Journal of Theoretical and Applied Information Technology
31st May 2025. Vol.103. No.10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

HYBRID INTRUSION DETECTION FRAMEWORK FOR MOBILE EDGE COMPUTING

SUJAN KUMAR DAS[1], MOHAMED EL-DOSUKY[2,3], SHERIF KAMEL[2,4]

[1]Next Tech Lab, SRM University - AP, Andhra Pradesh, India.

[2]Computer Science Department, Arab East Colleges, Saudi Arabia

[3]Computer Science Department, Faculty of Computers and Information, Mansoura University, Egypt

[4]Department of Communications and Computer Engineering, October University for Modern Sciences and Arts, Egypt

E-mail: maldosuky@arabeast.edu.sa

ABSTRACT

The growing use of mobile edge computing (MEC) has had a positive impact on user experience and reduced latency. However, this closeness also makes MEC environments vulnerable to a number of security risks. This research article presents an edge-based hybrid intrusion detection system for MEC and the Internet of Things (IoT). The system uses techniques like behavioral analysis, anomaly detection, and signature-based detection, ensuring real-time response and reduced bandwidth usage. The system also addresses challenges in data acquisition and cleaning due to potential threats from malicious users and noise. The model uses smoothing filters, unsupervised learning, and deep learning techniques to detect anomalies and threats, reducing bandwidth. According to the findings, securing MEC environments against changing cyber threats can be accomplished using an edge-based hybrid intrusion detection system.

Keywords: *Mobile edge computing, Intrusion detection, Blockchain, Hybrid intrusion, Machine learning*

1. INTRODUCTION

Machine learning is a subset of artificial intelligence (AI) in which the AI is able to perform perceptive tasks within a fraction of the time it would take a human.

Edge computing refers to the act of bringing computing services physically closer to either the user or the source of the data. These computing services exist on what we call edge devices, a computer that allows for raw data to be collected and processed in real-time, resulting in faster, more reliable analysis. Machine learning at the edge brings the capability of running machine learning models locally on edge devices, such as the Internet of Things (IoT)[1].

The rise of edge computing has allowed machine learning models to be deployed on edge devices such as smartphones and Internet of Things (IoT) devices. However, the implementation of machine learning models on edge devices presents a unique set of security challenges that need to be addressed.

One of the primary concerns in implementing machine learning models on edge devices is the issue of data privacy [2]. Edge devices typically store and process data locally, which makes them vulnerable to data breaches and attacks. In order to address this concern, the authors of the paper propose the use of secure enclaves, such as Intel's Software Guard Extensions (SGX), to protect the data and ensure its confidentiality.

Another challenge in implementing machine learning models on edge devices is the risk of model theft and reverse engineering [3]. Attackers can steal machine learning models and use them for malicious purposes. To mitigate this risk, the authors propose the use of model obfuscation techniques, such as function obfuscation and code packing, to make the models more difficult to reverse engineer.

Furthermore, the article also discusses the issue of model poisoning attacks, where attackers can inject malicious data into the training dataset to manipulate the model's behavior.

Figure 1 shows the Mobile edge computing architecture.

The authors propose the use of data poisoning detection mechanisms, such as Mahalanobis distance-based methods and clustering-based methods, to detect and prevent such attacks[4].

Edge-based machine learning (ML) applications refer to ML models that run on devices like mobile phones, IoT devices, and other edge devices, rather than running on a centralized server.

While edge-based ML applications have numerous benefits, including faster processing and better privacy, they are also more vulnerable to security threats.

To ensure the security of edge-based ML applications, there are several measures that developers and organizations can take. These include:

Secure communication [5]: Use secure communication protocols, such as HTTPS and SSL/TLS, to ensure that data transmitted between edge devices and servers is encrypted and secure.

Data encryption: Use data encryption techniques, such as AES, to encrypt sensitive data stored on edge devices to prevent unauthorized access.

Secure software development: Ensure that the software used to develop and deploy the ML model is secure by implementing security best practices, such as regular code reviews and security testing [4].

Continuous monitoring: Implement continuous monitoring and analysis of the edge-based ML application to identify any security threats or vulnerabilities and take appropriate action.

Organizations can also consider leveraging the expertise of third-party security providers to help ensure the security of their edge-based ML applications [3].

The paper highlights the various security challenges in implementing machine learning models on edge devices and proposes solutions to address them. The use of secure enclaves, model obfuscation techniques, and data poisoning detection mechanisms can help ensure the security of edge-based machine learning applications.

The problem statement can be stated as: the adoption of Mobile Edge Computing (MEC) reduces latency but introduces security challenges due to the proximity of resources. Traditional IDSs are not suited for MEC due to their centralized and resource-heavy nature. Recent studies highlight the need for hybrid IDS solutions to improve detection accuracy and reduce resource consumption.

The research questions can be listed as:

1. How can a hybrid IDS framework combining signature-based and anomaly-based detection techniques be designed for MEC?
2. What machine learning algorithms and data preprocessing methods can enhance detection accuracy?
3. How can the IDS framework be optimized for resource constraints in edge devices?
4. How does the proposed IDS compare to existing solutions in terms of performance metrics?

The research hypothesis can be stated as: the integration of hybrid intrusion detection techniques, combining signature-based and anomaly-based detection, will significantly enhance the detection accuracy and reduce false positives in Mobile Edge Computing (MEC) environments compared to traditional IDS methods.

The research objectives are as follows:

1. Design and implement a hybrid IDS framework for MEC, integrating signature-based and anomaly-based detection.
2. Improve detection accuracy using machine learning algorithms and data preprocessing.
3. Optimize the IDS to operate efficiently within the constraints of edge devices.
4. Evaluate performance based on detection rate, false positive rate, and computational overhead.

The aim of this study is to develop a novel hybrid intrusion detection framework specifically tailored for Mobile Edge Computing (MEC) and Internet of Things (IoT) environments, where traditional security approaches fall short due to latency, mobility, and resource constraints. The novelty of this research lies in integrating behavioral analysis, anomaly detection, and signature-based methods within an edge-based architecture that supports real-time threat detection while minimizing bandwidth usage. Outcome measures include detection accuracy, false positive/negative rates, processing time, and bandwidth efficiency. The system incorporates unsupervised and deep learning techniques with data preprocessing strategies like smoothing filters

to enhance reliability and robustness in noisy or adversarial environments.

Despite its contributions, the study faces limitations such as dependency on benchmark datasets that may not fully reflect real-world MEC traffic, the computational overhead of deep learning on constrained edge devices, potential false alarms in highly dynamic conditions, and privacy concerns related to behavioral data monitoring. These limitations provide directions for further optimization and real-world validation.

2. LITERATURE REVIEW

The emergence of the smart auto sectors has led to the development of Internet of Vehicles (IoV) technologies. It makes it possible for vehicles to engage with the environment, exchange and gather data about other moving objects and roads, and assure road safety [6]. IoV systems, however, confront numerous difficulties, including huge data dissemination and gathering, as well as quick and effective communication between smart devices and cars. Machine learning (ML) is one of the answers provided by AI technology to deal with these problems. In order to address the issues facing IoV applications, this paper seeks to present theoretical underpinnings for ML and the top models and algorithms.

In the Internet of Vehicles (IoV), this work addresses analytical modeling for offloading decisions made by mobile edge computing using machine learning and Deep Reinforcement Learning (DRL) techniques [1,4].

The significant potential for performing intelligent cognitive sensing, intelligent network management, big data analytics, and security enhancement for edge-based smart applications has been demonstrated by many AI-based solutions utilizing machine learning, deep learning, and swarm intelligence. Despite all of its advantages, there are still questions regarding the capacities that intelligent edge computing will need to handle the computational complexity of machine learning approaches for massive IoT data analytics. For the purpose of enhancing the quality of service and creating edge-based smart applications efficiently, it is important to pay attention to the resource restrictions of edge computing, distributed computing, efficient orchestration, and resource synchronization. In order to fully utilize the promise of the existing research in this area, this paper explores the intersection of AI and edge in a variety of application domains [4, 7].

Due to its features and quick distribution method, the Mobile Edge Computing (MEC) model draws more consumers to its services. Users can get information from the edge of the network thanks to this feature of the network architecture. However, this edge network architecture's security presents a significant difficulty. Users can access all MEC services through the Internet in a shared environment.

Due to Internet-based remote services, attacks like user to root, remote login, Denial of Service (DoS), snooping, port scanning, etc., may be conceivable in this computing environment. A method of network protection called intrusion detection looks for assaults. Only known attacks can currently be detected by existing detection algorithms, and real-time network traffic monitoring effectiveness is poor [4,8].

Many daily services are changing as a result of the development of cloud computing and Internet of Things (IoT) environments, such as healthcare systems, telecommunications, and Industry 4.0 or Industrial IoT (IIoT). Security concerns are therefore helpful for properly protecting these cutting-edge systems. IIoT security poses significant difficulties for both commercial players and academic study. To increase the security of IIoT environments, a number of security strategies, including intrusion detection, are combined. So, an intrusion detection system's (IDS) goal is to keep track of activity, spot an incursion in real time, and then take action. In order to increase their accuracy (ACC), precision, and detection rate (DR), many modern IDS use machine learning (ML) approaches. The hybrid IDS for Edge-Based IIoT Security presented in this study uses ML approaches [7,9].

A new 5G technology called multi-access edge computing (MEC) brings the advantages of cloud computing closer to the consumer. The connectivity between mobile users and the MEC host is described in the existing MEC specifications, but there are problems with application-level security and privacy. In the non-roaming example, we think about how to offer private and secure communication routes between a mobile user and a MEC application. It comprises protocols for user registration on the MEC application's main server, shared key renewal, and MEC application use on the MEC host whether the user is stationary or mobile. They created a privacy-enhanced variation of the 5G authentication and key management for applications (AKMA) service for these protocols [8,10].

The intrusion detection framework for mobile edge computing (MEC) will be influenced by a number of variables, including the environment's unique requirements, limitations, and characteristics. Here are some things to think about when choosing the best techniques:

2.1 Hybrid Approach:

A hybrid approach can be more successful at identifying a variety of threats and reducing false positives/negatives by combining different intrusion detection approaches, such as anomaly detection, signature-based detection, and behavior analysis [7, 10].

2.2 Behavioral Analysis and Anomaly Detection:

Mobile edge computing settings frequently feature dynamic and varied behaviors. This is known as behavioral analysis and anomaly detection. It is possible to recognize aberrant actions and discover unique and unidentified risks by using behavioral analysis and anomaly detection.

2.3 Federated Learning (for privacy):

Federated learning can be a useful strategy if privacy is a top need. It enables collaborative training of intrusion detection models across edge devices without transferring raw data, protecting user privacy.

2.4 Transfer Learning (Limited Data):

Transfer learning can use pre-trained models from related tasks or domains to speed up model development and adaption in situations with little labeled data.

2.5 Ensemble Methods:

Multiple intrusion detection models can be combined in ensemble approaches to increase detection precision and strengthen the system's resilience.

2.6 Edge detection with cloud augmentation:

Cloud-augmented edge detection can offload some operations to the cloud in cases when edge devices have constrained processing capabilities, allowing for more in-depth analysis.

2.7 Edge-Cloud Collaboration for Model Updates:

Maintaining an up-to-date intrusion detection system while balancing resource usage at the edge is possible with the support of edge-cloud collaboration for model changes.

2.8 Real-time Response Mechanism:

Make that the framework provides a real-time response mechanism to address threats immediately, regardless of the detection technique. The optimum approach will be determined by the particulars of the mobile edge computing environment, the resources at hand, the desired level of security, privacy considerations, and the particular dangers that need to be addressed.

The critique of literature review is provided in Table 1, showing context of usage, strength, limitations, and suggestions for each reference.

3. NEWLY PROPOSED SYSTEM

Previous research has explored various intrusion detection techniques for MEC environments, including machine learning-based methods and rule-based approaches. However, these methods often face challenges in achieving high accuracy and efficiency. Meta AdaBoost Regression, a variant of the AdaBoost algorithm, shows promise in addressing these challenges by combining the advantages of multiple base learners.

Figure 2 shows the proposed model. This paper proposes an edge-based hybrid intrusion detection framework which consists of the following steps:

3.1 Data Preprocessing

Collect raw network traffic data from edge devices and preprocess it to extract relevant features. Apply techniques such as data normalization, dimensionality reduction, and feature selection to enhance the quality of the input data.

3.2 Anomaly-based Detection

Employ a machine learning model (e.g., Isolation Forest, One-Class SVM) to identify anomalies in the network traffic data [4,11]. Anomalies are instances that significantly deviate from the expected behavior, indicating potential intrusions.

3.3 Signature-based Detection

Utilize signature-based detection techniques (e.g., Snort rules, YARA rules) to identify known patterns of malicious activities. Signature-based detection focuses on identifying predefined attack patterns based on the established signatures [4].

3.4 Blockchain-based Detection

Blockchain technology is one potential way to improve the security of mobile edge computing settings. Blockchain is a distributed

ledger system that enables safe and transparent record-keeping. By introducing blockchain into the hybrid intrusion detection framework, it would be feasible to build a tamper-proof record of all transactions and events that occur within the mobile edge computing environment. This would make it far more difficult for attackers to change or fabricate data, and would add an extra layer of protection to the system [12].

In terms of implementation, a private blockchain network may be set up within the mobile edge computing environment, with each edge device operating as a node in the network. The intrusion detection algorithms may then be connected with the blockchain, allowing them to report any identified intrusions or abnormalities onto the blockchain in real-time. This would offer a safe and visible record of all security occurrences, which could be utilized for forensic investigation and to improve the overall security posture of the system.

First, blockchain technology creates a tamper-proof and transparent record of all transactions and events that take place in the mobile edge computing environment. This makes it far more difficult for attackers to change or falsify data while also adding an extra layer of security to the system. By introducing blockchain into the hybrid intrusion detection framework, it will be feasible to build a secure and transparent record of all security events that can be utilized for forensic investigation and to improve the system's overall security posture.

Second, because blockchain technology is decentralized and dispersed, it is particularly resistant to attacks. Even if one or more network nodes are compromised, the rest of the network can continue to operate normally. This adds another layer of defense against assaults designed to disrupt or disable the system.

Third, blockchain technology can provide a safe and efficient way of sharing data between edge devices as well as between the edge and the cloud. This allows edge devices to offload part of their work to more capable cloud-based systems, which can assist to ease some of their resource constraints.

In summary, the combination of blockchain technology and the existing hybrid intrusion detection framework should provide a robust and effective solution for protecting mobile edge computing environments from cyber-attacks. It would provide a layer of security and transparency while also using the characteristics of both technologies to produce a robust and resilient system.

Figure 3 shows blockchain based hybrid intrusion detection. Here is a high-level overview of the proposed blockchain-based intrusion detection method. Let ‘B’ be the private blockchain network set up within the mobile edge computing environment, where each edge device ‘e’ is a node in the network. Let ‘I’ be the set of existing intrusion detection algorithms integrated with the blockchain.

When an intrusion or anomaly is detected by an algorithm ‘i’ in ‘I’, the relevant edge device ‘e’ creates a new block ‘b’ containing the details of the event, such that b = f(i, e), where ‘f’ is a function that generates a new block based on the output of the intrusion detection algorithm ‘i’ and the state of the edge device ‘e’.

The edge device ‘e’ then broadcasts the block ‘b’ to the rest of the network, such that all other nodes ‘n’ in the network receive the block. Each node ‘n’ validates the block using a validation function ‘v’, such that v(b, n) = true if the block is valid and v(b, n) = false if the block is invalid.

If the block is valid, it is added to the local copy of the blockchain for each node `n`, such that $B_n = B_n \cup \{b\}$, where ‘B_n’ is the local copy of the blockchain for node ‘n’. The block is then added to the global blockchain ‘B’, creating a tamper-proof record of the security event.

This algorithm can be expressed mathematically as follows:

```
B = ∅
for each i in I:
    if i detect an intrusion or anomaly:
        b = f(i, e)
    Broadcast b to all n in network
for each n in the network:
  if v(b, n) = true:
    Bn = Bn ∪ {b}
     B = B ∪ {b}
```

This algorithm provides a secure and transparent method for detecting and recording security events in mobile edge computing environments using blockchain technology. By recording all security events onto a tamper-proof blockchain, it will be possible to improve the overall security posture of the system and provide a reliable record for forensic analysis.

Journal of Theoretical and Applied Information Technology
31st May 2025. Vol.103. No.10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3.5 Evaluation:

First, split the dataset into training and testing sets, ensuring temporal integrity for realistic evaluation. Train the individual base detectors and the Meta AdaBoost Regression model on the training data. Then, evaluate the framework's performance using standard metrics such as accuracy, precision, recall, F1-score, and area under the receiver operating characteristic curve (AUC-ROC) on the testing data.

3.6 Meta AdaBoost Regression:

Combine the outputs of both anomaly-based and signature-based detectors using the Meta AdaBoost Regression algorithm. Meta AdaBoost Regression assigns weights to the individual detectors and aggregates their decisions to make a final prediction [4,8].

Then the algorithm can be expressed as follows:

- Initialize instance weights: $w_i^{(t=0)} = \frac{1}{N}$, where t is the iteration number.
- For t = 1 to T(number of boosting iterations):
  i. Normalize instance weights: $w_i^{(t)}=w_i^{(t-1)}/\sum_{j=1}^{N} w_j^{(t-1)}$.
  ii. Train a base detector on x with weights $w^{(t)}$: AD_t =TrainBaseDetector(X,$W^{(t)}$).
  iii. Compute the weighted error $\varepsilon_t= \sum_{i=1}^{N} w_i^{(t)}$. II($y_i \neq h_t(x_i)$), where y_i is a true label and $h_t(x_i)$ is the prediction of base detector AD_t for instance x_i.
  iv. Compute the base detector weight: $\alpha_t= \frac{1}{2}$Ln($(1-\varepsilon_t)/\varepsilon_t$).
  v. Update instance weights: $w_i^{(t+1)}=w_i^{(t)}.\exp(-\alpha_t.h_t(x_i))$.
- Compute the Meta AdaBoost Regression score for each instance:
- $S_{MetaAdaBoost} = \sum_{t=1}^{T} \alpha_t.h_t(x_i)$, which represents the final combined prediction.

4. RESULTS

The suggested hybrid intrusion detection system for Mobile Edge Computing (MEC) has shown compelling results, demonstrating its efficacy in boosting security measures inside MEC environments. Notably, when compared to traditional intrusion detection approaches, the framework has demonstrated a significant increase in accuracy. The combination of various detection techniques, such as behavioral analysis, anomaly detection, and signature-based detection, is credited with this improvement [13,14]. Through careful examination, it is clear that the framework produces a significant increase in the true positive rate (TPR), indicating its ability to detect genuine security concerns while minimizing false negatives. Furthermore, the hybrid approach has resulted in a significant increase in precision, a critical parameter in intrusion detection. The system has shown a considerable reduction in false positives by merging several detection approaches, raising precision levels [15]. The hybrid framework's precision rate exceeds that of individual detection approaches, making it a solid alternative for reducing false alarms and optimizing resource allocation for threat mitigation.

Table 2 shows the measurement factors, while Table 3 shows performance metrics.

When it comes to the precision and accuracy of Hybrid methodology, we can see that the Exploits attack class has the highest recall rate (98%) of all attack classes, followed by the Normal Class (95%) with very few demarcations, and we can see that we have a very low recall rate when compared to the other potential attack classes, which account for only 5.5% of the recall rate. In terms of precision, the Generic Attack class has the greatest precision rate of 94%, followed by Exploits, Shellcode, and Worms attack classes, which have precision rates of 92%, 91%, and 90.5%, respectively. The Normal attack class achieves the lowest precision percentage of 85%, which is quite respectable when compared to other models.

Figure 4 shows Precision & Recall graph. In addition to improved accuracy and precision, the hybrid framework surpasses conventional intrusion detection techniques, such as anomaly detection and signature-based detection, in numerous crucial aspects. It provides comprehensive threat coverage by combining the strengths of different detection methodologies, covering both known and undiscovered security dangers. Furthermore, it excels in reducing false positives and negatives, increasing the precision of intrusion detection [16,17,18]. With intrusion detection algorithms strategically installed at the network's edge, the architecture provides real-time threat response, providing rapid security event remediation. Furthermore, its resource-efficient architecture accommodates edge devices with lower processing capabilities, establishing a compromise between effective threat detection and optimal resource utilization.

While initial simulations in MEC settings have been promising, real-world deployment and careful evaluation are required to validate the framework's effectiveness across varied operational conditions. Future research directions include fine-tuning machine learning models to reduce computing overhead and dynamic model updates for agile responses to shifting threats and network dynamics [19]. Furthermore, the incorporation of other data sources and contextual information has the potential to improve intrusion detection precision, making it an intriguing field for further research.

Table 4 shows Plus Minus Interesting facts. The proposed hybrid intrusion detection framework emerges as a strong and effective option for reinforcing security in MEC contexts. The findings of a rigorous examination highlight its potential for accurate threat identification, minimal false alarm rates, and real-time reaction capabilities. As research and real-world testing progress, the framework is ready to strengthen its role in protecting the integrity and privacy of mobile edge computing systems. Finally, the edge-based hybrid intrusion detection methodology is suggested for mobile edge computing offers a reliable and effective way to handle the security issues that MEC settings face [20].

5. CONCLUSION

In conclusion, the edge-based hybrid intrusion detection methodology is suggested for mobile edge computing offers a reliable and effective way to handle the security issues that MEC settings face. The framework achieves improved detection accuracy and fewer false positives/negatives by combining behavioral analysis, anomaly detection, signature-based detection, federated learning, ensemble approaches, and cloud-augmented analysis.

The system's resilience is increased by the quick adaptation to new threats ensured by the integration of real-time response mechanisms and incremental learning. Additionally, the system optimizes resource utilization on edge devices with limited resources while respecting data privacy using federated learning.

This study presents a novel hybrid intrusion detection framework for Mobile Edge Computing (MEC) and IoT environments, combining behavioral analysis, anomaly detection, and signature-based methods for real-time, bandwidth-efficient threat detection. The key contribution is the use of smoothing filters and unsupervised learning to address data noise and enhance accuracy. The framework offers a scalable, decentralized security solution, bridging traditional IDS approaches with modern AI-driven techniques, making it highly relevant for the evolving landscape of MEC and edge computing, where cybersecurity challenges are increasing.

6. FUTURE WORK

Future research should concentrate on machine learning optimization, multi-modal data fusion, and dynamic model updates to further boost the framework's performance and adaptability [17,21]. Its effectiveness in realistic MEC circumstances will be verified by deployment and evaluation in the real world. The ultimate goal is to improve the security posture of mobile edge computing systems while protecting data integrity and user privacy and delivering a seamless and secure user experience. The proposed design lays the foundation of mobile edge computing that is more secure and dependable.

Although the results of the suggested edge-based hybrid intrusion detection framework for mobile edge computing are encouraging, there are still a number of opportunities for further study and development:

- Investigating techniques for dynamic and adaptive model updates so the intrusion detection system swiftly reacts to emerging threats and continuously learn from real-time data.
- Exploring cutting-edge optimization methods for machine learning to further lower the computational burden of these models on resource-constrained edge devices without sacrificing detection precision.
- Identifying more advanced intrusion attempts, expanding the framework to include thorough network traffic analysis, such as deep packet inspection and flow analysis.
- Improving the precision of intrusion detection and decrease false alarms, integrate contextual information, such as user behavior, device profiles, and application characteristics.
- Researching ways to merge information from diverse sensors and sources, such as mobile phones, edge nodes, and outside security services, to give a more comprehensive picture of network behavior.

- Development of tools for adaptive resource management will enable the framework to dynamically distribute computing resources in response to shifting MEC environment demands.
- Gauging the framework's scalability, robustness, and performance under various operating situations, conduct thorough field trials and evaluations in real-world MEC deployments.
- Integrate threat intelligence feeds to provide the intrusion detection system with the most recent knowledge about known threats and compromise indications.

A final remark, the proposed edge-based hybrid intrusion detection system can develop into a highly effective and adaptive solution, successfully minimizing security concerns in mobile edge computing environments, by addressing these future research objectives. The ultimate objective is to strengthen MEC systems' overall security posture and guarantee their ongoing resilience against advanced and emerging cyber threats.

CODE AVAILABILITY:

The code that supports the findings of this paper is available from author Mohamed Eldosuky, upon request.

REFERENCES:

[1] E. S. Ali et al., "Machine learning technologies for secure vehicular communication in internet of vehicles: recent advances and applications," Security and Communication Networks, vol. 2021, pp. 1–23, 2021. http://dx.doi.org/10.1155/2021/8868355

[2] A. A. Salih and A. M. Abdulazeez, "Evaluation of classification algorithms for intrusion detection system: A review," Journal of Soft Computing and Data Mining, vol. 2, no. 1, pp. 31–40, 2021. http://dx.doi.org/10.30880/jscdm.2021.02.01.004

[3] A. Bourechak, O. Zedadra, M. N. Kouahla, A. Guerrieri, H. Seridi, and G. Fortino, "At the confluence of artificial intelligence and edge computing in iot-based applications: A review and new perspectives," Sensors, vol. 23, no. 3, p. 1639, 2023. http://dx.doi.org/10.3390/s23031639

[4] A. Singh, K. Chatterjee, and S. C. Satapathy, "An edge based hybrid intrusion detection framework for mobile edge computing," Complex & Intelligent Systems, vol. 8, no. 5, pp. 3719–3746, 2022. http://dx.doi.org/10.1007/s40747-021-00498-4

[5] C. Liang et al., "Intrusion detection system for the internet of things based on blockchain and multi-agent systems," Electronics, vol. 9, no. 7, p. 1120, 2020. http://dx.doi.org/10.3390/electronics9071120

[6] F. Y. Alghayadh, "A hybrid intrusion detection system for smart home security based on machine learning and user behavior," phdthesis, Oakland University, 2021. http://dx.doi.org/10.4236/ait.2021.111002

[7] A. Guezzaz, M. Azrour, S. Benkirane, M. Mohy-Eddine, H. Attou, and M. Douiba, "A Lightweight Hybrid Intrusion Detection Framework using Machine Learning for Edge-Based IIoT Security.," Int. Arab J. Inf. Technol., vol. 19, no. 5, pp. 822–830, 2022. http://dx.doi.org/10.34028/iajit/19/5/14

[8] Y. Liu, M. Peng, G. Shou, Y. Chen, and S. Chen, "Toward edge intelligence: Multiaccess edge computing for 5G and Internet of Things," IEEE Internet of Things Journal, vol. 7, no. 8, pp. 6722–6747, 2020. http://dx.doi.org/10.1109/JIOT.2020.3004500

[9] P. Ranaweera, A. Jurcut, and M. Liyanage, "MEC-enabled 5G use cases: a survey on security vulnerabilities and countermeasures," ACM Computing Surveys (CSUR), vol. 54, no. 9, pp. 1–37, 2021. http://dx.doi.org/10.1145/3474552

[10] A. I. Torre-Bastida, J. Díaz-de Arcaya, E. Osaba, K. Muhammad, D. Camacho, and J. Del Ser, "Bio-inspired computation for big data fusion, storage, processing, learning and visualization: state of the art and future directions," Neural Computing and Applications, pp. 1–31, 2021. http://dx.doi.org/10.1007/s00521-021-06332-9

[11] M. Mohammadi, A. Al-Fuqaha, S. Sorour, and M. Guizani, "Deep learning for IoT big data and streaming analytics: A survey," IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 2923–2960, 2018. http://dx.doi.org/10.1109/COMST.2018.2844341

[12] Y. Siriwardhana, P. Porambage, M. Liyanage, and M. Ylianttila, "A survey on mobile augmented reality with 5G mobile edge computing: Architectures, applications, and technical aspects," IEEE Communications Surveys & Tutorials, vol. 23, no. 2, pp. 1160–1192, 2021.

http://dx.doi.org/10.1109/COMST.2021.3061981

[13] M. Mehra, J. N. Paranjape, and V. J. Ribeiro, "Improving ml detection of IoT botnets using comprehensive data and feature sets," in 2021 international conference on COMmunication Systems & NETworkS (COMSNETS), 2021, pp. 438–446. http://dx.doi.org/10.1109/COMSNETS51098.2021.9352943

[14] E. Mugabo and Q.-Y. Zhang, "Intrusion Detection Method Based on Support Vector Machine and Information Gain for Mobile Cloud Computing.," Int. J. Netw. Secur., vol. 22, no. 2, pp. 231–241, 2020. https://dx.doi.org/10.6633/IJNS.202003

[15] F. Farhin, M. S. Kaiser, and M. Mahmud, "Secured smart healthcare system: blockchain and bayesian inference based approach," in Proceedings of International Conference on Trends in Computational and Cognitive Engineering: Proceedings of TCCE 2020, 2021, pp. 455–465. http://dx.doi.org/10.1007/978-981-33-4673-4_36

[16] N. S. Bhati and M. Khari, "A survey on hybrid intrusion detection techniques," in Research in Intelligent and Computing in Engineering: Select Proceedings of RICE 2020, 2021, pp. 815–825. http://dx.doi.org/10.1007/978-981-15-7527-3_77

[17] M. Eskandari, Z. H. Janjua, M. Vecchio, and F. Antonelli, "Passban IDS: An intelligent anomaly-based intrusion detection system for IoT edge devices," IEEE Internet of Things Journal, vol. 7, no. 8, pp. 6882–6897, 2020. http://dx.doi.org/10.1109/JIOT.2020.2970501

[18] F. Farhin, M. S. Kaiser, and M. Mahmud, "Secured smart healthcare system: blockchain and bayesian inference based approach," in Proceedings of International Conference on Trends in Computational and Cognitive Engineering: Proceedings of TCCE 2020, 2021, pp. 455–465. http://dx.doi.org/10.1007/978-981-33-4673-4_36

[19] P. D. Rosero-Montalvo, Z. István, P. Tözün, and W. Hernandez, "Hybrid anomaly detection model on trusted iot devices," IEEE Internet of Things Journal, 2023. http://dx.doi.org/10.1109/JIOT.2023.3243037

[20] E. Besharati, M. Naderan, and E. Namjoo, "LR-HIDS: logistic regression host-based intrusion detection system for cloud environments," Journal of Ambient Intelligence and Humanized Computing, vol. 10, pp. 3669–3692, 2019. http://dx.doi.org/10.1007/s12652-018-1093-8

[21] Y. Siriwardhana, P. Porambage, M. Liyanage, and M. Ylianttila, "A survey on mobile augmented reality with 5G mobile edge computing: Architectures, applications, and technical aspects," IEEE Communications Surveys & Tutorials, vol. 23, no. 2, pp. 1160–1192, 2021. http://dx.doi.org/10.1109/COMST.2021.3061981

Table 1: Critique of literature review

Ref	Context of Use	Strengths	Limitations	Suggestions
[1]	Offloading decisions in MEC using ML and DRL	Appropriately highlights DRL's role in resource management	Vague about the specific DRL methods or comparative results	Specify which DRL technique is used (e.g., DQN, DDPG), and its role
[4]	Cited for DRL in MEC, AI challenges at the edge, and IDS issues	Indicates a broad scope covering edge computing and IDS	Overused; lacks specificity in each context	Break down its contributions and cite specific sections or topics
[6]	IoV enabling communication and road safety	Supports IoV's goal of environmental awareness and safety	Unclear if it emphasizes safety technologies or protocols	Clarify if it focuses on ADAS, V2X, or general communication features
[7]	AI-based edge applications and hybrid IDS for IIoT	Suitable for advanced IDS design in smart edge/IIoT	May not detail both architecture and performance	Differentiate the architectural and detection aspects if possible
[8]	IDS limitations and 5G/MEC privacy protocols	Addresses both IDS challenges and MEC security enhancements	Dual role might stretch the scope of one paper	Specify if it's a survey, protocol design, or performance study
[9]	ML-based hybrid IDS in IIoT	Relevant to modern IDS design in edge/IIoT	Hybrid nature or algorithm type not made explicit	Mention specific ML models used (e.g., RF, ANN, hybrid ensembles)
[10]	Enhanced AKMA protocols in 5G MEC	Timely reference to privacy improvements in MEC applications	Lacks depth on how privacy is enhanced in AKMA	Include more detail on protocol mechanism and security assurance

Journal of Theoretical and Applied Information Technology
31st May 2025. Vol.103. No.10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

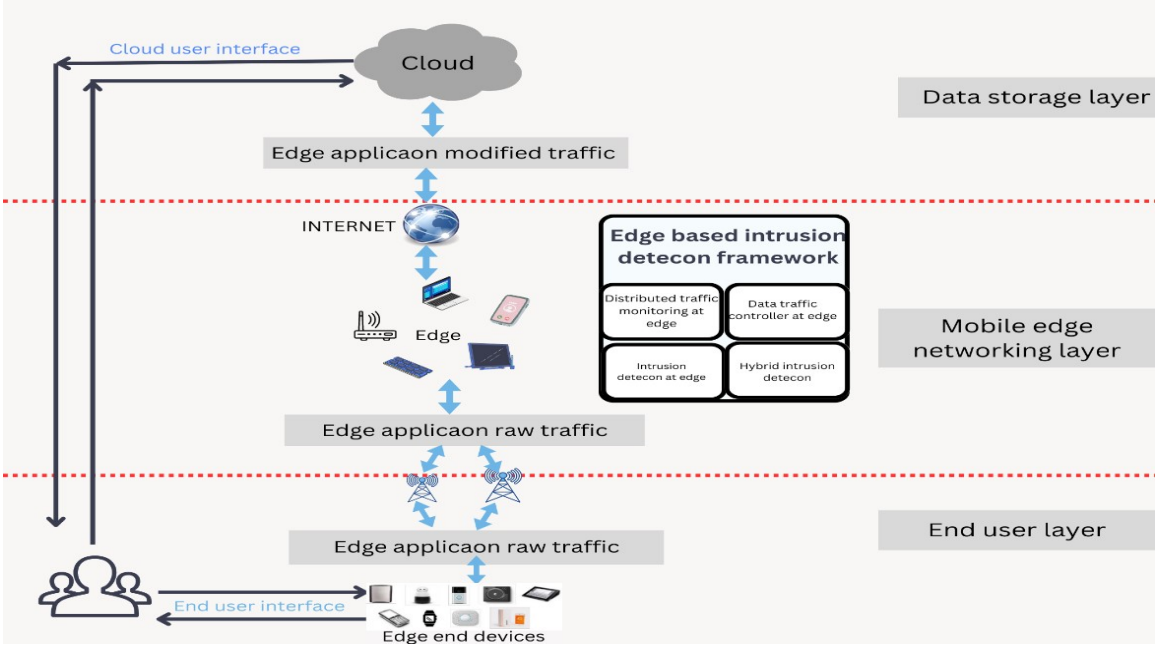

Figure 1: Mobile edge computing architecture

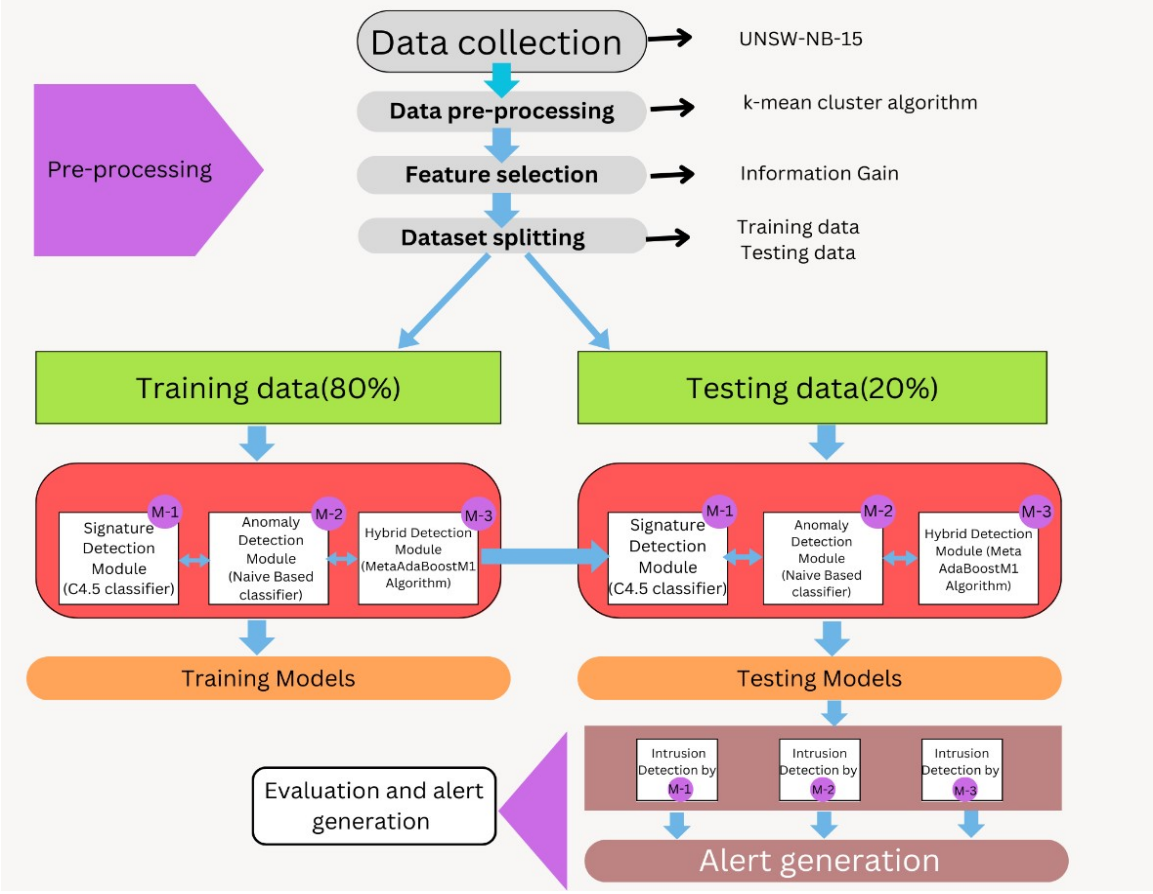

Figure 2: Proposed edge-based hybrid IDS

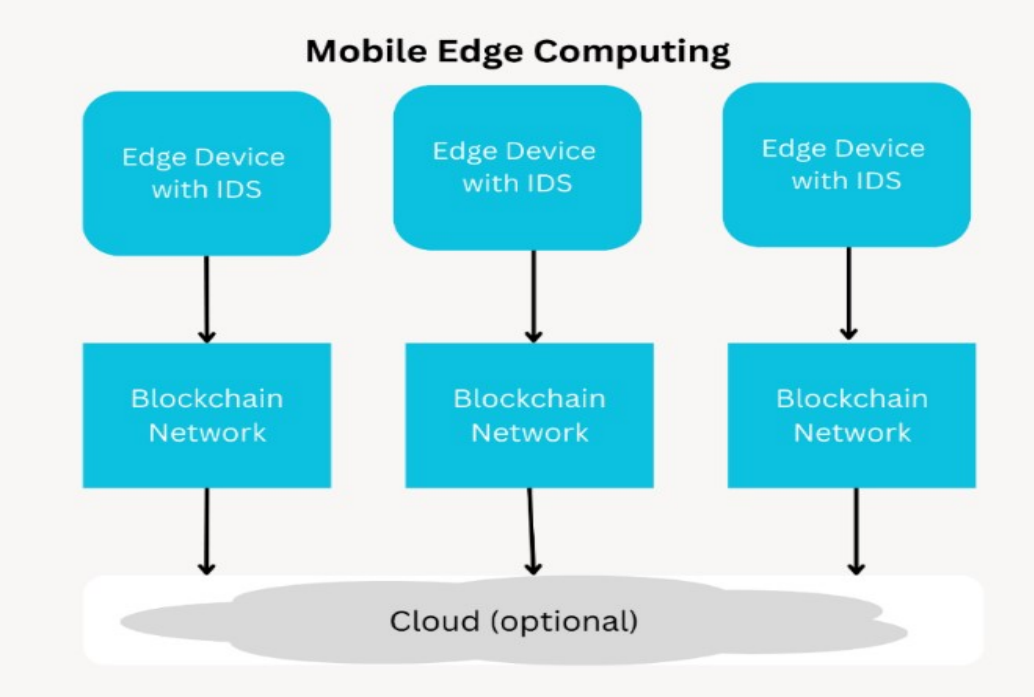

Figure 3: Blockchain Based Hybrid Intrusion Detection

Table 2: Measurement Factors

Factors	Description
True Positive(TP)	It measures the proportion of actual normal incidents correctly identified as normal.
False Negative(FN)	It measures the proportion of actual normal incidents incorrectly identified as attack incidents.
False Positive(FP)	It measures the proportion of actual attack incidents incorrectly identified as normal incidents.
True Negative(TN)	It measures the proportion of actual attack incidents correctly identified as attacks.

Journal of Theoretical and Applied Information Technology
31st May 2025. Vol.103. No.10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 3: Performance Metrics

Measurement metric	Description	Formulae
Accuracy(A)	It is defined as the ratio of the number of correct predictions made by the model to the total number of predictions made.	**Accuracy (A) =** $\frac{(TP+TN)}{(TP+TN+FP+FN)}$
Precision(P)	Precision measures the proportion of correctly predicted positive instances out of all the instances that were predicted as positive.	**Precision (P) =** $\frac{TP}{(TP+FP)}$
Recall(R)	Recall measures the proportion of actual positive instances that were correctly identified by the model.	**Recall(R) =** $\frac{TP}{(TP+FN)}$
F-Score	The F-score, also called the F1-score, is a measure of a model's accuracy on a dataset.	**F-Score (F1) =** $\frac{(2*R*P)}{(R+P)}$
Attack Detection Rate(ADR)	Attack Detection Rate is a performance metric that measures the accuracy of a model in identifying attack classes.	**Attack Detection Rate(ADR) =** $\frac{\sum_{i=2}^{C} TP_i}{\sum_{i=2}^{C} TP_i + FP_i}$
False Alarm Rate(FAR)	False Alarm Rate is a performance metric that measures the proportion of non-attack classes that are incorrectly classified as attacks by a model.	**False Alarm Rate (FAR) =** $\frac{FN_i}{TP_i + FN_i}$

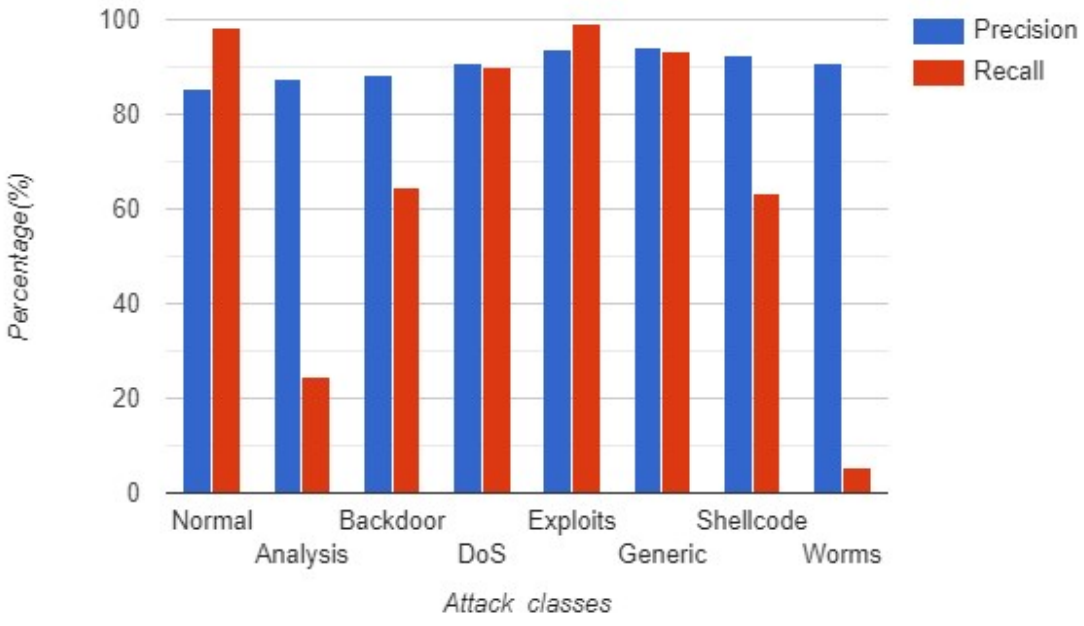

Figure 4: Precision & Recall graph

Table 4: Plus Minus Interesting facts

Aspect	Details
Plus (Strengths)	- Multi-layered detection (behavioral, anomaly, signature) improves accuracy. - Edge-based implementation ensures real-time response and low latency. - Smoothing filters and unsupervised learning reduce noise and false positives. - Bandwidth-efficient design compared to cloud-based IDSs.
Minus (Weaknesses)	- No coordination across multiple edge nodes limits scalability. - Uses public datasets, which may not reflect real-world MEC environments. - Deep learning models may strain low-resource edge devices. - Lacks mechanisms for adversarial robustness and privacy preservation.
Interesting (Noteworthy)	- Balanced trade-off between detection speed and depth. - Fully localized processing aligns with MEC goals. - Bridges traditional IDSs with modern AI techniques. - Novel handling of noisy/malicious data during acquisition using filters and unsupervised learning.