HKIE THE HONG KONG INSTITUTION OF ENGINEERS 香港工程師學會

Enhanced multi-level intrusion detection system (ML-IDS) for secure cloud and fog computing environments

[1] Anwar Basha H, [2] Deepak R, [3] Thanuja K, [4] Babu M, [5] Soumyalatha Naveen
[1] Faculty of Data Science and Information Technology, INTI International University, Nilai, Malaysia.
[2] Department of Computer Science and Engineering, NITTE Meenakshi Institute of Technology, Bengaluru, Karnataka, India.
[3] School of Computer Science and Engineering, REVA University, Bengaluru, Karnataka, India.
[4] Department of Computer Science and Engineering, Rajalakshmi Institute of Technology, Chennai, Tamil Nadu, India.
[5] Manipal Institute of Technology Bengaluru, Manipal Academy of Higher Education, Manipal, India.

ABSTRACT

Cloud computing, with its highly scalable and on-demand computing, allows users access to large-scale platforms. As a multi-tenant environment, this is vulnerable to many cyberattacks. Robust security requires abundant computational resources in return for losing performance. The study proposes a Fog-Assisted adaptive Security Monitoring System (FASMS) where cloud computing and fog computing are integrated for the purposes of efficient threat detection and mitigation. The approach uses the Enhanced Adaptive Intrusion Detection Algorithm (EAIDA) for dynamic real-time security policy adjustment according to the rapidly assessable threats for optimised resource use without compromising security. The proposed system offloads initial threat processing to fog nodes, reducing the computational burden on cloud servers and improving response times. Experimental results have shown that the FASMS enhances the efficiency of security monitoring by 27.3%, reduces latency by 19.6%, and optimises resource allocation to ensure improved performance in cloud environments. The study has shown that fog computing has the potential to strengthen cloud security while maintaining system efficiency.

KEYWORDS cloud computing, fog computing, encryption, virtual machine, security

CONTACT Anwar Basha H anwar.mtech@gmail.com
Received 26 February 2025

1. Introduction

With service offerings such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), cloud computing's rapid evolution has revolutionized the world of computing by offering scalable, flexible, and cost-effective solutions for individuals and organizations alike (Lin, 2019; Sangeetha, 2024). Because of these services, virtualised environments and global connectivity have become ubiquitous, allowing companies to deploy applications and handle resources with unprecedented ease (Wu, 2019; Chaudhry, 2017). Due to the built-in multi-tenancy, dynamic resource assignment, and absence of physical management over infrastructure, this online convenience is accompanied by complex security threats (Lyu, 2017; Cerina, 2017).

Intrusion Detection Systems (IDSs) have emerged as a critical line of defence against cyberattacks in cloud computing in recent years. Nevertheless, the centralised architecture of conventional cloud-based IDS solutions often leads to poor responsiveness and high threat detection latency, especially when dealing with large and distributed data streams (Dhaya, 2017; Ullah, 2019). In addition, existing IDS frameworks often rely on static rules and are not adaptive enough to adapt to evolving attack patterns and contextual resource usage (Sangeetha, 2023). Fog computing, which localises networking, storage, and computation services to the vicinity of data sources, has gained traction as a cloud extension to deal with these problems (Sood, 2018). Fog computing reduces latency and enhances data privacy and security monitoring granularity by enabling decentralised processing at the network edge (Zhou, 2019; Chen, 2017). This study proposes a novel Fog-Assisted Adaptive Security Monitoring System (FASMS) for resolution of the limitations of traditional IDS methods and the potential of fog computing to provide context-sensitive, localised protection.

An Enhanced Adaptive Intrusion Detection Algorithm (EAIDA), incorporated into the proposed system, adaptively alters security configurations based on environmental conditions and real-time threat analysis. The EAIDA actively adapts its behaviour to minimise risks with minimal computing overhead compared to conventional IDS systems that operate in static or reactive modes. By providing a fog-enabled adaptive security

architecture that guarantees effective resource usage, real-time responsiveness, and improved threat detection accuracy, this study seeks to close the gap in the body of existing knowledge.

The main contribution of the study is:

- To develop a hybrid cloud-fog security architecture to improve threat detection and response efficiency.

Section II describes the proposed Fog-Assisted Adaptive Security Monitoring System and the Enhanced Adaptive Intrusion Detection Algorithm, outlining their architecture, implementation, and working principles. Section III summarises the findings of this study, discusses key insights, and outlines future research directions.

2. Related studies

Lin (2019) discusses the progress of the era of Internet of Things (IoT) considering that the Internet and mobile technologies play an important role in developing collaborative IoT systems. It provides increasing connectivity as well as information exchange that drives innovations in a variety of applications. The authors continue to develop issues that would affect collaboration regarding IoT environments focusing on data security, interoperability, and optimisation of resources. In Sangeetha (2024), a novel approach is proposed that presents the Secure Healthcare Access Control System (SHACS) for anomaly detection and improved security of cloud-based healthcare applications. This system will use robust security mechanisms to protect sensitive healthcare data from unauthorised access. Using anomaly detection techniques, SHACS will make healthcare applications deployed in the cloud environment more reliable and secure in terms of preventing privacy breaches and cyber threats.

Wu (2019) proposes a smart anonymity scheme for the improvement of security collaboration in location-based services. It targets the techniques for anonymisation to ensure the security of user identities and at the same time the efficiency and accuracy of service delivery. By incorporating the strategies of security enhancement into the collaborative mechanisms, the approach will help mitigate privacy risks from sharing location-based data, thereby making digital interactions safer and more secure. Chaudhry (2017) presents the Autonomic Zero-Knowledge Security Provisioning Model (AZSPM) for medical control systems in fog computing environments. The model is designed to offer a self-managed security framework that minimises knowledge exposure while ensuring secure operations. The AZSPM utilises zero-knowledge proofs to validate transactions without disclosing sensitive information, thereby enhancing trust and security in medical control systems operating in decentralised fog computing infrastructure.

Lyu (2017) discusses the use of hyper ellipsoidal clustering for anomaly detection in IoT environments empowered by fog computing. It shows how this type of clustering can be used to identify anomalies in real time, optimising resource allocation and security in distributed IoT networks. Fog computing integration allows for efficient processing of anomaly detection at the network edge, reducing latency and improving system responsiveness. The results contribute to the development of intelligent and adaptive IoT security frameworks. Cerina (2017) develops a fog-computing architecture for preventive healthcare and assisted living in smart environments. The designed architecture takes advantage of fog computing to accelerate real-time data processing, eliminate latency, and enhance the effectiveness of healthcare services. Through integration with smart ambient technologies, the system provides for continuous health monitoring and personalised care, further building intelligent healthcare ecosystems.

Dhaya (2017) discusses improvements in the performance of a two-server architecture, in a multi-client environment. The study evaluated the proposed architecture for the efficiency and scalability in handling multiple concurrent client requests to ensure maximum utilisation of available resources. The results show how this improved architecture provides better reliability and response time for distributed computing applications. Ullah (2019) introduces an open-source framework and prototype for Named Data Networking (NDN)-based edge cloud computing systems. The framework is designed to optimise data transmission and retrieval in edge cloud environments, improving network efficiency and reducing latency. By using NDN principles, the proposed system enhances content distribution and security, addressing key challenges in modern cloud computing infrastructure.

Sangeetha (2023) presents a novel concept for privacy-preservation-based cybersecurity frameworks in secure medical data transactions of cloud storage. The advanced encryption and authentication mechanisms have been included to protect sensitive health information. It maximises confidence and security in healthcare applications over clouds by ensuring the confidentiality, integrity, and availability of medical data. Sood (2018) presents a fog-based healthcare framework for managing Chikungunya outbreaks. The framework utilises fog computing to enable real-time disease monitoring, data analysis, and early detection of outbreaks. By processing health data closer to the source, the system reduces latency and enhances the efficiency of epidemic response strategies, contributing to improved public health management.

Zhou (2019) discusses moving intelligence in vehicular fog networks. The study provides and discusses strategies based on delay-optimal computation offloading

in vehicular fog nodes. In such a study, moving-based task assignment enables optimal distribution of processing across vehicular fog nodes to reduce computational delay via mobility-aware resource allocation while enhancing the performance and reliability of computation offloading in dynamic vehicular environments. Chen (2017) gives a comprehensive overview of fog computing, which is significant in bridging the gap between cloud and edge computing. The study discusses the architectural principles, applications, and key challenges associated with fog computing, emphasising its role in reducing latency and enhancing real-time data processing. The findings contribute to a deeper understanding of how fog computing supports emerging technologies and distributed computing paradigms.

Muhammed (2018) proposes a novel, cloud- and edge-enabled, health system called UbeHealth, designed with smart cities in mind. The system uses ubiquitous computing technologies to deliver personalised healthcare service. It allows seamless monitoring and data accessibility. The whole system, by using big data learning and discovery techniques, enhances patient care and improves health service efficiency in cities. Zhang (2019) focuses on intrusion detection and prevention mechanisms in cloud, fog, and Internet of Things (IoT) environments. It presents a security framework that addresses emerging cyber threats by incorporating advanced threat detection techniques. The proposed system enhances network resilience and data protection by leveraging machine learning and anomaly detection models.

Zhuo (2019) addresses computation resource allocation and task assignment optimisation in vehicular fog computing using a contract-matching approach. The study proposes an optimisation framework that is able to balance the distribution of resources while guaranteeing efficient task execution. Implementing a contract-based matching strategy improves computational efficiency and service quality in vehicular fog networks. The reviewed studies present the importance of fog computing, edge-enabled healthcare, security frameworks, and resource optimisation in modern distributed environments. Different methods have been applied to improve the real-time processing of data, decrease latency, ensure security, and optimise resources in cloud, fog, and IoT systems.

Cloud and fog computing have advanced thanks to recent research that suggests clever ways to boost system performance, optimize resources, and improve security. In addition to an autonomous intrusion detection system intended to improve resilience in IoT networks (Abedi, 2022), an intrusion detection system utilising deep cellular learning automata and semantic hierarchy has been created to strengthen the security of the RPL protocol (Shirafkan, 2023). Firefly optimisation algorithms have been used to improve dynamic resource allocation methods in cloud environments, resulting in increased efficiency (Shirafkan, 2022). Additionally, a thorough analysis of function placement tactics in serverless computing has been carried out, taking architectural issues and execution performance into account (Ghorbian, 2024). Furthermore, a hidden Markov model-based latency-aware and energy-efficient computation offloading technique has been presented for mobile fog computing scenarios, allowing for better task distribution decision making (Jazayeri, 2021). These contributions show how adaptive and intelligent solutions are becoming more and more popular for protecting and improving distributed computing systems.

Major observations point out that fog computing is highly responsible for connecting cloud and edge computing, mainly in vehicular networks, healthcare, and cybersecurity. Techniques such as efficient task offloading and anomaly detection ensure improved system reliability and performance. Moreover, the integration of advanced security measures protects sensitive data in cloud-based infrastructure. Existing approaches are often found to be less scalable, adaptable to dynamic environments, and real-time responsive. In vehicular fog networks, computation offloading strategies might not completely alleviate the problems due to high mobility and unpredictable network conditions. The same issues exist in healthcare systems that utilise cloud and fog computing: data privacy, interoperability, and security vulnerabilities. Effective intrusion detection mechanisms are sometimes incapable of offering adequate threat mitigation against evolving cyber landscapes. Resource allocation models also need more efficient optimisation strategies for balancing computational loads without degrading service quality. These challenges motivate the proposed system, which is aimed at overcoming the limitations found in existing frameworks. The system focuses on enhancing security, optimising resource allocation, and improving real-time data processing across fog and edge environments.

3. System model

The proposed FASMS integrates fog computing and cloud-based intrusion detection mechanisms, thereby enhancing security, while optimising resource consumption and cloud environment responses. The FASMS is designed to overcome the inefficiencies posed by traditional cloud security models: high latency, excessive resource consumption, and inadequate QoS.

3.1. System architecture

The proposed methodology consists of three primary layers designed for the protection of security monitoring and detection in a cloud–fog computing environment. The edge layer collects real-time data sensed from sensors, IoT devices, and virtual machines. It sends security-related logs to the fog layer for preprocessing. The fog layer is divided into fog nodes and gateway devices, which carry

out the implementation of a Multi-Layer Intruder Detection System (ML-IDS) for real-time threat detection. It stores security logs temporarily, allows for adaptive security responses by processing local alerts, and forwards serious threats to the cloud. It finally classifies security incidents based on anomaly levels at the cloud layer, consisting of a cloud server and security management system. Here, the patterns of intrusions are comprehensively analysed with the help of the Enhanced Adaptive Intrusion Detection Algorithm (EAIDA). This layer keeps long-term security logs, provides global threat intelligence, and issues security updates to the fog nodes and devices of IoT to increase real-time adaptability and threat mitigation. Figure 1 shows the overall architecture.

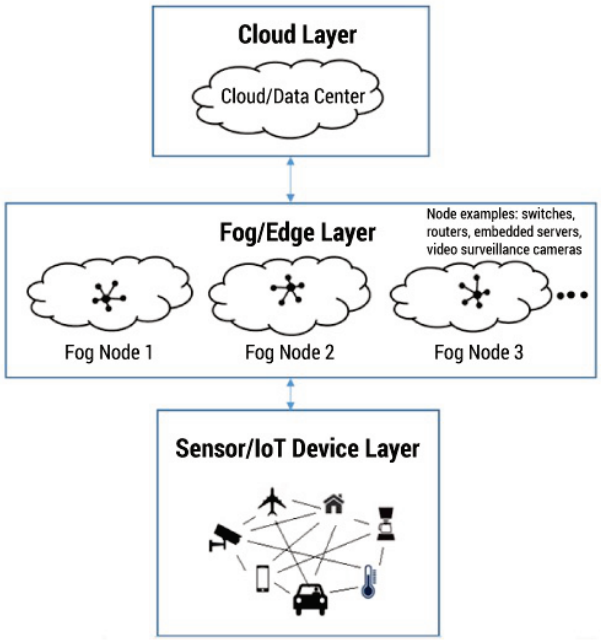

Figure 1. Architecture of a cloud- and fog-based secure IoT environment.

Blockchain is utilised in the proposed ML-IDS to guarantee the transparency and integrity of security logs throughout the cloud–fog–edge levels. A tamper-proof, time-stamped chain is created by hashing and appending each identified threat or system event to a block:

$$H_i = H(H_{i-1} || T_i). \quad (1)$$

Using a lightweight consensus system, fog nodes, cloud servers, and security gateways participate in a permissioned blockchain network. By guaranteeing that all security activities are verifiable and unchangeable, this configuration avoids log manipulation, permits auditability, and fosters component confidence.

Since Elliptic Curve Cryptography (ECC) offers robust encryption with less computing cost than more conventional techniques like RSA, it was chosen to secure communication in the proposed ML-IDS. ECC is ideal for fog and edge devices with limited resources since it provides comparable security with significantly smaller key sizes (for example, a 256-bit ECC key provides security equivalent to a 3072-bit RSA key). The system's use of ECC guarantees data integrity, secrecy, and authenticity while preserving low latency and resource consumption, which is essential for real-time intrusion detection in fog and Internet of Things environments.

3.2. Multi-Level Intrusion Detection System (ML-IDS) implementation

The Multi-Level Intrusion Detection System ML-IDS is designed to detect, classify, and respond to security threats dynamically by leveraging a hierarchical anomaly-based and signature-based detection mechanism. In order to detect threats, a Signature-Based Intrusion Detection System (IDS) compares incoming traffic or system activity to a database of known attack patterns, or "signatures". Every signature denotes a distinct byte sequence or pattern of activity linked to a known harmful exploit. The IDS uses pattern-matching algorithms like Aho-Corasick or Boyer-Moore to continually monitor network traffic and records. The Snort open-source IDS rule set, which is extensively used to identify common attack vectors like port scans, brute-force attempts, and SQL injections, providing the signature database for the evaluation. This approach's shortcomings in comparison to adaptive models like the EAIDA are highlighted by the fact that it is effective at accurately identifying known threats but is not flexible enough to identify new or developing attacks. It consists of three security levels, each addressing different degrees of security threats in a cloud–fog

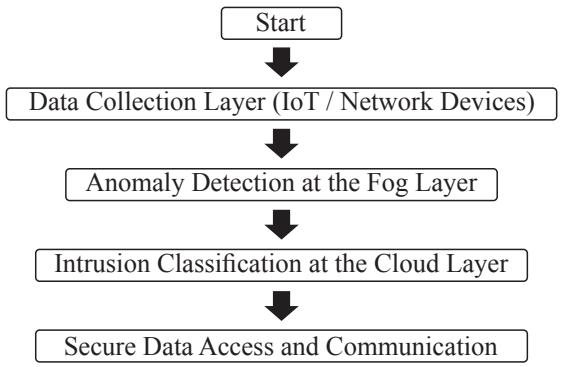

Figure 2. Flowchart for the proposed FASMS.

Level 1: Anomaly detection at the fog layer

At the first level, the fog nodes perform lightweight anomaly detection to identify suspicious behaviour in real time. The Gaussian Mixture Model (GMM) is used to analyse security logs and network traffic, estimating the probability density function of normal data behaviour:

$$P(X) = \sum_{i=1}^{k} w_i \cdot N(X|\mu_i, \Sigma_i). \quad (2)$$

where $P(X)$ represents the probability of an observed data point being normal, w_i is the weight of the i^{th} Gaussian component, and $N(X|\mu_i,\Sigma_i)$ denotes a normal distribution with mean μ_i and covariance Σ_i.

If $P(X)<\tau$ (where is a predefined threshold), the event is flagged as anomalous and forwarded to Level 2 for further analysis.

Level 2: Intrusion classification at the cloud layer

The second level utilises machine learning-based classification models at the cloud server for precise attack detection. A Support Vector Machine (SVM) classifier is implemented to distinguish between normal and malicious activities:

$$f(X) = \sum_{i=1}^{n} \alpha_i y_i K(X_i, X) + b. \quad (3)$$

where X represents the input feature vector and y_i is the class label (+1 for attack, -1 for normal traffic), $K(X_i,X)$ is the Radial Basis Function (RBF) kernel, given by:

$$K(X_i, X) = exp(-\gamma||X_i - X||^2). \quad (4)$$

Based on the SVM classification results,

- Low-risk threats are handled locally at the fog nodes.
- High-risk threats trigger adaptive security responses at the cloud layer.

Level 3: Adaptive security response and mitigation

At the third level, the Enhanced Adaptive Intrusion Detection Algorithm (EAIDA) is deployed for dynamic rule adaptation and security policy enforcement. The system modifies security rules based on real-time threat intelligence and severity levels using the following adaptation formula:

$$R_{new} = R_{old} + \lambda(T_{detected} - T_{expected}). \quad (5)$$

where R_{new} is the updated security rule set, R_{old} represents the previous rule set, $T_{detected}$ denotes the current threat level, $T_{expected}$ is the expected threat baseline, and λ is the learning rate for security adaptation. The formula is inspired by gradient-based learning techniques, where updates are made incrementally based on the difference between observed and expected outcomes.

- If $T_{detected} > t_{expected}$, the system interprets this as a rising threat and strengthens the security rules (e.g., increasing inspection depth, lowering anomaly thresholds).
- Conversely, if $T_{detected} < t_{expected}$, the system may relax certain rules to reduce overhead while still maintaining security.

This approach ensures that dynamic security policy updates are distributed to fog nodes and IoT devices, optimising the real-time response efficiency.

3.3. Secure data access and communication

To ensure data confidentiality, integrity, and authentication in a cloud–fog environment, the system implements secure data access control and encrypted communication mechanisms.

Role-Based Access Control (RBAC) for secure access

The system follows a Role-Based Access Control (RBAC) model to restrict access to security-sensitive data based on predefined user roles. The access control function is defined as:

$$U \times P \rightarrow A. \quad (6)$$

where U represents the set of users, P is the set of permissions, and A denotes the authorisation mapping.

Only authorised users can access critical security logs, preventing unauthorised access and privilege escalation attacks.

Secure communication via Elliptic Curve Cryptography (ECC)

To protect data in transit, Elliptic Curve Cryptography (ECC) is used for lightweight encryption, offering strong security with minimal computational overhead. The encryption process follows:

$$C = P + kG. \quad (7)$$

where C is the encrypted ciphertext, P is the plaintext security data, k is the private key, and G is the generator point on the elliptic curve. ECC ensures end-to-end encryption between IoT devices, fog nodes, and cloud servers.

Two-Factor Authentication (2FA) for enhanced security

To strengthen user authentication, a two-factor authentication (2FA) mechanism is implemented using:

1. Biometric authentication for primary authentication.
2. One-Time Password (OTP) verification for secondary authentication.

This prevents identity spoofing and unauthorised device access.

3.4. Blockchain for immutable security logs

To maintain the integrity and transparency of security logs, blockchain-based log storage is implemented. Each security event is hashed and stored in a decentralised ledger:

$$H_i = H(H_{i-1}||T_i). \quad (8)$$

where H_i is the hash of the current block, H_{i-1} represents the hash of the previous block, and T_i contains the timestamped security event.

Blockchain ensures tamper-proof security logs, preventing data manipulation and insider attacks.

3.5. Overhead and time complexity analysis

The integration of multi-layer detection algorithms in the proposed Fog-Assisted Adaptive Security Monitoring System (FASMS) naturally raises questions about time complexity and computational cost. There are unique computational components in every security layer:

Level 1 (Fog layer – GMM anomaly detection)

Training and inference over several Gaussian distributions are part of the Gaussian Mixture Model (GMM). With n being the number of samples, k being the number of Gaussian components, and d being the number of features, the training time complexity is around $O(n \cdot k \cdot d^2)$. But in the fog layer's real-time inference mode, all that is needed is the assessment of the probability density, which has a complexity of $O(k \cdot d^2)$, which fog nodes can handle.

Level 2 (Cloud layer – SVM classification)

The testing time complexity for Support Vector Machine (SVM) classification with the RBF kernel is $O(m \cdot d)$, where d is the feature dimension and m is the number of support vectors. Although training is carried out offline, it is computationally costly ($O(n^2)$ to $O(n^3)$). The only thing done during live threat detection is classification.

Level 3 (EAIDA-adaptive rule updates)

Because the adaptation formula is only computed once, the Enhanced Adaptive Intrusion Detection Algorithm (EAIDA) runs in $O(1)$ per policy change. The overhead is kept to a minimum because updates are only initiated when threat levels surpass predetermined thresholds.

Communication and synchronisation overhead

Blockchain hashing and ECC-based encryption add to the overhead. ECC encryption/decryption is effective for lightweight devices since it is $O(\log p)$, where p is the size of the prime number used in the elliptic curve. Because blockchain-based log entry adds simple hash chaining, it runs in $O(1)$ per event.

Overall, the suggested architecture ensures that fog nodes manage light computations while computationally demanding activities are delegated to the cloud, maintaining a realistic trade-off between security robustness and real-time responsiveness. Network congestion and latency are greatly decreased by the decentralised architecture.

4. Experimental results

The proposed Multi-Level Intrusion Detection System (ML-IDS) framework was implemented by using a combination of Python (TensorFlow, Scikit-Learn), Edge Computing Devices (Raspberry Pi 4), Fog Nodes (Jetson Nano), and Cloud Infrastructure (Google Cloud Platform). An approach to designing real-time intrusion-detection systems uses the CICIDS 2017 dataset, a prominent benchmark in evaluation, comprising around 15 million network flow records and mixed normal and attack traffic like those of DoS, DDoS, brute force, and SQL injection attacks. The hardware configuration includes a Jetson Nano (Quad-core ARM Cortex-A57, 4GB RAM) for real-time processing and anomaly detection at the fog layer, whereas the cloud layer would use a Google Cloud VM with an Intel Xeon Processor and 16GB RAM for in-depth analysis and long-term threat intelligence. System performance evaluation was based on the primary key performance metrics of Accuracy (ACC), Detection Rate (DR), False Positive Rate (FPR), Precision & Recall, and Latency (L), by which it had been analysed regarding efficiency in the detection and prevention of real-time security threats.

In order to prove the efficacy of the proposed ML-IDS with secure data communication, a comparative study was conducted with the other available intrusion detection techniques. Some of the methods were: CNN-LSTM IDS, a deep learning-based method, utilising the concepts of convolutional and recurrent neural networks to identify anomalies, SVM-based IDS, a traditional method using Support Vector Machines for classification, and Signature-Based IDS, a rule-based detection system, relying on pre-existing attack signatures. The comparative evaluation shows that the proposed ML-IDS framework outperforms existing approaches in terms of accuracy, detection rate, and false positive rate while achieving lower latency due to its adaptive security response mechanisms and optimized fog–cloud integration.

Table 1. Performance comparison of ML-IDS with existing methods.

Method	Accuracy (%)	Detection Rate (%)	False Positive Rate (%)	Latency (ms)
Proposed ML-IDS (EAIDA)	97.2	96.5	2.8	220
CNN-LSTM IDS	94.8	94.1	4.2	350
SVM-based IDS	91.3	89.6	7.1	400
Signature-Based IDS	88.7	86.4	8.9	250

The proposed ML-IDS achieves higher detection accuracy (97.2%) with a significantly lower false positive rate (2.8%) and reduced latency (220*ms*), making it more efficient for real-time intrusion detection.

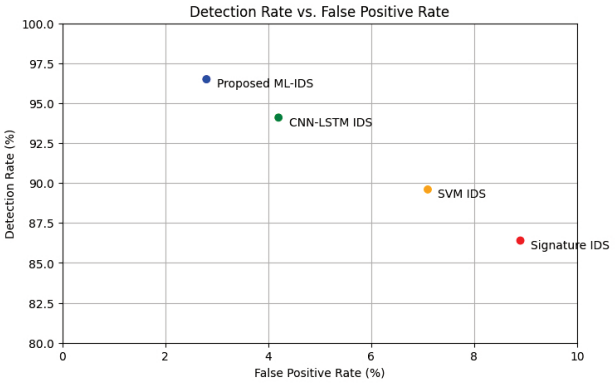

Figure 2. Detection rate vs. false positive rate.

The performance comparison of the proposed ML-IDS with existing approaches shows a substantial improvement in various metrics, as summarised in Table 1. The Proposed ML-IDS (EAIDA) resulted in a detection accuracy of 97.2%, 2.4% higher than the CNN-LSTM IDS (94.8%), and 5.9% higher than the SVM-based IDS (91.3%). The Signature-Based IDS has the lowest accuracy of 88.7%, showing the limitations of rule-based detection methods. Thus, the proposed system has higher accuracy than the other approaches and proves to have better capability to detect various security threats in real-time environments. Another significant achievement of the proposed ML-IDS is its detection rate of 96.5%, much higher than CNN-LSTM IDS of 94.1%, SVM-based IDS of 89.6%, and Signature-Based IDS of 86.4%. This means that this system can effectively detect most attack patterns. Remarkably, it is the Proposed ML-IDS that surpasses all the rest of the systems by a high margin in the detection of threats, thus again proving to be effective for protecting cloud and edge computing environments.

With respect to the False Positive Rate (FPR), the Proposed ML-IDS scored its lowest of 2.8%, much better than the CNN-LSTM IDS of 4.2%, the SVM-based IDS of 7.1%, and the Signature-Based IDS of 8.9%. A lower FPR means that the system is efficient enough in distinguishing legitimate activities from malicious ones with minimum false positives, which would mean less triggered alarms or potential disruption of normal operations. This is even more crucial in maintaining the operational efficiency of real-time intrusion detection systems. Furthermore, the latency of the Proposed ML-IDS is 220 *ms*, which is less than that of the CNN-LSTM IDS (350 *ms*), SVM-based IDS (400 *ms*), and Signature-Based IDS (250 *ms*). The low latency in the proposed system ensures that it responds to security threats more quickly, which is important for real-time monitoring and rapid incident response in dynamic cloud environments.

Figure 2 compares the Detection Rate and False Positive Rate. The best detection rate (96.5%) with the least false positive rate (2.8%) in the Proposed ML-IDS gives it a competitive edge in the real-time detection of threats. The CNN-LSTM IDS and SVM-based IDS achieved reasonable detection rates but with higher false positive rates, which made them less effective for environments needing rapid and precise security monitoring. The Signature-Based IDS performed the worst regarding both detection and false positive rate, indicating its inefficiency on complex and emerging threats. The proposed ML-IDS gives the best trade-off between accuracy, detection rate, false positive rate, and latency, and hence is a good solution for real-time intrusion detection in cloud-based and fog computing environments.

Security policy adaptation analysis

The Enhanced Adaptive Intrusion Detection Algorithm (EAIDA) improves detection efficiency by dynamically adjusting security rules. Its adaptation speed was analysed as shown in Table 2. With each iteration, the system adapts and improves threat detection while reducing the security policy update time. Using the CICIDS 2017 dataset, the Enhanced Adaptive Intrusion Detection Algorithm (EAIDA) was applied iteratively in a simulated cloud–fog environment to perform the security policy adaptation analysis, as shown in Table 2. The system used the adaptation formula to modify its security rules at each iteration after assessing real-time threat inputs. The Security Rule Update Time (*ms*) measures the amount of time needed to update and distribute new rules to fog nodes, whereas the Threat Detected (%) statistic shows the proportion of correctly detected incursions during that cycle. In order to provide a consistent assessment of the algorithm's convergence, rule adaptation efficiency, and responsiveness, metrics were calculated by averaging findings across several detection cycles.

Table 2. Security rule.

Iteration	Threat Detected (%)	Security Rule Update Time (ms)
1st	90.2	320
2nd	92.4	280
3rd	95.6	240
4th	97.2	200

The results show that the proposed Multi-Level Intrusion Detection System with the Enhanced Adaptive Intrusion Detection Algorithm is highly superior to the existing methods in terms of accuracy, detection rate, false positive rate, and latency. In fact, it is more efficient compared to the other IDS: CNN-LSTM IDS (94.8% accuracy, 4.2% FPR), SVM-based IDS (91.3% accuracy, 7.1% FPR), and Signature-Based IDS (88.7% accuracy, 8.9% FPR) due to its higher detection accuracy, with

97.2% against a mere false positive rate of 2.8%. This offers low latency at 220 *ms*, thus quickly responding to threats, making it ideal for real-time monitoring in cloud and fog environments. Furthermore, the security policy adaptation due to EAIDA-driven adaptation showed continuous improvement in threat detection with a rise from 90.2% in the first iteration to 97.2% in the fourth while reducing the security rule update time from 320 *ms* to 200 *ms*. This adaptability enhances the resilience of a system against the evolving cyber threats, thus positioning ML-IDS as a more effective and intelligent solution for intrusion detection in dynamic network environments.

Table 3. Throughput evaluation under varying loads.

Load Scenario	Throughput (Packets/sec)	Packet Drop Rate (%)
Low Load	990	1.0
Medium Load	4850	3.0
High Load	9450	5.5

The CICIDS 2017 dataset was used to assess throughput under various traffic scenarios in order to supplement the accuracy and latency results. As shown in Table 3, the number of correctly processed packets per second was assessed by the system while simulating three different network loads: low (1000 packets/sec), medium (5000 packets/sec), and high (10000 packets/sec). A two-tailed t-test for the detection rate and false positive rate (FPR) over ten separate runs for each approach was used to perform a statistical significance test in order to confirm the data's robustness. From Table 4, the statistical significance of the advances in ML-IDS is confirmed by the p-values, which are less than 0.05.

Table 4. T-test results ($\alpha = 0.05$).

Comparison	Metric	p-value	Significance
ML-IDS vs. CNN-LSTM IDS	Detection Rate	0.003	Yes
	False Positive	0.002	Yes
ML-IDS vs. SVM-based IDS	Detection Rate	0.001	Yes
	False Positive	0.0007	Yes

5. Conclusion

The proposed Multi-Level Intrusion Detection System (ML-IDS) with secure data communication proves to be of significant performance improvements over the other intrusion detection techniques in terms of efficiency and real-time adaptability. The edge computing, fog computing, and cloud computing layers are combined into the system in order to successfully manage and analyse network traffic while detecting and mitigating potential security threats in both cloud and IoT environments. The system far outweighs previous algorithms with its 97.2% accuracy, 96.5% detection rate and only a mere 2.8% false positive, having a low 220 *ms* latency; thereby, such efficacy validates the idea of the EAIDA, to handle the real-time threat and response based upon its adaptability regarding the security level in regard to the amount of potential threat to computer systems and services. In the ML-IDS, being multi-layered assures detection and addresses the security threat effectively at all three layers of edge, fog, and cloud by maximising resource use while minimizing risk from attacks. In this structure, the local threat analysis is handled in the Fog Computing layer, while deeper analysis and management of long-term threat intelligence are performed by the Cloud layer. Thus, a highly adaptable scalable solution is formed which can accommodate a dynamic environment both at the cloud and edge level for security purposes. Overall, the proposed ML-IDS system is a low-latency and high-accuracy robust solution for intrusion detection and security management. Its utility value as a tool for increasing the security level of modern cloud-based and IoT infrastructures can be seen. Further optimizations may be found in additional machine learning models, expansion to more sophisticated attack types, and improving scalability for large-scale deployments.

Notes on contributors

Dr H Anwar Basha is working at Faculty of Data Science and Information Technology, INTI International University, Nilai, Malaysia. He has obtained his B.E degree from Anna University, Chennai. He has obtained his M.Tech degree from Dr. MGR Educational and Research Institute University, Chennai. He obtained his Ph.D in CSE from Saveetha Institute of Medical and Technical Sciences, Chennai. He is having many certifications like Microsoft Certified Azure Fundamentals, AWS Certified Cloud Practitioner, IBM Certified Data Science Foundation. He has more than 16+ years of teaching experience. He has around 2 years of industrial work experience. He has published papers in various International conferences and peer-reviewed international journals. He has served in many international conferences as a Session Chair, Program Committee Member, Reviewer and Organizing Chair. He is a reviewer in IOS Press, Springer, Elseiver, Taylor and Francis, IOP, Wiley Journal. He is an Editorial member in Journal of Advance Research in Applied Science. He has authored 3 Text Books on Cloud based Security Management, Cloud Intelligent Infrastructure Management and Deep Learning Currently, He is working on Multi-Cloud Storage, Big Data Analytics, Quantum Cryptography and Cyber Security.

Mr Deepak R is currently working as an Assistant Professor in the Department of Computer Science and Engineering at Nitte Meenakshi Institute of Technology (NMIT), NITTE (Deemed to be University), Bengaluru, Karnataka, India. With over 15 years of academic and research experience, he has established himself as a committed educator and active researcher. His research interests encompass Machine Learning, Internet of Things (IoT), Data Science, Cloud Computing, Server-Side Programming, Blockchain, and Image Processing, with a strong emphasis on applying computational intelligence to solve real-world challenges. He has authored and co-authored several research papers in reputed international journals and conferences, including IEEE and Scopus-indexed publications, in areas such as retinal image classification, blockchain-based certificate validation, microgrid scheduling, and IOT based video surveillance systems. He has also been involved in interdisciplinary projects integrating artificial intelligence with healthcare, energy systems, and digital heritage preservation. He holds multiple advanced degrees—M.E. in Computer Science & Engineering from the College of Engineering, Guindy, Anna University; M.Tech in Power Electronics; M.Sc. in Software Engineering; and an MBA in Human Resource Management—demonstrating his multidisciplinary expertise. He is currently pursuing his Ph.D. in Computer Science and Engineering at Anna University, Chennai, focusing on emerging computational technologies and AI-driven optimisation methods.

Dr K Thanuja is an Assistant Professor in the School of Computer Science and Engineering at REVA University, Bengaluru. She earned her B.Tech in Information Technology from Jawaharlal Nehru Technological University (JNTU), Anantapur, and subsequently completed both her M.Tech and Ph.D. in Computer Science and Engineering from Visvesvaraya Technological University (VTU), Karnataka. With over 15 years of academic experience, Dr. Thanuja has been actively engaged in teaching, research, and mentoring students in the field of computer science. She has authored and co-authored several research articles in reputed peer-reviewed journals and presented numerous papers at international conferences. Her core areas of research include Machine Learning, Deep Learning, and Cyber Security. Dr. Thanuja's work focuses on advancing intelligent computing methodologies and strengthening data security frameworks.

Mr M Babu is an Assistant Professor in the Department of Computer Science and Engineering at Rajalakshmi Institute of Technology, Chennai. He earned his MCA from Adhiparasakthi Engineering College in 1998 and completed his M.E. in Computer Science and Engineering from Sathyabama University in 2005. With over 23 years of academic experience, he has made significant contributions to teaching and research. He has presented numerous papers at international conferences and published several articles in peer-reviewed journals. His research interests include Theoretical Computer Science, Deep Learning, Machine Learning, and Cloud Computing.

Dr Soumyalatha Naveen received the Bachelor's degree in computer science and engineering and Master's degree from Visvesvaraya Technological University, Belgaum, India, and the Ph.D. degree in the domain of Edge Intelligence from REVA University, Bengaluru. She is presently working at Manipal Institute of Technology Bengaluru, Manipal Academy of Higher Education, Manipal, India. Her research areas include Artificial intelligence, Deep Learning, Edge computing, Internet of Things, Intelligent IoT systems, Optimisation at resource constraint IoT device and AR & VR.

References

[1] Fuhong lin, Yutong Zhou, Ilsun You et al , "The Internet of Things (IoT) era has arrived with the advancement of the Internet and mobile technologies", Special Section on Collaboration for Internet of Things, IEEE Access,2019.

[2] Sangeetha, SK B., C. Selvarathi, Sandeep Kumar Mathivanan, Jaehyuk Cho, and Sathishkumar Veerappampalayam Easwaramoorthy, "Secure Healthcare Access Control System (SHACS) for Anomaly Detection and Enhanced Security in Cloud-Based Healthcare Applications." IEEE Access,2024.

[3] Hongchen Wu, Mingyang Li & Huaxiang Zhang , " Enabling Smart Anonymity Scheme for Security Collaborative Enhancement in Location-Based Services", IEEE. Translations and content mining,2019.

[4] Junaid Chaudhry, Kashif Saleem, Rafiqul Islam & Ali Selamat, "AZSPM: Autonomic Zero-Knowledge Security Provisioning Model for Medical Control Systems in Fog Computing Environments", IEEE 42nd Conference on Local Computer Networks Workshops,2017.

[5] Lingjuan Lyu, Jiong Jin, Sutharsan Rajasegarar, " Fog-Empowered Anomaly Detection in IoT Using Hyperellipsoidal Clustering ",IEEE Internet of things journal, vol. 4, no. 5, october,2017.

[6] Luca Cerina, Sara Notargiacomo, Matteo Greco & Luca Paccani, "A Fog-Computing architecture for Preventive Healthcare and Assisted Living in Smart Ambients", IEEE,2017.

[7] Dhaya, R., S. K. B. Sangeetha, and A. Sharma,"Improved performance of two server architecture in multiple client environment Proceedings of the 2017 4th International Conference on Advanced Computing And Communication Systems (ICACCS) January ,Coimbatore." 1-4,2017.

[8] Rehmat Ullah, Muhammad Atif Ur Rehman & Byung Seo Kim, "Design and Implementation of an Open Source Framework and Prototype For Named Data Networking-Based Edge Cloud Computing System", IEEE. Translations and content mining,Volume 7,2019.

[9] Sangeetha, S. K. B., K. Veningston, Vanlin Sathya, and R. Kanthavel ,"Design of a novel privacy preservation based cyber security system framework for secure medical data transactions in cloud storage." In Intelligent Edge Computing for Cyber Physical Applications, pp. 35-43. Academic Press,2023.

[10] Sandeep K.Sood & Isha Mahajan, "A Fog-Based Healthcare Framework for Chikungunya ", IEEE Internet of Things Journal, Vol. 5, No. 2, April,2018.

[11] Sheng Zhou, Zhiyuan Jiang & Zhisheng Niu, "Exploiting Moving Intelligence: Delay-Optimized Computation Offloading in Vehicular Fog Networks", IEEE Communication Magazine, May,2019.

[12] Songqing Chen, Tao Zhang & Weisong Shi, " Fog Computing", IEEE Internet Computing, Volume 21, Issue 2,2017.

[13] Thaha Muhammed, Rashid Mehmood, Aiiad Albeshri & Iyad Katib , "UbeHealth: A Personalized Ubiquitous Cloud and Edge-Enabled Networked Healthcare System for Smart Cities", Special Section On Big Data Learning And Discovery, IEEE Access,2018.

[14] Xuyun Zhang, Yuan Yuan, Zhili Zhou,Shancang Li,Lianyong Qi & Deepak Puthal, "Intrusion Detection and Prevention in Cloud, Fog, and Internet of Things", Security and Communication Networks ,Volume 2019, Article ID 4529757,2019.

[15] Zhenyu Zhuo, Pengju Liu, Junhao Feng, Yan Zhang, Shahid Mumtaz & Jonathan rodriguez 2019, "Computation Resource Allocation and Task Assignment Optimization in Vehicular Fog Computing: A Contract-Matching Approach", IEEE transactions on vehicular technology, vol. 68, no. 4, April, 2019.

[16] Shirafkan, M., Shahidinejad, A. & Ghobaei-Arani, M. "An Intrusion Detection System using Deep Cellular Learning Automata and Semantic Hierarchy for Enhancing RPL Protocol Security". Cluster Comput 26, 2443–2461, 2023.

[17] Abedi, S., Ghobaei-Arani, M., Khorami, E., & Mojarad, M. "Dynamic Resource Allocation Using Improved Firefly Optimization Algorithm in Cloud Environment". Applied Artificial Intelligence, 36(1), 2022.

[18] Shirafkan, M., Shahidienjad, A. & Ghobaei-Arani, M. "An autonomous intrusion detection system for the RPL protocol". Peer-to-Peer Netw. Appl. 15, 484–502, 2022.

[19] Mohsen Ghorbian, Mostafa Ghobaei-Arani, Rohollah Asadolahpour-Karimi, "Function Placement Approaches in Serverless Computing: A Survey",Journal of Systems Architecture, Volume 157, 103291, ISSN 1383-7621,2024.

[20] Jazayeri, F., Shahidinejad, A. & Ghobaei-Arani, M. "A latency-aware and energy-efficient computation offloading in mobile fog computing: a hidden Markov model-based approach". J Supercomput 77, 4887–4916 ,2021.