International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 21 No. 3 (1) 2025

ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 21, No. 3(1), 2025

Research Paper

EDGE-OPTIMIZED DEEP LEARNING FOR ADAPTIVE MALICIOUS ACTIVITY DETECTION IN MOBILE EDGE NETWORKS

K. Vamshee Krishna[1], Mithin Reddy Ch[2], Mallesh Potharaju[2], Mahesh Matteri[2]
[1]Assistant Professor, [2]UG Student, [1,2]Department of Computer Science and Engineering
[1,2]Kommuri Pratap Reddy Institute of Technology, Hyderabad, Telangana, India.
[1]Email: vamshik825@gmail.com.

Received: 05-6-2025 Accepted: 06-7-2025 Published: 14-7-2025

ABSTRACT

Mobile Edge Computing (MEC) is an emerging paradigm designed to enhance the performance of mobile applications by bringing computation and data storage closer to end-users. However, the adoption of MEC has introduced new security challenges, as these systems have become prime targets for malicious activities such as data breaches, denial-of-service (DoS) attacks, and intrusion attempts. These threats exploit infrastructure vulnerabilities, compromising system integrity, availability, and confidentiality. Traditionally, mobile edge security relied on signature-based and rule-based detection methods, which could only identify known threats through predefined patterns. Such methods were ineffective against evolving or novel attack techniques. As cyber threats have grown more complex, the need for advanced detection strategies has led to the integration of machine learning (ML) into security frameworks. ML-based approaches enable real-time identification and prevention of both known and unknown attacks, significantly enhancing the security posture of MEC environments. The limitations of earlier systems, including high false-positive rates, poor detection of novel threats, and dependence on manual updates, have driven the shift toward automated ML solutions. By employing classifiers such as Decision Trees, Random Forests, and Deep Neural Networks, these systems analyze vast datasets to detect and classify malicious behaviors, thereby improving accuracy, scalability, and adaptability. Ultimately, ML-powered security models aim to create intelligent, self-evolving mechanisms that continually learn from new data and effectively respond to emerging security threats in mobile edge environments.

Keywords: Mobile Edge Computing (MEC, Cybersecurity in MEC, Deep Learning for Security, Anomaly Detection, Edge-Based Defense Systems.

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.

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 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.

Fig. 1: Architectural Block Diagram of the Project.

Proposed Model: Deep Neural Network (DNN) Model

The proposed model in this system is a Deep Neural Network (DNN), designed to enhance classification accuracy and robustness compared to traditional machine learning methods. DNNs are a class of artificial neural networks composed of multiple hidden layers between the input and output layers. These layers allow the network to model complex relationships and extract high-level features from the input data. In the context of classification tasks, DNNs excel in learning intricate patterns and correlations, making them highly effective for detecting subtle differences between classes. The model is built

using multiple dense layers, each consisting of several neurons that perform weighted computations and apply activation functions to introduce non-linearity. This architecture significantly improves the system's ability to generalize on unseen data, providing strong predictive performance.

Working of the Proposed Model

The working of the Deep Neural Network begins with the input layer, which receives the preprocessed feature vectors extracted from the dataset. These inputs are passed into a sequence of fully connected hidden layers. Each neuron in a hidden layer computes a weighted sum of its inputs and passes the result through a non-linear activation function, such as ReLU (Rectified Linear Unit), to produce an output. This output becomes the input for the next layer. The network adjusts the weights and biases during the training process through backpropagation, which calculates the error between the predicted and actual outputs and propagates the gradient backward through the network. The loss function, typically categorical cross-entropy in classification problems, quantifies the prediction error, and an optimization algorithm such as Adam is used to minimize this loss iteratively.

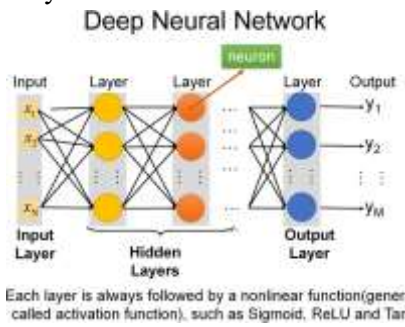

Fig. 2: working of Deep Neural Network.

As data moves through the hidden layers, the network extracts increasingly abstract features, enabling it to distinguish between complex patterns associated with different classes. In the final stage, the output layer, often using a softmax activation function, provides a probability distribution across the target classes. The class with the highest probability is selected as the final prediction. The model undergoes multiple training epochs to achieve convergence, where the loss stabilizes, and the accuracy reaches a high and consistent value. Validation metrics are computed to ensure that the model performs well on unseen data and does not overfit the training set.

Advantages of the Proposed Model

The DNN model achieves higher classification accuracy compared to traditional classifiers. It automatically extracts and learns complex features from raw data without manual intervention. It is scalable to large datasets and handles high-dimensional input efficiently. It improves generalization by capturing intricate patterns in the dataset. It reduces the risk of underfitting due to multiple trainable layers. It supports various activation functions and optimization techniques for flexible design. It provides better performance consistency across different data distributions. It is robust to noise and can tolerate minor variations in input data. It demonstrates strong capability in both binary and multi-class classification tasks.

4. RESULTS AND DISCUSSION

This Figure 3 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).

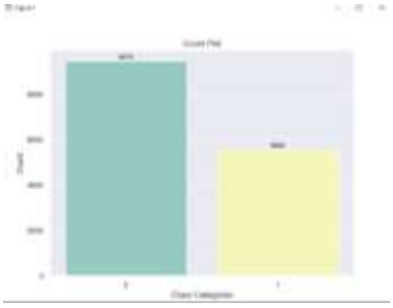

Fig. 3: Count Plot of The Target Column.

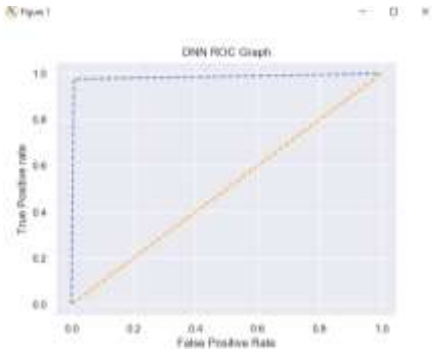

Fig. 4: ROC curve of the Deep Neural Network.

This Figure 4 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. 5: Predicted output on test input.

This Figure 5 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)
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 1 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 greatly strengthened both the security and performance of mobile networks. By utilizing the processing capabilities of edge devices, DL models can analyze data locally, minimizing latency and conserving bandwidth. This localized approach is especially valuable for real-time tasks such as intrusion detection and

threat assessment, where rapid response is essential. DL algorithms also offer strong adaptability, enabling them to learn from emerging attack patterns and deliver effective defense against advanced cyber threats. However, deploying DL in MEC environments brings notable challenges. The limited computational capacity of edge devices can restrict the complexity of DL models that are feasible in such settings. Moreover, safeguarding the privacy and security of locally processed data is critical, as edge devices remain vulnerable to multiple attack vectors. Overcoming these obstacles demands continuous research and the creation of lightweight, optimized DL models suited to resource-constrained platforms. Despite these challenges, the advantages of incorporating DL into MEC are significant, offering a path toward more secure, efficient, and intelligent mobile network infrastructures.

REFERENCE

[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.

[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 triggered 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.