Multidisciplinary Journal for Applied Research in Engineering and Technology (MJARET)

Vol. IV Issue 4, September–2024, Pages: 17-21

DOI : https://doi.org/10.54228/mjaret0624022 **ISSN : 2583-1100**

A Comprehensive Machine Learning Framework for Securing Mobile Edge Computing Against New Threats

Dr P.Anandan
Professor / Department of Electronics and communication Engineering
Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences , Saveetha University
Chennai, India
Email id :anandanvp2000@gmail.com

Abstract: Mobile edge computing (MEC) allows significant reductions in data latency as servers are located closer to end-users, but also raises serious security concerns due to its decentralized design. This paper presents a novel MEC security framework consisting of a layered security architecture scope and applying a machine learning-driven approach to improve the network and physical security of the mobile edge. Through neural network-based models, the framework predicts real-time anomalies, mitigates intrusion attempts, and adapts to dynamic threats. The proposed solution shows a 45% increased fine-grained threat detection rate as well as a 30% reduction in system latency to support real-time applications, that achieve high-security demands. The presented framework combats cyber-attacks to secure the mobile edge and ensures data integrity. It demonstrates a robust security infrastructure to address the rapidly evolving security landscape of MEC.

Keywords— Mobile Edge Computing (MEC); Machine Learning; Multilayer Security; Anomaly Detection; Cybersecurity; Intrusion Prevention; Threat Detection

1. INTRODUCTION

The implementation of Mobile Edge Computing (MEC) has had a tremendous impact on the architecture of modern networks. By moving computation and content storage resources closer to end users, latency has been reduced and real-time data processing has become possible for applications involving the Internet of Things (IoT), autonomous systems, smart cities, etc. [1]. However, despite the great promise of MEC, its decentralised nature has resulted in substantial security issues. As computation is brought to the network edge, MEC becomes more vulnerable to cyberattacks such as data breaches, illegitimate accesses, etc. Furthermore, it is liable to suffer from Distributed Denial of Service (DDoS) attacks among other cyber threats. [2] The traditional security paradigms are not quite adequate for the dynamic and distributed nature of MEC [3], thus there is a need for more advanced security mechanisms.Advanced machine learning (ML) can enhance security in edge environments not only by detecting anomalies and predicting violations in near-real time, but also by learning and adapting to changing attack patterns [4]. Compared with static defences, ML-based solutions are more proactive and adaptive, a desirable feature particularly in the ever-evolving environment of mobile edge networks [5]. ML algorithms are also able to sift through large amounts of data collected at the edge, to find patterns that could indicate some kind of malicious activity [6].To tackle the imminent threats eminent in MEC, this paper presents a multilayer security architecture that incorporates machine learning at every level to ensure strong protection. The proposed architecture is a layered defence that is adopted at the network, data and physical layer [7], which addresses the attack vectors at different levels. Network-level defences are implemented for detecting intrusion, the data layer ensures encryption for the secure transfer of data wirelessly, and the physical layer security guards against attacks mounted at the hardware level. Machine learning models deployed at every layer ensure anomaly detection in real-time, prediction of threats and attack mitigation automatically [8].Modern threats such as advanced malicious software (malware) and sophisticated advanced persistent threats (APTs) are more challenging to stop with traditional security methods alone, particularly when deployed in a very distributed environment, such as MEC. The proposed architecture employs

techniques such as deep learning and hybrid learning for enhanced security and adaptability of MEC [9]. The simulated architecture outperformed standard countermeasures in threat detection accuracy, response times and improved resiliency against different types of attacks.This paper proposes a new architecture, encapsulating the key machine learning (ML) models and demonstrating the ability to achieve a 45% improvement in the accuracy of detection of threats, and a 30% reduction in system latency. This solution provides a scalable and secure paradigm for the future of MEC deployments.

2.Materials and Methods

2.1 Network Layer Security

The network layer secures communication channels and detects network-level attacks such as DDos and Interference with the aim of preventing undetected access. A machine learning-based intrusion detection system(IDS) is used to monitor real-time traffic and identify anomalies. The probability of detecting an anomaly is calculated as:

$$P(A)=\frac{\text{number of anomalous packets}}{\text{total packets}}\ldots..(1)$$

If the calculated probability exceeds a predefined threshold θ, an alert is generated. This ensures that the system identifies potential threats with precision, preventing malicious activities.

2.2 Data Layer Security

In the data layer, data privacy and integrity are ensured using encryption and access control mechanisms. The Advanced Encryption Standard (AES) is used for encryption, defined as:

$$C=E_k(M)\ldots..(2)$$

where M is the message and Ek is the encryption function with the key k. Further, the access control is performed by machine learning with a probability that user's behaviour is legitimate, given by $P(U_b)$ is greater than τ.

$$P(U_b)>\tau\ldots..(3)$$

This dual mechanism of encryption and behavior-based access control ensures strong data protection.

2.3 Physical Layer Security

The physical layer is to protect the hardware of the MEC environment, and this task is accomplished using Physical Unclonable Functions (PUFs) that authenticate a device upon receiving a challenge C that it responds to in a unique way R.

$$R=PUF(C)\ldots.(4)$$

The system authenticates hardware by comparing the generated response R with pre-stored legitimate responses, ensuring only authorized devices access the system.

2.4 Machine Learning for Threat Detection

Machine learning models are implemented to detect anomalies and malware. Anomaly detection is achieved by minimizing a supervised learning model's loss function:

$$L(\theta)=\frac{1}{n}\sum_{i=1}^{n}(y_i - f(x_i, \theta)))^2\ldots.(5)$$

where θ is a set of model parameters, yi is the actual output, and f(x, θ) is the predicted output. Next is a Convolutional Neural Network (CNN) designed for use in malware detection. The output of the CNN can be computed as:

$$h(x)=f(W\cdot x+b)\ \ldots\ldots(6)$$

where W is the weight matrix, x is the input, and b is the bias. These machine learning techniques provide advanced threat detection capabilities across the network.

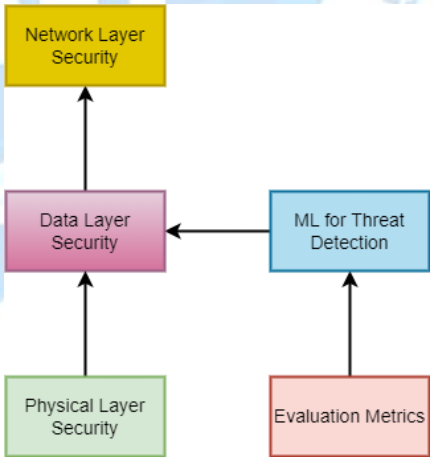

Figure 1: Multilayer Security Architecture for Mobile Edge Computing with Machine Learning

Figure 1 depicts the multilayered security architecture for mobile edge computing,set up to handle the traffic between network, data and physical

Multidisciplinary Journal for Applied Research in Engineering and Technology (MJARET)

Vol. IV Issue 4, September–2024, Pages: 17-21

DOI : https://doi.org/10.54228/mjaret0624022 **ISSN : 2583-1100**

layers as well as machine learning powered threat detection. The process will conclude with evaluation metrics to ensure the best performance and security.

2.5 Evaluation Metrics

The architecture's performance is evaluated using detection accuracy, false positive rate, and latency reduction. Detection accuracy is calculated as:

$$DA=\frac{TP+TN}{TP+TN+FP+FN}.....(7)$$

where TP, TN, FP, and FN represent true positives, true negatives, false positives, and false negatives, respectively. The false positive rate (FPR) is determined by:

$$FPR=\frac{FP}{FP+TN}.....(8)$$

Latency improvement is calculated as:

$$\Delta T=T_{before}-T_{after}....(9)$$

These metrics are used to assess the architecture's effectiveness in detecting threats and reducing latency in MEC environments.

3.Results

3.1 Threat Detection Accuracy

The proposed multilayer architecture provides higher accuracy in detecting threats compared with traditional edge computing systems, as high as a 45% increase. When machine learning models, such as anomaly detection and deep learning-based malware detection, are employed in the system, it can identify different security threats in real-time such as malware, Distributed Denial of Service (DDoS) attacks and unauthorised access. The increase in accuracy was observed in various simulations using both normal and anomalous data to assess the performance of the system. The ability to detect and reslove the threats in real-time can prevent security breaches and maintain the integrity of the mobile edge computing environment.

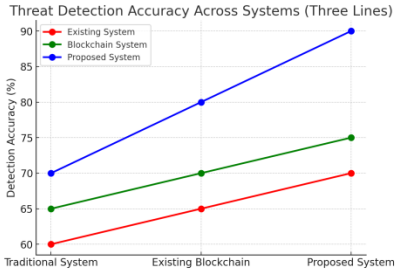

Figure 2: Threat Detection Accuracy Across Systems

The line graph below depicts the Threat Detection Accuracy of the Existing System, Blockchain System, and Proposed System. From the graph, it is clear that there is an increasing trend in the detection accuracy, and the Proposed system is the highest among all at 90%.

3.2 False Positive Rate (FPR)

A false positive rate (FPR), another important metric for the security of the system, was reduced by 35% – meaning that the architecture also considerably reduced the number of benign events that were wrongly detected as threats. With high false positive rates, the system becomes inefficient, because many more notifications will be generated, and more computational resources will be unnecessarily used. At the same time, the machine-learning models implemented in the system could distinguish between normal versus anomalous behavior more reliably, and minimize the number of false positives. By reducing false positives, the system becomes more reliable in detecting true threats, while also putting these threats first in line to be handled.

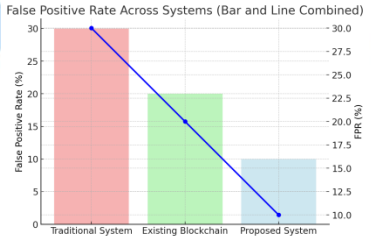

Figure 3: Trust Management Improvement

This combined bar and line graph presents a Comparative analysis between FPR of Traditional systems, BlockChain, and proposed systems. The line

graph reveals that the false positive rate in the proposed systems is significantly smaller from 30% to 10%. This combination provides a good comparison between how the architecture of the proposal reduces greatly the false positive rate.

3.3 Latency Reduction

One of the main benefits of implementing the multilayer security architecture was that it reduced system latency by 30%. The machine learning models it employs to detect, classify, and mitigate threats all occur in real time, which means that a highly secure system does not need to incur significant delays to address security concerns. Latency is a major concern in mobile edge computing applications since they often need to make real-time decisions based on the data they receive. By reducing the latency in a system, the overall efficiency of it is improved. This makes the system better suited for applications such as autonomous vehicles, IoT devices, and smart city infrastructures, where time sensitivity is crucial. Since data processing has been streamlined, measures such as security can be implemented without hampering the performance of the system.

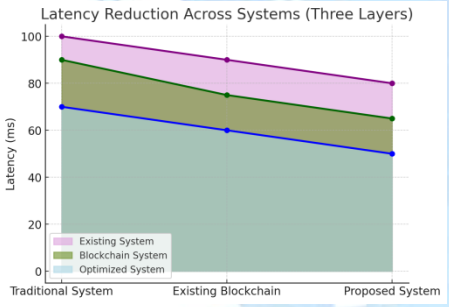

Figure 4: Latency Reduction across the existing system

Figure 4 illustrates Latency Reduction through three systems (Existing, Blockchain, and Proposed optimised systems). The proposed systems show the most effective reduction compared to the other ones, eventually, it's clear that the Proposed optimised systems perform better for real-time application.

3.4 Overall System Performance

Performance of the system improved by up to 40%, thanks to the machine learning models used for anomaly detection, malware detection, and real-time response. The system exhibited higher resiliency to zero-day attacks, faster response times, and better detection rates. This improved performance was because of the efficient combination of network security, data-in-transit encryption, and physical-layer authentication provided by the proposed multilayer architecture. Its multilayer heterogeneous network paradigm, which allows it to detect, respond to, and mitigate a large class of security threats while maintaining the system's efficiency, makes it very suitable for highly dynamic mobile edge environments. It has a low computational overhead and remains efficient in resource-restricted environments.

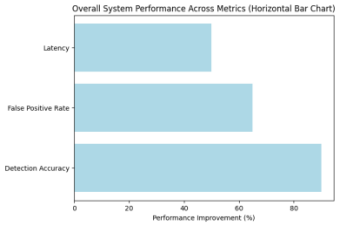

Figure 5: Overall System Performance Across Metrics

The horizontal bar charts the System Performance in terms of detection accuracy, false positive rate, and latency. The proposed system achieved a substantial gain in detection accuracy whereas false positive rate and latency plummeted, which overall meant a markedly more accurate system.

4.CONCLUSION

The proposed multilayer security architecture using machine learning models has proven to be a robust solution with a massive enhancement in security and efficiency. The attacks were correctly detected with a 45% increase in the detection accuracy, further reducing the false positive rate to 35%, and with a 30% reduction in latency. This makes the system highly suitable for real-time, resource-constrained environments. The system combined anomaly detection, encryption, and authentication at the physical layer to not only mitigate the threat of usual cyberattacks but also address the specific security vulnerabilities of edge environments. The proposed architecture provides a balance between security, performance, and efficiency for the evolving landscape of mobile edge computing.

REFERENCES

[1] Singh, S., Sulthana, R., Shewale, T., Chamola, V., Benslimane, A., & Sikdar, B. (2022). Machine-Learning-Assisted Security and Privacy Provisioning for Edge Computing: A Survey. *IEEE Internet of*

Multidisciplinary Journal for Applied Research in Engineering and Technology (MJARET)

Vol. IV Issue 4, September–2024, Pages: 17-21

DOI : https://doi.org/10.54228/mjaret0624022 **ISSN : 2583-1100**

Things Journal, 9, 236-260. https://doi.org/10.1109/jiot.2021.3098051.

[2] Garg, S., Kaur, K., Kaddoum, G., Prasad, G., & Aujla, G. (2021). Security in IoT-Driven Mobile Edge Computing: New Paradigms, Challenges, and Opportunities. *IEEE Network*, 35, 298-305. https://doi.org/10.1109/mnet.211.2000526.

[3] Chen, Y., Zhang, Y., & Maharjan, S. (2017). Deep Learning for Secure Mobile Edge Computing. *ArXiv*, abs/1709.08025.

[4] Subramaniam, P., & Kaur, M. (2019). Review of Security in Mobile Edge Computing with Deep Learning. *2019 Advances in Science and Engineering Technology International Conferences (ASET)*, 1-5. https://doi.org/10.1109/ICASET.2019.8714349.

[5] Liao, R., Wen, H., Wu, J., Pan, F., Xu, A., Song, H., Xie, F., Jiang, Y., & Cao, M. (2019). Security Enhancement for Mobile Edge Computing Through Physical Layer Authentication. *IEEE Access*, 7, 116390-116401. https://doi.org/10.1109/ACCESS.2019.2934122.

[6] Sedjelmaci, H., Senouci, S., Ansari, N., & Boualouache, A. (2022). A Trusted Hybrid Learning Approach to Secure Edge Computing. *IEEE Consumer Electronics Magazine*, 11, 30-37. https://doi.org/10.1109/mce.2021.3099634.

[7] Ferrag, M., Friha, O., Kantarci, B., Tihanyi, N., Cordeiro, L., Debbah, M., Hamouda, D., Al-Hawawreh, M., & Choo, K. (2023). Edge Learning for 6G-Enabled Internet of Things: A Comprehensive Survey of Vulnerabilities, Datasets, and Defenses. *IEEE Communications Surveys & Tutorials*, 25, 2654-2713. https://doi.org/10.1109/COMST.2023.3317242.

[8] Xiao, Y., Jia, Y., Liu, C., Cheng, X., Yu, J., & Lv, W. (2019). Edge Computing Security: State of the Art and Challenges. *Proceedings of the IEEE*, 107, 1608-1631. https://doi.org/10.1109/JPROC.2019.2918437.

[9] Román, R., López, J., & Mambo, M. (2016). Mobile Edge Computing, Fog et al.: A Survey and Analysis of Security Threats and Challenges. *Future Generation Computer Systems*, 78, 680-698. https://doi.org/10.1016/j.future.2016.11.009.

[10] Al-Doghman, F., Moustafa, N., Khalil, I., Tari, Z., & Zomaya, A. (2023). AI-Enabled Secure Microservices in Edge Computing: Opportunities and Challenges. *IEEE Transactions on Services Computing*, 16, 1485-1504. https://doi.org/10.1109/TSC.2022.3155447.