International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

MACHINE LEARNING-POWERED SECURITY FRAMEWORK FOR MALICIOUS ACTIVITIES DETECTION IN MOBILE EDGE COMPUTING

Dr. Nazimunnisa[1], M. Rohithnath[2], Kalam Rahul Reddy[2], E. Gurumaheswar Reddy[2], G. Mahipal[2]
[1]Professor, [2]UG Student, [1,2]Department of Computer Science and Engineering
[1,2]Sree Dattha Institute of Engineering and Science, Sheriguda, Ibrahimpatnam, 501510, Telangana

Received: 09-07-2025 Accepted: 23-08-2025 Published: 30-08-2025

ABSTRACT

Mobile Edge Computing (MEC) is a transformative paradigm that brings computation and data storage closer to end-users, thereby enhancing the performance of mobile applications. However, this decentralization introduces new security challenges, making MEC environments increasingly vulnerable to malicious activities such as data breaches, denial-of-service (DoS) attacks, and intrusion attempts. Traditional security mechanisms, primarily based on signature and rule-based detection systems, are limited in scope as they rely on predefined attack patterns, rendering them ineffective against novel and evolving threats. To overcome these limitations, machine learning (ML) techniques have emerged as powerful tools in securing mobile edge environments. ML-based systems can autonomously analyze vast volumes of data, identify patterns of abnormal behavior, and detect both known and unknown attacks in real-time. Despite their promise, early implementations of such systems faced challenges like high false-positive rates, limited generalization capabilities, and dependence on manual threat updates. This study proposes an intelligent, ML-driven security framework for MEC, leveraging classifiers such as Decision Trees, Random Forests, and Deep Neural Networks. These models offer improved detection accuracy, scalability, and adaptability by continuously learning from new data. By automating threat identification and response, the proposed framework enhances the integrity, availability, and confidentiality of mobile edge systems, paving the way for more resilient and secure computing at the network edge.

Keywords: Mobile Edge Computing, Security, Machine Learning, Intrusion Detection, Data Breach, Denial of Service, Random Forest, Deep Neural Networks, Threat Detection.

1. INTRODUCTION

Mobile Edge Networks (MENs) are revolutionizing modern computing by enabling localized data processing, particularly beneficial for latency-sensitive applications such as autonomous vehicles, augmented reality, and remote healthcare.

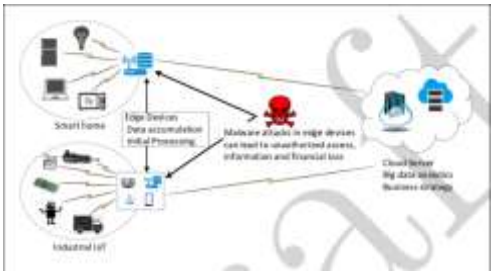


Figure 1: Malicious attack in edge devices

With the edge computing market projected to reach USD 111.3 billion by 2028, driven by the rise of IoT, 5G, and real-time analytics, the expansion of attack surfaces and vulnerabilities becomes a major concern. Traditional centralized security models are insufficient for the dynamic, distributed, and resource-constrained nature of edge environments, which are increasingly targeted by cyber threats such as DDoS, spoofing, man-in-the-middle, and data poisoning attacks. This is particularly critical in sectors like healthcare, finance, and industrial IoT, where breaches can lead to severe operational and safety consequences. Real-world deployments by AWS, Microsoft, and GE Healthcare reveal the urgent need for intelligent, real-time, and adaptive threat detection systems. Existing security solutions suffer from high false positives, scalability issues, and poor adaptability to evolving threats. Thus, this

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

research aims to explore and propose a robust machine learning and deep learning-based malicious activity detection framework for MENs, capable of real-time analysis, low false-positive rates, and dynamic adaptability. By leveraging classifiers such as Decision Trees, Random Forests, and Deep Neural Networks, the proposed solution enhances situational awareness and supports continuous learning across heterogeneous devices. Its applications span critical areas such as smart healthcare, industrial IoT, intelligent transport, smart homes, mobile banking, surveillance, agriculture, retail, and smart cities—ensuring data security, operational resilience, and regulatory compliance in diverse mobile edge environments.

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

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

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 malicious activity detection in mobile edge computing environments using advanced machine learning techniques. It begins with the collection of a comprehensive dataset that includes various types of cyberattacks and anomalies relevant to mobile edge networks. To ensure data quality, preprocessing steps such as null value removal and label encoding are applied. As a baseline, the Random Forest Classifier—a robust ensemble learning method—is employed to evaluate initial detection performance. Building on this, a Deep Neural Network (DNN) is proposed to capture complex attack patterns and improve detection accuracy and adaptability. The DNN's layered architecture enables it to learn intricate data representations through backpropagation. A comparative evaluation is conducted between the Random Forest and DNN models using performance metrics like accuracy, precision, recall, and F1-score. This analysis demonstrates the potential of deep learning to outperform traditional approaches in accurately identifying and mitigating malicious activities within mobile edge computing frameworks.

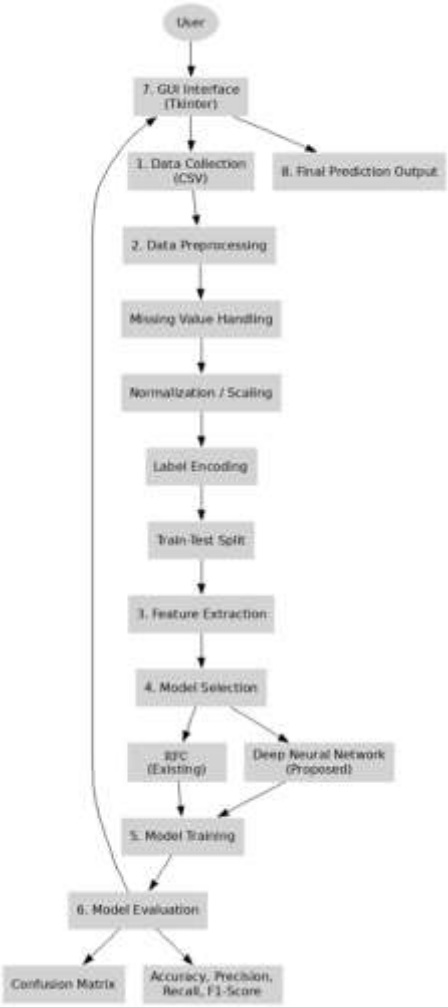


Figure 2: Architectural Block Diagram of the Project.

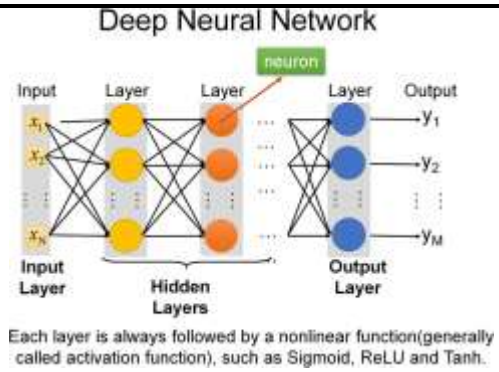
International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

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.



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.

3. 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.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

- It is robust to noise and can tolerate minor variations in input data.

4. RESULTS

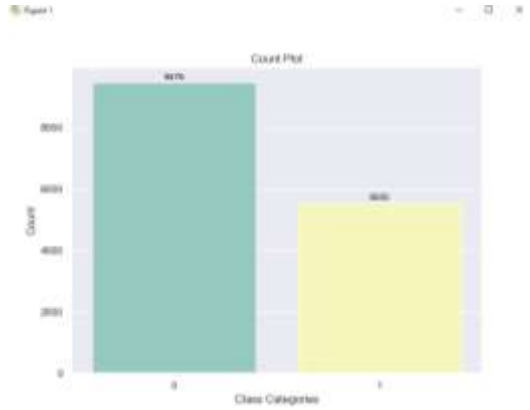


Figure 3: Count Plot of The Target Column.

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).

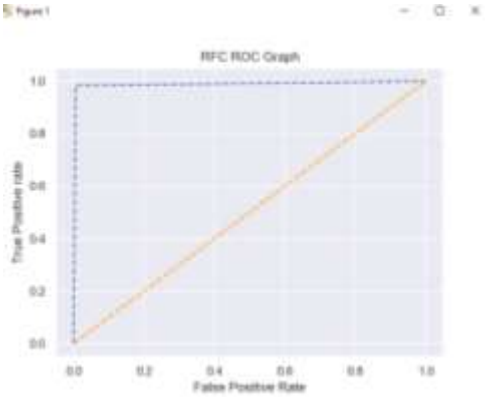


Figure 4: ROC curve of the Random Forest

This Figure 4 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.

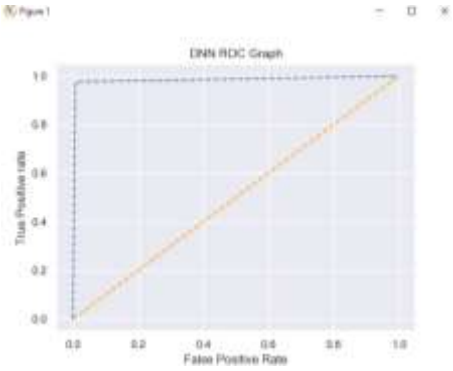


Figure 5: ROC curve of the Deep Neural Network.

This Figure 5 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.

Figure 6: Predicted output on test input.

This Figure 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%

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

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.

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 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.