

JULY 2025

# CYBER GAZETTE

NEWS LETTER

JULY 2025



DEPARTMENT OF  
COMPUTER SCIENCE AND ENGINEERING  
(CYBER SECURITY)



School of Engineering

DAYANANDA SAGAR UNIVERSITY

MAIN CAMPUS,  
HAROHALLI, KANAKAPURA - 562112

# RESEARCH ACCOMPLISHMENTS

## Exploiting Machine Learning for Vulnerable Road Users' Protection of Moving Objects on Trajectory Motion: Dealing with Action Transformation Using AI Agent-Based Technologies

Dr. Dilip Kumar Jang Bahadur Saini has published his research paper titled "Exploiting Machine Learning for Vulnerable Road Users' Protection of Moving Objects on Trajectory Motion: Dealing with Action Transformation Using AI Agent-Based Technologies" in the Arabian Journal for Science and Engineering, Springer Nature (SCIE Q1 publication)

Link: <https://link.springer.com/article/10.1007/s13369-025-10346-z>.



**SPINGER NATURE Link.**

Exploiting Machine Learning For Vulnerable Road Users' Protection of Moving Objects on Trajectory Motion: Dealing with Action Transformation Using AI Agent-Based Technologies

View this article on Springerlink

Abstract

Machine learning for object detection, also known as the understanding of generalized motion planning, has been used for self-driving cars and robot navigation. In this paper, we propose a novel approach for trajectory motion planning for trajectory prediction of moving objects on a road using machine learning. This approach focuses on predicting the next two coordinates of moving objects, maintaining their computing using technologies. Machine learning techniques are used to predict the next two coordinates of moving objects. Finally, machine learning is used to predict the next two coordinates of moving objects. Although machine learning techniques are used to predict the next two coordinates of moving objects.

Abstract

Machine learning for object detection, also known as the understanding of generalized motion planning, has been used for self-driving cars and robot navigation. In this paper, we propose a novel approach for trajectory motion planning for trajectory prediction of moving objects on a road using machine learning. This approach focuses on predicting the next two coordinates of moving objects, maintaining their computing using technologies. Machine learning techniques are used to predict the next two coordinates of moving objects. Finally, machine learning is used to predict the next two coordinates of moving objects. Although machine learning techniques are used to predict the next two coordinates of moving objects.

## RESEARCH ACCOMPLISHMENTS

## Novel Approach for Identification of Ayurveda Plant Using New Age Technology

Dr. Dilip Kumar Jang Bahadur Sainihas published his research paper titled " Novel Approach for Identification of Ayurveda Plant Using New Age Technology" in the Proceedings of Fourth International Conference on Computing and Communication Networks ICCCN 2024, Volume 6

Link: [Novel Approach for Identification of Ayurveda Plant Using New Age Technology](#) | SpringerLink



# RESEARCH ACCOMPLISHMENTS

## SCAM-QUAVs: Side Channel Attacks Mitigation and Countermeasures of Quantum-Safe UAVs

Prof.Naveen Kulkarni has successfully presented a research paper titled

"SCAM-QUAVs: Side Channel Attacks Mitigation and Countermeasures of Quantum-Safe UAVs" at the IEEE International Conference on Electronics, Computing and Communication Technologies (IEEE CONECCT 2025), held from July 10–13, 2025 at Sterlings Mac Hotel, Bengaluru.

The conference was organized by the IEEE Bangalore Section, and the paper presentation contributes to emerging research in quantum-safe cybersecurity for unmanned aerial vehicles (UAVs).



# RESEARCH ACCOMPLISHMENTS

## FBCA-IoMT: A Federated Binary Contrastive Autoencoder Framework for Anomaly Detection

Prof. Archita Bhattacharyya has digitally presented a research paper titled

"FBCA-IoMT: A Federated Binary Contrastive Autoencoder Framework for Anomaly Detection" at the 10th International Conference on ICT for Sustainable Development (ICT4SD 2025), held virtually from 17–19 July 2025, based in Goa, India.

The presentation was part of a global academic platform focusing on the role of Information and Communication Technologies in achieving sustainable development goals. The event was supported by Springer Nature and several national and international industry partners.



# RESEARCH ACCOMPLISHMENTS

## Personalized Federated Learning for Privacy-Preserving and Scalable IoT-Driven Smart Healthcare

Dr. Dilip Kumar Jang Bahadur Saini has published a conference paper titled “Personalized Federated Learning for Privacy-Preserving and Scalable IoT-Driven Smart Healthcare” at the 3rd International Conference on Inventive Computing and Informatics (ICICI), 2025 in Bangalore.

Date of Conference: 04-06 June 2025

DOI: [10.1109/ICICI65870.2025.11069877](https://doi.org/10.1109/ICICI65870.2025.11069877)



### Personalized Federated Learning for Privacy-Preserving and Scalable IoT-Driven Smart Healthcare

Dr. Kavita Jang Bahadur Saini<sup>1</sup>, Nitin & Shanti<sup>2</sup>, Amit Pimparkar<sup>3</sup>, Prashantadev V.<sup>4</sup>, Kavita P.<sup>5</sup> and  
Tathita V.<sup>6</sup>

<sup>1</sup>Department of Computer Science & Engineering, Jayashankar Telangana Krishi Vidyapeeth, School of Engineering,

<sup>2</sup>Department of Computer Science & Engineering, Jayashankar Telangana Krishi Vidyapeeth, School of Engineering,

<sup>3</sup>Department of Computer Science & Engineering, Jayashankar Telangana Krishi Vidyapeeth, School of Engineering,

<sup>4</sup>Department of Computer Science & Engineering, Jayashankar Telangana Krishi Vidyapeeth, School of Engineering,

<sup>5</sup>Department of Computer Science & Engineering, Jayashankar Telangana Krishi Vidyapeeth, School of Engineering,

<sup>6</sup>Department of Computer Science & Engineering, Jayashankar Telangana Krishi Vidyapeeth, School of Engineering,

<https://doi.org/10.1109/ICICI65870.2025.11069877>

**Abstract:** The need to keep pace with the rise of chronic health conditions has led to a significant increase in the number of patients seeking medical, preventive, diagnostic, and related services. Existing traditional centralized learning methods, however, are not well-suited for this scenario. Federated learning (FL) is a decentralized learning paradigm that allows data to be shared among multiple parties while maintaining privacy and improving performance. However, privacy and performance are often in conflict. In this paper, we propose a personalized federated learning model that leverages existing knowledge partitioning and privacy-preserving techniques to maintain privacy and improve performance against an centralized entity and maintain privacy and performance against federated entities. The proposed model is designed to handle the challenges of privacy preservation and performance optimization in a federated learning environment. The designed framework undercomes certain system and data heterogeneity challenges by using a federated learning approach. The proposed framework is evaluated using a federated learning system to reduce diversity of data sources and mitigate all the issues, such as data heterogeneity, data privacy, and data security. This research is intended to provide a foundation for the new generation of privacy-preserving, secure, and personalized healthcare systems.

**Keywords:** Personalized Federated Learning (PFL), Smart Healthcare, Federated Learning System, Privacy-Preserving Federated Learning, Edge Intelligence and Federated Model Aggregation.

#### 1. INTRODUCTION

The exponential growth of the Internet of Things (IoT) as the backbone for the connected society, increasing disease detection and prevention, and improving the quality of life of the general population are some of the major challenges in the modern healthcare system. Preventing numerous diseases, providing preventive measures, monitoring health conditions, and providing medical treatment are the main goals of modern healthcare systems [1]. However, classical centralized machine learning methods being various challenges related to data privacy, communication cost, and heterogeneity, patient conditions

fluctuate [2]. To overcome these challenges, Federated learning (FL) is a decentralized learning paradigm that facilitates distributed model training with data privacy is ensured by learning the patient data in the edge devices [3].

Though having its benefits, traditional FL is plagued by several challenges [4].

(i) Heterogeneous Data Distribution: Medical data is different across patient sources due to varied medical conditions, treatment, and geographical locations [5].

(ii) Challenges in Personalization: A global model learned in FL might not be well generalized to the local data due to individual patient's learning profile's performance [6].

(iii) Security and Privacy Issues: Federated learning is a highly sensitive process due to its distributed and sensitive nature that can leak sensitive medical information [6].

To overcome these challenges, the work introduces Personalized Federated Learning for Privacy-Preserving and Scalable IoT-Driven Smart Healthcare (PFL-ICICI). The proposed framework is designed to overcome the following challenges:

- **Adaptive Model Interactions:** Each device learns a personalized model that automatically adjusts to its environment and performs data exchange based on cross-learning and local fine-tuning [7].

- **Privacy-Preserving Model Aggregation:** We propose a federated learning approach that minimizes the risk of privacy leakage among different update [8].

- **Scalable and Efficient Communication:** A lightweight communication process minimizes bandwidth usage, decreasing communication time and increasing service efficiency [9].

In order to implement PFL, we have chosen a cross-device FL global model. PFL-ICICI proposes a hybrid personalized federated learning approach that uses a global model to aggregate local models and then uses local datasets to create global knowledge models. This allows for each patient's model to learn from the data of the larger population while being in personalized predictive systems. PFL-ICICI also implements

# RESEARCH ACCOMPLISHMENTS

**REVIEWER for the 11th International Conference on Electronics, Computing and Communication Technologies, IEEE CONECCT (July 10-13,2025) organized by IEEE Bangalore section**

Dr.Dilip Kumar Jung Bahadur Saini acted as REVIEWER for the 11th International Conference on Electronics, Computing and Communication Technologies, IEEE CONECCT (July 10-13,2025) organized by IEEE Bangalore section at Sterling's Mac Hotel, Bangalore.



## FACULTY ACCOMPLISHMENTS

Session chair for the International Conference on Emerging Technologies in Computing and Communication (ETCC)

**Dr. Durbadal Chattaraj has contributed as a session chair for the International Conference on Emerging Technologies in Computing and Communication (ETCC) held on June 26<sup>th</sup> – 27<sup>th</sup> 2025 organized by PES University EC Campus, Bangalore.**



# FACULTY ACCOMPLISHMENTS

5-Days Faculty development program on “Cyber Security” organized by the department of Computer Studies, Haribhai V.Desai College of Arts and Commerce, Pune, Maharashtra in association with Pencil Bitz

Dr.Devi Priya V S has actively participated in the 5-Days Faculty development program on “Cyber Security” organized by the department of Computer Studies, Haribhai V.Desai College of Arts and Commerce, Pune, Maharashtra in association with Pencil Bitz, from 14<sup>th</sup> July to 18<sup>th</sup> July 2025.



# STUDENT ACCOMPLISHMENTS

Pratiksha Guggari (ECE), Rahul (CSE), and Sachin Pujappa Baluragi- ENG22CY0020(Cybersecurity) — has secured the 2nd Runner-Up position at the prestigious Agentic Ethereum Hackathon India, held at Scaler School of Technology on 12–13 July 2025.

Their innovative project addressed the theme "DeFi + Financial Inclusion Agents", showcasing their technical excellence and creativity in blockchain-based financial solutions.

Their remarkable performance earned them a \$1000 cash prize and a place among the top minds in Ethereum development!



# STUDENT ACCOMPLISHMENTS

Prajwal N Halvi(ENG22CY0037) has successfully completed the UI/UX Course offered by Tutedude on 15th July 2025. Course covered essential aspects of user interface and user experience design.  
Certificate ID: TD-PRAJ-UI-1609



# STUDENT ACCOMPLISHMENTS

Prajwal N Halvi(ENG22CY0037) has successfully completed the Figma Bootcamp organized by LetsUpgrade EdTech Pvt. Ltd. from 17th July 2025 to 19th July 2025. The 3-day intensive bootcamp focused on practical skills and design fundamentals using Figma, a leading interface design tool.

The bootcamp was conducted in collaboration with:

NSDC – National Skill Development Corporation

ITM Edutech Training Pvt. Ltd.

GDG MAD

Date of Issue: 19 July 2025

Certificate No.: LUEFGJUL125180



# STUDENT ACCOMPLISHMENTS

Mr. Adeesh Lokesh Poojary (USN: ENG22CY0025) has successfully completed one-month internship at the MAHE-ISAC Centre of Excellence for Cybersecurity, Manipal Academy of Higher Education, from 25th June to 25th July 2025.

Under the mentorship of Dr. Srikanth Prabhu, Professor at the School of Computer Engineering, he made significant contributions in the domain of resume classification and extraction—a vital area in cybersecurity automation and data handling.



# STUDENT ACCOMPLISHMENTS

Mr. Manish Jaju(ENG23CY0105) has successfully achieved student level credential for completing the course titled “Introduction to Cybersecurity” and “Networking Basics” by CISCO Networking academy on July 9,2025 and July 19,2025.



# STUDENT ACCOMPLISHMENTS

Mr. Manish Jaju(ENG23CY0105) has successfully completed the online non-credit course “Connect and Protect: Networks and Network Security”, authorized by Google and offered through Coursera. The course was completed on July 24, 2025, highlights his commitment to strengthening expertise in network infrastructure and cybersecurity principles.



# STUDENT ACCOMPLISHMENTS

Mr.Prateep P(ENG23CY0027) has successfully earned the prestigious (ISC)<sup>2</sup> Certified in Cybersecurity (CC) credential. This globally recognized certification, issued on 13th July 2025, validates his foundational knowledge and commitment to cybersecurity principles and best practices.



# STUDENT ACCOMPLISHMENTS

Mr. Manish Jaju(ENG23CY0105) has successfully completed the online non-credit course “Play It Safe: Manage Security Risks”, authorized by Google and delivered through Coursera, on July 26, 2025. This course strengthens his understanding of security risk management, data protection strategies, and cybersecurity best practices. Verified by Coursera, the certification affirms his proactive approach to professional development in the field of cybersecurity.



# STUDENT ACCOMPLISHMENTS

Mr.Kishan.G.A(ENG23CY0020) has received certificate of completion for the course titled "Cybersecurity Analyst Job Simulation" by Forage("Inspiring and empowering future professionals" on July 28,2025. Over the period of July 2025, Kishan G A has completed practical tasks in: Identity and access management (IAM) fundamentals, IAM strategy assessment, Crafting custom IAM solutions, Platform integration.

