10.48047/jocaaa.2025.34.05.46

Adaptive Malicious Activity Detection in Mobile Edge Networks Using Deep Neural Network

Cherlapally Swapna[1*], B. Jai Prakash[2], J. Manikanta Sai Gopi Krishna[2], M. Ranjith Kumar[2], B.Karthik[2], MD Faizzan Ali[2]

[1]Assistant Professor, [2]UG Student, [1,2]Department of Information Technology,

[1,2]Malla Reddy Engineering College and Management Sciences, Kistapur, Medchal, 501401, Telangana, India

*Corresponding author: swapnacsm@mrem.ac.in

Received: 02.03.2025 Revised: 15.04.2025 Accepted: 25.05.2025

ABSTRACT

Mobile Edge Computing (MEC) enhances the performance of mobile applications by enabling computation and data storage closer to end users. However, this distributed architecture also introduces new security vulnerabilities, making mobile edge networks increasingly susceptible to malicious activities such as data breaches, denial-of-service attacks, and intrusion attempts. Traditional security mechanisms in MEC environments primarily rely on signature-based and rule-based detection techniques, which are limited to recognizing known attack patterns and often fail to detect novel or evolving threats. Additionally, these approaches suffer from high false-positive rates and require frequent manual updates. To overcome these limitations, this research proposes an adaptive malicious activity detection framework based on machine learning and deep neural networks. The proposed system employs classification algorithms including Decision Trees, Random Forests, and Deep Neural Networks to analyze network and system behavior and identify malicious activities in real time. By learning complex patterns from large-scale data, the model effectively detects both known and previously unseen attacks while continuously adapting to emerging threat patterns. Experimental analysis demonstrates improved detection accuracy, scalability, and robustness compared to traditional methods. This adaptive, self-learning approach provides a proactive and reliable security solution for safeguarding mobile edge networks and ensuring data integrity, availability, and confidentiality in next-generation computing environments.

Keywords: Mobile Edge Computing, Malicious Activity Detection, Deep Neural Network, Machine Learning, Network Security, Intrusion Detection, Adaptive Security, Cybersecurity, Real-Time Threat Detection.

1. INTRODUCTION

Mobile Edge Networks (MENs) are transforming modern computing paradigms by enabling data processing closer to the data source. According to a report by MarketsandMarkets, the global edge computing market is projected to reach USD 111.3 billion by 2028, growing at a CAGR of 20.3% from 2023. This explosive growth is mainly driven by the proliferation of IoT devices, 5G infrastructure, and real-time analytics. While this offers ultra-low latency and improved performance for latency-sensitive applications such as autonomous vehicles, augmented reality, and remote surgeries, it also expands the attack surface for cyber threats. The distributed nature of edge computing, coupled with limited resource nodes, makes MENs highly vulnerable to malicious activity, particularly from internal and external adversaries exploiting network vulnerabilities.

10.48047/jocaaa.2025.34.05.46

A growing concern in mobile edge environments is the rise of cyberattacks including man-in-the-middle attacks, distributed denial of service (DDoS), data poisoning, spoofing, and privilege escalation attacks. Research by Palo Alto Networks found that over 57% of threats in edge environments go undetected due to insufficient threat visibility. Edge nodes, unlike centralized servers, lack robust cybersecurity infrastructure, often relying on lightweight protection mechanisms. Attackers exploit this limitation to implant malware, exfiltrate sensitive data, or disrupt operations. These vulnerabilities are intensified in sectors like healthcare, finance, and industrial IoT, where the consequences of a breach can be devastating, ranging from data theft to operational failures.

Furthermore, mobile edge environments experience dynamic changes in traffic patterns, device mobility, and user behavior, which make traditional security solutions obsolete or inefficient. According to Cisco's Annual Internet Report (2023), by 2025, 75% of all enterprise data will be processed at the edge rather than centralized data centers. This migration necessitates a more intelligent, context-aware, and scalable detection system to identify and mitigate malicious activities in real time. Therefore, the integration of advanced analytics, particularly data-driven machine learning models, is imperative for real-time anomaly detection and security automation in edge networks.

2. LITERATURE SURVEY

R. Braden et. al. [1] discusses the fundamental requirements for internet host communication layers, providing an early framework for secure data transmission. The report outlines critical security considerations necessary for maintaining the integrity and confidentiality of communications, which serve as the foundation for modern mobile edge security mechanisms. The study highlights vulnerabilities in host-based communication that can be exploited by malicious entities, necessitating advanced security measures. M. Korczy´nski and A. Duda [2] introduce Markov chain fingerprinting to classify encrypted traffic, an approach that enhances threat detection without decrypting data. This method is particularly relevant for mobile edge security as it enables anomaly detection while preserving user privacy. Their research demonstrates the effectiveness of probabilistic models in distinguishing between normal and malicious activities within encrypted network streams, a crucial aspect in preventing security breaches.

B. Anderson and D. McGrew [3] propose a machine learning-based approach to identifying encrypted malware traffic using contextual flow data. The study emphasizes the limitations of traditional signature-based detection and highlights the need for adaptive techniques that can analyze traffic behavior in real time. Their work underscores the importance of leveraging AI-driven models to enhance security at the edge of the network, where conventional methods struggle to provide timely threat identification. E. Rescorla [4] presents an update on the Transport Layer Security (TLS) protocol, detailing improvements in encryption standards that enhance security for mobile and edge computing environments. The paper addresses vulnerabilities in earlier versions of TLS and introduces mechanisms that mitigate risks associated with data interception and manipulation. The research is instrumental in securing communication channels against sophisticated cyber threats in edge networks.

C. Xu et al. [5] conduct a comprehensive survey on regular expression matching techniques for deep packet inspection, highlighting their application in network security. Their findings reveal the efficiency and accuracy of different matching algorithms in detecting malicious activities. The study also explores hardware-accelerated solutions that improve the performance of real-time security systems, making them more suitable for mobile edge environments where low latency is critical. [6] C. Meyer and J. Schwenk provide a chronological analysis of SSL/TLS attacks, examining the

10.48047/jocaaa.2025.34.05.46

weaknesses exploited in previous breaches. Their work is crucial in understanding the evolution of security threats and the necessity for continuous improvement in cryptographic protocols. The study emphasizes the role of proactive security measures in preventing similar attacks in mobile edge networks.

Y. Zhao et al. [7] investigate exception-triggered DoS attacks on wireless networks, revealing vulnerabilities that can disrupt edge computing operations. Their research discusses the impact of such attacks on network availability and proposes countermeasures to mitigate the risk. The findings highlight the importance of robust security frameworks capable of identifying and preventing denial-of-service threats in real-time. [8] J. Salowey et al. explore session resumption mechanisms in TLS to enhance security without maintaining server-side state. The study demonstrates how these mechanisms improve authentication efficiency while minimizing the risks associated with session hijacking. Their work contributes to the development of lightweight security solutions for mobile edge computing, where resource constraints are a major concern.

R. Hummen et al. [9] tailor end-to-end IP security protocols for the Internet of Things (IoT), addressing the challenges posed by limited processing capabilities in edge devices. The research introduces optimized security mechanisms that balance performance with protection, ensuring secure communication in IoT-driven edge networks. Their findings support the need for scalable security solutions that can adapt to diverse mobile edge computing environments. B. Anderson, S. Paul, and D. McGrew [10] analyze how malware utilizes TLS for encrypted communication without requiring decryption. Their research presents a method to identify malicious patterns in encrypted traffic, demonstrating the potential of machine learning in security applications. The study reinforces the importance of behavioral analysis techniques in detecting cyber threats in mobile edge environments.

3. PROPOSED SYSTEM

The proposed system aims to enhance the detection of malicious activities in mobile edge computing environments by leveraging advanced machine learning techniques. This approach involves the collection and preprocessing of a comprehensive dataset containing various malicious activity records. Initially, the dataset undergoes preprocessing steps, including the removal of null values and label encoding, to ensure data quality and consistency. Subsequently, the system employs the Random Forest Classifier algorithm as a benchmark to evaluate its performance in identifying malicious patterns. Building upon this, a Deep Neural Network (DNN) algorithm is proposed to improve detection accuracy and adaptability. Finally, a performance comparison between the Random Forest and DNN models is conducted to assess the efficacy of the proposed system in accurately identifying and mitigating malicious activities within mobile edge computing frameworks.

Step 1: Malicious Activities Dataset

The initial phase involves the collection of a comprehensive dataset encompassing various types of malicious activities pertinent to mobile edge computing environments. This dataset serves as the foundation for training and evaluating the machine learning models. It includes records of different attack vectors, system vulnerabilities, and anomalous behaviors observed in mobile edge networks. The diversity and richness of this dataset are crucial for developing a robust detection system capable of identifying a wide range of malicious activities.

Step 2: Dataset Preprocessing

Once the dataset is compiled, preprocessing steps are undertaken to prepare the data for model training. This involves the removal of null or missing values to prevent inconsistencies that could

10.48047/jocaaa.2025.34.05.46

affect model performance. Label encoding is applied to convert categorical variables into numerical formats suitable for machine learning algorithms. These preprocessing steps ensure that the dataset is clean, structured, and ready for effective training of the models.

Step 3: Existing Algorithm (Random Forest Classifier)

In this step, the Random Forest Classifier algorithm is utilized to establish a baseline for detecting malicious activities. Random Forest is an ensemble learning method that constructs multiple decision trees during training and outputs the mode of the classes for classification tasks. It operates by creating a 'forest' of uncorrelated decision trees whose collective output is more accurate than that of any individual tree. This algorithm is known for its robustness and ability to handle large datasets with higher dimensionality.

Step 4: Proposed Algorithm (Deep Neural Network)

Building upon the baseline, a Deep Neural Network (DNN) is proposed to enhance detection capabilities. DNNs are a class of neural networks with multiple layers between the input and output layers, capable of modeling complex patterns in data. The architecture typically consists of an input layer, multiple hidden layers, and an output layer, with each layer comprising numerous interconnected neurons. The network learns by adjusting the weights of these connections through backpropagation during training, enabling it to capture intricate data representations and improve detection accuracy.

Step 5: Performance Comparison

The final step involves a comparative analysis of the performance between the Random Forest Classifier and the Deep Neural Network models. Key metrics such as accuracy, precision, recall, and F1-score are evaluated to determine the effectiveness of each model in detecting malicious activities. This comparison provides insights into the advantages of

10.48047/jocaaa.2025.34.05.46

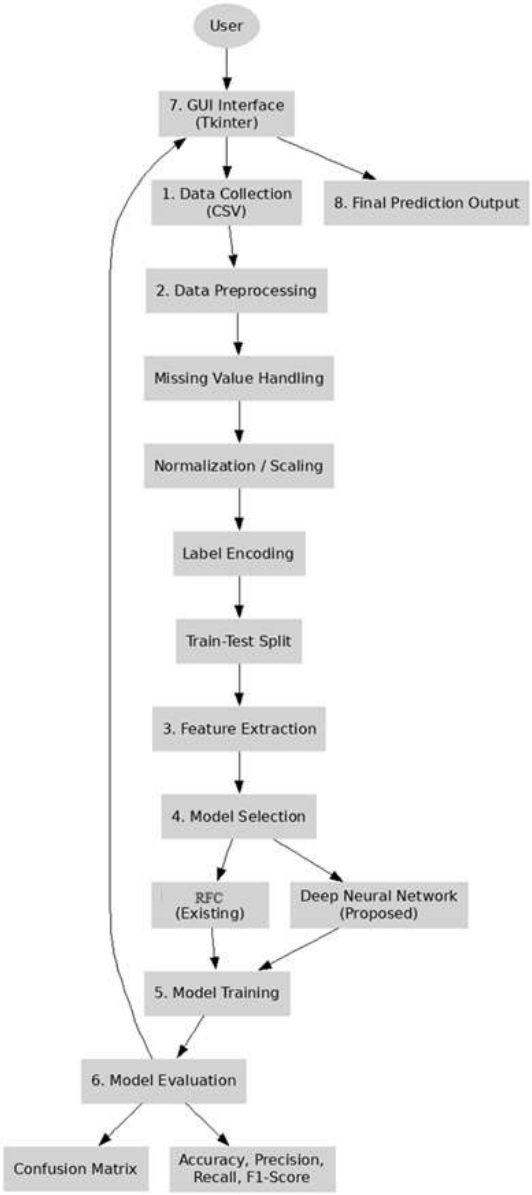

Fig. 1: Architectural Block Diagram of the Project.

employing deep learning techniques over traditional machine learning methods in the context of mobile edge security.

4. RESULTS AND DISCUSSION

The Figure 2 shows desktop application provides a user-friendly interface for analyzing data and detecting malicious activities in mobile edge security using machine learning techniques. The user can easily upload data, preprocess it, train different models, compare their performance, and make predictions.

10.48047/jocaaa.2025.34.05.46

Fig. 2: User Interface.

Fig. 3: Loaded Dataset.

This Figure 3 shows a snapshot of a dataset related to mobile edge security, loaded for analysis or machine learning purposes. The data includes various features related to app permissions and system settings, and a class label that is likely used for a classification task. The fact that it's a training dataset suggests that this data will be used to train a model to detect malicious activities in mobile edge environments. The large number of columns (216) indicates a rich dataset with many potential features for analysis.

10.48047/jocaaa.2025.34.05.46

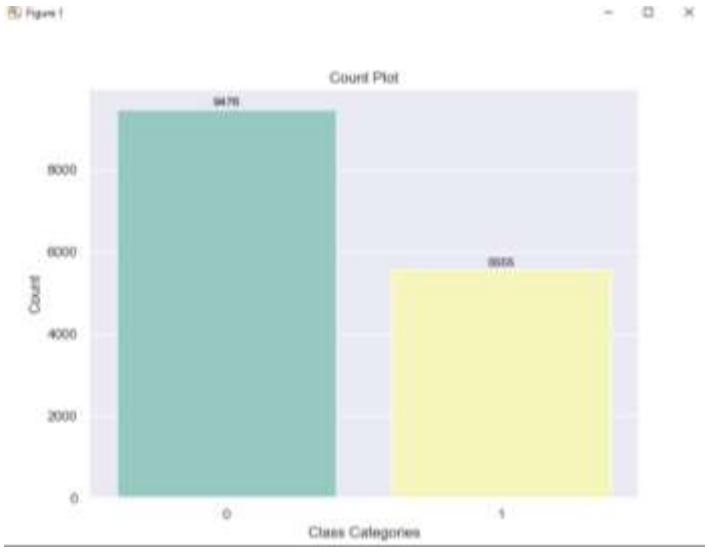

Fig. 4: Count Plot of The Target Column.

This Figure 4 shows count plot visualizes the distribution of two classes, revealing a significant class imbalance. This information is crucial for understanding the data and making informed decisions about further analysis or modelling. The class imbalance might reflect a real-world phenomenon. For example, if this data represents credit card transactions, it's natural to have many more legitimate transactions (Class 0) than fraudulent ones (Class 1).

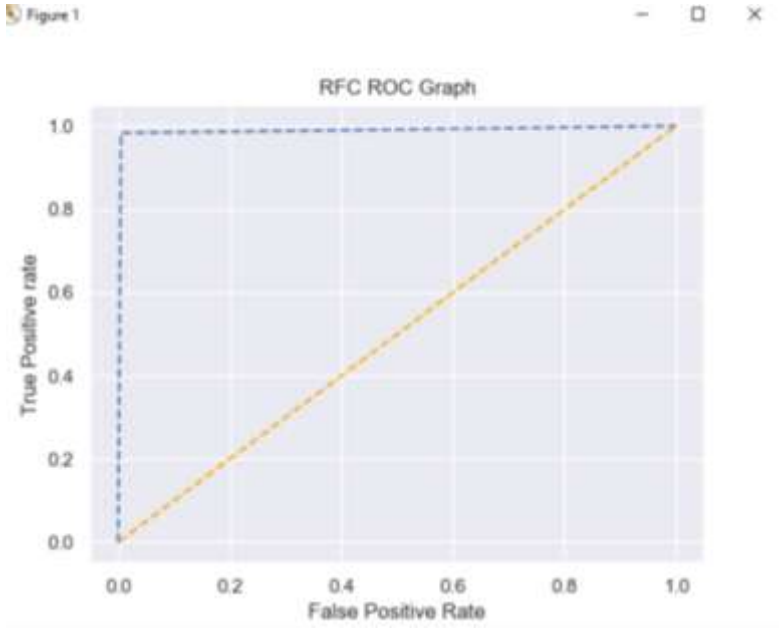

Fig. 5: ROC curve of the Random Forest

This Figure 5 shows the ROC curve demonstrates the excellent performance of the Random Forest Classifier. The high AUC and the shape of the curve indicate a model with strong predictive power. However, it's crucial to consider potential overfitting and evaluate the model's performance on diverse datasets to ensure its real-world applicability.

10.48047/jocaaa.2025.34.05.46

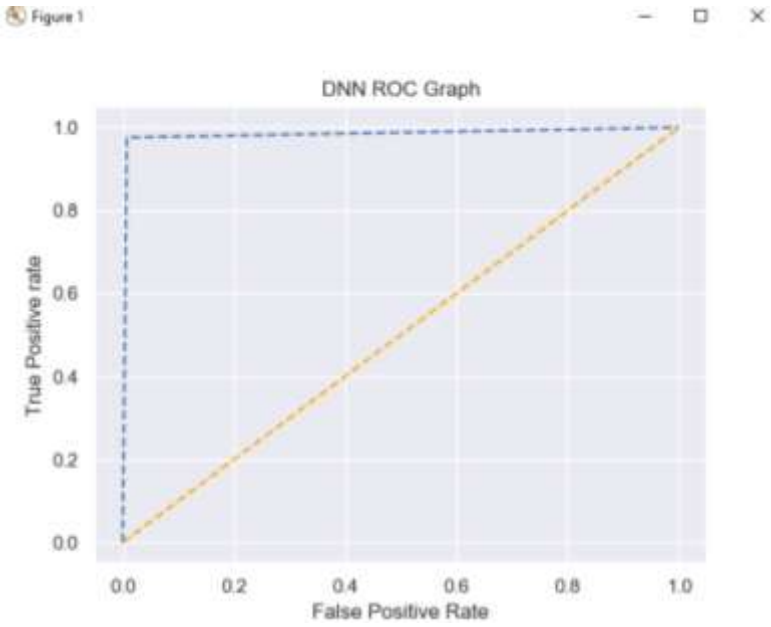

Fig. 6: ROC curve of the Deep Neural Network.

This Figure 6 shows the ROC curve illustrates the very strong performance of the Deep Neural Network model. The high AUC and the curve's shape indicate a model with excellent predictive capabilities. Further evaluation and validation are essential to confirm its robustness and generalizability.

Fig. 7: Predicted output on test input.

This Figure 7 shows the output of a security system classifying data as either "Secured" or "Attack Detected" based on binary data representing network traffic or system events. The system appears to be using pattern recognition to identify attacks, highlighting its potential usefulness in real-time security monitoring.

Metric	Random Forest (RF)	Decision Tree (DT)	Deep Neural Network (DNN)

10.48047/jocaaa.2025.34.05.46

Accuracy	99.17%	97.87%	99.67%
Precision	99.19%	97.53%	99.67%
Recall	99.00%	98.10%	99.43%
F1-Score	99.09%	97.68%	99.55%

Table 1: Performance metrics of all models.

The performance comparison table presents metrics for three classification models: Random Forest, Decision Tree, and Deep Neural Network. Among the three, the Deep Neural Network model achieved the highest overall accuracy (99.67%) with excellent precision, recall, and F1-score, indicating strong performance in both identifying and correctly classifying positive and negative cases. The Decision Tree model, while still accurate (97.87%), showed slightly lower precision and recall, particularly for the minority class. The Random Forest performed closely to DNN with balanced metrics and fewer misclassifications. Confusion matrices further illustrate that Random Forest made the least errors, reinforcing its superiority for this task.

5. CONCLUSION

The integration of deep learning (DL) into mobile edge computing (MEC) has significantly enhanced the security and efficiency of mobile networks. By leveraging the computational power of edge devices, DL models can process data locally, reducing latency and conserving bandwidth. This localized processing is particularly advantageous for real-time applications such as intrusion detection and threat analysis, where swift responses are crucial. Moreover, the adaptability of DL algorithms enables them to learn from evolving attack patterns, providing robust Défense mechanisms against sophisticated cyber threats. The deployment of DL in MEC environments presents several challenges. Edge devices often have limited computational resources, which can constrain the complexity of DL models that can be effectively implemented. Additionally, ensuring the privacy and security of data processed at the edge is paramount, as these devices are susceptible to various vulnerabilities. Addressing these challenges requires ongoing research and the development of optimized DL models tailored for resource-constrained environments. Despite these hurdles, the potential benefits of integrating DL into MEC for enhanced security are substantial, paving the way for more resilient and efficient mobile networks.

REFERENCES

[1]. R. Braden, “Requirements for Internet hosts-communication layers,” RFC 1122, Internet Engineering Task Force, Tech. Rep., Oct. 1989.

[2]. M. Korczy´nski and A. Duda, “Markov chain fingerprinting to classify encrypted traffic,” In Proc of IEEE INFOCOM, Toronto, ON, Canada, pp. 781-789, 2014.

[3]. B. Anderson and D. Mcgrew, “Identifying encrypted malware traffic with contextual flow data,” In Proc of the 2016 ACM Workshop on Artificial Intelligence and Security, New York, NY, USA, pp. 35-46, 2016.

10.48047/jocaaa.2025.34.05.46

[4]. E. Rescorla, “The transport layer security (TLS) protocol version 1.3,” RFC 8446, Internet Engineering Task Force, Tech. Rep., Aug. 2018.

[5]. C. Xu, S. Chen, J. Su, S. M. Yiu, and L. C. K. Hui, “A survey on regular expression matching for deep packet inspection: Applications, algorithms, and hardware platforms,” IEEE Communication Surveys and Tutorials, vol. 18, no. 4, 4th Quart., pp. 2991-3029, 201.

[6]. C. Meyer and J. Schwenk, “Lessons learned from previous SSL/TLS attacks: A brief chronology of attacks and weaknesses.” IACR Cryptology ePrint Archive, vol. 2013, p. 49, 2013.

[7]. Y. Zhao, S. Vemuri, J. Chen, Y. Chen, H. Zhou, and Z. Fu, “Exception trig-gered DoS attacks on wireless networks,” In Proc. of the 2009 IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), pp. 13–22, 2009.

[8]. J. Salowey, H. Zhou, P. Eronen, and H. Tschofenig, “Transport layer security (TLS) session resumption without server-side state,” RFC 5077, Internet Engineering Task Force, Tech. Rep.

[9]. R. Hummen, H. Wirtz, J. H. Ziegeldorf, J. Hiller, and K. Wehrle. “Tailoring end-to-end IP security protocols to the internet of things,” In Proc. Of 21st IEEE International Conference on Network Protocols (ICNP), pp. 1-10, 2013.

[10]. B. Anderson, S. Paul, and D. McGrew, “Deciphering malwares use of tls (without decryption),” J. Comput. Virol. Hacking Techn., vol. 14, no. 3, pp. 1–17, 2016.

C. Meyer and J. Schwenk, “Lessons learned from previous SSL/TLS.