adsjac.com ISSN 3067-4166

AMERICAN DATA SCIENCE JOURNAL FOR ADVANCED COMPUTATIONS (ADSJAC)

OPEN ACCESS. PEER-REVIEWED. GLOBALLY FOCUSED.

Deep Learning for Secure Mobile Edge Computing in Cyber-Physical Transportation Systems

Dr.Aaluri Seenu[1*], Dr.P.R.Sudha Rani[2], Pandi Devi Krishna Madhuri [3], Srivarshini Sandaka [3],

Vakala Yamini [3], Polamuru Tapaswi [3], Vaddi jerusha [3]

[1]Professor, Department of CSE,Shri vishnu Engineering College for Women Bhimavaram,Andhra Pradesh,India.

Corresponding Author Email:aaluriseenu@svecw.edu.in-ORCID: 0000-0002-4975-1943

[2]Professor, Department of CSE,Shri vishnu Engineering College for Women Bhimavaram,Andhra Pradesh,India.

Email:prsudharanicse@svecw.edu.in-ORCID: 0000-0003-2189-777X

[3]Undergraduate, Department of CSE,Shri vishnu Engineering College for Women Bhimavaram,

Andhra Pradesh,India.

Abstract

Key capabilities like sensing, communication, and traffic management are enabled by a cyber-physical transportation system (CPTS), which employs a wide variety of sensors and mobile wireless devices. These features are made possible by mobile edge computing (MEC), which enables a collaborative processing of real-time, compute-intensive activities directly at the edge of the network by a variety of linked devices, including moving automobiles and traffic sensors. As a result of MEC's ability to integrate computing, networking, and physical processes, cyber-physical systems have much more room to grow, especially in the transportation sector. However, there is an immediate need for strong security procedures since transport systems are becoming more interdependent and vulnerable to cyber threats due to the increasing use of edge computing. In response, this study introduces a deep learning model that actively seeks for and fixes security flaws using unsupervised learning methods. This project seeks to enhance the security of MEC in CPTS by using deep learning algorithms to predict network assaults and mitigate their negative impacts. We show how deep learning may be used to the real-world problem of cyber threat identification and mitigation by integrating state-of-the-art neural network designs into a safe computing framework for the edge.

Keywords:Cyber-Physical Systems, cyber-attacks, cyber-security, cyber-transportation, mobile edge computing.

I. INTRODUCTION

A key component of smart cities, cyber-physical transportation systems (CPTS) propel developments in autonomous cars, dynamic route optimisation, and traffic management. By using mobile edge computing (MEC), CPTS may analyse data locally, which speeds up transportation operations by lowering latency and facilitating real-time decision-making. Cyberattacks may interrupt services and jeopardise safety, but this integration also brings new security vulnerabilities. In order to address these concerns, this study explores how deep learning methods may be used to protect CPTS MEC settings against various network assaults, including spoofing, Distributed Denial of Service (DDoS), and phishing. Power grids, public transportation, medical care, & home automation are just a few areas where Cyber-Physical Systems (CPS) have proliferated, revolutionising contemporary life. A strong defence against cyberattacks is necessary for many of these systems because of their importance to vital services, life-support equipment, and critical infrastructure.The complexity and inherent weaknesses of real-world systems make the achievement of a completely safe and attack-free CPS very difficult. Because different parts of the system are designed differently, ensuring CPS security isn't easy. The many pieces of proprietary and commercial control and monitoring software and hardware that make up CPS are vast and varied. Potential attack surfaces are introduced by each component and how it interacts

with others. In order to shore up their security posture and identify limits that leave them open to different types of assaults, it is essential to have a good grasp of CPS's vulnerabilities, threats, and defence mechanisms.

Assessing security threats is made more challenging by the complexity and variety of CPS components, which in turn are affected by the dynamic interplay between cyber & physical aspects. There is a pressing need for all-encompassing security measures since it is very difficult to detect, track, and react to assaults that target various components of CPS. The goal of this study is to provide new ways to protect CPS by examining the existing state of CPS security and privacy measures and finding shortcomings.
To begin, we provide a definition of CPS and explain how they differ from more conventional control systems and IT networks; we then highlight the specific security concerns that systems provide.Then, taking into account the cyber, physical, & cyber-physical aspects of these

systems, we organise the current CPS security research into a cohesive framework that deals with dangers, weaknesses, assaults, and controls. We provide light on the unique security challenges encountered by each system by analysing typical CPS applications, including systems for industrial control, electric power plants, medical CPS, or autonomous cars.

First, we provide a thorough CPS security architecture that separates a system's cyber, cyber-physical, & physical parts.

2. We pinpoint the origins of such threats and the reasons behind them.

3. We draw attention to current security holes and show how they manifest in the real world to show how they got there.

4. The effects of alleged CPS assaults on different parts of the system are examined.

5. We highlight the current control methods and point out the problems with protecting CPS applications that have not been addressed.

II. LITERETURE SURVEY

1. A model for detecting assaults in MEC has been published by Chen et al. [15] using a Deep Belief Network (DBN). In this case, the DBN model's accuracy is enhanced by active feature learning, and it is more closely linked to other ML models in comparison. This study's DBN model updates its parametric values using a contrastive divergence approach, and it learns attack characteristics using 512 hidden units. The experimental assessment used 10 datasets for experimentation, and the given DBN model outperformed the compared models by 6% in terms of accuracy. On the other hand, the computational cost of the provided DBN model was high due to the inclusion of complicated data models.
2. An effective Intrusion Detection System (IDS) for discovering suspicious behaviours in vehicles to infrastructure networks, in-vehicles networks, and vehicles to vehicles communications was provided by Ashraf et al. [17] in the context of ITS. In order to identify invasive occurrences in AVs, the autoencoder model was combined with the Long Short-Term Memory (LSTM) network. Results from testing the provided IDS on two online datasets showed that it outperformed the state-of-the-art methods in terms of detection accuracy. The offered IDS, however, is rather time-consuming and has issues with disappearing gradients.
3. In order to assist with MEC in transportation CPS, Zhou et al. [18] introduced a novel lightweight stacked CNN model. The given convolutional neural network (CNN) model incorporates compression and factorisation convolutional layers to enhance context awareness and decrease MEC latency. The findings shown that compared to typical CNN models, the provided stacked CNN model reduced the number of unnecessary parameters while retaining a greater level of accuracy. Here, an experiment was carried out on a real-time MEC platform to assess the efficacy of the stacked CNN model. The findings shown that the stacked CNN model successfully keeps the model size and accuracy high on a real-time MEC platform. But it was computationally expensive to use the layered CNN model.

4. A system for regulating the traffic lights has been described by Kumar et al. [19] as an application of ITS. You may choose between three different modes in the given system: emergency, priority, and fair. This case makes use of a deep reinforcement learning technique to alternate between yellow, green, and red traffic lights at different phases, while a Fuzzy Inference System (FIS) determines the best mode (emergency, priority, or fair) depending on the current traffic situation. The findings demonstrated that, when compared to the current systems, the proposed solution performed better across all assessment metrics. The maintenance cost of reinforcement learning was too high, and it creates overload.
5. A novel framework for transport control has been proposed by Rathore et al. [20] that makes use of CPS and sensor technologies to make effective decisions. The offered framework depicts road networks using data on road conditions, vehicle speeds, traffic intensity, and trip times to build city graphs. In order to create a smart and efficient transport system, the traditional graph approach requires both authorities and commuters. In this case, the data streams were processed using an Apache GraphX software application. Processing time and throughput were used to evaluate the performance of the given framework, and the findings showed that it outperformed the current systems. Several physical systems, including industries, ITS, and cities, are now integrated with the CPS to enhance its intelligence, efficiency, comfort, and energy. Here, Traffic Flow Prediction (TFP) was crucial to the ITS.

6. The Adaptive Neuro FIS (ANFIS) model was used by Jain et al. [21] to effectively control ITS energy and total factor productivity (TFP). Research in this area has shown that the ANFIS model can calculate engine torque, and that ITS traffic flow estimates were obtained by combining a fuzzy wavelet neural network with the sailfish optimisation method. The results of the experiments conducted on a benchmark dataset proved that the proposed model performed better than the previous models. Unfortunately, there are four issues with the ANFIS model in the ITS: the curse of dimensionality, computational expense, interpretability loss, and difficulty in selecting the membership function.

III. PROPOSED METHODOLOGY

In order to overcome the difficulties associated with communications security in MEC settings, the article "Deep Learning towards Secure Edge Computing with Mobile Devices in Cyber-Physical Transport Systems" makes use of a number of techniques. The primary approaches covered here:

Deep learning in cyber-physical systems:A model for deep learning tailored to learning attack characteristics was created by the authors. In the setting of MEC, where the number of communications traffic has grown substantially as a result of linked edge devices, this model is essential for identifying unknown assaults. We go over some of the ways deep learning may be used in CPS here. Therefore, in order for it to be used in security-related activities like CPSs, deep learning must first be introduced.

The field of data science is now heavily investing in DL as a means to improve application performance [12]. Deep learning algorithms are multi-layered hierarchies that can extract ideas and characteristics from underlying data by explaining higher-level aspects in terms of lower-level features [14]. Applications such as cyber-physical systems security may benefit greatly from these designs [12], [15]. A number of concealed layers make up the deep structures [4]. Because of its multi-level design, Deep Learning techniques may express more abstract data visualisations. When compared to shallow ANNs, Deep Learning models demonstrated superior generalisation competency in several real-world applications. Anomaly detection, malware detection, vulnerability recognition, interruption detection, blackout prevention, attack and destruction prevention, and cyber-physical system (CPS) security are some of the main areas where deep learning has been successfully used.

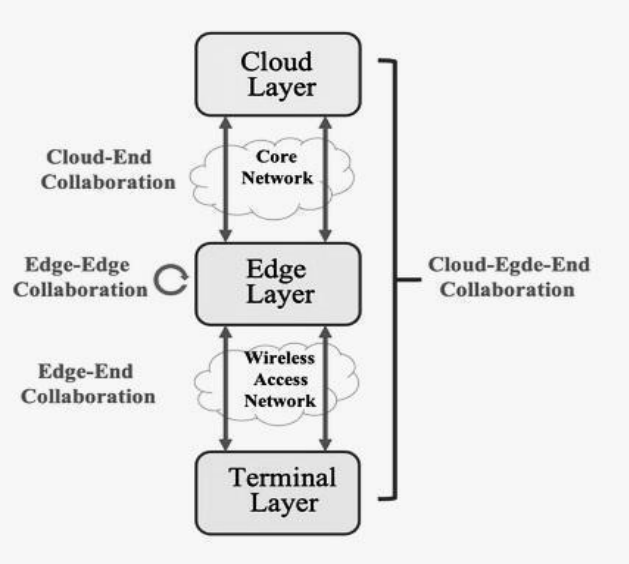

Figure 2: Three layers of cloud-edge-end framework

Unsupervised Learning:The model actively learns by using unsupervised learning approaches.Particularly helpful for discovering novel and unidentified attack patterns, this method enables a model to learn on data without requiring labelled instances.

Active Feature Learning:In order to better identify unknown assaults, the research focuses on active feature learning. To improve the model's responsiveness to new security risks, it is necessary to dynamically detect and learn characteristics that may indicate such dangers.

Experimental Evaluation:The authors performed trials utilising ten distinct datasets to verify the efficacy of their suggested methodology. The model's performance may be evaluated across many situations and datasets with the aid of this thorough examination.

Comparative Analysis:In the study, four more methods that rely on machine learning are compared to the suggested deep learning model. Their method outperforms the alternatives by 6% in this comparison, proving their method's superiority. Addressing the essential problem of communication safety in these increasingly linked systems, these solutions work together to improve the security of edge computing devices in cyber-physical transportation contexts.

Mobile Edge Computing (MEC) for Cyber-Physical Transportation Systems (CPTS), deep learning (DL) algorithms can play a critical role in improving security, performance, and efficiency. MEC allows computation and data processing to occur closer to the source of the data, typically at the network edge, such as in vehicles or roadside infrastructure, which is crucial for real-time processing in transportation systems.

Deep learning algorithms can greatly enhance the capabilities of Mobile Edge Computing for Cyber-Physical Transportation Systems. These models can be used to address a wide range of problems, including traffic management, real-time decision-making, anomaly detection, vehicle communication security, and privacy-preserving systems. As the systems become more

distributed and complex, deep learning will play a crucial role in ensuring both performance and security while optimizing the user experience in transportation systems

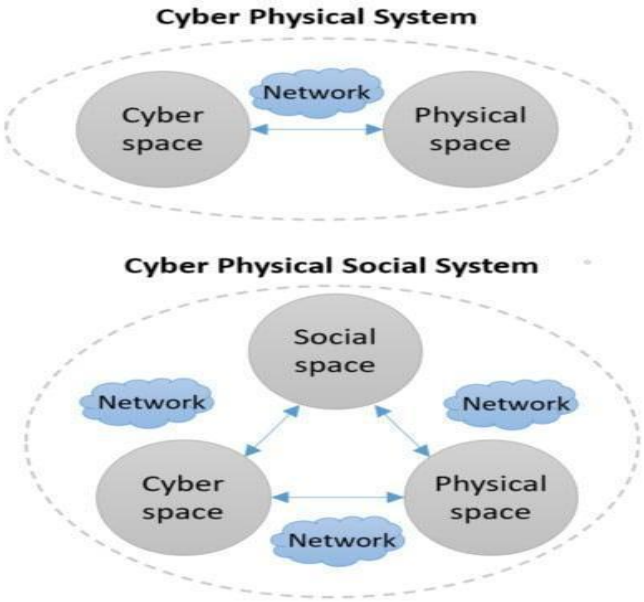

Figure 3: Cyber Physical system

By combining advanced models such as auto encoders, CNNs, RNNs, and reinforcement learning, MEC systems can achieve a highly secure, scalable, and efficient security framework. Furthermore, integrating privacy-preserving techniques like federated learning and differential privacy will help ensure that data confidentiality is maintained without sacrificing security.

CNNs are typically used for image and video recognition, which can be useful in a transportation system for tasks such as identifying road signs, detecting obstacles, or monitoring vehicle movements. CNN's can process visual data from cameras mounted on vehicles or infrastructure to identify road conditions or traffic violations (e.g., detecting a red light violation). This is useful in intelligent transportation systems (ITS) where real-time monitoring and feedback are necessary. It can also be used to identify anomalous patterns or objects in the system,

which can help detect malicious attacks or misbehaving vehicles.

Feature-Learning-Based Detection: There are two main schools of thought when it comes to current attack detection approaches, which are based on feature learning techniques: stat-ic-learning and dynam-ic-learning. The moment an organization's actual performance deviates from its intended one, we say that it has failed. Because of its accidental nature, the failure becomes apparent. An issue's source could be within or outside the system. Both physical properties (such component connector broking) and design flaws may lead to internal issues. Environmental factors, such as noise, may be the starting point for peripheral (or external) defects. There are two types of faults: permanent and transitory. Having said that, a momentary issue only lasts for a short while. It might make a mistake, which could result in an endless loop of failure. The same holds true for physical inputs and defects; they might be temporary or permanent, but design flaws are always permanent. Irregular flaws are those that cannot be replicated analytically. Soft mistakes might result from this kind of mistake. This picture depicts the infrastructure of cyber-physical systems and the Internet of Things, or CPS/IoT. The physical layer and the control layer are two examples of the many architectural levels that could experience failure [13]. Any disruption, direct tampering, or actual object destruction might compromise the physical layer. Device connections are possible at the network layer. Uncertainties in the surrounding environment and the manipulation of control signals and extents may affect the control layer's monitors and controllers. The information layer is primarily susceptible to concerns pertaining to confidentiality and authenticity when it comes to data acquisition.

Static-Learning-Based Attack Detection

Without actually executing the malware, the techniques in this kind of malware detection look at the attack's source code. In addition, they study the patterns of security threats by analysing their static properties. This understanding may help us understand how assaults work and how to protect ourselves from them. After that, we will go over the key publications concerning static learning-based detection approaches. I propose SigPID. It memorises the MEC devices' permission use patterns statically. By using three stages of trimming, SigPID finds the most important permits without analysing all of them. Malicious and benign behaviours are further classified using the machine learning-based categorisation algorithms. may be used as a static analysis framework to deconstruct attack code and extract attack characteristics.

In addition, the characteristics that were extracted are evaluated using a support vector machine. In [7], the idea of using DroidMat to extract various features from the AndroidManifest.xml file is put up. When modelling harmful assaults using clustered extracted characteristics, the k-means technique is used.

In order to automatically classify and identify harmful threats, techniques based on Bayesian networks, decision trees, k-nearest neighbours, random forests, and support vector machines are used in [8]. Then, in [9], a system is built using a trained support vector machine classifier; this system then collects static aspects of assaults from Android systems.

Dynamic-Learning-Based Attack Detection

In order to understand the dynamic behaviour characteristics of assaults, such as the strength of strategy of eavesdroppers, this detection looks at attacks while they are running. Our next stop is a survey of seminal publications on dynamic learning-based detection techniques. By continuously examining the textual meaning of network data, an automated technique for detecting attacks is suggested in [10]. In addition, a model for dynamic attack detection in network traffic is developed using text semantics feature analysis in this study. To identify unknown assaults on the Android system, a method using neural networks that are artificial.Additionally, this study makes use of recurrent neural networks and feedforward neural networks. So, the dynamic feature is used to train the model via recurrent neural networks. Attack detection techniques have made more and more use of feature learning in the last decade. You may see a selection of machine learning techniques utilised in previous research to identify harmful attacks.

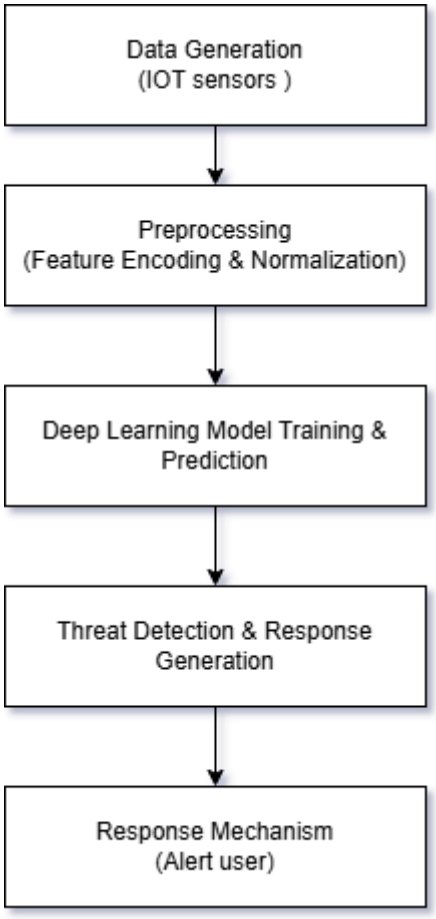

Figure 4: Data processing function sequence diagram

Security Intimidations in CyberPhysical Systems: One of the primary goals of computer networks' security measures is to detect vulnerabilities and prevent harmful assaults on the devices. However, with cyber-physical systems, vulnerabilities in the physical realm and the unpredictable behaviour of the physical environment are becoming more apparent. Below is a breakdown of the several types of assaults that may be used on different layers of cyber-physical systems:

Physical Layer: Data Leakage: Theft of sensitive data from different devices, including secret keys - Disruption of Service: launching DoS assaults by tinkering with different settings.

Network Layer: Jamming: Creating an excessive amount of fake traffic to overwhelm the communication system. -Collision: Data collisions or protocol violations caused by manipulation of timing or power. - Misdirections in routing: Data flooding, discriminatory fact promotion, and collisions are all results of tampering with the routing process.

Control Layer: Getting out of sync: Disregarding or tampering with the timing of things. Information leakage and denial of service are possible outcomes.

Information Layer: Theft or sniffing out of data by means of eavesdropping. The fear of disclosure constitutes one of the most significant obstacles to maintaining privacy. A variety of assaults might likewise be carried out using data. Cyber physical system refuge intimidation models could detail the possible threats and consequences.

IV. CONCLUSION

By providing unmatched responsiveness and performance at the network's periphery, Mobile Edge Computing (MEC) has unquestionably ushered in a new age of computing. The enormous promise of MEC is not without its security risks, the most serious of which being Distributed Denial of Service (DDoS) assaults. Intrusion Detection Systems (IDSs) that rely on weak Machine Learning (ML) models have been a major problem for MEC security. Although these technologies have been helpful, it is now clear that they can't identify or mitigate DDoS assaults correctly. When it comes to the ever-changing MEC environment, superficial ML models just can't keep up with the attackers' strategies.

In light of these limitations, this research introduces a hybrid DL approach to DDoS attack detection in MEC settings. An autoencoder and a multi-layer perceptron network make up the suggested hybrid DL model's architecture. From a massive sample of network traffic, the AE extracts the key properties needed to detect DDoS network payloads. In order to successfully categorise various forms of DDoS attacks, the AE model's compressed and reduced characteristics are then input into MLP. Comprehensive trials using the most pertinent publicly accessible dataset (NF-UQ-NIDS-V2) were conducted to verify the efficacy of the suggested model. The suggested AE-MLP performs better than individual models in most cases, according to the testing data. In a similar vein, other relevant investigations were compared to the suggested model. The suggested model outperformed its competitors in terms of accuracy. Due to its ability to swiftly identify malicious or benign patterns in massive amounts of traffic data, a combination of approaches is better suited for intrusion detection systems. Nevertheless, cloud-edge cooperation is recommended because of the time component in hybrid setups. This approach proposes training a hybrid model in the cloud and then deploying it to a MEC environment to identify DDoS attacks effectively.

V. REFERENCES

[1] B. Wang, F. Gao, S. Jin, H. Lin, G.Y. Li, Spatial- and frequency-wideband effects in millimeter-wave massive MIMO systems, IEEE Trans. Signal Process. 66 (13)(2018) 3393–3406.

[2] X. Hu, C. Zhong, Y. Zhu, X. Chen, Z. Zhang, Programmable metasurface-based multicast systems: Design and analysis, IEEE J. Sel. Areas Commun. 38 (8) (2020) 1763–1776.

[3] Y. Xu, C. Shen, D. Cai, G. Zhu, Latency constrained non-orthogonal packets scheduling with finite blocklength codes, IEEE Trans. Veh. Technol. 69 (10) (2020) 12,312–12,316.

[4] X. Hu, C. Zhong, Y. Zhang, X. Chen, Z. Zhang, Location information aided multiple intelligent reflecting surface systems, IEEE Trans. Commun. 68 (12) (2020) 7948–7962.

[5] X. Li, Y. Zheng, W.U. Khan, M. Zeng, D. Li, G.K. Ragesh, L. Li, Physical layer security of cognitive ambient backscatter communications for green internet-of-things, IEEE Trans. Green Commun. Netw. 5 (3) (2021) 1066–1076.

[6] D. Cai, P. Fan, Q. Zou, Y. Xu, Z. Ding, Z. Liu, Active device detection and performance analysis of massive non-orthogonal transmissions in cellular internet of things, Sci. China Inf. Sci. (99) (2022) 1–17.

[7] X. Hu, J. Wang, C. Zhong, Statistical CSI based design for intelligent reflecting surface assisted MISO systems, Sci. China: Inf. Sci. 63 (12) (2020) 1–10.

[8] P.K. Malik, R. Sharma, R. Singh, A. Gehlot, S.C. Satapathy, W.S. Alnumay, D. Pelusi, U. Ghosh, J. Nayak, Industrial internet of things and its applications in industry 4.0: State of the art, Comput. Commun. 166 (2021) 125–139.

[9] X. Li, J. Li, Y. Liu, Z. Ding, A. Nallanathan, Residual transceiver hardware impairments on cooperative NOMA networks, IEEE Trans. Wirel. Commun. 19(1) (2020) 680–695.

[10] W. Xu, Z. Yang, D.W.-K. Ng, M. Levorato, Y.C. Eldar, M. Debbah, Edge learning for b5 g networks with distributed signal processing: Semantic communication, edge computing, and wireless sensing, IEEE J. Sel. Top. Sign. Proces. 2022 (2022)1–10.

[11] P. Singh, A. Nayyar, A. Kaur, U. Ghosh, Blockchain and fog based architecture for internet of everything in smart cities, Future Internet 12 (4) (2020) 61.

[12] Y. Nie, J. Zhao, F. Gao, F.R. Yu, Semi-distributed resource management in UAVaided MEC systems: A multi-agent federated reinforcement learning approach, IEEE Trans. Veh. Technol. 70 (12) (2021) 13,162–13,173.

[13] L. Chen, Intelligent ubiquitous computing for future UAV-enabled MEC network systems, Cluster Comput. 2021 (25) (2021) 1–10.

[14] J. Zhao, X. Sun, Q. Li, X. Ma, Edge caching and computation management for real-time internet of vehicles: An online and distributed approach, IEEE Trans.Intell. Transp. Syst. 22 (4) (2021) 2183–2197.

[15] S. Tang, L. Chen, Computational intelligence and deep learning for next generation edge-enabled industrial IoT, IEEE Trans. Netw. Sci. Eng. 9 (3) (2022)105–117.

[16] J. Zhao, Q. Li, Y. Gong, K. Zhang, Computation offloading and resource allocation for cloud assisted mobile edge computing in vehicular networks, IEEE Trans. Veh. Technol. 68 (8) (2019) 7944–7956.

[17] X. Lai, Outdated access point selection for mobile edge computing with cochannel interference, IEEE Trans. Veh. Tech. 71 (7) (2022) 7445–7455.

[18] Z. Zhao, X. Lei, G.K. Karagiannidis, A. Nallanathan, System optimization of federated learning networks with a constrained latency, IEEE Trans. Veh.Technol. 71 (2022) 1095–1100.

[19] Y. Guo, S. Lai, Distributed machine learning for multiuser mobile edge computing systems, IEEE J. Sel. Top. Signal Process. PP (99) (2021) 1–12.

[20] H. Mughal, M. Bilal, U. Ghosh, G. Srivastava, S.C. Shah, Efficient allocation of resource-intensive mobile cyber–physical social system applications on a heterogeneous mobile ad hoc cloud, IEEE Trans. Netw. Sci. Eng. 9 (3) (2022) 958–969.

[21] X. Lai, Y. Deng, G.K. Karagiannidis, A. Nallanathan, Secure mobile edge computing

networks in the presence of multiple eavesdroppers, IEEE Trans. Commun.70 (1) (2022) 500–513.

[22] J. Xu, J. Yao, Exploiting physical-layer security for multiuser multicarrier computation offloading, IEEE Wirel. Community. Lett. 8 (1) (2019) 9–12.

[23] J. Lu, Analytical offloading design for mobile edge computing based smart internet of vehicle, EURASIP J. Adv. Signal Process. 2022 (2022) 44.

[24] L. Zhang, DQN based mobile edge computing for smart internet of vehicle, EURASIP J. Adv. Signal Process. 2022 45.

AUTHORS

Dr. Aaluri Seenu received his B. Tech degree in Computer Science and Engineering from Kakatiya University, India, and the M. Tech and Ph.D. in Computer Science and Engineering from JNTUH and ANU respectively. Currently, he is a Professor in the Department of Computer Science and Engineering at SVECW. His research interests include Data Mining, Neural Networks, Cybersecurity, Secure Software Development, data protection strategies, multimedia encryption, cloud computing infrastructures, algorithm analysis, ethical hacking, network security protocols, emerging programming languages, and artificial intelligence in security frameworks.

Ms. Pandi Devi Krishna Madhuri is an undergraduate student in department of CSE

at Shri Vishnu Engineering

College For Women(A), Bhimavaram, AndhraPradesh, India - 534202.Her area of interest is Deep Learning ,Cybersecurity ,SpringBoot and OAuth2.

She has practical experience in developing websites, SpringBoot API Development, Machine Learning and DeepLearning Models.

Ms. Srivarshini Sandaka is an undergraduate student in the Department of Computer Science and Engineering at Shri Vishnu Engineering College for

Women (A), Bhimavaram, Andhra Pradesh, India – 534202. Her areas of interest include Full Stack Development, computer networks,Machine Learning, Deep Learning,Data Analytics,Artificial Intelligence and Cloud computing.

Ms. Vakala Yamini is an undergraduate student in the Department of Computer Science and Engineering at Shri

Vishnu Engineering College for Women (A), Bhimavaram, Andhra Pradesh, India – 534202. Her areas of interest include Full Stack Development, Machine Learning, Deep Learning, Data Science, and Artificial Intelligence. She has worked on several projects, including Beyond QWERTY(Voice Based Form Filling), Dine Sense.

Ms. Polamuru Tapaswi is an undergraduate student in the Department of Computer Science and Engineering at Shri Vishnu

Engineering College for Women (A), Bhimavaram, Andhra Pradesh, India – 534202. Her areas of interest include Full Stack Development, computer networks,Machine Learning, Deep Learning, Data Science, and Artificial Intelligence.

Ms. Jerusha vaddi is an

undergraduate student in the Department of Computer science and Engineering at Shri Vishnu Engineering College for Women(A),Bhimavaram,Andhra Pradesh,India -534202. Her areas of interest include Machine Learning, Computer Networks, Artificial intelligence, Cybersecurity and Cloud Computing.

Dr. P. R. Sudha Rani received B. Tech degree from Karunya University, Coimbatore, India and the M. Tech and Ph. D in Computer Science and Engineering from Andhra University and ANU respectively. Currently she is a professor at the department of Computer Science and Engineering, SVECW. Her research interests include algorithm analysis, data mining, cryptography, multimedia encryption, disease correlation analysis, graph theory, optimization techniques, secure software development, data protection strategies, cloud computing infrastructures, machine learning, artificial intelligence in security applications, network security protocols, bioinformatics, and privacy-preserving data analysis.