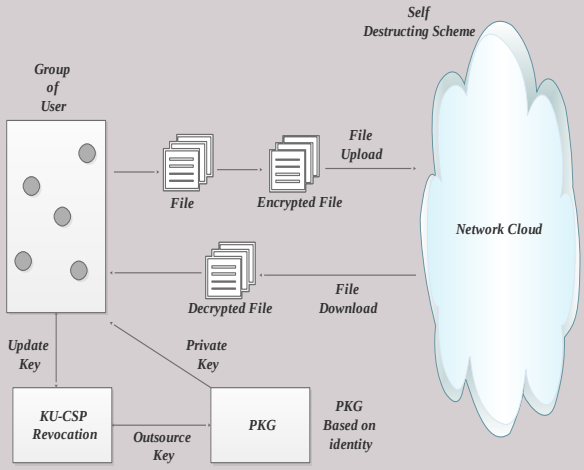


Figure 2: System Architecture

C. Experimental Setup

The IDE tool for the development of the system is NetBeans 8.1 and JDK 1.8 were included in the system as a front end on the Windows level. The program can be run on any regular computer. The system would not have to think about running a specific machinery.

ALGORITHM FORMULATION

In a short amount of time, data storage evolves into a technique of preference. Since data is protected remotely rather than locally, consumers from both the home and the technical sphere are inclined to do

so. If the dispersed storage is not completely confident, it means that users have "the possibility to incorporate knowledge about the online cloud."

Regardless of whether customers find cloud-based information to be a major cause for concern, the fact remains that it can be a difficult problem, especially because we trade data on cloud servers.

Assume S represents the system where.

S = {Φ, KDC, CS}

Table 1

Algorithm – Biometric based Encryption

i. User

Φ = {R̄, £, ¥, €, δ} Where,

R̄= User Registration

£= User Login

¥= Request for Key

€= Encryption of

Data δ= User

Revocation

ii. Key Distribution Centre KDC= {α, β}

Generating set of Keys

α= {α1, α2, α3 ... αn}

Where α represents the set of public keys.

β= {β1, β2, β3 ... βn}

Where β represents the set of private keys generated with respect to the public key.

iii. Cloud Server is CS: {U, D} ;

D: {F, T}

where

J: File to be Uploaded

D: the process of self-destruction

F: Number of files

T: Time Interval

To address this issue in a competent and effective manner, the Revocable IBE conspires, and the primary refreshing technique are both already available. In addition, cloud architecture experience needs to be improved to enable the utilization of contemporary safe information structures in distributed computing. In this sense, a figure (or any encoded document) can contain a temporary amount of time. If the characteristics of the figurative content fit the configuration of the key, and if all possible occurrences are permitted to take place, then the figurative content must be decrypted. After a client has specified an end time, the information is permanently removed from the cloud server in a secure mannerAn Example of equation.

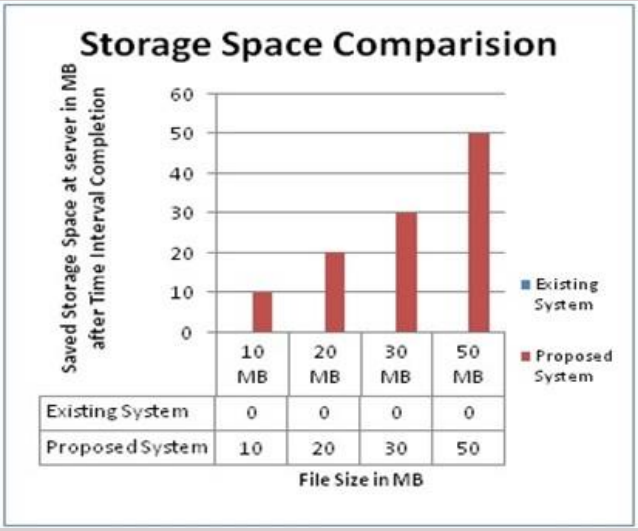


Figure 2: Storage Space Comparison Graph

RESULT & DISCUSSION

The graph illustrates the difference between some of the system's storage space and the proposed storage space, the system has been unable to retrieve the data from the public cloud, but the constructed methodology will delete the data from the public cloud after a stated amount of time, minimizing the cloud server's storage space. The various files on the cloud server are shown in the x-axis, while the storage in the y-axis is stored in mb.

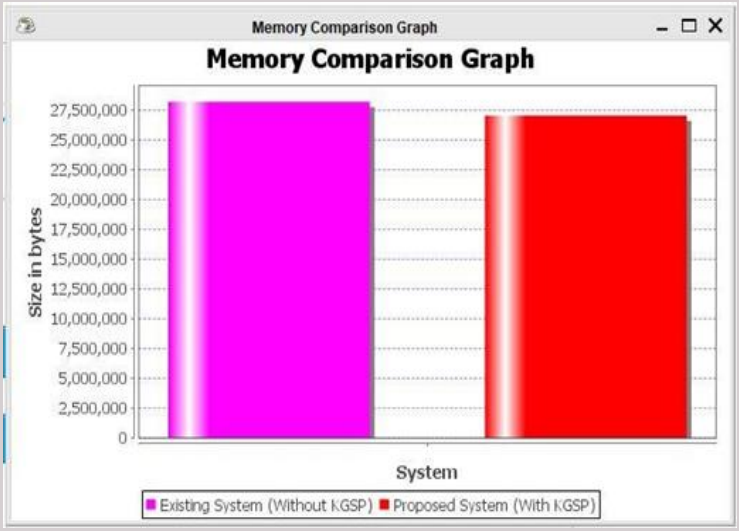


Figure 3: Memory Comparison

Figure 3 and 4 shows the comparison of space and time complexity of the system implemented with and without dedicated key distribution server. From the graph, implementation of dedicated key generation server reduces the complexity and make the system more efficient.

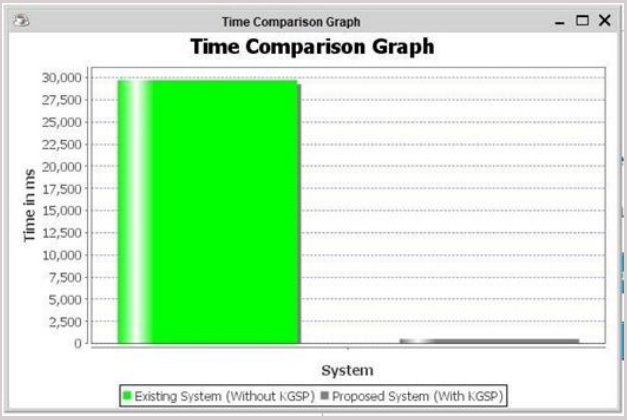


Figure 4: Storage Space Comparison Graph

CONCLUSION

The rapid expansion of flexible cloud administration has resulted in the emergence of several previously unanticipated issues. One of the most significant challenges is figuring out how to securely remove information that has been outsourced and stored in the cloud. This paper proposed an information self-destructing mechanism that can achieve the time defined ciphertext in distributed computing to resolve the issues. This mechanism would resolve the issues by performing an adaptable wonderful get to control between the consent specified time and moment self-decimation after coming close to shared and outsourced information. IBE is also familiar with the catch-22 situation that arises

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

when a character is repudiated by an estimate that can be revocably outsourced. There is no need for a safe channel or client verification during the key updating process that takes place between the client and the KU-CSP. In addition, the framework is equipped with features such as unfailing viability for both PKG measures and client shared secret key size because of the utilization of the key updating service that is made available by the cloud server, further the time comparison establishes that proposed technique with GSP is more efficient as compared to without GSP. The framework proposed is equipped with features such as unfailing viability for both PKG measures and client shared secret key size because of the utilization of the key updating service that is made available by the cloud server, further the time comparison establishes that proposed technique with GSP is more efficient as compared to without GSP. Results show that the proposed system with GSP reduces processing time by approximately 0.001 times.

References

[1] Jin Li, Jingwei Li, Xiaofeng Chen, Chunfu Jia, and Wenjing Lou, “Identity-Based Encryption with Outsourced Revocation in Cloud Computing”, in IEEE transactions on computers, vol. 64, no. 2, february 2015.

[2] W. Aiello, S. Lodha, and R. Ostrovsky, “Fast digital identity revocation,” In Advances in Cryptology CRYPTO98). New York, NY, USA:Springer, 1998, pp. 137-152.

[3] A. Boldyreva, V. Goyal, and V. Kumar, “Identity-based encryption with efficient revocation,” in Proc. 15thACMConf. Comput. Commun.Security (CCS08), 2008, pp. 417-426.

[4] D. Boneh and M. Franklin, “Identity-based encryp-tion from the Weilpairing,” in Advances in Cryptology CRYPTO „01), J. Kilian, Ed.Berlin, Germany: Springer, 2001, vol. 2139, pp. 213-229.

[5] A. Sahai and B. Waters, “Fuzzy identity-based encryption,”in Advances in Cryptology (EUROCRYPT‟05), R. Cramer, Ed. Berlin, Germany: Springer, 2005, vol. 3494, pp. 557-557.

[6] J. Li, C. Jia, J. Li, and X. Chen, “Outsourcing encryp-tion of attribute based encryption with mapreduce,” in Information and Communications Security. Berlin, Heidel-berg:Springer, 2012, vol. 7618, pp. 191-201.

[7] B. Zhang, J. Wang, K. Ren, and C. Wang, “Privacy-assured Trans. Emerging Topics Comput., vol. 1, no. 1, p. 166-177, Jul. Dec. 2013 outsourcing of image reconstruction service in cloud,” IEEE.

[8] R. Patil Rashmi, Y. Gandhi, V. Sarmalkar, P. Pund and V. Khetani, "RDPC: Secure Cloud Storage with Deduplication Technique," 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2020, pp. 1280-1283, doi: 10.1109/I-SMAC49090.2020.9243442.

[9] J. Li, X. Chen, J. Li, C. Jia, J. Ma, and W. Lou, “Fine-grained access control system based on outsourced attribute-based encryption,” in Proc. 18th Eur. Symp. Res. Comput. Secu-rity (ESORICS), 2013,pp. 592-609.

[10] R. Canetti, S. Halevi, and J. Katz, “A forward-secure publickey Encryption scheme,” in Advances in Cryptology (EUROCRYPT'03), E. Biham, Ed. Berlin, Germany: Springer, 2003, vol. 2656,pp. 646-646.

[11] P. Mell and T. Grance, “The NIST Definition of Cloud Computing,” Nat. Inst. Stand. Technol., Tech. Rep. SP 800 - 145, 2011.

[12] C. Wang, K. Ren, and J. Wang, “Secure and practical outsourcing of linear programming in cloud computing,” in Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM), 2011, pp. 820–828.

[13] M. Green, S. Hohenberger, and B. Waters, “Outsourcing the decryption of ABE ciphertexts,” in Proc. 20th USENIX Conf. Security (SEC‟11), 2011, pp. 34–34.

[14] Y. Hanaoka, G. Hanaoka, J. Shikata, and H. Imai, Identity-based hierarchical strongly key-insulated encryption and its application, in Advances in Cryptology (ASIACRYPT05), B. Roy, Ed. Berlin, Germany: Springer, 2005, vol. 3788, pp. 495 514.
[15] D. Boneh, X. Ding, G. Tsudik, and C. Wong, A method for fast revocation of public key certificates and security capabilities, in Proc. 10th USENIX Security Symp., 2001, pp. 297308.
[16] B. Libert and J.-J. Quisquater, Efficient revocation and threshold pairing based cryptosystems, in Proc. 22nd Annu. Symp. Principles Distrib. Comput., 2003, pp. 163171.
[17] H. Lin, Z. Cao, Y. Fang, M. Zhou and H. Zhu, "How to design space efficient revocable IBE from non-monotonic ABE", Proc. 6th ACM Symp. Inf. Comput. Commun. Security (ASIACCS'11), pp. 381-385, 2011.
[18] Boneh D. and Boyen X. Efficient selective-id secure identity-based encryption without random oracles Advances in Cryptology (EUROCRYPT'04) Cachin C., and Camenisch J., Eds., Berlin, Germany: Springer, 2004, vol. 3027, pp. 223–238.
[19] Boneh D. and Boyen X. Secure identity based encryption without random oracles Advances in Cryptology (CRYPTO'04) Franklin M., Ed., Berlin, Germany: Springer, 2004, vol. 3152, pp. 197–206
[20] Waters B. Efficient identity-based encryption without random oracles Advances in Cryptology (EUROCRYPT'05) Cramer R., Ed., Berlin, Germany: Springer, 2005, vol. 3494, pp. 114–127
[21] P. Singh, P. Khanna and S. Kumar, "Communication Architecture for Vehicular Ad Hoc Networks, with Blockchain Security," 2020 International Conference on Computation, Automation and Knowledge Management (ICCAKM), Dubai, United Arab Emirates, 2020, pp. 68-72, doi: 10.1109/ICCAKM46823.2020.9051499.
[22] Gupta, A., Khanna, P., Kumar, S. (2021). A Hybrid Blockchain-Secured Elderly Healthcare Environment. In: Tanwar, S. (eds) Blockchain for 5G-Enabled IoT. Springer, Cham. https://doi.org/10.1007/978-3-030-67490-8_16
[23] Kumud Tiwari, Sachin Kumar, Pooja Khanna, Anil Kumar, "Blockchain-based transaction validation for patient interoperability in Healthcare 4.0", Blockchain Applications for Healthcare Informatics, Academic Press, 2022, Pages 1-26, ISBN 9780323906159, https://doi.org/10.1016/B978-0-323-90615-9.00017-7.
[24] Kumar, S., Khanna, P., Pragya, Tripathi, S. (2023). Biometric Assisted Multi-modal Encryption Key for Secured FHSS Communication. In: Bhattacharyya, S., Banerjee, J.S., Köppen, M. (eds) Human-Centric Smart Computing. Smart Innovation, Systems and Technologies, vol 316. Springer, Singapore. https://doi.org/10.1007/978-981-19-5403-0_12
[25] S. Priya, G. Srivastava and S. Kumar, "Blockchain Integrated Crowdfunding Platform for Enhanced Secure Transactions," 2021 4th International Conference on Recent Developments in Control, Automation & Power Engineering (RDCAPE), Noida, India, 2021, pp. 280-285, doi: 10.1109/RDCAPE52977.2021.9633380.

2nd International Symposium
on
Securing Next-Generation Systems
using
Future Artificial Intelligence Technologies
SNSFAIT – 2023
25th May 2023
Organized By
Department of Computer Science & Engineering,
Maharaja Agrasen Institute of Technology, Delhi, India
in collaboration with
IEEE ComSoc Delhi Chapter

Digital Twining in Intelligent Farming Systems

Ankur Rawat1, Lucknesh Kumar,[2], Inderjeet Kaur [3] and Ashish Sharma[4]

[1,2,3] *Ajay Kumar Garg Engineering College, Ghaziabad, India*
[4] *Guru Gobind Singh Indraprastha University, Dwarka, Delhi, India*

Abstract

The agriculture industry needs to adopt the latest technologies to manage and market crops in a more efficient manner. By using IOT and other digital solutions, farmers can increase their yield and profitability by streamlining the process of controlling and marketing their crops. Digital farming aims to provide customers and farmers with a range of solutions to address current issues such as resource management and food security. With a complex set of variables to consider, such as climate change, digital techniques can significantly improve decision-making support and efficiency. Digitalization can also help prevent crop hoarding and establish optimal prices for crops throughout the year. By using digital twins, all crop availability can be displayed in one location, making contract farming possible without needing a large number of fields in one area. This approach can encourage corporate investment in agriculture and increase the export of crops between countries. Additionally, the use of digital twins allows us to keep track of all services, agreements, and transactions between farmers and merchants on a transparent platform. Using IOT devices that utilize machine learning algorithms, we can automatically determine relevant prices and check the quality of crops. This will enable farmers to get the best value for their crops while providing consumers with high-quality produce. Overall, digitalization can revolutionize the agriculture industry and help us address current and future challenges.

Keywords [3]
IOT, Digital Twins, Machine Learning, Crops Management, Crop recognizing device.

Introduction

The use of digital twin technology in combination with IoT systems can significantly improve crop management and sales. Digital twin technology involves creating a virtual replica of a physical object or system, which can be used to simulate and analyze different scenarios and outcomes. In the context of crop management, a digital twin can be used to model a specific farm, taking into account factors such as soil quality, weather conditions, irrigation systems, and crop types.

SNSFAIT 2023, May 12–05, 2023, Delhi, India
EMAIL: ankur1910067@akgec.ac.in(A.1); kumarlucknesh@akgec.ac.in(A.2); kaurinderjeet@akgec.ac.in (A.3); ashishsharma411@gmail.com (A. 4)
ORCID: 0009-0000-5670-2579 (A. 1); 0009-0005-9663-8256 (A. 2); 0000-0002-3594-1877 (A. 3); 0000-0003-4402-9561 (A. 4)

Real-time data on various aspects of the farm, such as soil moisture levels, temperature, and humidity, can be collected using IoT systems. This data can be used to update the digital twin and make predictions about future crop yields, potential pest outbreaks, and other factors that could affect the success of the farm.

Digital twin technology and IoT systems can also be utilized for crop selling. Data on crop quality, quantity, and market prices can be collected and used by the digital twin to predict the best time to sell the crops for maximum profit. In addition, IoT sensors and digital twins can assist farmers in optimizing their crop management practices by identifying areas for improvement, such as modifying irrigation schedules or utilizing different fertilizers. This can result in increased crop yields and a more efficient and environmentally friendly farming operation. The combination of digital twin technology and IoT systems has the potential to transform crop management and sales, empowering farmers to make decisions based on data that leads to increased efficiency, profitability, and sustainability.

The paper is divided into 5 sections. Section 1 gives the overview of the digital twin technology in crop management. The remainder of the paper is structured as follows, Section 2 briefly describes the Systematic Literature Review (SLR) and digital twin terminologies, its uses in data analyzing and integration levels. The concepts of contract farming and “one nation- one market” is also briefed in this section. Section 3 looks to conceptualizes the methodology using NoIR IOT based camera used in crop recognizing. Results are discussed in section 5. Finally, the paper concludes in Section 6.

Background Study

In many countries, the increasing population results in a shortage of agricultural land and food supply. Reports suggest that hunger-related factors cause the death of 20 million people every year. The Food and Agriculture Organization (FAO) estimates that there are currently 435 million severely malnourished people in the world [1]. Despite this, almost 2.5 billion tonnes of food produced annually is lost or wasted, with one-third of it being lost during the production process. According to the Boston Consulting Group (BCG), the value of this wasted food is estimated to be $230 billion [2]. Some countries, like India, are facing a food surplus crisis, as reported by the Food Corporation of India (FCI). The buffer stocks in India contain 30 lakh tonnes of sugar, 221 lakh tonnes of rice, and 478 lakh tonnes of wheat [3]. This highlights the mismanagement of food resources and the need for digitalization to address this issue. Fortunately, there are many modern technologies and methods that can help to regulate poor food management and save countless lives. Many nations, such as Liberia 76.9%, Somalia 60.2%, and Guinea-Bissau 55.8%, rely heavily on agriculture as a major contributor to their economy [4], with the sector accounting for a significant portion of their GDP. Therefore, it is crucial for these countries to have efficient and transparent crop management systems that can improve the quality and quantity of their crops and generate greater profits. To achieve this, advanced technologies can be utilized to create automated crop management and distributed systems.

Crops are categorized based on several factors such as growth and maturation, root depth, climate, season, and carbon dioxide absorption [5]. During harvest season, there is a surplus of supply and equal demand, causing crop prices to decrease automatically. Farmers who rely solely on crops for income sell their produce at a lower price and may not make any profit. Conversely, after harvest season, there is a shortage of crops and equal demand, causing prices to rise, making it costly for customers to

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

purchase the same food. This results in a loss for producers during harvest season due to the high supply and for consumers after the harvest season due to low supply. To mitigate this problem, technology and digital twin methodology can be utilized to set prices for every crop for the entire year, ensuring that prices remain stable during and after harvest. This will enable both farmers and consumers to make a profit since prices will remain constant throughout.

Many farmers across the country are facing losses as they have to purchase all their inputs, such as seeds, fertilizer, and other supplies, at retail prices and sell their produce at wholesale costs [6]. This is in contrast to the manufacturing industry, where raw materials are bought at wholesale prices and products are sold at retail prices. Through the use of digitization, we can provide farmers with inputs at wholesale prices, reducing their production costs and increasing their profits. Despite the fact that 47 countries have implemented 67 reforms to assist farmers in growing their businesses, many farmers are still unaware of these programs and are missing out on their benefits [7]. By digitizing the agricultural sector, we can quickly disseminate useful information to farmers and reduce the number of struggling farmers.

Digitizing the agriculture sector can help farmers who struggle to sell their crops at a profitable price by providing them with access to technologies. Additionally, small-scale and marginal farmers often cannot afford high-quality seeds due to their high cost and limited availability in nearby stores. However, the quality of the seed used in farming is crucial for achieving higher crop yields and sustained agricultural productivity. Ensuring high-quality seed distribution is just as critical as seed production [8]. By leveraging digitization, we can provide door-to-door services to farmers and monitor the availability of high-quality seeds in their area, thereby addressing this issue.

Farmers in certain regions may not be familiar with the latest technologies available for agriculture. The lack of proper equipment is a major challenge faced by farmers, making it difficult for them to adapt to modern agricultural practices. However, with adequate training, farmers can significantly improve their lives and the productivity of their farms. The use of modern equipment is crucial for this purpose. Through digitization, we can provide farmers with access to new technologies that can greatly benefit them.

Farmers face numerous daily challenges, resulting in their status as price takers rather than price makers. Additionally, the global population is growing exponentially. In this context, ensuring food security for the world's expanding population while ensuring long-term sustainable growth is a crucial goal. To achieve this, we must implement the "One Nation, One Market" principle by leveraging digital twins and cutting-edge technologies such as IoT and other advanced technologies.

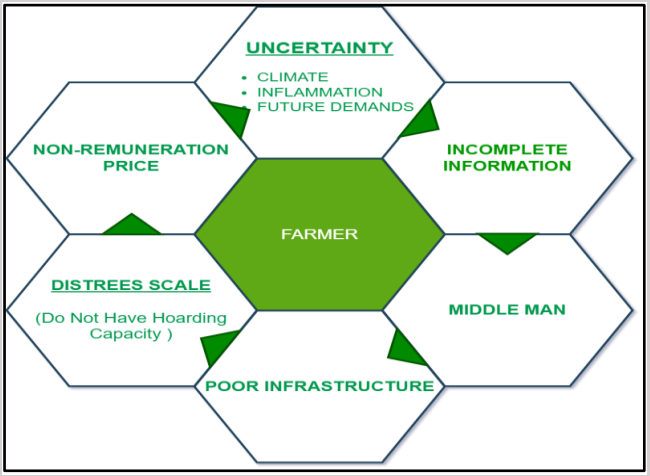


Figure1. Issues faced by farmers

By eliminating intermediaries and facilitating direct communication between farmers and retailers through digitalization, agricultural prices can benefit both parties. Various advanced technologies are available in the market that can be utilized to establish a system that enables seamless connection between farmers and retailers.

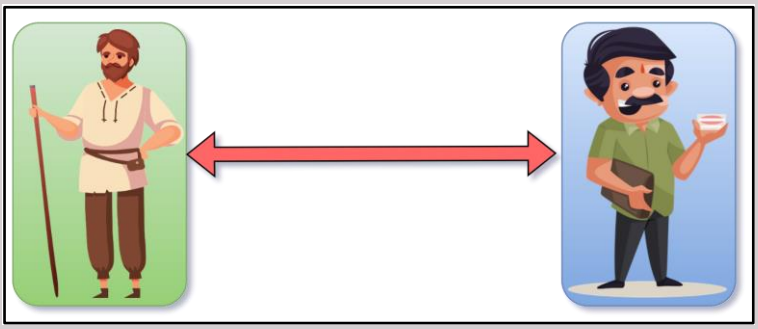


Figure2. Direct communication between farmers and retailers

In many regions, farmers lack literacy and are not familiar with modern technologies, making it difficult for them to adopt digitalization in agriculture [9]. Hence, to make the agricultural sector more digital, it is crucial to design user-friendly digital services with simple graphical user interfaces that can be easily used by anyone with basic computer skills, ensuring accessibility and convenience for all.

Modeling terminology of a Digital Twin

A Digital Twin is a digital representation of a physical object or system, which is used to simulate and analyze its behavior in real-world conditions. The following are some common modeling terminologies used in Digital Twin development:

1. Model: The Digital Twin model represents a physical object or system through a mathematical model that includes data on its design, construction, operation, and maintenance.

2. Inputs: Inputs for the Digital Twin model include various types of data, such as sensor readings, environmental conditions, and user inputs, used to simulate the behavior of the physical object or system.

3. Outputs: Outputs generated by the Digital Twin model can provide performance metrics, predictive analytics, visualizations, and other data-driven insights, based on the inputs fed into the model.

4. Simulation: Simulation involves running the Digital Twin model to predict how the physical object or system will behave under different conditions, allowing potential issues to be identified and performance to be optimized.

5. Validation: Validation involves verifying that the Digital Twin model accurately represents the physical object or system by comparing the model outputs to real-world data.

6. Optimization: Optimization is the process of using the Digital Twin model to identify ways to improve the performance of the physical object or system, including changes to design, maintenance, or operational processes.

7. Machine learning: Machine learning is a type of artificial intelligence that enables the Digital Twin model to learn from data and improve its predictions over time, helping to identify patterns and optimize performance.

8. Analytics: Analytics involves using data to gain insights into the performance of the physical object or system, which can include descriptive, predictive, and prescriptive analytics.

The use of digital technology can enable farmers to engage in contract farming, which involves an agreement between farmers and processing and/or marketing firms for the production and supply of agricultural products at predetermined prices [10]. By leveraging digital twin technology, individual farmers can easily participate in contract farming. This can provide small farmers with access to new markets that would otherwise be inaccessible to them.

There are various types of crops available, and the price of each crop is determined by its quality. However, assessing the quality of crops can be challenging for humans to do accurately with the naked eye. Hence, utilizing machine learning (ML) and Internet of Things (IoT) technology can help verify the quality of crops and establish prices based on their respective quality levels.

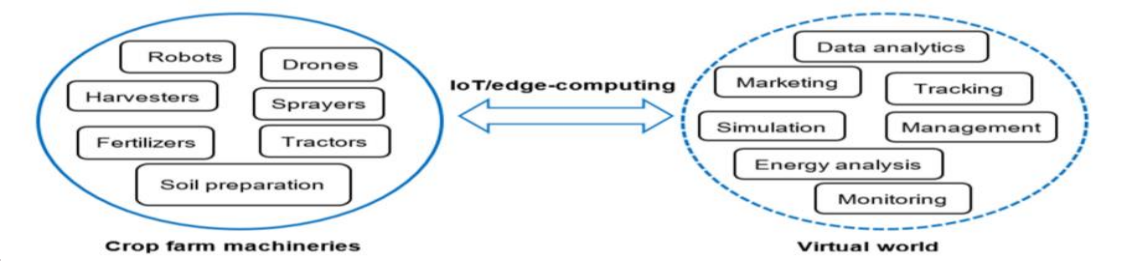


Figure3. showing crop farm machineries and virtual world outcomes using IOT/edge-computing

Digital Twin at data integration level

A digital twin is a virtual representation of a physical system or process that enables real-time monitoring, analysis, and optimization. In the realm of data integration, a digital twin can be employed to create a unified view of data from multiple systems or sources.

To generate a digital twin for data integration, you must first identify the various systems or sources that you want to integrate. These sources may comprise databases, APIs, file systems, and other data repositories. You must then develop a data model that represents the structure and relationships of the data in each of these sources.

Subsequently, you can employ this data model to create a digital twin of the integrated data. This could involve creating a virtual database or data warehouse that consolidates all of the data from different sources, or it could involve generating a real-time data stream that aggregates data from multiple sources as it is made available. The digital twin can be utilized for a range of purposes, such as real-time data monitoring and analysis, forecasting future trends and outcomes, and optimizing processes based on data insights. With the aid of advanced analytics techniques, including machine learning, the digital twin can even be used to automate decision-making processes and enable autonomous operations.

Digital Twin in Contract Farming

a. Contract farming

Contract farming (CF) involves an agreement made in advance between farmers (producers) and buyers for the production and distribution of agricultural products, where the terms and conditions are agreed upon by both parties. These terms often include the price to be paid to the farmer, the quantity and quality of the product required by the buyer, and the delivery date of the product to the customer. The contract may also specify details on how production will be carried out or whether the buyer will supply inputs like seeds, fertilizer, and technical guidance [11].

CF has been used for many years, but its use has increased in recent times, especially in developing nations, due to the growing demand for food and agricultural products brought on by globalization. As more people live in cities and seek food that is safe to consume and produced in an environmentally friendly and socially responsible manner, food markets have become more competitive. In this new environment, agricultural product buyers must

collaborate more closely with their supply chain partners to obtain high-quality raw materials directly from farmers and satisfy the demand for food products from their clients, including supermarkets, eateries, hotels, schools, and hospitals.

Contracting with farmers can help businesses that process agricultural goods ensure a steady supply of raw materials that match their quality and quantity requirements.

b. How Digital Twin use in Contract Farming (CF)

The main challenge associated with contract farming is that small-scale farmers with limited land holdings are often unable to participate because the firms require a minimum quantity of crops from a single location. However, advancements in technology, such as the digital twin technique, have made it possible for individual farmers to engage in contract farming. By creating a virtual community of farmers interested in contracting with the same business, we can connect and facilitate their participation digitally. While implementing this solution is complex and poses real-world challenges, it is feasible with the latest technologies and commitment. It is important to consider that many farmers around the world may be illiterate and lack the necessary infrastructure to use such advanced methods. Therefore, a user-friendly system with simplified processes and a one-click service can be created to make it accessible to everyone.

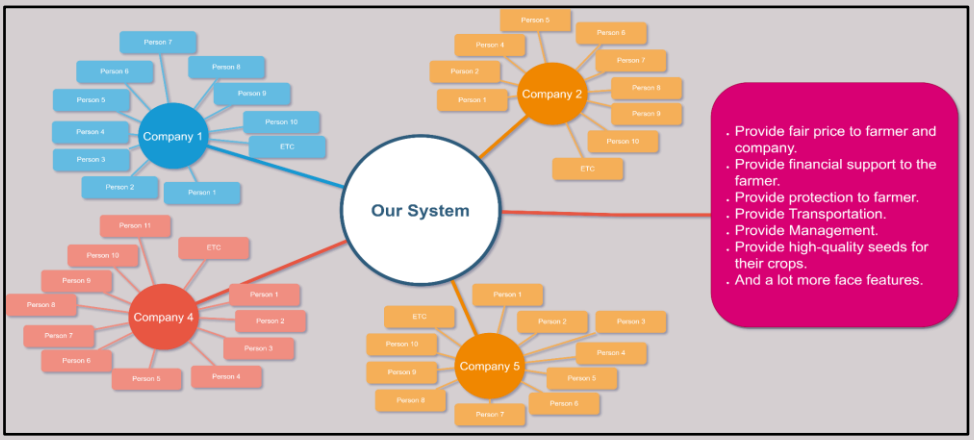


Figure4. showing crop farm machineries and virtual world outcomes using IOT/edge-computing

In the digital realm, the combination of technology and human effort can make anything possible. Consequently, it is feasible to quantify crop production by utilizing digital tools, and we can also assess the quality of crops through specialized machine learning algorithms.

Digital Twin in "One Nation One Market" Strategy

Each country is comprised of multiple states or districts, and each district in turn is composed of several small villages. In some states, the production of certain crops is high, while in others, it is low. Consequently, the demand for specific crops can be higher in some regions than in others. If digital platforms are utilized to gather crop production data during the harvesting season, it would

be possible to predict the crop production levels for each state based on the demand. This would allow for the calculation of crop prices for the entire year. If production exceeds demand, exporting crops becomes feasible, and farmers can reap more financial benefits, while consumers would be content with buying crops at a consistent price throughout the year. This approach can prevent crop hoarding in the country, help each state acquire crops at a reasonable price, and encourage private sector investment in agriculture.

Digital Twin in Data Collection

By utilizing Digital Twins as the primary tool for farm management, physical flows can be separated from planning and control. This allows farmers to remotely manage operations using (almost) real-time digital information, eliminating the need for on-site human labor and direct observation [12]. By assembling information from various sources, such as weather stations, drones, and soil moisture sensors, farmers can gain insight into the status of their crops, the condition of their land, and weather patterns. The latest technologies, including advanced AI and ML algorithms, make all of this possible. In fact, emerging trends in the computer industry, such as blockchain technology, cloud computing, the internet of things (IoT), machine learning (ML), and deep learning (DL), have already been applied by researchers to address complex problems in fields such as healthcare, cybercrime, biochemistry, robotics, metrology, banking, medicine, and food [13].

Digital Twin in Data Analyzing

By automating analytics through the Internet of Things (IoT) and other machine-driven methods, we can obtain various data from sensors and other sources without the need for human intervention [14]. Farmers can use the digital twin they have in place to simulate different scenarios and make predictions about the outcomes. The analysis can assist farmers in optimizing their crop management techniques, increasing crop production, and improving resource efficiency. By analyzing the collected data, they can predict soil composition and capacity, create digital product descriptions, forecast weather patterns, identify persistent stress factors, and much more. Several companies are employing Artificial Intelligence (AI) and other technologies to model and forecast weather, which can be integrated into our agricultural digital twin. Understanding the soil's composition and capacity where crops are grown is a critical aspect of land-based agriculture. In order to create an agricultural digital twin, we must measure and comprehend this information and take appropriate action, such as changing irrigation or fertilizer application, based on data analysis. By pinpointing areas and processes where the agricultural system's resources are under stress, we can reduce water usage and fertilizer waste. Identifying and addressing issues such as invasive species, poor soil quality, and pollution through careful analysis and inquiry, such as "How might we," can significantly improve agricultural performance. With the ability to plan, analyze, and simulate crop growth, we can increase yields, reduce strain on water resources, and improve soil quality.

Digital Twin in Monitoring and Refining

It is important to monitor the crop health and gather data consistently throughout the entire cycle. As more data is accumulated, the digital twin can be refined and crop management can be adapted accordingly.

Methodology Used

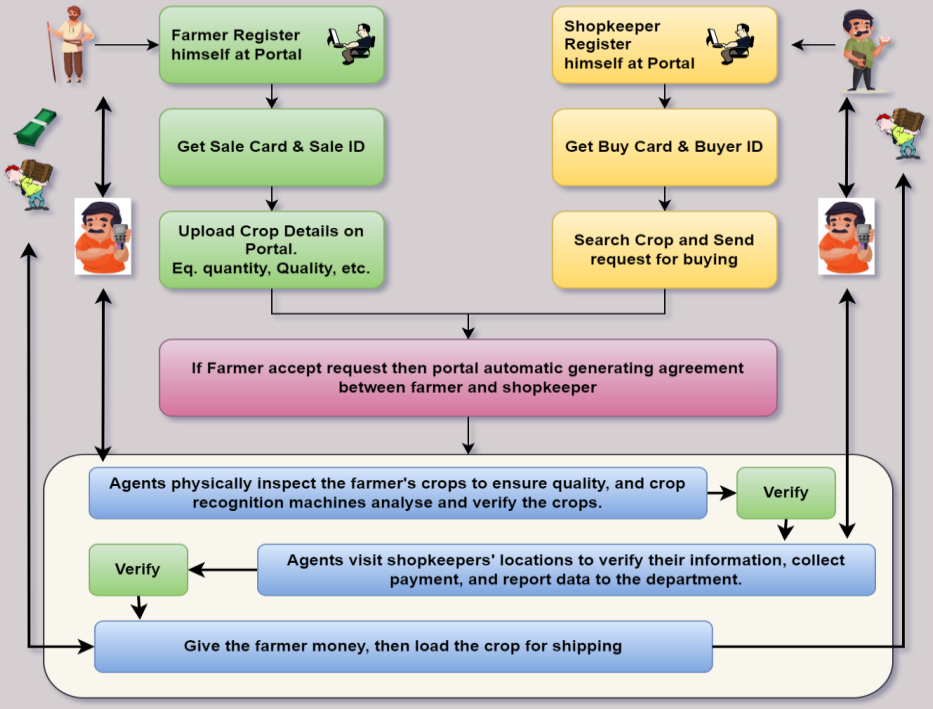


Figure5. Methodology Used

The above presented methodology represents a transparent system, utilized by both literate and illiterate farmers. The registration is required for both farmers and shopkeepers for gathering information, assistance can easily be provided through nearby cybercafes and govt agencies. After successful registration, farmers can submit their crops' quantity and quality with a single-click based system in this application or server as shown in Figure 5 as discussed below:

- A shopkeeper approaches the farmer after a farmer upload crops in order to buy those crops and sends a request to buy crop.
- If farmer accepts the request, then portal automatically generates an agreement between the farmer and shopkeeper.
- System is able to create automatic agreements, which can act as a proof of transactions done between farmers and shopkeepers.
- When farmers are ready to sell their crop and shopkeeper are ready to buy crops then a physical verification is required to check the quality and quantity of crops to finalize the transaction.
- Therefore, an agent (Human) goes to farmer house and check the crop quality and quantity and also check the quality of crop by using Al algorithm-based machine. The unit is comprising of a Pi NoIR infrared powered camera which captures the images of the crop and check the quality of crops.

Crops are ready to be sold when everything is in order. If everything is in order, farmers should find a way to transport their goods to storekeepers of storekeeper can also manage the transport and the transport changes can be deducted from either side (farmer or shopkeeper). Here, all farmers upload their crop output so that the system can determine the price of crops for the entire year based on the precise amount of crop output in a given area.

Result and Discussion

Digitization in agriculture is the process of enhancing and optimizing farming methods through the use of technologies like sensors, drones, and data analytics. The working of crop recognizing device used in our system are shown in figure 6 below.

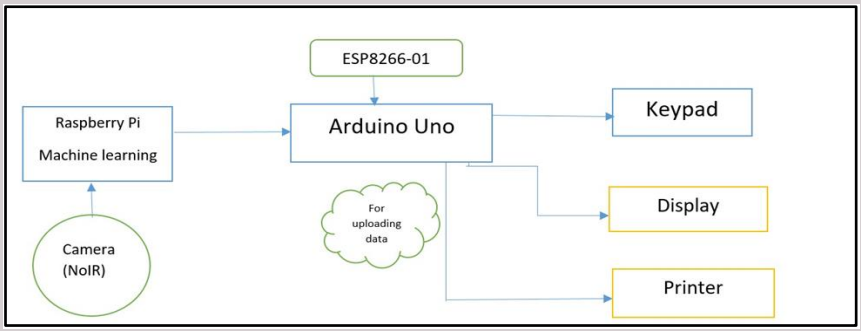


Figure6. Block diagram of crop recognizing device

This IoT-enabled device is designed for quality checks of crops and generates real-time receipts for farmers using AI techniques. In order to ensure the expected result, several major steps such as data collection, implementation, testing, and troubleshooting, need to be conducted. The prototype is built by combining the part of crop recognition and IoT together. This machine firstly scans the crop using the inbuilt camera (), and crop quality analysis is done as per the category. The details of the crops are shown in Table1.

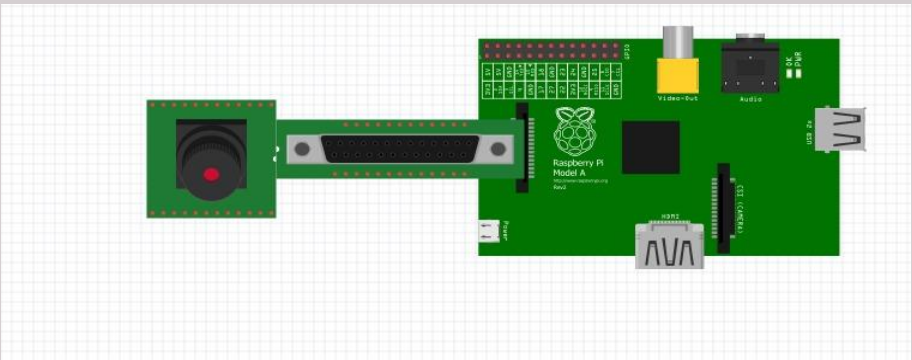


Figure7. IOT Enabled Crop Quality Check System

Table 1. Details of Crops with their quality index

CURRENT DETAILS OF CROPS				
CROP ID	CROP NAME	1st	2nd	3rd
9	RICE	35.000	30.000	20.000
10	WHEAT	20.000	17.000	14.000
12	COTTON	300.000	260.000	210.000
13	GROUNDNUT	90.000	80.000	66.000
14	SOYBEAN	80.000	72.000	65.000
15	MUSTARD	50.000	45.000	38.000
16	MAIZE	20.000	17.000	15.000
17	BAJRA	35.000	32.000	25.000
18	URAD	90.000	82.000	71.000
21	PEAS	85.000	77.000	64.000
23	MMMM	1.000	1.000	1.000

First Quality Second Quality Third Quality

Figure8. Quality of rice grain detected from IOT device

The quality and quantity of the crop are monitored by an on-ground agent. The above data is uploaded to the server for further processing taking place on the web portal. The real-time receipt is generated after successful verification of the above crop data and provided to the farmer. The buyer verification is done by an on-ground verification agent after submitting his records and token amount (minimum) for the receipt-generated amount. As a final step, the measured crop should be transported using the most economical transportation medium (suggested by the portal), to the buyer's place.

Conclusion

Digitization provides farmers with access to data and insights that can help them make better decisions and optimize their operations. By using data analytics and precision agriculture technologies, farmers can reduce waste, increase yields, and improve productivity on their farms. This is particularly important in the current economic climate, where profit margins are often slim. By gathering and analyzing data on their crops, farmers can make more informed decisions about when to plant, water, fertilize, and harvest their crops, potentially resulting in higher yields and higher-quality crops.

Digitization can also help farmers implement more environmentally friendly farming practices, such as reducing pesticide use and conserving soil and water. This can improve long-term agricultural productivity and environmental sustainability. Ultimately, the digitization of agriculture has the

potential to revolutionize how farmers conduct business by providing them with access to data and insights that can guide their decisions, increase productivity, and enhance profitability.

References

[25] Prause, L. "Digital Agriculture and Labor: A Few Challenges for Social Sustainability. Sustainability" 2021, 13, 5980. https://doi.org/10.3390/su13115980
[26] Gennaro, B.C.; Forleo, M.B. "Sustainability perspectives in agricultural economics research and policy agenda." Agric. Food Econ. Article number: 17, 2019.
[27] Jakku, E.; Taylor, B.; Fleming, A.; Mason, C.; Fielke, S.; Sounness, C.; Thorburn, P. "If they don't tell us what they do with it, why would we trust them? Trust, transparency and benefit-sharing in Smart Farming." NJAS Wagening. J. Life Sci. 2019, 90–91, 100285. https://doi.org/10.1016/j.njas.2018.11.002
[28] Basso, B.; Antle, J. "Digital agriculture to design sustainable agricultural systems." Nat. Sustain. 2020, 3, 254–256. DOI: 10.1038/s41893-020-0510-0
[29] Goel, R.K.; Yadav, C.S.; Vishnoi, S.; Rastogi, "Smart agriculture–Urgent need of the day in developing countries." Sustain. Comput. Inform. Syst. 2021, 30, 100512. https://doi.org/10.1016/j.suscom.2021.100512
[30] Mehrabi, Z.; McDowell, M.J.; Ricciardi, V.; Levers, C.; Martinez, J.D.; Mehrabi, N.; Wittman, H.; Ramankutty, N.; Jarvis, "A. The global divide in data-driven farming." Nat. Sustain. 2021, 4, 154–160. DOI: 10.1038/s41893-020-00631-0
[31] Cor Verdouw , Bedir Tekinerdogan , Adrie Beulens , Sjaak Wolfert "Digital twins in smart farming" Agricultural Systems Volume 189, April 2021, 103046 https://doi.org/10.1016/j.agsy.2020.103046
[32] Vishal Meshram , Kailas Patil , Vidula Meshram , Dinesh Hanchate , S.D. Ramkteke " Machine learning in agriculture domain: A state-of-art survey" Artificial Intelligence in the Life Sciences Volume 1, December 2021, 100010 https://doi.org/10.1016/j.ailsci.2021.100010
[33] http://www.womenaid.org/press/info/food/food4.html
[34] https://greenly.earth/en-us/blog/ecology-news/global-food-waste-in-2022
[35] https://timesofindia.indiatimes.com/business/india-business/indias-wheat-rice-stock-to-be-just-over-buffer-level-in-october/articleshow/92444616.cms
[36] https://www.worldatlas.com/articles/countries-most-dependent-on-agriculture.html
[37] https://www.adda247.com/upsc-exam/classification-of-crops-based-on-season-kharif-rabi-and-zaid-crops/
[38] https://www.fao.org/resources/digital-reports/disasters-in-agriculture/en/
[39] Zhong Fan; Charles Day; Chris Barlow " Digital Twin: Enabling Technologies, Challenges and Open Research" IEEE Access (Volume: 8) 28 May 2020. DOI: 10.1109/ACCESS.2020.2998358
[40] https://www.worldbank.org/en/news/press-release/2019/10/21/47-countries-make-67-reforms-to-help-farmers-grow-their-business
[41] https://www.jiva.ag/blog/what-are-the-most-common-problems-and-challenges-that-farmers-face
[42] https://www.researchgate.net/publication/290532517_A_study_on_impact_of_literacy_of_farmers_during_the_purchase_of_agricultural_inputs
[43] https://www.fao.org/3/y0937e/y0937e02.htm
[44] https://www.fao.org/in-action/contract-farming/background/what-is-contract-farming/en/
[45] https://mentormate.com/blog/the-future-of-farming-7-ways-a-digital-twin-can-be-applied-to-agriculture/

2nd International Symposium
on
Securing Next-Generation Systems
using
Future Artificial Intelligence Technologies
SNSFAIT – 2023
25th May 2023
Organized By
Department of Computer Science & Engineering,
Maharaja Agrasen Institute of Technology, Delhi, India
in collaboration with
IEEE ComSoc Delhi Chapter

Implementation of Property Rental Website Using Blockchain with Soulbound Tokens for Reputation and Review System

Sanskar Sharma [1], Aryan Kumar [1], Nidhi Sengar [1] and Ajay Kumar Kaushik [1]

[1] *Maharaja Agrasen Institute of Technology (GGSIPU), PSP Area, Plot No. 1, Sector-22, Rohini, Delhi-110086, India*

Abstract

The rising number of rental scams is a concern for the community as certain illegal practices tarnish the sector's image. Landlords rent the property without a written rental agreement to charge excessive maintenance charges, tenants provide wrong background information or refuse to pay rent or maintenance, and so on. This paper proposes introducing a decentralized profile reputation system using soulbound tokens and digital currency for transactions in rental listing websites to minimize the number of rental frauds. A non-transferable non-fungible token is provided to the new user that records their reputation across their time on the website. The lease agreement is secured via a smart contract and only initiates once the security deposit has been paid by the selected tenant and signed by the landlord. All rental transactions take place on-chain, and only registered users with a tenant-landlord relationship can give reviews. This ensures the credibility of the review system. The decentralized ledger can also be used to supervise property rental affairs. This method facilitates convenient and authentic background checks, easy transactions, and market supervision.

Keywords : Blockchain, Soulbound Tokens, Real-estate, Reputation building, Rental Website, Web3, NFTs, IPFS [4]

International Symposium on Securing Next-Generation Systems using Future Artificial Intelligence Technologies (SNSFAIT 2023), May 05-12-2023, Delhi, India

EMAIL: sanskarsharma1822@mail.com (S. Sharma); aryankumar05@gmail.com (A. Kumar); nidhisengar@mait.ac.in (N. Sengar); Ajayk08@gmail.com (A. K. Kaushik)

ORCID: 0000-0003-2431-5587 (S. Sharma)

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

1. Introduction

The real estate sector is an important area in stimulating economic growth. Real estate is a type of property to possess and use. The developments of the real estate sector boosted the growth of retail, hospitality, entertainment, housing, and services business. An electronic version of the real estate industry, Internet real estate is the concept of disseminating housing estates for sale or rent online, and for consumers seeking to buy or rent properties through such platforms. The Internet real estate industry has faced several criticisms due to the lack of rules and regulations to protect developers and buyers. People who are looking to rent a property are often caught in housing and lease scams. In such cases, deceivers show themselves as either brokers or owners of the desired unit and tell the interested tenants to make transactions to their accounts for renting the house. Once the amount is transacted, they escape and disconnect with the renters. Tenant scams on the other hand take advantage of unassuming landlords who fail to implement the right procedures for screening renters, writing contracts, and collecting payments. Scams can take many forms and can be costly for landlords, both in terms of time and money. Some common examples include submitting false employment records, faking credit reports, forging checks and pay stubs, attempting to reset the eviction process, stealing a landlord's listing, and hiding property damages. These types of scams can put a landlord's income and business at risk. Today, numerous landlords and property management companies in urban corridors have transitioned from in-person dealings with rental applicants to digital interactions to cater to customer preferences. However, this has made it more difficult to verify application validity. In fact, between 2016 and 2018, 97% of property management companies have experienced fraud in some capacity, with 80% experiencing it up to 20 times, according to the Forrester study. Overall, about 59% of rental applications are submitted online, and this digitization of the rental application process has opened new avenues for fraud. The shift from in-person to digital applications, coupled with the COVID-19 pandemic, has also played a role in the increase of fraud in the rental housing industry.[1]

1.1. Proposed Solution

To solve such problems, the paper proposes the use of a property rental website which uses blockchain as its main technology. This will be achieved by minimizing online rental fraud and introducing profile reputation using Soulbound Token (SBT) for customers. It will allow tenants to look for available rental options, and landlords to list their properties. A Soulbound Token will be issued to the user that will monitor their profile reputation and authenticity. A soulbound token is a publicly verifiable and non-transferable non-fungible token (NFT) that can be used to represent an individual's credentials, affiliations, and commitments. Landlords can list their properties in the form of smart contracts on the network. A smart contract is a paperless digital code that defines a set of promises on prewritten conditions that the parties of a transaction have agreed upon [2]. Listing involves paying a minimal crypto fee to the admin as a security deposit which can be liquidated if the user violates the terms and conditions. A rental agreement only initiates once the tenant has successfully deposited the security fees which can further be retrieved when the agreement period ends. The terms and conditions of rent between the parties will be secured via a smart contract and all transactions henceforth will take place

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

via smart contract methods. These programs are executed on a decentralized network of blockchain that provides the benefit of being immutable. Only users that have been in the tenant-landlord relationship can give reviews to each other, thus ensuring that the review system is credible. This could help revolutionize the online rental industry by minimizing the number of frauds and scams and increasing the trust between landlords and tenants.

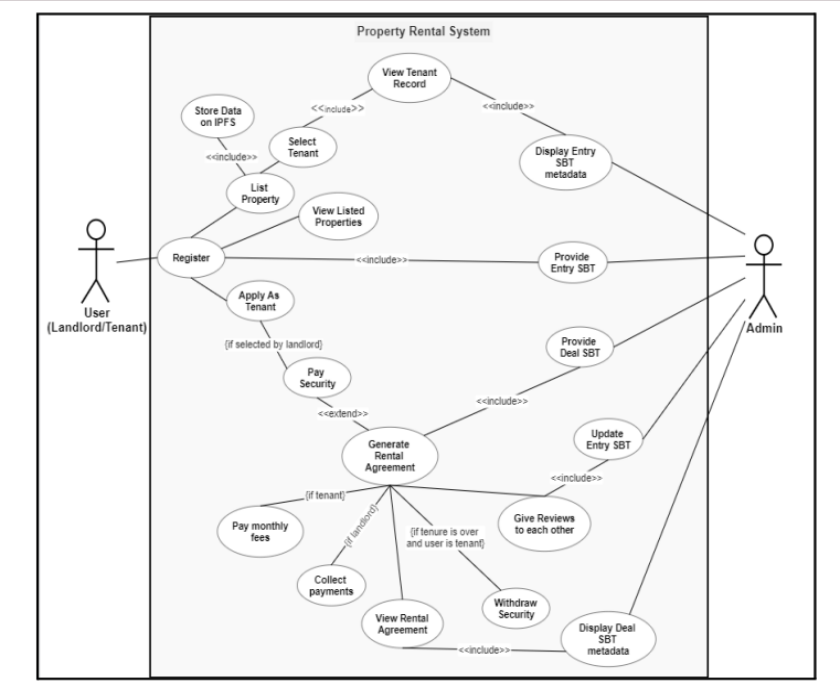


Figure 1: Use Case Diagram

2. Technical Background

2.1. Blockchain

Blockchain is an open, distributed ledger that records transactions between parties efficiently and in a verifiable and permanent manner. The present state of blockchain is often compared to that of the Internet in the mid-1990s, still in its infancy, when its value and potential were not understood. A blockchain is a decentralized and digital system that records transactions or events across multiple devices and locations. It functions as a public ledger of all the activities that the participating parties have conducted. The system uses the consensus of its participants to validate each transaction and once entered, it cannot be altered. One of the primary advantages of blockchain technology is its increased security and transparency, which fosters trust among participants. But its benefits go beyond that, as it

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

also improves speed, efficiency and automation, resulting in significant cost savings. The use of blockchain technology reduces paperwork and minimizes errors, leading to less overhead and transaction costs, and in many cases eliminates the need for intermediaries to verify transactions. Every user has a wallet address associated with them which is used to carry out transactions on the chain. One of the crucial features of blockchain is its transparent nature. The transaction is visible to all the users on the chain and thus any type of fraud or deceit can be caught by the nodes of the chain and such a user is removed from taking part in any other activities of the chain.

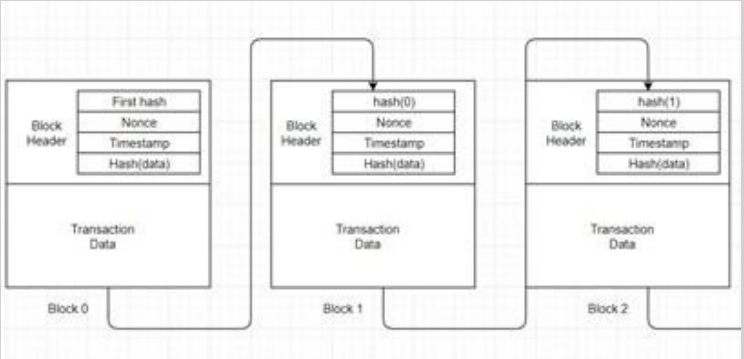


Figure 2: Blockchain Structure

The immutable attribute of blockchain is credited to its structure. The chain is built up by segments called blocks. Every time a transaction takes place, the nodes mine a block, generating a unique hash with its header. This hash is then used as an input in the next block to be minted and thus forms a chain. If any user tries to tamper with the data, they end up with a hash different from the other nodes of the chain. And as soon as such action is detected, the node is removed from the chain. Advantages of using blockchain to pay rent [4]:

1. Increased flexibility: Blockchain-based payments enable digital and mobile transactions, allowing landlords and tenants to make and receive payments 24/7, with no restrictions of traditional banking hours.
2. Easier cross-border payments: - Renting internationally can be challenging, especially when dealing with different currencies. Cryptocurrency allows for immediate, low-cost international transactions, saving time and money for both parties
3. Lower transaction fees: Online rental platforms often impose fees for credit card payments, typically 2.5%-2.9% of the rent amount, paid by the tenant. However, by using cryptocurrency, both parties can avoid these fees and potentially save hundreds or even thousands of dollars over time.
4. Greater privacy for renters: - Blockchain-based payments also provide increased privacy for tenants, as it uses anonymous addresses that change for every transaction. This means that payments do not require personal information, credit card numbers or account numbers, making the transaction untraceable.

2.2. Smart Contracts

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

A smart contract is a paperless digital code that describes a set of contracts on prewritten conditions that the parties of a transaction have decided upon. The parties interacting can set conditions that can launch a series of actions when required or when the conditions are met [2]. The use of smart contracts can automate the process of managing rental properties, enabling efficient and streamlined operations. For example, a smart contract can be used to automatically gather rent payments and distribute them to the landlord, or to automatically initiate the eviction process if a tenant fails to pay rent. Overall, the usage of smart contracts in the real estate industry can enhance the efficiency, safety, and transparency of property transactions and surveillance.

2.3. Reputation

Reputation systems operate by establishing trust relations based on evidence of a party's past behaviour. These systems rely heavily on trust data as the primary form of exchanged information. Such systems maintain mechanisms to monitor and record the reputations and credibility of participants [5].

2.4. Non-Fungible Token (NFT)

A non-fungible token is a unique, digital asset stored on a blockchain, that cannot be replaced by another identical asset. The term "fungible" originates from economics and accounting, referring to items that can be exchanged for equivalent items. Common forms of currency, like cash, are fungible as they are considered of comparable value and can be used as a medium of exchange. NFTs are unique, one-of-a-kind tokens, which makes them non-fungible [6].

2.5. Soulboud Token (SBT)

A soulbound token is a type of non-transferable, non-fungible token that can be publicly verified and represents an individual's credentials, affiliations, and commitments. These tokens are used to track reputation and are added to addresses but cannot be bought or sold [7].

2.6. InterPlanterary File System (IPFS)

The InterPlanetary File System (IPFS) is a decentralized method for sharing and accessing files through a peer-to-peer network. Unlike traditional systems which rely on a centralized server, IPFS utilizes a distributed network of nodes to store and distribute data. This allows for the sharing and access of a variety of content including documents, images, audio and video files, and more, all without the need for a centralized server infrastructure.

2.7. Uniform Resource Identifier (URI)

A Universal Resource Identifier (URI) is a string of characters that identifies a name or a resource on the Internet. URIs can be broken down into two types: URLs (Uniform Resource Locators) and URNs (Uniform Resource Names). A URL, or Uniform Resource Locator, is a subset of URIs (Uniform Resource Identifiers) that identify the location of a resource on the Internet. For example,

https://www.example.com/index.html" is a URL that identifies the resource located at the root of the "example.com" domain, which is an HTML file named "index.html".

3. Related Works

The applications and need for soulbound tokens were introduced by Weyl in 2022 [8]. This paper presents the importance and necessity of a decentralized identity in web3. It depicts how non-transferable tokens can be used to build trust across economic activities and personal brand building. Hildebrandt further worked on establishing soulbound tokens as a method for an authentic decentralized profile in the anonymous network of blockchain accounts [9]. The relationship between user experience and customer reviews has also been studied and evidence of the role of reviews in trust building has been established. Askalidis & Malthouse demonstrated this through an analysis of the number of reviews to the conversions rate in 2016 [10]. The findings indicate about a 270% increase in conversion rate. The equation used includes an exponential deterioration of the weightage of reviews with time. Varma also conducted a study in 2020 to indicate the impact of social media identity in e-commerce and how this is subjected to reviews. A few studies focus on blockchain immutability for credible review systems. In 2018, Wang introduced the utilization of the blockchain ledger to avoid fraudulent and manipulative reviews [11]. It discusses the importance of reviews in the e-commerce segment. The system validates a new review by verifying the identity of purchasers. There are significant studies on the subject of peer-to-peer reputation systems and their importance. Works by Battah in 2021, Mekouar in 2009 and Dennis & Owen in 2015 [5,12,13] describe the disadvantages of the centralized reputation system. These studies show how the current system is prone to attacks, as well as how merchants and other entities can profit from these attacks on centralized servers which manage the stature of all users. The characteristic of transparency and immutability of blockchain makes tampering with such data extremely difficult. An attacker must have access to the majority of the chain, to manipulate data (51% attack), which gets exponentially harder as the number of active nodes on the chain increases. In 2018, Karamitsos implemented blockchain in the field of real estate utilizing its immutability, transparency and security [14]. The paper extends the advantages of decentralization to the real estate sector and proposes the use of smart contracts for securing sensitive data such as rental agreements, ownership papers etc. It further depicts the uses of smart contracts in tackling problems of real estate such as modification of data, lack of trust among parties and need for intermediation. Wang demonstrated a housing rental system using a redactable blockchain. A landlord would submit the documents verified by a trusted third-party organization to the accounting node, which after verifying will list the property to insure credibility. Xue worked on introducing an alliance chain to this system [15]. An alliance chain is a decentralized organizational structure in which multiple organizations can participate. It allows landlords to list their properties on the application, and tenants to submit their applications, which are then verified by the alliance chain. Once the tenants' intentions are cleared, the data is added to the chain.

4. Proposed Method

The present methods of online rental systems in real estate have posed certain problems. For example, there is no way to track the authenticity of the customer or the landlord and hence committing a scam on either end is highly likely. The terms and conditions of the contract may not be clear and can be altered to suit either party. To tackle this, the system will be introduced on blockchain and SBTs will be used for profile reputation with the help of an online rental website. Steps involved:

- Upon successful registration, an Entry Token SBT will be issued to the user who may enter as a tenant or a landlord. This token will be used to track the reputation, number of properties etc. of the user. After this, every time the user tries to log in, it checks for the Entry Token Id associated with the user's wallet address and if the user is blacklisted due to their reputation having a value less than the minimum set in terms and conditions.

```
{
  "name": "Entry Token",
  "image": "Sample String",
  "attributes": {
    "userName": "Sample Name",
    "fatherName": "Sample Name",
    "reputation": 100,
    "reviews": [
      "Sample String"
    ],
    "numberOfReviews": 100,
    "isTenant": false,
    "dealTokens": [
      "Sample String"
    ],
    "permanentAddress": "Sample Addr",
    "profession": "Sample Profession",
    "phoneNumber": "9999999999",
    "emergencyContact": "9999999999",
    "propertiesOwned": [
      "Sample String"
    ],
    "nearestPoliceStation": "Sample Addr",
    "aadharNumber": "Sample String",
    "proofOfAddress": "Sample String",
    "passportPhoto": "Sample String"
  }
}
```


Figure 3: Sample Entry Token URI

- If the user is a landlord, they will have the option to list a property. A separate contract will be created for all individual properties. The property data including information such as property images, rent, location, current reviews etc. are hosted on IPFS and stored in their respective smart contracts. This data is also kept in a centralized server to facilitate the searching of properties using required filters. Changes will be triggered to modify the landlord's Entry Token upon listing a property.

- If the user is a tenant, they can approach the listed property. After successful negotiations and commitments, the tenant pays the security deposit. After this, an SBT called Deal Token will be issued to the tenant via the property contract. The tenant period will also commence henceforth, storing the due dates of rent and the termination period of the contract. The agreement cannot be terminated before the set tenure end date unless both parties agree or if anyone violates the terms and conditions stated. In case the tenant violates the rental agreement, the landlord has the right to revoke the security deposit.
- The tenant can pay the rent and have access to other features of the property as long as the Deal Token associated with the particular property is valid. During this time, the landlord can review

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

the tenant and vice-versa. The reviews will remain on the Entry Token of both users and the contract forever. Since only the members with a tenant-landlord relationship can review each other, the possibility of review bombs is minimized and the credibility is increased.

- After the contract period is over, the Deal Token will be maintained in the Entry Token of the tenant and they can withdraw their security deposit. The tenant record is updated in the property contract.

4.1. Smart Contracts and their Functionalities

1. Admin.sol - Admin.sol is the administrative smart contract. It is used to monitor the market status and provide Entry Token SBT to all new users. The mapping of Token Id to Token URI is used to retrieve user data stored on IPFS. Gas: 2590763 gas; Transaction cost: 2252837 gas.

2. PropertyFactory.sol - PropertyFactory.sol is a smart contract that is used to deploy Property contracts in real time. This contract is accessible only to verified members or users with an Entry Token Id provided by the admin. A user willing to list their property can access the functionality of this contract to upload property data and pay minimal collateral to the admin. This deposit can be liquidated on the violation of the terms and conditions. Gas: 4294054 gas; Transaction cost: 3733960 gas.
3. Property.sol (Template) - Property.sol is a template smart contract. Each property listed on the website has its Property contract deployed with its data in the state variables. This contract is used to mint Deal Token SBTs and provide these to the selected tenant after they have paid the property security money. This amount is stored in the contract and can be retrieved back by the tenant once the rental agreement has successfully ended. The contract contains an array of reviews given to the property and all methods necessary for all other rental transactions. Gas: 3828185 gas; Transaction cost: 3328856 gas.

4.2. Equations

The reputation system is a vital component of the website as it implements accountability. The most recent behaviour has slightly more relevance over past experiences, therefore the equation must give priority to the current review. In the case of rental review history, all conduct is crucial. Thus, the weight of reviews must not degrade [5]. The review system is based on a star rating system with a range of [1,5], where 1 indicates multiple violations and 5 indicates excellent behaviour. The use of $1 - log_5 x$ ensures that each rating holds different graveness and each rating directs to an appropriate degradation of reputation. The equation for determining a user's reputation score is

$$R = \frac{[1.01 \times (R_{max} - \{R_{min} \times [1 - log_5 x]\})] + [R \times (n-1)]}{n} \quad (1)$$

where R is the current reputation score stored on the Entry Token URI. R_{max} is the maximum reputation score allowed. It is set to a constant value of 100. R_{min} is the minimum reputation score possible. It has a constant value of 50. n is the total number of reviews. x is the current rating score given which falls in the range [1,5]. The current rating score is multiplied with a factor of 1.01 to give higher weightage to the latest reviews over older ones [5].

The sum of current The current reputation must not exceed the maximum reputation score allowed. Equation (2) is used to prevent overflow.

$$R \geq R_{max} \Rightarrow R = 100 \quad (2)$$

If a user's reputation score falls below this threshold, their collateral will be liquidated and their low score on the Entry Token will prohibit them from accessing the website in the future. Equation (3) is the liquidation equation.

$$R < R_{min} \Rightarrow R = R_{min} \quad (3)$$

4.3. Performance Analysis

4.3.1. Cost

Securing the data stored is an essential part of the system. This data includes sensitive information such as rental agreements, verification documents, ownership papers, images and property data and the reviews of users and properties. Data storage can have one of three approaches - a centralized cloud system, a decentralized storage IPFS, and storing all data on-chain. While the first approach is the quickest and most cost-efficient, it does carry the disadvantage of being centralized. Between the latter two, the unit of measurement is the gas used. The cost of storing a 256-bit word on the smart contract is 20k gas [16].

Table 1

Difference in cost of storage methods

Storage Method	Gas Used approx.(1kb data)	Cost[17](in ETH)
Storing data directly in smart contract	640,000	0.029356
Storing the IPFS hash of data in the smart contract (string)	85,000	0.003898

While both approaches provide the same immutability and security to the data, the gas used in storing data on-chain is huge, making it an extremely expensive process. Therefore, it is not a viable method to store data such as property images or contract documents, that can be multiple and can have a size of more than 1kb directly on the chain.

4.3.2. Time

Renting or finding a lease property can be a tedious and labour-intensive process. Clients may have to wait several days for a formal agreement, and additional paperwork can prolong the process. The presence of both parties is also required to prevent deceit. This can be reduced by introducing the blockchain. Automating each process reduces the overall time. Using SBT also reduces the time to check backdoor references. decentralized applications further make the concept of long-distance rentals easy and secure. The time taken for the agreement is subject to negotiation between the two parties. The collection of rent, maintenance or other fees can be done by one withdrawal transaction. Reading data that the SBT holds from a blockchain is relatively quick. Other operations such as writing data or making transactions can take longer, depending on the specific blockchain, the speed of the network, and the complexity of the operation. The average time taken to add a block to Ethereum is approximately 14.4 seconds [18].

4.3.3. Security

The decentralized ledger of blockchain offers the advantage of being immutable and transparent. All transactions across the system are visible to members. Most blockchains use consensus algorithms to ensure that the data recorded on the blockchain is accurate and valid. These algorithms require multiple nodes on the network to reach a consensus about the validity of a transaction before it is added to the blockchain. The security of the data helps to transform the network from a trust-based system to a cryptographic-guarantee-based network. Blockchains use cryptographic hashing to secure the data stored on them. Cryptographic hashing involves taking a piece of data and running it through a mathematical algorithm, which produces a unique ”hash” that represents the data. This hash can be used to verify the authenticity of the data without revealing its actual content.

5. Conclusion and Future Scope

In conclusion, the security and time-saving advantages provided by the model can act as a method to improve the current state of online property rental systems. The applications of SBTs in this field use the significance of decentralized identities to tackle real-world problems. The reputation of these decentralized 'souls' is utilized and stored on the blockchain. The network provides security to the data due to its immutable attribute. Uploading data to a peer-to-peer distributed server IPFS instead of any other cloud services ensures that the data used on the website as property information, rent agreement information and profile information is secure from being tampered with. The confidentiality and credibility provided by the review system help prevent attacks such as review bombs, that could have a massive impact on businesses. The model ensures that individuals are saved from the hassle of effort and time the current system takes. Verification of documents and records can be done within minutes using the system. The user SBT system also ensures that the members are safeguarded from attackers that disguise themselves as lawful associates. Such members are detected by the community and discarded from having access to the app again. The attacker will carry the blacklisted non-transferable NFT with his wallet thereafter.

Decentralized identities and their application can help improve the blockchain network. Studies for the use of SBTs in education and healthcare for documents and user data have already shown the advantages of using SBTs. The model presented uses these applications to counter the less-regulated systems of online property renting. Introducing blockchain to the sector can help tackle its problems of speed, safety and fraud. There are several potential areas for future research in this field. One potential direction is the integration of real estate transactions. Another can be the introduction of an automated system to report false reviews to improve their credibility. Another area can be around an automated entity that can verify the documents before they are uploaded on-chain. This can further increase the authenticity of the listed properties and user profiles.

6. References

[1] Misunderstanding And Inconsistency: The State Of Fraud In The Rental Housing Industry – Property Management Companies Lack A Layered And Systemic Approach To Fraud | Apartment Management Magazine. (2018, September 21). Apartment Management Magazine. https://www.aptmags.com/blog/misunderstanding-and-inconsistency-the-state-of-fraud-in-the-rental-housing-industry-property-management-companies-lack-a-layered-and-systemic-approach-to-fraud/

[2] Peranzo, P. (2022, September 1). Smart Contracts in Real Estate: Benefits, Use Cases, and Examples. Imaginovation. Retrieved January 9, 2023, from https://imaginovation.net/blog/smart-contracts-in-real-estate/

[3] Smart Contracts in Real Estate: Benefits, Use Cases, Examples, ???? URL: https://imaginovation.net/blog/smart-contracts-in-real-estate/.

[4] J. Hall, Five Advantages Of Using Bitcoin To Pay Rent, 2022. URL: https://bitcoinmagazine.com/business/five-advantages-of-using-bitcoin-to-pay-rent.

[5] A. Battah, Y. Iraqi, E. Damiani, Blockchain-Based Reputation Systems: Implementa- tion Challenges and Mitigation, Electronics 10 (2021) 289. URL: https://www.mdpi.com/ 2079-9292/10/3/289. doi:10.3390/electronics10030289.
[6] U. W. Chohan, Non-Fungible Tokens: Blockchains, Scarcity, and Value, 2021. URL: https://papers.ssrn.com/abstract=3822743. doi:10.2139/ssrn.3822743.
[7] What are soulbound tokens (SBTs) and how do they work?, 2022. URL: https://cointelegraph.com/news/what-are-soulbound-tokens-sbts-and-how-do-they-work.
[8] E. G. Weyl, P. Ohlhaver, V. Buterin, Decentralised Society: Finding Web3's Soul, 2022. URL: https://papers.ssrn.com/abstract=4105763. doi:10.2139/ssrn.4105763.
[9] F. Hildebrandt, The future of soulbound tokens and their blockchain accounts, Hochschule Mittweida, 2022, pp. 18–24. URL: https://monami.hs-mittweida.de/frontdoor/index/index/docId/13450. doi:10.48446/opus-13450.
[10] G. Askalidis, E. C. Malthouse, The Value of Online Customer Reviews, in: Proceedings of the 10th ACM Conference on Recommender Systems, ACM, Boston Massachusetts USA, 2016, pp. 155–158. URL: https://dl.acm.org/doi/10.1145/2959100.2959181. doi:10.1145/ 2959100.2959181.
[11] C. Wang, W. Jia, Y. Chen, Housing Rental Scheme Based on Redactable Blockchain, Wireless Communications and Mobile Computing 2022 (2022) 1–10. URL: https://www.hindawi.com/journals/wcmc/2022/1137130/. doi:10.1155/2022/1137130.
[12] L. Mekouar, Y. Iraqi, R. Boutaba, Reputation-Based Trust Management in Peer-to-Peer Systems: Taxonomy and Anatomy, in: X. Shen, H. Yu, J. Buford, M. Akon (Eds.), Handbook of Peer-to-Peer Networking, Springer US, Boston, MA, 2010, pp. 689–732. URL: https://doi.org/10.1007/978-0-387-09751-0_24. doi:10.1007/978-0-387-09751-0_24.
[13] R. Dennis, G. Owen, Rep on the block: A next generation reputation system based on the blockchain, in: 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), 2015, pp. 131–138. doi:10.1109/ICITST.2015.7412073.
[14] I. Karamitsos, M. Papadaki, N. B. A. Barghuthi, Design of the Blockchain Smart Contract: A Use Case for Real Estate, Journal of Information Security 09 (2018) 177–190. URL: https:// www.scirp.org/journal/doi.aspx?doi=10.4236/jis.2018.93013. doi:10.4236/jis.2018.93013.
[15] Q. Xue, Z. Hou, H. Ma, H. Zhu, X. Ju, Y. Sun, Housing rental system based on blockchain Technology, Journal of Physics: Conference Series 1948 (2021) 012058. URL: https:// iopscience.iop.org/article/10.1088/1742-6596/1948/1/012058. doi:10.1088/1742-6596/1948/ 1/012058.
[16] D. D. Wood, Ethereum: A secure decentralised generalised transaction ledger, 2014.
[17] etherscan.io, Ethereum Average Gas Price Chart | Etherscan, ????. URL: https://etherscan. io/chart/gasprice.
[18] etherscan.io, Ethereum Average Block Time Chart | Etherscan, ????. URL: http://etherscan. io/chart/blocktime.

2nd International Symposium
on
Securing Next-Generation Systems
using
Future Artificial Intelligence Technologies
SNSFAIT – 2023
25th May 2023
Organized By
Department of Computer Science & Engineering,
Maharaja Agrasen Institute of Technology, Delhi, India
in collaboration with
IEEE ComSoc Delhi Chapter

Risk Monitoring for Confidentiality of Healthcare Data

[1]Ahmed F. Siddiqu1, [1]Aditya J. Paul, [1]Sushruta Mishra

[1]*Kalinga Institute of Industrial Technology, India*

Abstract

The Internet of Medical Things (IoMT), the newest component of the Internet of Things, offers uses for intelligent healthcare systems. It is crucial to the healthcare industry's efforts to improve the accuracy, reliability, and efficiency of electronic devices. IoMT can connect genuine, physical items in the real world for information sharing and communication. Therefore, it is crucial to utilize access control to guarantee the proper use of private data during the data sharing process. In this research paper we have tried to discuss three cutting edge access based control mechanisms in a comparative fashion to understand and overcome the limitations of the classical access control methods. The healthcare industry's future regarding their risk monitoring strategies was also covered in this research paper.

Keywords

Internet-of-Medical-Things(IOMT), Risk Monitoring, Healthcare, Sensors, Privacy, Access Control, SADAC, MLS-ABAC, DF-RBAC-SC

International Symposium on Securing Next-Generation Systems using Future Artificial Intelligence Technologies (SNSFAIT 2023), May XX-XX, 2023, Delhi, India
EMAIL: ahmedfarazsiddiqui1@gmail.com (A. F. Siddiqui); 2005986@kiit.ac.in (A. J. Paul): sushruta.mishrafcs@kiit.ac.in ((S.Mishra)
ORCID: 0000-0003-3929-1100 (S.Mishra)

1. Introduction

The Internet-of-Medical-Things (IoMT) [1], [2] applies the Internet-of-Things (IoT) to the medical and healthcare sectors by using edge computing and big data analytics to identify trends in medical datasets and by connecting medical resources and services via a variety of network services. The introduction of IoMT has made it possible to realize the link between medical personnel, patients, and numerous pieces of medical equipment, giving patients with high-quality equipment assistance at any time and location. To gather health data, sensor devices are placed into the bodies of patients [3, 4, 5]. These gadgets include sensors for weight, blood pressure, temperature, and heart rate. After using this data for analysis, the user selects a pertinent diagnosis scheme for diagnosis based on the analysis' findings. In this manner, a contact-less patient diagnostic working paradigm is described.

Users may perform real-time interactions anytime, anyplace, and from any location to benefit from services like tele-care because of the intelligent nature of IoMT networks and the openness of its related applications. There are clearly issues with information security and privacy due to this instant connectivity. It is crucial to regulate user behavior based on different access levels, or a multi-level access control method. For instance, access to the information in a healthcare network is restricted to authorized entities that meet the access control requirements (e.g., roles and resources).

Access control is a key security feature that ensures that, when certain environmental criteria are met, only authorized subjects have access to particular resources for a given activity [6]. The four components that make up this concept are subjects (such as people or devices), resources or objects (such as web pages, bank accounts, or database records), actions (such as read, write, and execute), and environmental factors (e.g., date, location).

The concepts and principles of access control implementations were introduced by Sandhu et al. in 1994 [6], who also described many models that serve as the foundation for the majority of contemporary access control implementations. [7]

Table 1

Comparison between original access control models

Access control method	Basis of permission allocation	Access control decision-maker	Advantages	Disadvantages
DAC	Access control matrix and access control list (ACL)	Data Owner	Easy to manage, search, authorization.	When faced with complex environments, multiple ACLs are required and difficult to manage.
MAC	Security Level	Central Organization	Meet multi-level security requirements.	Flexibility is poor.
RBAC	Role	Central Organization	Simplify access management.	It is easy to cause character explosions.

2. Objectives of the Paper

The objectives of the study are mentioned below:-

- Determining the security issue with the healthcare industry's data sharing and storage methods as well as the goals of the suggested solution.
- Comparison and defining three different access control models for healthcare.
- Explaining the design of the access control models through a scenario of the healthcare context.
- Discussing about the use, ramifications, and the potential of the suggested strategy in future.

3. Related Works

Most studies focus primarily on two aspects: encryption and access control, in order to prevent unwanted access while guaranteeing data confidentiality, in order to address the issues of privacy leaks created by centralized cloud storage. Conventional access control techniques, like Discretionary Access Control (DAC) [8], put the user first. The data owner creates access policies, and an access control matrix and access control list are used to implement access control (ACL). However only basic environments are appropriate for this technique. Using static ACL, users may quickly query and control personal resources. Nevertheless, this approach is only appropriate in straightforward environments. More ACLs are required for remote environments where user rights frequently change, and it is challenging to maintain. Via the central authority, Mandatory Access Control (MAC) [9] distributes the subject's and object's access permissions in accordance with the security level. As a result, once the security level is established, the access privileges follow suit. Consequently, the largest drawback of strict access control is its lack of flexibility. RBAC [10] is a technique for allocating access privileges to subjects in accordance with their jobs. Limited roles can represent several users, which simplifies the administration of authority between the subject and the object. But the conventional approach to role-based access control is typically centralized, the distribution of user roles lacks fine granularity, and the distribution of roles and permissions is static, which is incompatible with the modern dispersed and dynamic network design. As a result, DF-RBAC was conceptualized, a dynamic and fine-grained role-based access control model that enables resource proprietors to designate roles in a flexible manner while also ensuring the security of those roles [11].

The shortcomings of static authorization in the case of RBAC are efficiently solved by Attraction-based Access Control (ABAC) [12], a fine-grained and dynamic access control mechanism. It is a versatile access control mechanism since it grants users access privileges in accordance with qualities and supports complicated contexts. The National Institute of Standards and Technology (NIST) provided a comprehensive ABAC guide in 2014, and it was updated in 2019 through [13]. This document begins by defining it and outlining the many parts that make it work. Second, it talks about

how ABAC is put into practice within a company. The guide's primary goal is to illustrate the key difficulties that arise throughout such an implementation.

Data confidentiality is not provided by the ABAC paradigm. The MLS-ABAC model, which not only functions using the original workflow of the regular ABAC model but also assures data secrecy, was developed to address this flaw [14]. There ABAC implementations have been used in cloud storage and the Internet of Things [15], [16], [17], [18], [19], [20], where the use of blockchain technology is recurrently considered to prevent data from manipulation or unauthorized access [21], [22], [23].

Similar to ideas like "software as a service" or "malware as a service," security as a service (SECaaS) has gained popularity in recent years [24], [25]. SECaaS is a business strategy in which a service provider incorporates security services into a company infrastructure more efficiently than the majority of people or businesses can do on their own (typically on a subscription basis). In this context, SADAC (Security Attribute-based Dynamic Access Control), a novel method for dynamic access control based on the subject's security attributes, was presented and is primarily meant to be used in business networks and environments linked to ISPs [26].

4. Comparative Analysis of three access control models

In this section, we shall discuss the various features of the following models:

- SADAC(Security Attribute-based Dynamic Access Control)
- MLS-ABAC(Multilevel Attribute-based Access Control)
- DF-RBAC-SC(Dynamic and Fine-grained Role-based access control using Smart Contracts)

4.1.SADAC(Security Attribute-based Dynamic Access Control)

SADAC (Security Attribute-based Dynamic Access Control)[26] is a novel zero-trust network access control scheme that collects (i) multiple security-related attributes about communications (such as ports, IP addresses, data volume, and duration), applications installed and permissions involved, resource consumption (such as RAM, CPU, and battery) and device protection mechanisms (such as screen locking method); (ii) uses these attributes over time to authorize or deny access in a dynamic, continuous manner. and (iii) the ML scheme that supports SADAC (MSNM) presents diagnosis capabilities to allow identifying specific causes for access restrictions. The general operational workflow shown in Figure 1.

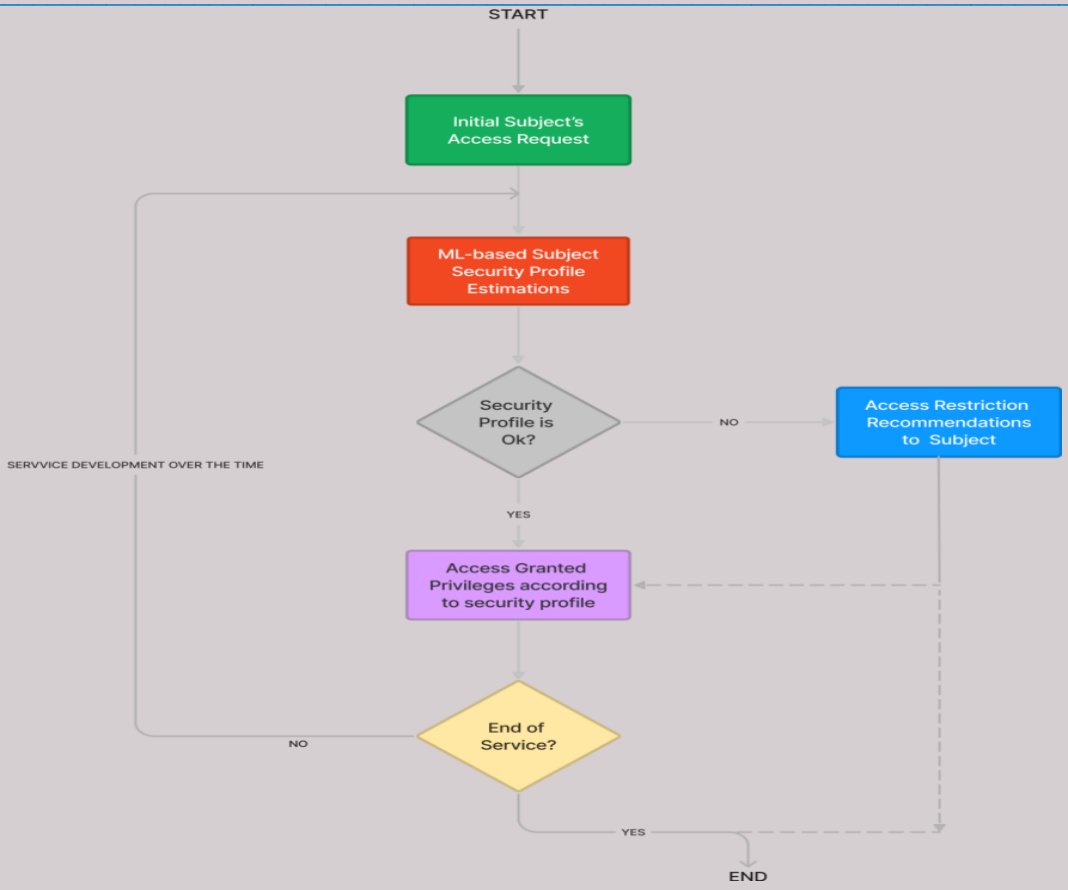


Figure 1: General operational workflow of SADAC

We shall understand this through an example of a device in a WiFi environment: Through an Access Point, each mobile device communicates with the surroundings (AP). This kind of engagement is deceptive. On the one hand, a mobile-network discussion is conducted in order to manage the access itself. Nonetheless, the device offers the network some particular security features or properties. The usage of a SADAC-specific app, which may be downloaded from the ISP network and installed on the device, makes this process easier.

The AP implements the dPEP module, so that:

- It obtains the security features connected to a certain device or user, which can be done either once at the time of association with the AP or repeatedly over time.
- The dPDP will determine the appropriate security profiles for the device/user based on the security features that the AP has forwarded to it.
- If the dPDP determines that a particular device or user is not complying with a security policy, it instructs the AP/dPEP to restrict or even forbid the device from continuing to access the network.

Each mobile device's security profile is estimated by the dPDP module using the related security attributes. Also, it will decide whether to expand or restrict network access. Both the security policy

repository created for the environment and the repository of security attributes for the network's connected devices are taken into account in order to accomplish this [27] [28].

SADAC is capable of diagnostics and is based on security. Additionally, it can be combined with the usage of additional traits and circumstances, whether or not they are security-related, to make more complicated and ambitious access control decisions. Moving the estimation and diagnosis modules to the final devices would also make it simple to expand it in order to strengthen user privacy. The security profile of people and devices should be taken into account as a confidence measure to allow access to ICT environments, despite the sensitive nature of the problem itself and the potential remedies to be adopted.

4.2.MLS-ABAC(Multilevel Attribute-based Access Control)

MLS-ABAC(Multilevel Attribute-based Access Control) scheme[30], the cloud server first determines the data user's security level, then searches the database based on the security level.

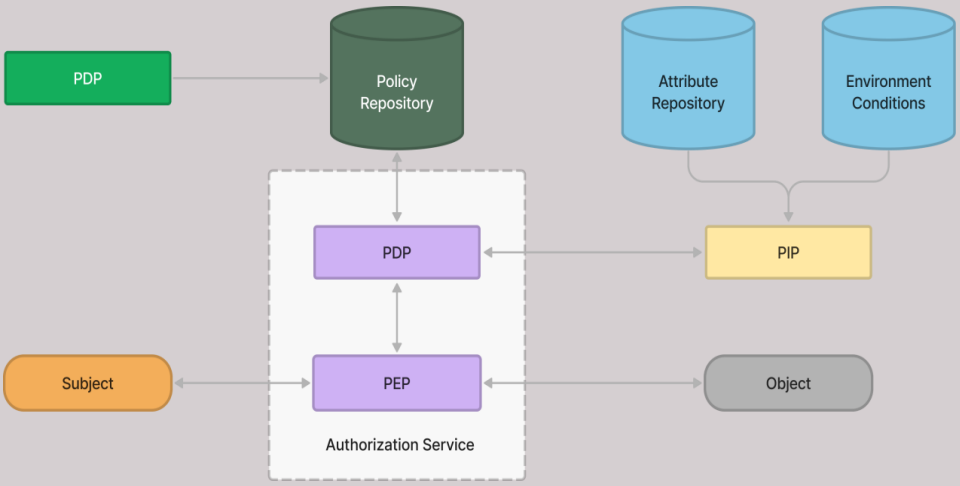


Figure 2: NIST's ABAC model

NIST's ABAC Figure 2 The model is satisfied by the Multi-Level Security ABAC (MLS-ABAC) scheme. This design is effective and is based on the Ciphertext-Policy ABE decryption technique. Furthermore, based on actual application circumstances, only authorized data users are able to decrypt the ciphertext and verify the message's integrity after retrieval.

Anything that is transferred to the cloud that is sensitive (such as medical records) should be securely kept (i.e. encrypted). The data should only be readable by an authorized user who possesses the security key. As a result, incorporating ABAC into Attribute-Based Encryption (ABE) gives us the opportunity to encrypt the information that has been outsourced and shield it from the cloud system

itself. Even if a cloud system were sincere and curious, it would be impossible for it to access the private data using ABE Figure 3 depicts the MLS-ABAC architecture.

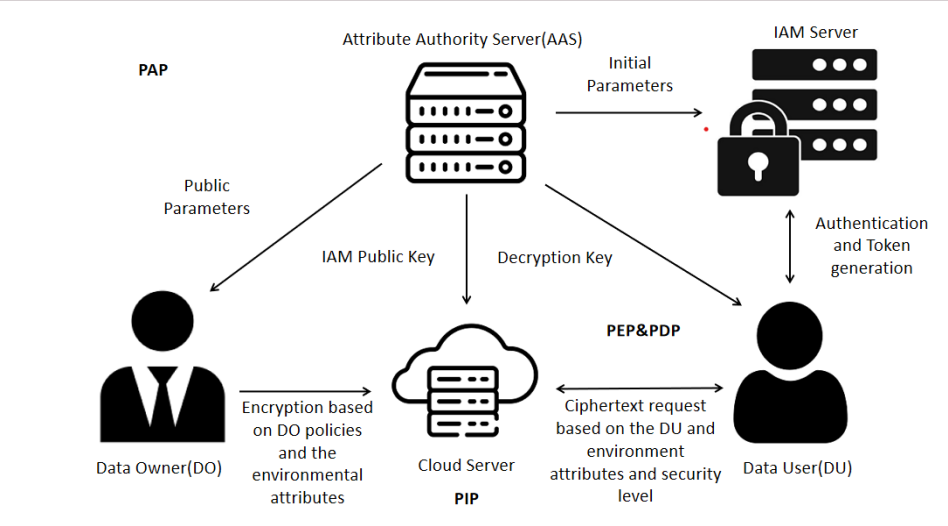


Figure 3: MLS-ABAC model

- Attribute Authority Server (AAS) - It is a dependable party that creates both the secret keys and system parameters for the data users.
- Identity and Access Management Server (IAMS) - Based on sets of security levels, the Identity and Access Management Server (IAMS) generates tokens for users corresponding to their access security level. Notably, these sets are created, deleted, and updated by AAS, who then submits them to the IAMS.
- Cloud Server (CS) - In order to store ciphertexts that are offloaded from IoT data providers, the Cloud Server (CS) functions as a repository. As a data consumer, CS also verifies the authenticity of the tokens it has obtained from another IoT device. The defined predicate functions are then used by CS to determine whether access should be permitted.
- Data Owner(DO) - By specifying a security level, Data Owner (DO), an IoT data producer, can share a sensitive message with consumers. In order to achieve this, it creates a ciphertext that also contains certain metadata. Consequently, in order to stop data leaking, the DO selects the ciphertext's security level and uploads the ciphertext together with the corresponding security level to CS.
- Data User(DU) - A lightweight IoT device called Data User (DU) wishes to read data from the CS using its credentials (i.e., data consumer). It communicates the token to CS after requesting one from the IAMS in order to accomplish this. The DU can get the ciphertext if it successfully completes the verification process. Lastly, the DU can decrypt the ciphertext to discover information if its properties meet the access policy. Otherwise, it learns nothing.

We shall explain the methodology with an example of a hospital: In Figure 4, the set of static characteristics is {UserType, HospitalId}, while the set of dynamic attributes is {Section, Time}. The four security levels in our suggested paradigm are Top Secret, Secret, Confidential, and Unclassified, with User A belonging to Security Level Secret. User A belongs to the security level Top Secret, User B and User C to Secret, User D and User E to Confidential, and User F to Unclassified. Users are given

this partial order hierarchy by the system administrator (in this case, IAMS), who also notifies them when the system's rules change[29].

In this system, the entity User E has the ability to download information that has been uploaded with Confidential and Unclassified security levels, as well as to decrypt information that has been encrypted with User E's static and dynamic properties. Additionally, if User E's security level is raised to Secret, it will be able to download any material posted to security levels Secret and lower and decode any information that has been encrypted using the static and dynamic characteristics of the application. According to the aforementioned situation, the system administrator can easily grant User E access to the wrapped data that has been uploaded to the Confidential security level.

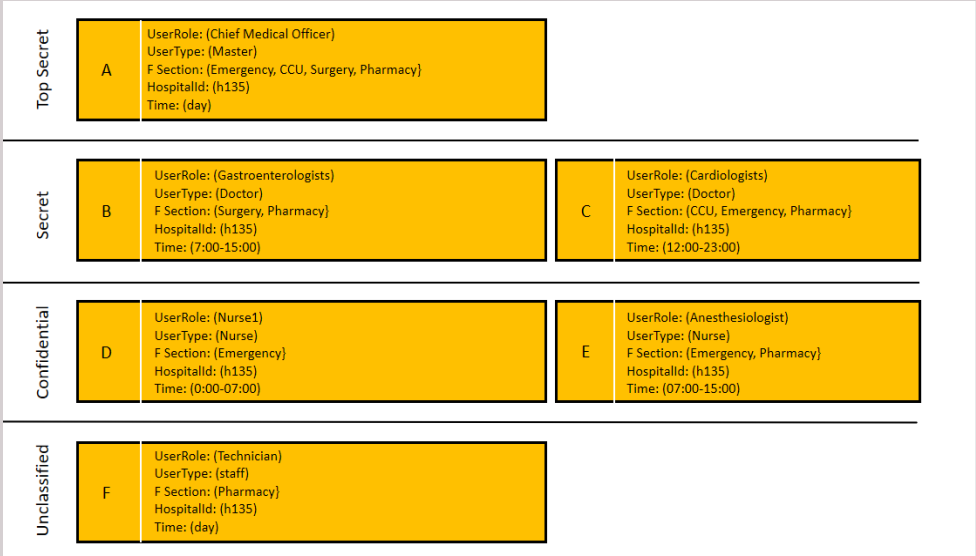


Figure 4: Multi-level Security with ABAC Example

The management of access control is made easier and the security and privacy of IoT systems are improved by adding a security level verification before partial decryption. MLS-ABAC is effective when lightweight alternatives to heavyweight functions are used, such as the suggested lightweight CP-ABE[30], lightweight Ascon-hash, and Ascon[29],[31], authenticated encryption algorithms. In addition to taking security level verification and dynamic attributes into account, MLS-ABAC uses an authorized encryption strategy to safeguard the data integrity of the plain text in the event of outsourced decryption. As an added bonus, it formalizes the suggested access control model by including a conceptual and formal model as well as performance metrics to illustrate the use-case and implementation of the MLS-ABAC scheme.

4.3.DF-RBAC-SC(Dynamic and Fine-grained Role-based access control using Smart Contracts)

Using DF-RBAC-SC(Dynamic and Fine-grained Role-based access control using Smart Contacts) [32] [33] [34] we can verify the user-role assignments of organizations in a secure way in a cross-organizational setting. DF-RBAC-SC is a smart contract-based authentication mechanism that is suitable for the trans-organizational exploitation of roles, in order to accomplish these objectives. A challenge-response protocol and a smart contract make up the two primary components of the DF-RBAC-SC. The user-role assignments are made using the smart contract (SC), which is subsequently broadcast on the blockchain. Figure 5 depicts the DF-RBAC-SC access framework.

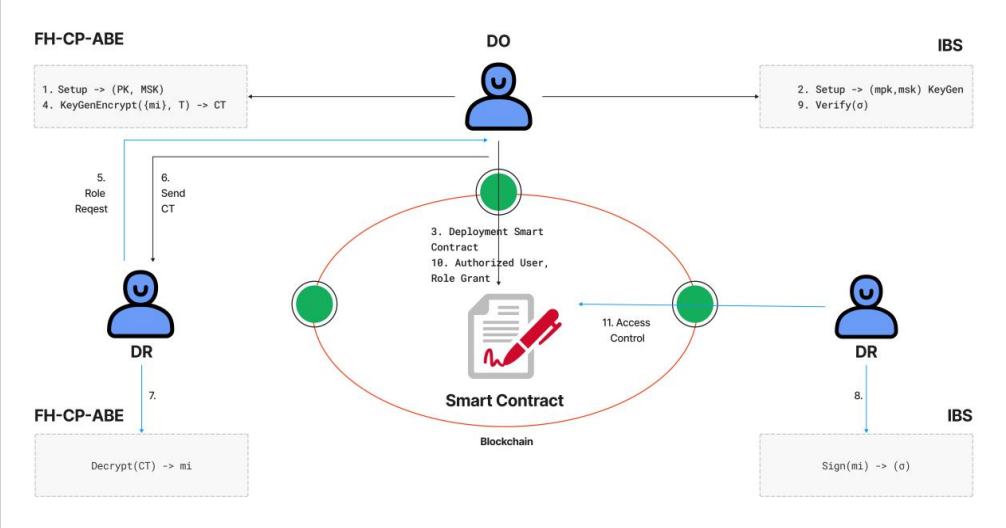


Figure 5: Flow chart of access framework of DF-RBAC

We shall explain the methodology using an example of a hospital: Imagine that a hospital (A-Hospital), a role-issuing entity, wants to administer a "patient" role for its patients. The RBAC-smart SC's contract would then be made and published on the Ethereum network. Utilizing the clever contract, it may carry out a command to add a user (patient) to the database. In addition to the role that will be assigned to the patient, A-Hospital will also include the patient's externally owned address (EOA), the role's expiration date and any other personalizations. The user then claims to have the patient's position from A-Hospital and asks for a service from a service-providing company such as a pathology lab.

The service provider(pathology lab) checks the smart contract made by A-Hospital based on the claim and uses that to verify all the facts it requires. Following a thorough review of all the information, the hospital can use the challenge-response protocol to determine whether the unknown user has access to the corresponding EOA that was given the role, conclusively demonstrating that the unknown user was, in fact, given a patient role by A-Hospital. Because the information the hospital needs is available publicly or is already in the user's possession, it is important to note that the hospital does not need to be aware of the role in advance and is not required to enter into any agreements with or contact A-Hospital on behalf of the patient who received the role.

It is suggested to use DF-RBAC-SC with cryptography. This framework enables the resource owner to assign user responsibilities in a flexible manner. At the same time, it may confirm the roles

that have been allocated, carry out the function of accessing the activity log for security audit purposes, and guarantee the security of the entire architecture. It has demonstrated through safety and experimental research that our framework is workable.

5. Future scope of healthcare informatics

The digital transformation has only steadily and graciously affected the medical industry [35].High-end sensors and other similar devices are being used in smart hospitals and related environments to generate and gather massive volumes of extremely complicated medical data in real-time with demanding data processing needs. The growth of AI and the internet of medical things (IoMT) as well as the advent of digital health care reforms has been closely related. These systems, also known as health care IoT, are made up of a networked arrangement of medical devices—mostly sensors and small-scale devices—and software programmes that enable communication across various software-based healthcare systems [36].

When it comes to managing medical records, the health care sector has already experienced a significant level of digitization in the form of electronic health records (EHR) [37]. The bulk of the pharmaceutical and related sectors already use digital datasets or cloud-based systems to start electronic record-keeping for massive amounts of organizational and research data. The term "edge computing" (EC) is a new one, but it has the ability to fully address the needs relating to system reaction times and data privacy protection [38]. It serves as a framework for adding privacy protection and a means for lessening load in server-based solutions. The "man-in-the-middle" function is often performed by the edge server, which also serves as an instantaneous query and data management system and only connects to the server for high priority or high complexity tasks [39]. Many attempts are being undertaken to study and broaden EC's reach into closely linked and related sectors, wherever there is potential for distributed architecture, as a result of substantial research being done in this area. As a result, many distributed learning models have been developed, including Edge intelligence [40], distributed learning, and federated learning.

6. Conclusion

These days, ICT security is of the utmost importance. The upcoming use of technologies like IoT(Internet of Things) and BYOD(Bring Your Own Device) will make this scenario even worse. The security profile of the subjects in healthcare system (devices/users) is dynamically evaluated in order to allow, limit, or refuse access to services and resources of the network over time, in light of the growing relevance and impact of security threats. We intended to provide a deep insight into some of the access control models that can be used to identify risks of data leak and privacy loss in the healthcare industry as the data is sensitive, personal and very detailed.

We can conclude that among DAC, MAC, RBAC we prefer RBAC as it is a great combination of both DAC and MAC and it gives us the best of both worlds. RBAC is an intermediate model between MAC and DAC, as it provides greater flexibility than MAC while it is more manageable than DAC. This has boosted the acceptance of RBAC in the corporate world. Hence we discussed the three most suitable models under RBAC i.e. SADAC, MLS-ABAC, DF-RBAC-SC for a healthcare system that can help us protect sensitive information and identify risks and deal with them.

7. Acknowledgements

I would like to extend my heartfelt appreciation to everyone who helped make this research effort a success. First and foremost, I would like to express my sincere gratitude to Dr. Sushruta Mishra who served as my research guide for the study for all of his tremendous support. Also want to express my gratitude to my co-author Ahmed Faraz Siddiqui, who worked with me on the studies and paper preparation.

8. References

[1] Kumar P, Gupta GP, Tripathi R. An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks. Comput Commun 166. (2021):110-124.
[2] Kumar M, Verma S, Kumar A, Ijaz MF, Rawat DB, et al. ANAF-IoMT: A novel architectural framework for IoMT-enabled smart healthcare system by enhancing security based on RECC-VC. IEEE Trans Ind Inform 18(12). (2022):8936-8943.
[3] Wang R-B, Wang W-F, Xu L, Pan J-S, Chu S-C. Improved DV-hop based on parallel and compact whale optimization algorithm for localization in wireless sensor networks Wirel. Netw. (2022):1-18.
[4] Chen C-M, Chen Z, Kumari S, Lin M-C. LAP-IoHT: A lightweight authentication protocol for the internet of health things Sensors 22(14). (2022):5401.
[5] Liang L-L, Chu S-C, Du Z-G, Pan J-S. Surrogate-assisted Phasmatodea population evolution algorithm applied to wireless sensor networks Wirel. Netw. (2022):1-19.
[6] Sandhu RS, Samarati P. Access control: Principle and practice. IEEE Commun Mag 32(9). (1994):40-48.
[7] Benantar M. Access control systems: Security, identity management and trust models: Springer. (2006).
[8] Qihua W, Hongxia J. Data leakage mitigation for discretionary access control in collaboration clouds. Proceedings of the 16th ACM symposium on access control models and technologies. (2011), pp. 103-112.
[9] Sven B, Stephen H, Ahmad-Reza S. Flexible and fine-grained mandatory access control on android for diverse security and privacy policies 22nd {USENIX} security symposium ({USENIX} security 13). (2013), pp. 131-146.
[10] Hongjiao L, Shan W, Xiuxia T, Weimin W, Chaochao S. A survey of extended role-based access control in cloud computing. In: Proceedings of the 4th international conference on computer engineering and networks: Springer. (2015), pp. 821-831.
[11] Liu D, Dong A, Yan B, Yu J. DF-RBAC: Dynamic and fine-grained role-based access control scheme with smart contract. Procedia Comput Sci 187. (2021):359-364.
[12] Hu Vincent C, Richard KD, Ferraiolo David F, Jeffrey V. Attribute-based access control Computer 48(2). (2015):85-88.
[13] Hu VC, Ferraiolo D, Kuhn R, Schnitzer A, Sandlin K, Miller R, Scarfone K. Guide to attribute based access control (ABAC) definition and considerations. NIST Spec Publ 800-162. (2019).
[14] Aghili SF, Sedaghat M, Singelée D, Gupta M-A. MLS-ABAC: Efficient Multi-Level Security Attribute-Based Access Control scheme. Future Gener Comput Syst 131. (2022):75-90.

[15] Hao J, Huang C, Ni J, Rong H, Xian M, Shen X. Fine-grained data access control with attribute-hiding policy for cloud-based IoT. Comput Netw 153. (2019):1-10.
[16] Ravidas S, Lekidis A, Paci F, Zannone N. Access control in internet-of-things: A survey. J Netw Comput Appl 144(15). (2019):79-101.
[17] Kayes ASM, Rahayu W, Watters P, Alazab M, Dillon T, Chang E. Achieving security scalability and flexibility using fog-based context-aware access control. Future Gener Comput Syst 107. (2020):307-323.
[18] Aftab MU, Oluwasanmi A, Alharbi A, Sohaib O, Nie X, Qin Z, Ngo ST. Secure and dynamic access control for the Internet of Things (IoT) based traffic system PeerJ Comput. Sci. (2021):1-26.
[19] Bhatt S, Pham TK, Gupta M, Benson J, Park J, Sandhu R. Attribute-based access control for AWS Internet of Things and secure industries of the future. IEEE Access 9. (2021):107200-107223.
[20] Zhang Y, Yutaka M, Sasabe M, Kasahara S. Attribute-based access control for smart cities: A smart-contract-driven framework. IEEE Internet Things J 8(8). (2021):6372-6384.
[21] Lyu Q, Qi Y, Zhang Z, Liu H, Wang Q, Zheng N. SBAC: A secure blockchain-based access control framework for information-centric networking Netw. J Comput Appl 149. (2020):1-17.
[22] Ghaffari F, Bertin E, Crespi N, Behrad S, Hatin J. A novel access control method via smart contracts for internet-based service provisioning. IEEE Access 9. (2021):81253-81273.
[23] Liu Y, Qiu M, Liu J, Liu M. Blockchain-based access control approaches, 8th IEEE International Conference on Cyber Security and Cloud Computing, CSCloud/7th IEEE International Conference on Edge Computing and Scalable Cloud, EdgeCom. (2021), pp. 127-132.
[24] Carvalho M SE. CaaS-security as a service. Inf Syst. (2011):20-24.
[25] Sharma D, Dhote CA, Potey M. Security-as-a-service from clouds: A comprehensive analysisInt. J Comput Appl 67(3). (2011):1-4.
[26] García-Teodoro P, Camacho J, Maciá-Fernández G, Gómez-Hernández JA, López-Marín VJ. A novel zero-trust network access control scheme based on the security profile of devices and users. Comput Netw 212. (2022):109068.
[27] Rose S, Borchert O, Mitchell S, Connelly S, Zero Trust. Architecture. NIST Spec Publ. (2020):800-207.
[28] Garvis J, Chapman JW, Zero Trust. Security, an enterprise guide A press: Berkeley, CA. (2021).
[29] Aghili SF, Sedaghat M, Singelée D, Gupta M. MLS-ABAC: Efficient Multi-Level Security Attribute-Based Access Control scheme. Future Gener Comput Syst 131. (2022):75-90.
[30] Secure Schemes for Secret Sharing and Key Distribution Technion – Israel Institute of Technology: Faculty of Computer Science. (1996).
[31] Dobraunig C, et al. Ascon v1. 2 submission to nist, NIST round, Volume 2. (2019).
[32] Cruz JP, Kaji Y, Yanai N. RBAC-SC: role-based access control using smart contract. IEEE Access 6. (2018):12240-12251.
[33] Guide to attribute based access control (abac) definition and considerations [Draft]. NIST Spec Publ 800(162). (2013):1-54.
[34] Liu D, Dong A, Yan B, Yu J. DF-RBAC: Dynamic and fine-grained role-based access control scheme with smart contract, procedia computer science, Volume 187. (2021), 359-364,ISSN 1877-0509.
[35] Beranger J, Rizoulieres R. The digital revolution in health: John Wiley & Sons. (2021).
[36] Elayan H, Aloqaily M, Guizani M. Digital twin for intelligent context-aware IoT healthcare systems. IEEE Internet Things J 8(23). (2021):16749-16757.

[37] Yadav P, Steinbach M, Kumar V, Simon G. Mining electronic health records (EHRs) a survey. ACM Comput Surv 50(6). (2018):1-40.

[38] Khan WZ, Ahmed E, Hakak S, Yaqoob I, Ahmed A. Edge computing: A survey. Future Gener Comput Syst 97. (2019):219-235.

[39] Shi W, Cao J, Zhang Q, Li Y, Xu L. Edge computing: Vision and challenges. IEEE Internet Things J 3(5). (2016):637-646.

[40] Gupta R, Reebadiya D, Tanwar S. 6G-enabled edge intelligence for ultra -reliable low latency applications: Vision and mission. Comput Stand Interfaces 77. (2021):article 103521.

Book Chapter

2nd International Symposium
on
Securing Next-Generation Systems
using
Future Artificial Intelligence Technologies
SNSFAIT – 2023
25th May 2023
Organized By
Department of Computer Science & Engineering,
Maharaja Agrasen Institute of Technology, Delhi, India
in collaboration with
IEEE ComSoc Delhi Chapter

An efficient heart disease prediction model using particle swarm optimized ensemble classifier model

[1]Priyanka Dhaka and [2]RuchiSehrawat[3]Priyanka Bhutani

[1]Research Scholar Guru Gobind Singh Indraprastha University and Assistant professor,

Maharaja Surajmal Institute, GGSIPU Janakpuri Delhi 110058

pridhaka92@gmail.com

[2]Assistant Professor

University School of Information and Communication Technology, GGSIPU Delhi

ruchi.sehrawat@ipu.ac.in

[3]Assistant Professor

University School of Information and Communication Technology, GGSIPU Delhi

priyanka.b@ipu.ac.in

Abstract

Nowadays, the leading cause of death worldwide is heart disease. Since it takes expertise and in-depth knowledge to predict cardiac disease, it is a challenging task. Recently, Internet of Things (IoT) technology has been used in system of healthcare to gather sensor data for the prediction of cardiac disease. The analysis of heart disease has earned the attention of many researchers, however the findings of these diagnoses are rarely accurate, and protecting the data is also difficult. By combining the classifier, a PSO optimized ensemble classifier model was created to overcome this issue. The IoT nodes in this scenario are scattered throughout the environment and initially the patient data is collect to enable the health prediction and healthcare monitoring. Due to the growth of encryption-based cloud data protection, the data is secured once it has been gathered. Therefore, the data is transmitting to the cloud server securely. The enabled optimization aids in fine-tuning the classifier's hyper- and fusion-parameters. The PSO optimized ensemble classifier method accomplished accuracy, F-measure, sensitivity, and specificity of 97.62%, 97.75%, 97.97%, and 97.66% for the heart disease dataset and for Kaggle dataset 96.71%, 97.33%, 97.99%, and 97.25% is attained.

Keywords: Heart disease prediction, Ensemble classifier model, deep CNN, BiLSTM, Particle swarm optimization

1. Introduction

Health is not only the lack of disease; it's a state of total mental, well being and physical.People's desire for a better life includes a vital aspect of health. Due to a variety of problems, such as subpar healthcare services, significant differences between urban and rural areas, and a scarcity of doctors and nurses during the most challenging periods the global health issue has unfortunately produced a conundrum [5].

Health conditions can be diagnosed diagonally and prevented in their early stages with the right care. With the use of various diagnostic tools like CT, MRI, and PET, abnormalities that exist within our bodies might be discovered rapidly. The unpredictability of the development of progressive illnesses has been a healthcare systems problem, and there is a strong need for funds for the whole thing from hospital beds to doctors and nurses as a result of the world's enormous population growth [1]. One of today's most essential and difficult health issues is the automatic detection of heart disease [2].

Early disease detection and diagnosis are made possible with remote patient monitoring, and the medical history of the patient can be saved in a database for future exploit. Since medical servers and databases contain medical records, they are essential for getting the relevant patient's health records [4]. A wide number of healthcare applications are projected to benefit from IoT and wearable monitoring devices. The IoT was quickly adopted by the healthcare sector [8, 9] because incorporating IoT features into medical devices improves both the quality and efficiency of services. A heart disease monitoring device that uses IoT technology may record and transfer the patient's physical information in real time to a hospital centre located far away. [10]. The human body's most vital organ is the heart. Heart disease is a serious health problem [6]. Data mining and machine learning (ML) approaches shorten computation times and costs. One of the applications of ML is the identification of medical conditions and interventions to improve a patient's daily life. Heart disease is typically thought to predominantly afflict the elderly, although it is actually spreading more widely among all age groups.

- ***Ensemble classifier model:*** The ensemble classifier model is developed by the standard hybridization of deep CNN and the BiLSTM which effectively learns the features and makes the predictions more accurate.
- ***PSO optimized ensemble classifier model:*** PSO optimization effectively tunes the parameters by increasing the velocity minimizes the computational time and provides the optimized output.
- The optimization tuned the ensemble classifier effectively and makes the predictions with less computational complexity.

The manuscript is written as follows in accordance with its organizational structure: Existing efforts and their methodology are described in Section 2. The system model for heart disease detection is explained in Section 3. The interpretation of the particle swarm optimization is in

Section 4. In part 5, the results of heart disease detection are provided, in section 6, the conclusion is provided.

2. Literature review:

A IoT based disease prediction model utilized the MDCNN classifier was introduced by Mohammad Ayoub Khan [2]. Although this method produced better performance and accuracy, it was unable to encode object location and orientation. An ensemble deep learning technique was reported by Farman Ali et al. [3]. This technique produced better dimensionality and accuracy, however it has an over fitting problem. A decision tree model was created by Shakila Basheer et al.[4] for the use of a continuous and patient monitoring remote system in the early heart disease prediction process.Although this approach was simple to comprehend and implemented, it was too slow to be effective. A smart healthcare system for IOT was presented by Md. Milon Islam et al. [5] that can track a patient's vital signs in real-time. Although it was quite expensive, this approach produced high sensitivity and quick response times. An effective neural network with convolutional layers was created by Aniruddha Dutta et al. [5] to categorize clinical data that was highly class-imbalanced. The test accuracy of this technique was higher, but the classifiers had poor recall values, which is the actual positive rate for detecting coronary heart disease. KVV Reddy et al. [14] presented a Correlation-based feature selection method was presented for feature extraction that detected coronary heart disease and three single classifiers and three ensembles classifier were used for selecting the features that performed better and go through the overfitting problem. Osman taylam et al.[15] adaptive neuro-fuzzy and statistical approach naïve bays classifier, adaptive neuro-fuzzy inference system that predicted the risk factors of cardiovascular disease with less error rate the output probability is not trustable.

2.1 Challenges

- A difficult task for heart disease prediction is extracting pertinent and significant information from the data.
- Another difficulty for machine learning (ML)-based systems is choosing useful feature weights after selecting features from structured data.
- Partitioning a severely unbalanced dataset presents many difficulties and introduces biases that cannot be avoided in the performance of a classifier..

3. System model of smart healthcare

The PSO optimized ensemble classifier system is composed of three operational phases: accurate disease prediction utilising the acquired data, device and patient identification using an encryption method on a modified ECC diffi-Huffman algorithm (EDH), and data collection using dispersed IoT nodes.

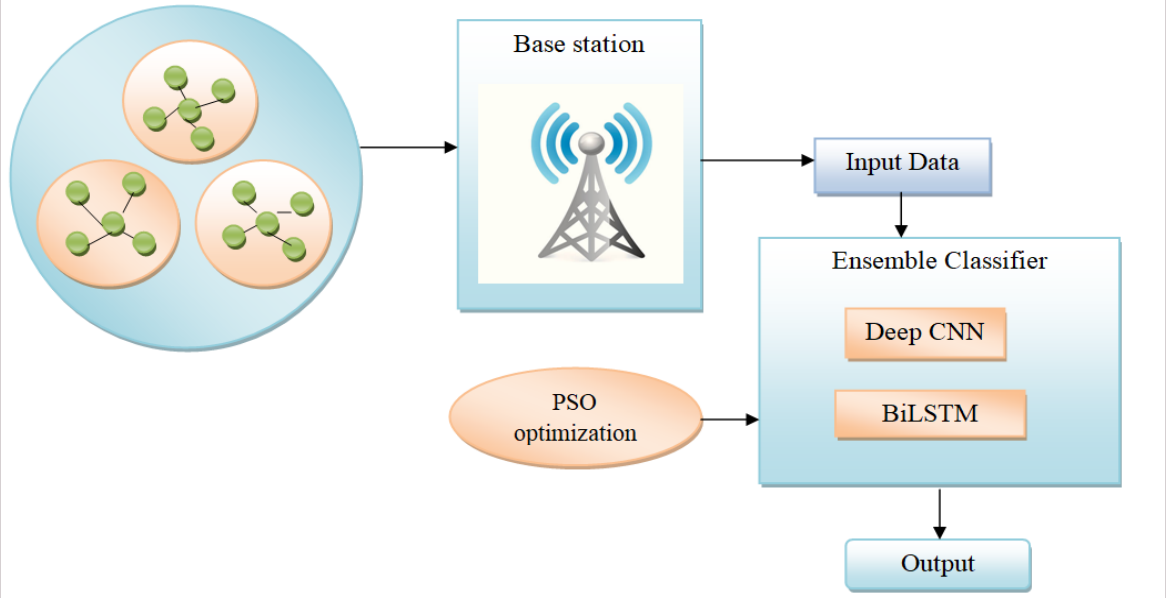


Figure 1: Diagrammatic representation of heart disease prediction

In order to provide health status prediction, IoT nodes scattered across the sensing environment to acquire patient data in step one, as shown in figure 1. The advancement of encryption-based cloud data protection ensures that the data is safe from hackers after it has been collected. As a result, the data is securely sent to the cloud server, where the clinician would obtain the patient's medical records and examine the information to offer a diagnosis suggestion.

3.1 Data Acquisition and Authentication

Data acquisition is the process of compiling information from all pertinent sources. It is essential to protect the patient information gathered during the monitoring phase since it often helps clinicians to identify patients correctly. To prevent unwanted users from accessing the data stored in the cloud, the collected data must be encoded. For the purpose of securely updating patient medical records on the cloud server, throughout the authentication process, the information is verified and approved. The previously published and current modified EDH is used to encrypt medical reports. This technique generates a key, produces a signature at the sender end, and validates the signature at the receiver end. The acquired data is then securely transferred to the target via a modified EDH, which the authorized clinician decrypts to offer the patients a diagnosis

4. Ensemble classifier model for disease prediction:

To train the preprocessed heart disease data, the deep CNN and BiLSTM are combined. in the Ensemble classifier. Due to the combined performance, Ensemble classifier model achieves superior accuracy and efficiency against the deep learning model.

4.1 Deep CNN model

Heart disease is predicted using the deep CNN. It is a basic feed-forward neural networks that have been trained using a PSO optimized ensemble classifier. Figure depicts the illustrated representation. It is used to categorize the data and automatically identify the important features. Four layers are presented in the Deep CNN, and they are outlined below.

i) Convolutional layer:

A convolutional layer produces several feature maps by extracting a range of local patterns at each small location in the input space using a set of convolutional filters.

ii) Pooling layer:

The pooling layer creates a single output from local regions of the convolution feature maps in order to down-sample the feature maps produced from the earlier convolutional layers.

iii) Fully-connected layer

The outcomes from earlier layers in this layer are integrated to provide the activation function is a sigmoid function, depending on whether the final feature representations are for classification or regression**.**

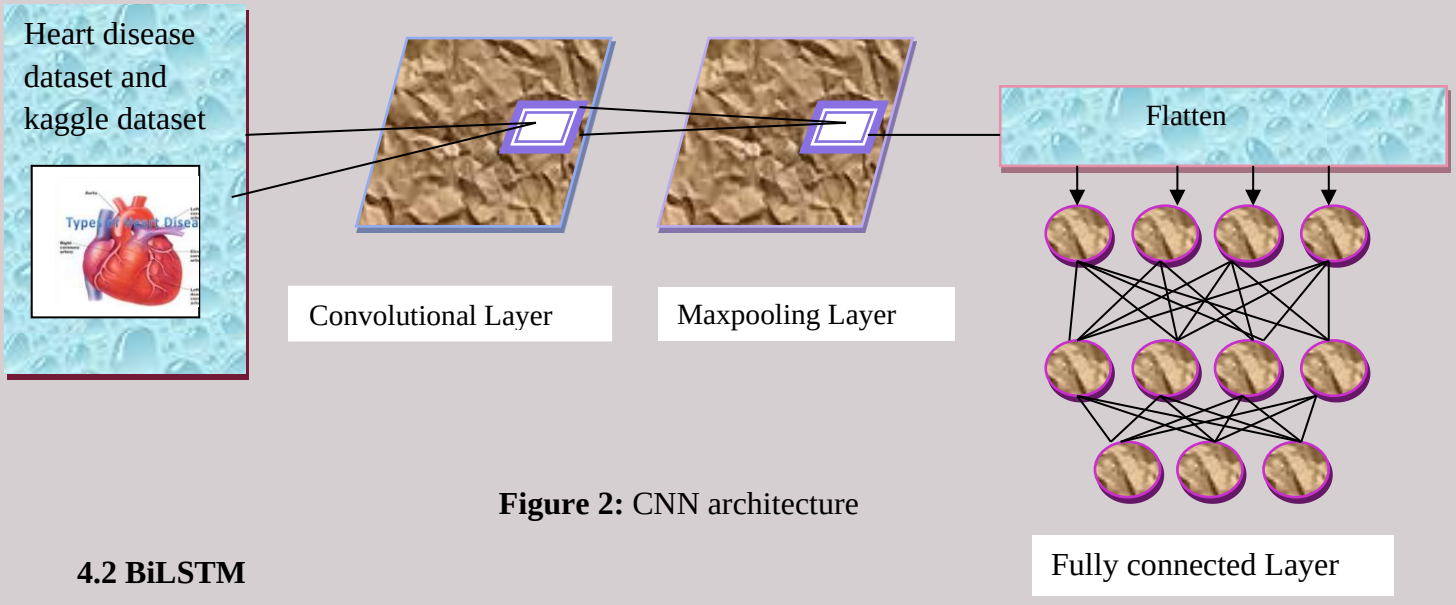


Figure 2: CNN architecture

4.2 BiLSTM

A brand-new technique called the BiLSTM has emerged in recent years. The heart disease and kaggle database are subjected to both forward and backward analysis in this method. A Bi-

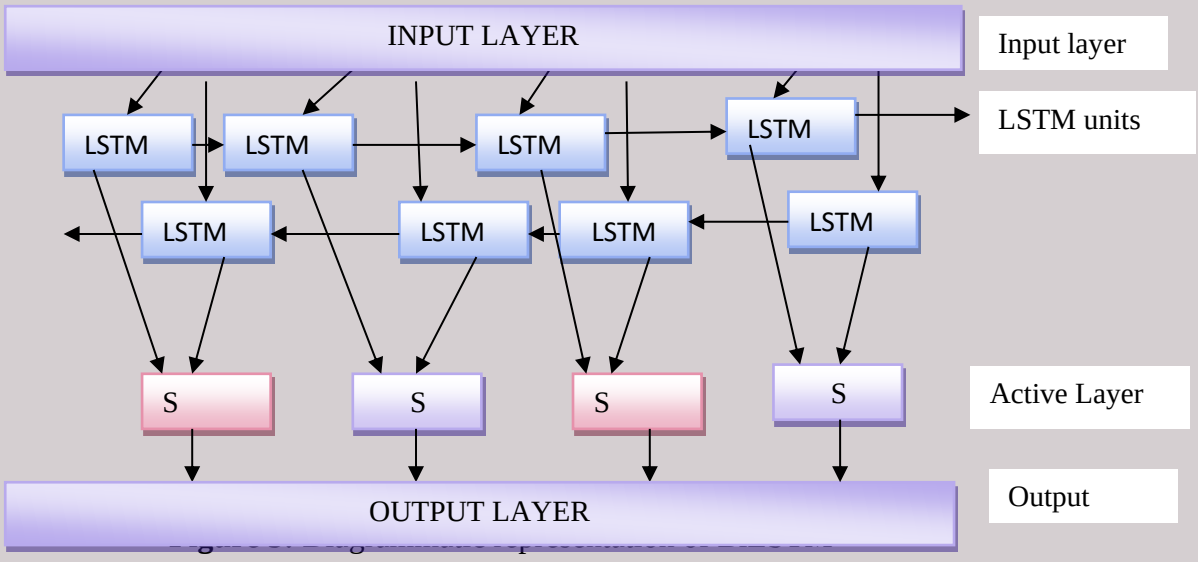
LSTM has three layers. Input gates, forget gates, and output gates are all there in the memory block that is located in the hidden layers. These gates regulate both the features and the amount of the extracted data. Depending on the forget gate and the input gate the most recent information will be store in a cell state, also the outdated data will be removed. The output gate completes the output of the network model after the end of the cell state update. This makes it possible for the output of Bi-LSTM units to generate a representation that considered both past and future data automatically.

$$HF = u(e_1 y + e_2 H_{F-1} + S_a) \quad (1)$$

$$HB = u(e_3 y + e_5 H_{B+1} + S_b) \quad (2)$$

$$HO = h(e_4 H + e_6 H_B + S_c) \quad (3)$$

HF denotes the forward layer, HB denotes the backward layer, HO denotes the output layer, u is an update function for the cells' state vectors in the Bi-LSTM block's hidden layers, h denotes the output layer activation function, weight is denoted as e, bias is denoted as S



4. Particle swarm optimization

Position and velocity are the main characteristics of the PSO algorithm's particles. In order to determine the value of the objective function for each particle position, a population of particles is randomly placed anywhere inside the search region. The initial values of the velocities are

set to zero or chosen at random inside predetermined bounds. Therefore, if U_j are the velocities of the j particles, then a starting setting is possible as follows,

$$U_j = 0 \qquad j = 1,2,....m \tag{4}$$

where, m denotes the population size.

The initial velocities can be assigned in a variety of ways. The velocity of each particle is then updated using the proper formula. These velocity measurements are used to update the particle positions. After that, it is decided if the objective function has improved. The values of the particle positions are considered as the new positions if improvements are made. Additionally, the swarm's global optimal position for each particle is updated. Until a specified convergence condition is fulfilled, this process is repeated. After that, the process is terminated and the answers are given. Then provide the precise algorithm for updating the velocity and position values.

The following equation, applied at time s, yields the velocity of each particle. In reality, the values of s correspond to the process's iteration or generation numbers, starting at $s = 0$.

$$U_j^{(s+1)} = U_j^{(s)} + dp_1 \bullet \left[Y_{pbest}^{(s)} - Y_j^{(s)}\right] + cp_2 \bullet \left[Y_{gbest}^{(s)} - Y_j^{(s)}\right] \tag{5}$$

Where d and c are typically positive constants that the user sets at the process's beginning. These parameters need to be carefully chosen because they have a big impact on the process's effectiveness and how the technique converges, properly emphasizing the local and global search components of the algorithm. $Y_{pbest}^{(s)}$ represents the particle's optimal location vector in the immediate area as determined by the objective function $f\left(Y_j\right)$. $Y_{gbest}^{(s)}$ represents the current best position in the world. This vector provides the ultimate optimal position vector and is continuously updated during each cycle. The current values of the velocity and position vectors are $U_j^{(s)}$ and $Y_j^{(s)}$, respectively. At each stage of the method, the values p_1, p_2 are reselected from the uniform random distribution vector p in the range of 0 to 1. $\bullet$ in equation (5) stands for the Hadamard or Schur multiplication,. For instance, if c and d are two-element vectors, then the equation becomes,

$$d \bullet c = \begin{bmatrix} d_1 \\ d_2 \end{bmatrix} \bullet \begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} d_1 & c_1 \\ d_2 & c_2 \end{bmatrix} \tag{6}$$

The velocity adjustment equation's final two terms, (5), which indicate the algorithm's two opposing aspects, must be emphasized. First, make sure the local area has been sufficiently explored to determine an acceptable level of local minimum accuracy. In order to find a global minimum and prevent being stuck at a local minimum, it is also important to make sure the

entire region is investigated. In this procedure, randomness is important. Therefore the selection of d and c in (2) is challenging and essential in assuring the compatibility of these two goals. The updated velocity values can be used to calculate the new position values.

$$Y_j^{(s+1)} = Y_i^{(s)} + U_j^{(s+1)} \tag{7}$$

This equation drives the process along to the next point, where it can be improved after being tested. Large values of velocity indicate quick exploration of the region but possible omission of important optima. The algorithm may advance very slowly if modifications to Y_j are made inanely slowly. A thoughtful selection of parameters can guarantee steady advancement.

5. Result

This section illustrates the effectiveness of the Ensemble classifier model and other traditional methods for predicting heart disease using the Kaggle [10] and heart disease dataset [11].

5.1 Experimental setup

Utilizing the MATLAB programme in Windows 10 with 8GB RAM, aEnsemble classifier model is implemented.

5.2 Dataset description

Kaggle dataset (DB1) [11]: This database is produced by integrating a number of Hungary, Cleveland and statlog datasets that are independently available and that meet specific criteria. The Cleveland database has 303 instances of Heart, but the Hungarian database only has 270.

Heart disease dataset (DB2) [12]: This database offers 76 attributes only 14 datasets are employed in the research. These data are used in a preliminary study to establish the absence or presence of heart disease.5.4 Comparative methods

5.3 Comparative methods

Hybrid Fuzzy based DT [12] (T-1), HuS-based deep CNN (T-2), Hybrid social hunting-based deep CNN (T-3), deep BiLSTM [17] (T-4), and WOM-based deep BiLSTM (T-5) are the methods

5.3.1 Comparative based on the DB1

The Performance of the existing ensemble classifier and the PSO-optimized ensemble classifier are compared in Figure 4. First, the suggested PSO optimised ensemble classifier's accuracy improvement rate is measured and it achieved a rate of 0.10% improvement when compared to the WOM based deep BiLSTM in figure 4a. The PSO optimised ensemble classifier, which achieved a rate of 0.10% improvement when compared to the prior technique, is also measured

to determine the improvement rate in terms of F-measure shown in figure 4b. Similarly, figure 4c shows the sensitivity is evaluated and an improvement rate of 0.05% is obtained. When comparing the final results to the previous method, the specificity measurement showed an improvement rate of 0.15% in figure 4d.

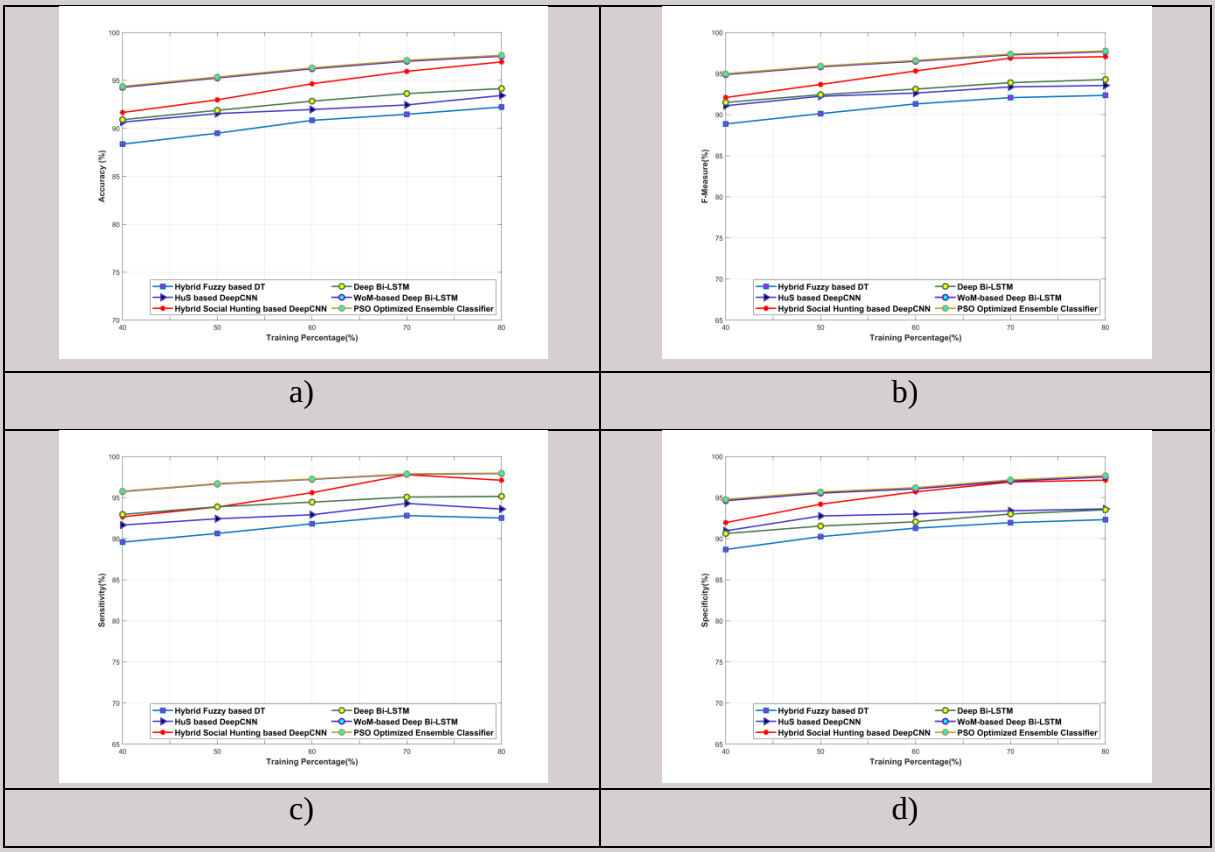


Figure 4. Comparative analysis for heart disease dataset a) accuracy b) F-measure c) sensitivity d) specificity

5.3.2 Comparative based on DB2

The performance of the existing ensemble classifier and the PSO-optimized ensemble classifier are compared in Figure 5. First, the suggested PSO optimised ensemble classifier's accuracy improvement rate is measured and it achieved a rate of 0.08% improvement when compared to the WOM based deep BiLSTM in figure 4a. The suggested PSO optimised ensemble classifier, which achieved a rate of 0.08% improvement when compared to the previous technique, is also measured to determine the improvement rate in terms of F-measure shown in figure 4b. Similarly, figure 4c shows the sensitivity is evaluated and an improvement rate of 0.01% is observed. As a result of comparing the final specificity measurement to the previous approach, an improvement rate of 0.13% was observed in figure 4d.

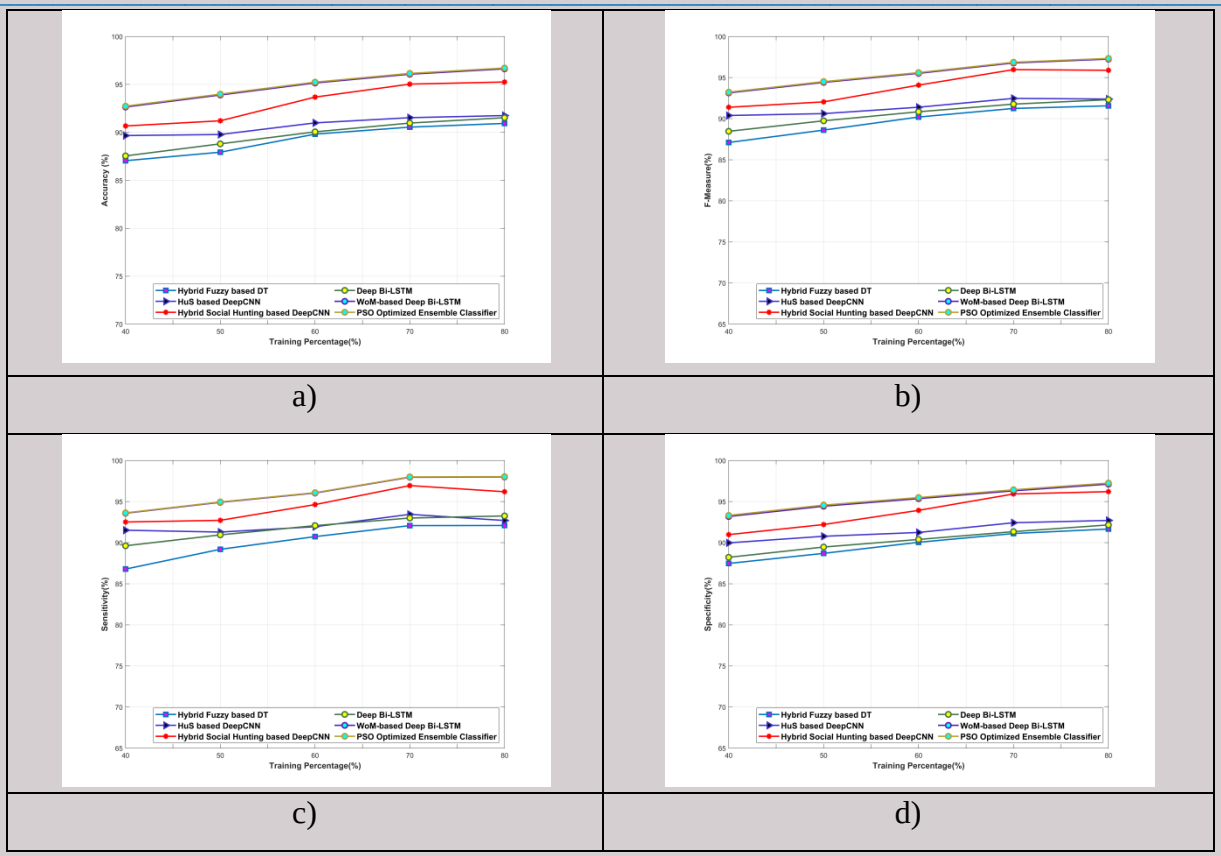


Figure 5. Comparative analysis for heart disease dataset a) accuracy b) F-measure c) sensitivity d) specificity

5.4 Comparative discussion

As shown in tables 1 and 2, the PSO optimised ensemble classifier is more effective at detecting the heart disease and improving the classifier performance. As a result, using the Kaggle dataset, the Ensemble classifier model outperformed all other models by 97.62%, 97.75%, 97.97%, and 97.66%. The model's achieved efficiency for the dataset for heart disease is 96.71%, 97.33%, 97.99%, and 97.25%, respectively.

Table 1. Comparative performance using the Kaggle dataset

Methods	DB1			
	TP 80			
	Accuracy	F-measure	Sensitivity	Specificity
T-1	92.22	92.35	92.51	92.32
T-2	93.43	93.55	93.61	93.62
T-3	96.93	97.05	97.11	97.12

T-4	94.15	94.27	95.15	93.52
T-5	97.53	97.66	97.93	97.52
PSO optimized ensemble classifier	97.62	97.75	97.97	97.66

Table 2. Comparative performance using heart disease dataset.

Methods	**DB2**			
	TP 80			
	Accuracy	**F-measure**	**Sensitivity**	**Specificity**
T-1	90.93	91.56	92.09	91.66
T-2	91.75	92.39	92.70	92.71
T-3	95.25	95.89	96.20	96.21
T-4	91.53	92.31	93.25	92.16
T-5	96.63	97.25	97.99	97.13
PSO optimized ensemble classifier	96.71	97.33	97.99	97.25

6. Conclusion

The prediction of heart disease has become an emerging topic among researchers where the influence of technology in medical field is literally important for diagnosing the heart disease. In this research, a PSO optimized ensemble classifier is used to predict heart disease effectively. The modified EDH model is used to securely transfer the IoT environment's collected data via the network in advance. The fusion parameters present in the ensemble classifier model are tuned using the PSO and the medical data can be transmitted on the network securely using the ECC-diffi-Huffman algorithm with less time. The PSO method accomplished accuracy, F-measure, sensitivity, and specificity of 97.62%, 97.75%, 97.97%, and 97.66% for heart disease dataset and for Kaggle dataset 96.71%, 97.33%, 97.99%, and 97.25% is attained. The ensemble classifier can also be used to detect infections early on, allowing for effective treatment to reduce the severity of the condition. In future more efficient classifier will be used to increase the prediction accuracy since this PSO optimized ensemble classifier method prediction is slightly less for real time applications. This research mainly focuses on heart disease prediction where it does not focused on specified feature selection techniques and in future the model will be designed with advanced feature selection models.

Reference

[1] Pandey, Honey, and S. Prabha. "Smart health monitoring system using IOT and machine learning techniques." In 2020 sixth international conference on bio signals, images, and instrumentation (ICBSII), pp. 1-4. IEEE, 2020.
[2] Khan, Mohammad Ayoub. "An IoT framework for heart disease prediction based on MDCNN classifier." IEEE Access 8 (2020): 34717-34727.
[3] Ali, Farman, Shaker El-Sappagh, SM Riazul Islam, DaehanKwak, Amjad Ali, Muhammad Imran, and Kyung-Sup Kwak. "A smart healthcare monitoring system for heart disease prediction based on ensemble deep learning and feature fusion." Information Fusion 63 (2020): 208-222.
[4] Basheer, Shakila, Ala Saleh Alluhaidan, and Maryam AyshaBivi. "Real-time monitoring system for early prediction of heart disease using Internet of Things." Soft Computing 25, no. 18 (2021): 12145-12158.
[5] Islam, MdMilon, AshikurRahaman, and MdRashedul Islam. "Development of smart healthcare monitoring system in IoT environment." SN computer science 1 (2020): 1-11.
[6] Khan, Mohammad Ayoub, and Fahad Algarni. "A healthcare monitoring system for the diagnosis of heart disease in the IoMT cloud environment using MSSO-ANFIS." IEEE Access 8 (2020): 122259-122269.
[7] Dutta, Aniruddha, TamalBatabyal, MeheliBasu, and Scott T. Acton. "An efficient convolutional neural network for coronary heart disease prediction." Expert Systems with Applications 159 (2020): 113408.
[8] Riazul Islam SM, KwakDaehan, HumaunKabir M, Hossain M, Kwak Kyung-Sup. The Internet of Things for health care: a comprehensive survey. IEEE Access. 2015;3:678–708. https://doi.org/10.1109/ACCESS.2015.2437951.
[9] Lin T, Rivano H, Le Mouel F. A survey of smart parking solutions. IEEE Trans IntellTransp Syst. 2017;18:3229–53. https://doi.org/10.1109/TITS.2017.2685143
[10] G. Joyia, R. Liaqat, A. Farooq, and S. Rehman, ‘‘Internet of medical Things (IOMT): Applications, benefits and future challenges in healthcaredomain,’’ J. Commun., vol. 12, pp. 240–247, Jan. 2017, doi: 10.12720/jcm.12.4.240-247
[11] Kaggle dataset for heart disease, “https://www.kaggle.com/sid321axn/heart-statlog-cleveland-hungary-final”, accessed on April 2021.
[12] Heart disease dataset, “https://archive.ics.uci.edu/ml/datasets/heart+disease“, accessed on April 2021.
[13] Dhaka, P. and Nagpal, B., 2023. WoM-based deep BiLSTM: smart disease prediction model using WoM-based deep BiLSTM classifier. Multimedia Tools and Applications, pp.1-22.
[14] Reddy, K. V. V., Elamvazuthi, I., Aziz, A. A., Paramasivam, S., Chua, H. N., & Pranavanand, S. (2023). An Efficient Prediction System for Coronary Heart Disease Risk Using Selected Principal Components and Hyperparameter Optimization. Applied Sciences, 13(1), 118.
[15] Taylan, O., Alkabaa, A. S., Alqabbaa, H. S., Pamukçu, E., & Leiva, V. (2023). Early Prediction in Classification of Cardiovascular Diseases with Machine Learning, Neuro-Fuzzy and Statistical Methods. Biology, 12(1), 117.

ABOUT MAIT

Maharaja Agrasen Institute of Technology was established in 1999. MAIT is affiliated to GGSIPU and is also an ISO 9001-2015 Certified Institute.

It is a known fact that technological development brings a considerable improvement in the quality of human life. In the age of globalization role of sustainable technology, development is very crucial for the progress and well-being of a nation. Keeping this in mind at Maharaja Agrasen Institute of Technology Delhi, we are committed to create young, dynamic Engineers and Entrepreneurs.

MAIT also understands that the primary role of education is to equip students with the technical knowledge and confidence for the transformation of society. In addition to providing students with content knowledge, education helps instil values and attitudes that align with those expected in a society. We strongly believe in academic excellence and do not compromise in discipline and standards of teaching. MAIT has also set specific objectives and planned activities for achieving excellence in all spheres of technical and Management Education.

ABOUT CSE

The Department of Computer Science and Engineering at Maharaja Agrasen Institute of Technology, Delhi was established in year 1999. It was formed to provide an outstanding research environment complemented by excellence in teaching. The Department offers B.Tech. degree affiliated to Guru Gobind Singh Indraprastha University, Delhi. The CSE department at MAIT has a team of experienced and highly qualified faculty who are committed to providing quality education to the students. the Computer Science and Engineering department at Maharaja Agrasen Institute of Technology offers a comprehensive learning experience, combining theoretical knowledge with practical skills. It prepares students for a successful career in the field of computer science and equips them with the necessary skills to adapt to the evolving technology landscape. The curriculum is designed to meet the current industry demands and trends, and department offers specializations in following areas:

1. Artificial Intelligence

2. Artificial Intelligence and Machine Learning

3. Machine Learning and Data Analytics

4. Full Stack Development

Department works with the vision "To be centre of excellence in education, research and technology transfer in the field of computer engineering and promote entrepreneurship and ethical values".

Publication Partners

Partners

MAHARAJA AGRASEN INSTITUTE OF TECHNOLOGY
MAHARAJA AGRASEN CHOWK, SECTOR -22, ROHINI, DELHI-86
Ph.: 011-27582095, 8448186931 | E-mail: mait@mait.ac.in | Web.: www.mait.ac.in