applied sciences

MDPI

Article

A Secured Intrusion Detection System for Mobile Edge Computing

Khalid Alsubhi

Department of Computer Science, King Abdulaziz University, Jeddah 21589, Saudi Arabia; kalsubhi@kau.edu.sa

Abstract: With the proliferation of mobile devices and the increasing demand for low-latency and high-throughput applications, mobile edge computing (MEC) has emerged as a promising paradigm to offload computational tasks to the network edge. However, the dynamic and resource-constrained nature of MEC environments introduces new challenges, particularly in the realm of security. In this context, intrusion detection becomes crucial to safeguard the integrity and confidentiality of sensitive data processed at the edge. This paper presents a novel Secured Edge Computing Intrusion Detection System (SEC-IDS) tailored for MEC environments. The proposed SEC-IDS framework integrates both signature-based and anomaly-based detection mechanisms to enhance the accuracy and adaptability of intrusion detection. Leveraging edge computing resources, the framework distributes detection tasks closer to the data source, thereby reducing latency and improving real-time responsiveness. To validate the effectiveness of the proposed SEC-IDS framework, extensive experiments were conducted in a simulated MEC environment. The results demonstrate superior detection rates compared to traditional centralized approaches, highlighting the efficiency and scalability of the proposed solution. Furthermore, the framework exhibits resilience to resource constraints commonly encountered in edge computing environments.

Keywords: privacy; security; IDS; edge computing; mobile computing

Citation: Alsubhi, K. A Secured Intrusion Detection System for Mobile Edge Computing. *Appl. Sci.* **2024**, *14*, 1432. https://doi.org/10.3390/app14041432

Academic Editor: Luis Javier García Villalba

Received: 13 December 2023
Revised: 3 February 2024
Accepted: 6 February 2024
Published: 9 February 2024

1. Introduction

The rapid proliferation of mobile computing has revolutionized the way users interact with information technology, ushering in an era of unprecedented connectivity and pervasive computing. With the advent of resource-constrained devices and the burgeoning demand for low-latency applications, mobile edge computing (MEC) has emerged as a paradigm-shifting technology, pushing computational capabilities closer to end-users [1–3]. While MEC offers numerous benefits, its unique characteristics also pose distinct security challenges, necessitating innovative solutions to safeguard the integrity and confidentiality of data processed at the edge. In this context, the focus of this paper is on the development and exploration of a cutting-edge solution: a secured edge-based intrusion detection framework tailored explicitly for mobile computing environments.

Securing intrusion detection systems (IDSs) in the context of mobile edge computing (MEC) introduces a myriad of challenges and considerations. The convergence of mobile devices with edge computing resources creates a dynamic environment where traditional security measures may fall short. One notable concern is the increased attack surface due to the distributed nature of MEC, making it imperative to safeguard communication channels and data exchanges. Mobile devices, being inherently vulnerable to diverse cyber threats, amplify the need for robust intrusion detection mechanisms. Additionally, the reliance on wireless communication within MEC introduces potential vulnerabilities, emphasizing the necessity for secure transmission protocols and encryption. The integration of edge resources in processing and storing sensitive information calls for stringent access controls and authentication mechanisms to thwart unauthorized access. Furthermore, the seamless integration of signature-based and anomaly-based detection in MEC's IDS introduces

complexities in ensuring real-time responsiveness without compromising accuracy. As MEC environments operate in a resource-constrained setting, optimizing intrusion detection algorithms for efficiency becomes paramount. Addressing these security challenges requires a holistic approach, encompassing cryptographic protocols, secure communication channels, access controls, and tailored intrusion detection strategies to fortify the resilience of mobile edge computing against evolving cyber threats.

The central objective is to fortify the security posture of MEC by introducing a robust and adaptive intrusion detection system that leverages the capabilities of edge computing resources [4]. The need for such a framework arises from the dynamic nature of MEC environments, where the edge serves as the focal point for data processing and communication. Conventional intrusion detection systems designed for traditional computing infrastructures may not seamlessly translate to the intricacies of edge computing, necessitating a dedicated approach that aligns with the unique characteristics and constraints of mobile computing environments. The contribution of this paper can be summarized as follows:

- This paper proposes a secured edge computing-based intrusion detection system (SEC-IDS) approach to intrusion detection, acknowledging the significance of real-time responsiveness and low-latency decision-making in mobile computing scenarios.
- By distributing intrusion detection tasks closer to the data source, the framework aims to reduce the impact of latency, enhance the scalability of the system, and improve overall network security.
- Furthermore, our proposed framework incorporates a hybrid detection approach, combining signature-based and anomaly-based techniques. This amalgamation enables the system to detect both known attack patterns and previously unseen threats, thereby providing a comprehensive defense against a diverse range of cyber threats.
- Additionally, a dedicated secure communication layer is integrated into the framework to mitigate potential attacks on the intrusion detection system itself, ensuring the overall robustness of the proposed solution.

Through this research, we strive to contribute to the ongoing discourse on securing mobile computing environments, emphasizing the critical role that intrusion detection plays in fortifying the integrity and confidentiality of data processed at the edge. The subsequent sections will delve into the intricacies of our secured edge-based intrusion detection framework, its design principles, implementation details, and comprehensive evaluation, shedding light on its efficacy in addressing the evolving security challenges within the realm of mobile computing.

The rest of the paper is organized in such a way that Section 2 describes the comprehensive literature background and related state-of-the-art methods. Section 3 explains the types of attacks on mobile edge computing discussed in this study. Further, Section 4 presents the SEC-IDS proposed framework in detail. Section 5 discusses the implementation, results, and comparative analysis with the existing methods. Lastly, we conclude our study in Section 6.

2. Literature Review

2.1. Background

In this section, we introduce the background studies of used technologies for the proposed study. Further, these technologies are evaluated as well.

A. Edge Computing

The rapid evolution of computing paradigms, coupled with the pervasive integration of Internet of Things (IoT) devices [5], has led to a paradigm shift in network architecture. Edge computing, with its emphasis on decentralized data processing at the network periphery, has emerged as a transformative approach to address the challenges posed by the massive influx of data and the demand for low-latency, high-throughput applications. However, the distributed nature of edge computing introduces new security concerns, necessitating innovative solutions to safeguard critical data and infrastructure. In the

context of edge computing, the security architecture must evolve to address the unique characteristics and challenges associated with this decentralized paradigm [6]. Traditional security models, primarily designed for centralized architectures, may prove insufficient to protect the diverse and dynamic edge computing environments. Intrusion detection systems (IDSs) play a pivotal role in identifying and mitigating potential threats, ensuring the integrity, confidentiality, and availability of data and services.

B. IDS (Intrusion Detection System)

Intrusion detection systems play a pivotal role in identifying and mitigating cybersecurity threats, offering organizations a proactive defense mechanism. However, understanding their limitations is paramount in designing a comprehensive security strategy that addresses the evolving nature of cyber threats [7]. As cybersecurity landscapes continue to advance, the need for innovative approaches and the integration of complementary technologies becomes imperative to enhance the overall resilience of network defenses. Edge-based IDS security architecture represents a crucial advancement in the domain of cybersecurity, tailoring intrusion detection mechanisms to the specific requirements and constraints of edge computing environments. Unlike conventional IDS that operate within centralized data centers, edge-based IDS is strategically positioned at the network periphery, closer to the data sources and endpoints. This proximity not only reduces latency but also enables timely detection and response to security incidents, a critical consideration in the context of emerging applications such as autonomous vehicles, smart cities, and industrial IoT. The architecture of edge-based IDS encompasses a range of components and functionalities designed to fortify the security posture of edge computing environments. This includes the deployment of intrusion detection sensors, distributed detection engines, and secure communication protocols [8]. The dynamic and resource-constrained nature of edge devices necessitates the optimization of detection algorithms and the efficient utilization of computing resources. Consequently, the security architecture must strike a delicate balance between detection accuracy and minimal impact on system performance.

2.2. Related Work

The fundamental idea behind the Internet of Things (IoT) centers on the proliferation of intelligent nodes seamlessly integrated into our daily social interactions [9]. This underscores the imperative for cutting-edge intrusion detection methods specifically tailored to address the unique challenges posed by IoT and EDGE computing networks, emphasizing the importance of adopting approaches grounded in artificial intelligence. In the realm of IoT, digital devices interconnected via the internet aim to establish connections for individuals through smart IoT applications, resulting in network-distributed environments characterized by limited power, storage, and memory capacities.

Intrusion detection systems (IDSs) assume a critical role in identifying and responding to intrusive actions and behaviors, prompting administrators to take automated actions [10]. Employing signature methods, IDSs detect intrusions by comparing signatures to predefined intrusive events stored in the database [11]. While this ensures swift detection and diminishes false alarms, a significant drawback is evident: only known intrusions can be identified. Anomaly detection treats all intrusive activities as anomalous, flagging any activity deviating from standard treatment as a potential intrusion. Anomaly-based detection offers a substantial advantage in detecting zero-day attacks and variations of known attacks. Numerous existing approaches leverage traditional machine learning environments for intrusion detection. Robust anomaly detection methods utilizing artificial neural networks (ANN) and deep learning surpass the limitations of conventional approaches [12–15]. The adaptability of ANN features renders them applicable across diverse domains, with a specific focus on enhancing intrusion detection. These advanced approaches prove immensely beneficial in the realms of modern computing and EDGE computing.

In [16], a deep belief network tailored for the Edge of Things (EoT) is presented, offering the capability to detect intrusive activities within the EoT network. The proposed framework comprises modules for data collection, feature extraction, and classification.

However, the computational demands and associated costs of this model are notably high. Addressing the critical security concerns in the Internet of Things (IoT) network, ref. [17] introduces a robust intrusion detection system (IDS) incorporating a multi-agent system, blockchain, and deep learning algorithms. While this approach demonstrates high efficiency, the amalgamation of three diverse techniques introduces complexity and increases response time.

For mobile edge computing, ref. [10] proposes a network IDS that captures tcpdump packets, extracts and analyzes features, and forwards legitimate packets into the network. The model employs a topic model to learn normal behavioral patterns, but its detection accuracy is compromised when new types of packets enter the network. In addition, ref. [18] introduces a data-driven mimicry and game theory-based IDS for edge computing networks, investigating new attacks based on game income and balance points. Efforts are made to reduce the IDS cost. Also, ref. [19] suggests a traffic inspection and classification-based distributed attack model for IoT applications, leveraging the flexibility of cloud-based architectures with edge computing. However, relying on a traffic classification-based mechanism may yield inaccurate results with new network traffic.

Further, authors in [20] proposed the ZBIDS model, a security framework designed to enhance network protection by logically dividing the network into distinct zones, each with specific security requirements. This hierarchical architecture allows for tailored intrusion detection mechanisms in each zone, ensuring a more effective and flexible approach to network security. ZIDS employs pattern recognition and signature-based methods to identify known attack patterns or anomalies in network behavior. Each zone is equipped with zone-specific intrusion detection modules and customized rulesets, enabling targeted threat detection. The system generates real-time alerts upon detecting suspicious activities, triggering automated responses based on the severity of the threat. Security policies are defined for each zone, guiding the acceptable and unacceptable activities within that segment. ZIDS enforces these policies to ensure compliance with predefined rules and regulations. The model maintains comprehensive logs of network activities and detected intrusions, providing detailed reports for post-incident analysis and continuous security improvement. The ZIDS model is scalable, making it adaptable to diverse network environments and varying security needs. Overall, ZIDS offers a robust and hierarchical approach to intrusion detection, enhancing the security posture of networked systems.

Similarly, authors in [21] proposed the EEACK-IDS (enhanced energy-aware clustering and key management-based intrusion detection system) model as an innovative intrusion detection framework designed for wireless sensor networks (WSNs). It combines energy-efficient clustering and key management techniques to enhance the overall security and energy efficiency of WSNs. EEACK-IDS employs an energy-efficient clustering approach to organize sensor nodes into clusters, minimizing energy consumption and prolonging the network's operational lifetime. The model incorporates robust key management mechanisms to secure communication within and between clusters. Key distribution and updating strategies enhance the resilience of the network against potential attacks. EEACK-IDS integrates an intrusion detection system that continuously monitors network activities to identify and respond to potential security threats. The model introduces enhanced security measures to protect against various types of attacks, including data tampering, eavesdropping, and node compromise. EEACK-IDS undergoes performance evaluation to assess its effectiveness in terms of intrusion detection accuracy, energy consumption, and network lifetime. The model aims to achieve a balance between security and energy efficiency, making it suitable for resource-constrained WSNs.

Another security-related IDS model, SAZIDS (smart ant colony-based zone intrusion detection system), was proposed in [22]. The model is an innovative intrusion detection framework designed for wireless sensor networks (WSNs). It leverages the principles of ant colony optimization to create an intelligent and adaptive system for detecting intrusions in WSNs. The model organizes the WSN into distinct zones, each with its own set of security requirements. Ant agents patrol these zones, monitoring network activities and identifying

potential intrusions. SAZIDS prioritizes energy efficiency, a critical consideration for resource-constrained WSNs. The intelligent ant agents optimize their routes and activities to minimize energy consumption while maintaining effective intrusion detection. The decentralized nature of SAZIDS enhances its scalability and resilience [23]. Ant agents operate autonomously, contributing to the robustness of the intrusion detection system. SAZIDS undergoes performance evaluation to assess its effectiveness in terms of intrusion detection accuracy, energy efficiency, and adaptability to changing network conditions.

3. Types of Attacks on Mobile Edge Computing

Routing Information Protocol (RIP) [24] is a dynamic routing protocol commonly used within computer networks to facilitate the exchange of routing information between routers. While RIP is a widely adopted protocol, its simplicity can make it vulnerable to various types of attacks.

Route Flapping: In this attack [25], a malicious actor advertises false or poisoned routing information to routers in the network. The attacker may advertise unreachable or undesirable routes, leading routers to make incorrect routing decisions. Route poisoning can disrupt normal network operations by causing routers to forward traffic along incorrect paths, leading to connectivity issues and potential data interception. Route flapping involves continuously and rapidly advertising and withdrawing routes. This activity can consume network resources and cause instability in the routing tables of neighboring routers. Route flapping can lead to network congestion, increased bandwidth usage, and potential service disruptions as routers struggle to adapt to frequent changes in routing information.

Denial of Service (DoS): A Denial-of-Service attack [26] on RIP can involve overwhelming the RIP routers with excessive traffic or malformed packets, causing them to become unresponsive or leading to degraded performance. A successful DoS attack can result in a loss of network connectivity, rendering the RIP routers incapable of providing routing services and potentially disrupting overall network functionality.

Spoofing Attacks: [27] Malicious entities may attempt to spoof RIP packets by forging the source address to appear as a trusted router within the network. This can allow the attacker to inject false routing information. Spoofed RIP packets can mislead routers into accepting unauthorized routing updates, potentially leading to traffic interception, rerouting, or other security compromises. Table 1 presents an overview of all these attacks as follows.

Table 1. Overview of possible attacks for IDS in mobile edge computing.

Attack	Description
Route Flapping	Route flapping is a network instability issue where a route alternates between available and unavailable states in a rapid and repetitive manner.
Denial of Service (DoS)	A Denial-of-Service attack aims to disrupt the normal functioning of a system or network by overwhelming it with a flood of traffic, rendering it incapable of providing routing services.
Spoofing Attacks	Spoofing attacks involve the impersonation of a legitimate entity or source by falsifying information.
Unauthorized Access	Unauthorized access refers to gaining entry or privileges to a system or network without proper authorization. Attackers exploit vulnerabilities to bypass security mechanisms and access sensitive information or resources.
Malware Injection Attack	A malware injection attack involves inserting malicious code or software into a system or application. This code can compromise the integrity of the system, steal sensitive information, or perform unauthorized actions.

Unauthorized Access: Unauthorized access [28] to routers running RIP can result in an attacker gaining control over the routing tables and configurations. This can lead to the manipulation of routing information. Unauthorized access allows attackers to modify routing tables, redirect traffic, or cause network outages, compromising the overall integrity and security of the network.

Malware Injection Attack: A malware injection attack [29–32], also known as a code injection attack, is a type of cybersecurity threat where malicious code is inserted into a legitimate application or system with the intent of compromising its functionality, stealing sensitive information, or gaining unauthorized access. This form of attack exploits vulnerabilities in software, allowing the attacker to execute arbitrary code and manipulate the targeted system for malicious purposes.

4. Proposed SEC-IDS Framework

In the evolving landscape of ubiquitous connectivity, the increasing prominence of mobile edge computing (MEC) underscores the critical need for robust security measures within edge environments. This paper addresses this imperative by presenting a groundbreaking intrusion detection system (IDS) framework tailored explicitly for MEC. The SEC-IDS framework stands out by leveraging a certificate authority (CA) infrastructure, introducing a novel approach to enhance the security landscape of mobile edge networks. At its core, the framework employs CA principles to validate and authenticate communication channels between edge devices and services operating within the MEC ecosystem. By integrating this CA-based approach, the SEC-IDS not only establishes a foundation for trusted communication but also reinforces the overall integrity and confidentiality of data exchanged at the edge. This innovative framework represents a significant stride in fortifying the security posture of MEC environments, offering a reliable and scalable solution to address the unique challenges posed by the dynamic and distributed nature of edge computing.

Figure 1 presents the proposed CA-based SEC-IDS for edge computing.

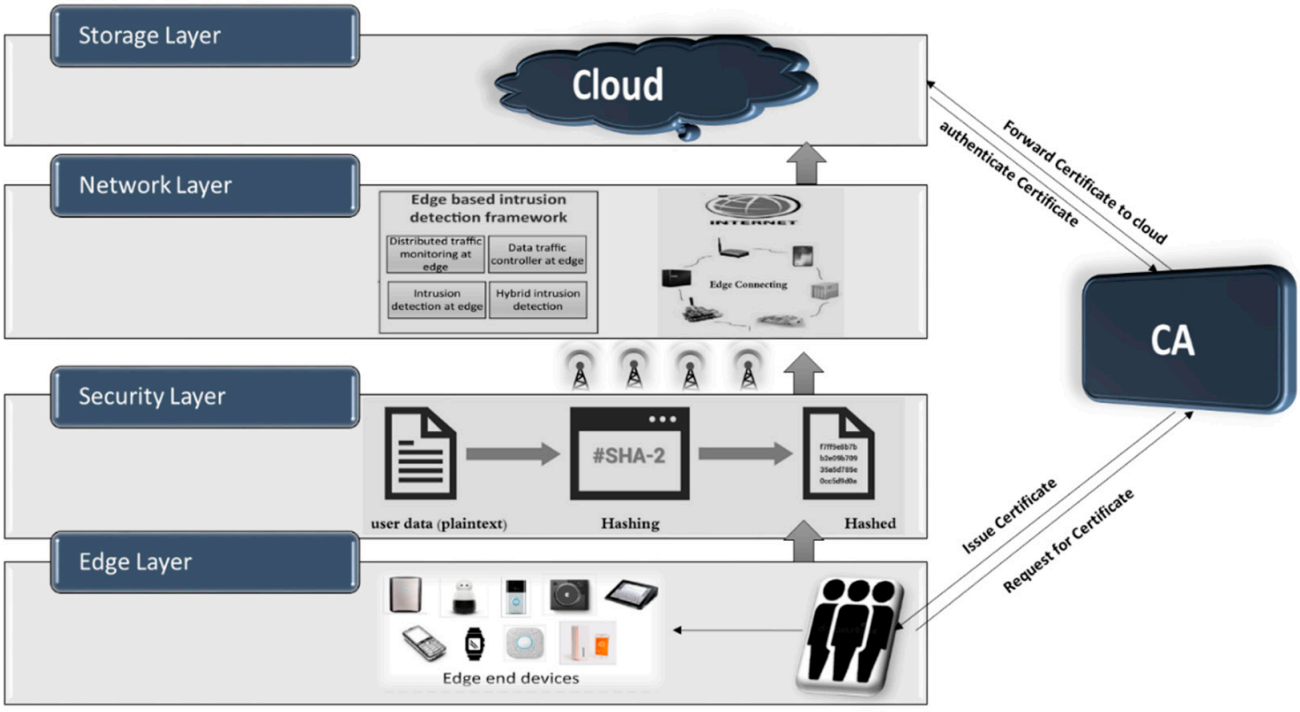

Figure 1. CA-based secured IDS for mobile-based edge computing.

The key components of the framework include:

Certificate Management System:

A robust system for issuing, distributing, and managing digital certificates for edge devices within the MEC environment. Certificates play a pivotal role in establishing secure communication channels. Equation (1) is used to generate the digital signature as follows:

$$cd = \text{CA.Sign}(d) \tag{1}$$

$$Verify(cd,p) \tag{2}$$

In the proposed model for mobile edge computing (MEC) with the SEC-IDS (Secured Edge Computing Intrusion Detection System) framework, the certificate management system (CMS) plays a crucial role in enhancing the security and trustworthiness of communication channels within the MEC ecosystem. The CMS serves as the central component responsible for the issuance, distribution, renewal, and revocation of digital certificates, adding an additional layer of authentication and validation to the communication process. The primary functions of the certificate management system in the proposed model include:

- *Certificate Issuance:* The CMS generates digital certificates for entities within the MEC environment, such as edge devices and services. These certificates serve as cryptographic credentials, attesting to the authenticity and legitimacy of the entities involved in communication.
- *Public Key Distribution:* The CMS facilitates the distribution of public keys associated with the issued certificates. This is essential for enabling secure communication through encryption and ensuring that only authorized entities can decrypt and access sensitive information.
- *Certificate Renewal and Revocation:* The CMS manages the lifecycle of digital certificates, overseeing their renewal to maintain up-to-date cryptographic credentials. Additionally, it handles the revocation of certificates in cases of compromised security or changes in entity authorization status, thereby promptly mitigating security risks.
- *Authentication and Trust Establishment:* By relying on the CA infrastructure, the CMS contributes to the establishment of a trusted communication channel within the MEC ecosystem. Digital certificates issued and managed by the CMS serve as trusted indicators, allowing entities to verify the authenticity of their counterparts before engaging in data exchange.
- *Integrity and Confidentiality Assurance:* Through the issuance and verification of digital signatures, the CMS ensures the integrity of data transmitted within the MEC environment. It also plays a vital role in maintaining the confidentiality of communication by managing the encryption keys associated with the certificates.
- *Policy Enforcement:* The CMS enforces security policies related to certificate usage, ensuring that entities adhere to predefined security standards and access controls. This contributes to a consistent and well-regulated security posture within the MEC infrastructure.

Intrusion Detection Module:

An advanced IDS module that monitors network traffic, analyzes communication patterns, and detects anomalous behavior within the MEC infrastructure. The IDS is designed to identify potential security threats and trigger alerts for timely response.

Behavioral Analytics:

Integration of behavioral analytics and machine learning algorithms to enhance the detection capabilities of the IDS. This allows the system to adapt and evolve, identifying both known and novel intrusion patterns.

Real-time Response Mechanism:

A real-time response mechanism that allows the IDS to take immediate action upon detecting suspicious activities. This may include isolating compromised devices, blocking malicious communication, or triggering notifications to administrators.

The proposed CA-based framework addresses the unique security challenges of MEC environments by providing a trusted foundation for communication and implementing proactive intrusion detection measures. By combining the principles of CA with state-of-the-art intrusion detection technologies, the proposed framework aims to establish a secure and resilient MEC ecosystem, safeguarding critical data and services at the network edge. The step by step procedure of proposed CA-IDS approach is presented in Algorithm 1 as follows.

Algorithm 1: CA-Based IDS for Mobile Edge Computing

Inputs:
D—Set of all edge devices in the MEC environment.
C—Set of digital certificates.
T—Set of network traffic data.
M—Machine learning model for anomaly detection.
A—Set of intrusion alerts.
Output:
C—Set of digital certificates issued by the CA.
A—Set of alerts indicating potential intrusions.
Act—Actions taken based on the alerts.
Process:

1. *Initialization*

Initialize the certificate authority (CA) and intrusion detection system (IDS) components.

2. *Certificate Management:*
   2.1 For each device \(d\) in \(D\):
      2.1.1 Generate a unique public–private key pair for \(d\).
      2.1.2 Create a digital certificate \(c_d\) for \(d\) signed by the CA.
      2.1.3 Add \(c_d\) to the set of certificates \(C\).
3. *Intrusion Detection*
   3.1 For each network packet \(p\) in \(T\):
      3.1.1 Extract sender and receiver information from \(p\).
      3.1.2 Verify the authenticity of the sender using \(C\).
      3.1.3 If sender is not authenticated:
         3.1.3.1 Generate an intrusion alert \(a\) for the unauthorized sender.
         3.1.3.2 Add \(a\) to the set of alerts \(A\).
4. *Behavioral Analytics:*
   4.1 Train machine learning model \(M\) using features extracted from \(T\).
5. *Real-time Response:*
   5.1 For each alert \(a\) in \(A\):
      5.1.1 Determine the severity and type of intrusion.
      5.1.2 Take appropriate real-time response actions (e.g., isolate device, block communication).
6. Continuously repeat steps 3, 4, and 5 to adapt to evolving network conditions.

Security analysis of proposed SEC-IDS Framework

Let *C* be the set of digital certificates issued by the CA, *T* be the set of network traffic data, and Verify(*cd*,*p*) be the certificate verification function for network packet *p* using certificate *cd*. The lemma states that if the verification process is successful for all network packets in *T* based on the digital certificates in *C*, then the communication between devices

in the MEC network is considered authenticated. Mathematically, the lemma can be expressed as

$$\forall p \in T, \forall cd \in C\text{:Verify}(cd,p) = \text{True} \Longrightarrow \text{Communication is Authenticated}$$

In this lemma, the quantifiers $\forall\forall$ denote universal quantification, stating that the verification holds for all network packets and certificates. The implication ($\Longrightarrow$) indicates that if the verification process is true for all combinations of packets and certificates, then the communication is authenticated in the MEC network. This lemma captures the essential property of the algorithm, emphasizing the importance of successful certificate verification for secure communication.

5. Implementation and Results

To assess the efficacy and functionality of the proposed framework, we employed NS-2 (Network Simulator 2) as the chosen tool for implementation. NS-2 is a versatile and widely adopted discrete event network simulator that provides a platform for the creation and evaluation of complex network scenarios. In this context, we specifically utilized NS-2 to implement a certificate authority (CA)-based intrusion detection system (IDS) tailored for mobile edge computing (MEC) environments. The utilization of NS-2 allows for the simulation and thorough examination of both security and performance aspects within a controlled and replicable environment. This choice of simulation tool facilitates the modeling of diverse network conditions and scenarios, enabling comprehensive testing of the CA-based IDS for MEC. Through NS-2, we can emulate various intrusion scenarios, assess the system's responsiveness to security threats, and evaluate its overall performance under different conditions. The use of NS-2 ensures a robust and versatile platform for the validation and refinement of the proposed framework, contributing to a more thorough understanding of its capabilities and limitations in the context of MEC security. The following parameters in Table 2 were used during the evaluation:

Table 2. Simulation parameters and perspective values.

Simulation Parameters	Value
Channel	Wireless Channel
MAC	802.11
Antenna Type	Omni Antenna
Routing protocol	AODV
Initial Energy	100 Joules
Traffic Type	CBR

Figure 2 demonstrates the superior performance of the proposed SEC-IDS system in accurately identifying attacks when compared to existing detection strategies like ZBIDS, EEACK-IDS, and SAZIDS. SEC-IDS showcases a 3.45% improvement by delivering the content with a ratio of 900 in 3 ms, which is a massive improvement over SAZIDS, a significant 12.14% enhancement over the current ZBIDS strategy, and an 8.28% higher detection rate than EEACK-IDS. Similarly, we also evaluated the detection rate and compared with existing approaches as shown in Figure 3.

Figure 4 displays the assessment of the false alarm rate. The proposed SEC-IDS showcases its effectiveness in reducing the false alarm rate when contrasted with established exploration methods like ZBIDS, EEACK-IDS, and SAZIDS. SEC-IDS manifests a notable 20.18% improvement over SAZIDS, a significant 16% enhancement over EEACK-IDS, and an overall performance improvement of 9.95% by minimizing the FAR up to 1.2, which is ignorable in the given strategies.

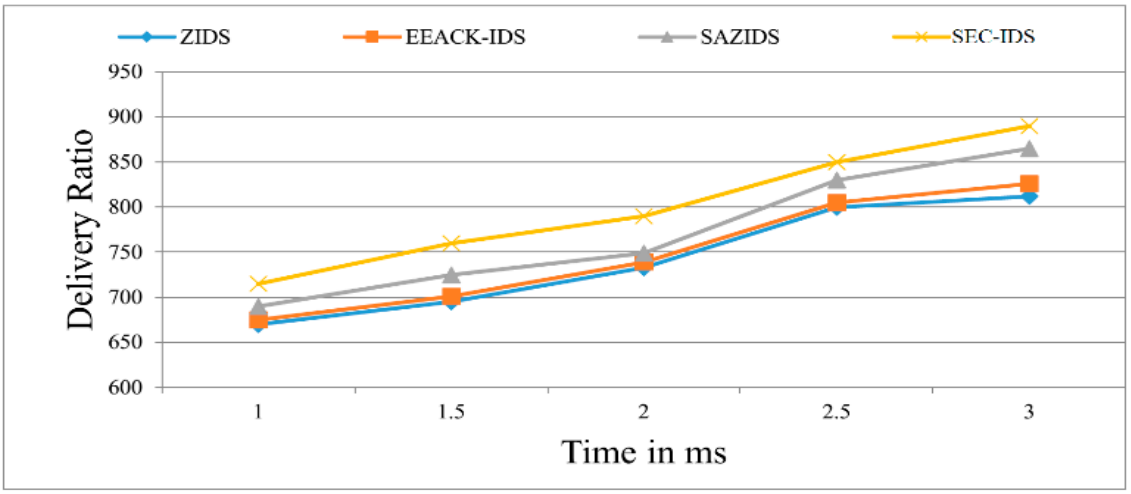

Figure 2. Data delivery ratio of the proposed model compared with existing models.

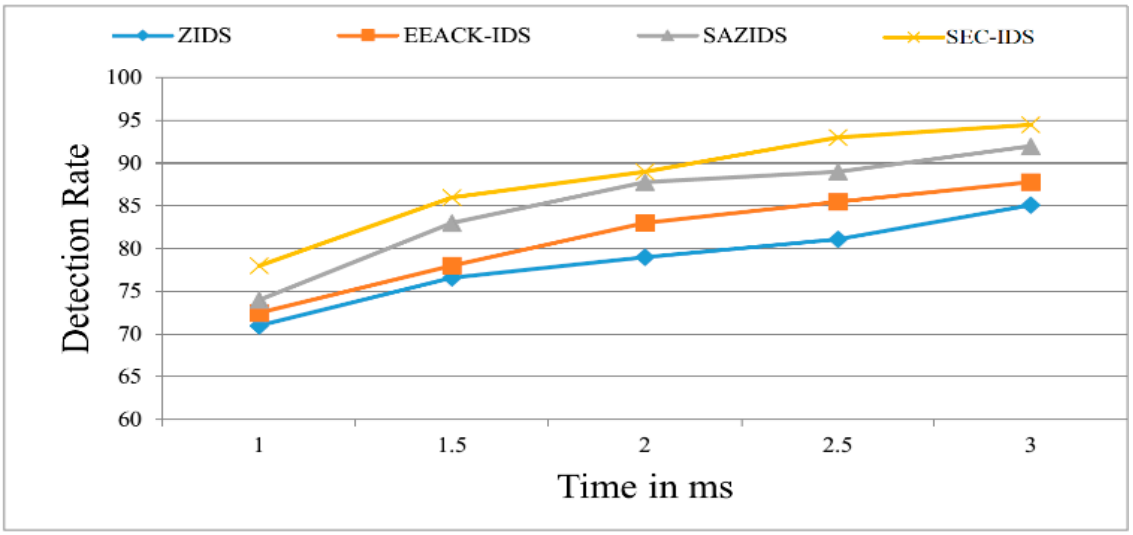

Figure 3. Intrusion detection rate of the proposed model compared with existing models.

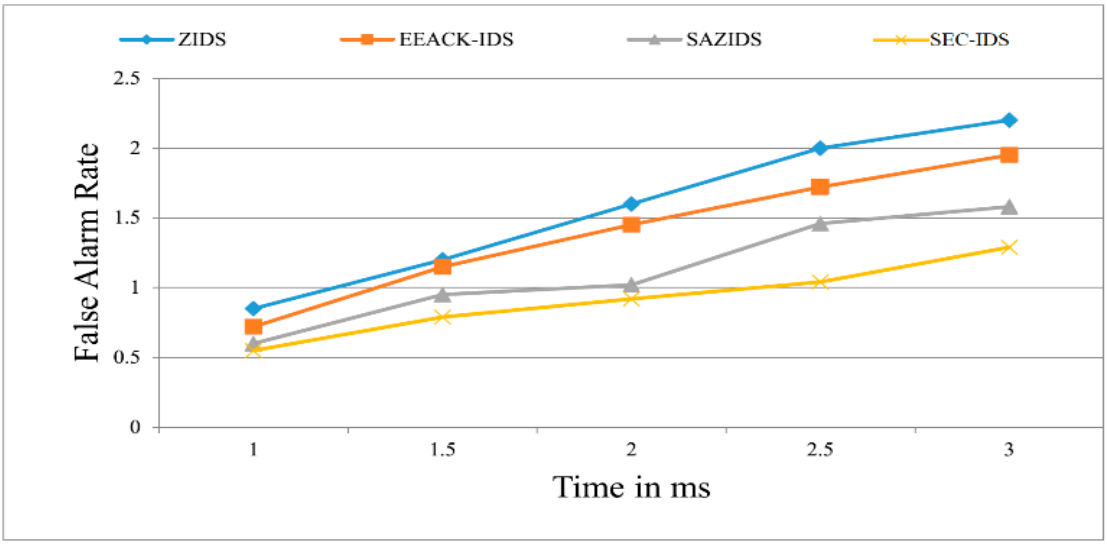

Figure 4. False alarm rate of the proposed model compared with existing models.

Figure 5 illustrates the assessment of the link change rate, revealing that SEC-IDS adeptly reduces this rate when compared to the established methods of ZBIDS, EEACK-IDS, and SAZIDS. SEC-IDS showcases a significant 16.16% improvement over SAZIDS, a substantial 45.8% enhancement over ZBIDS, and a notable 44% better performance than EEACK-IDS.

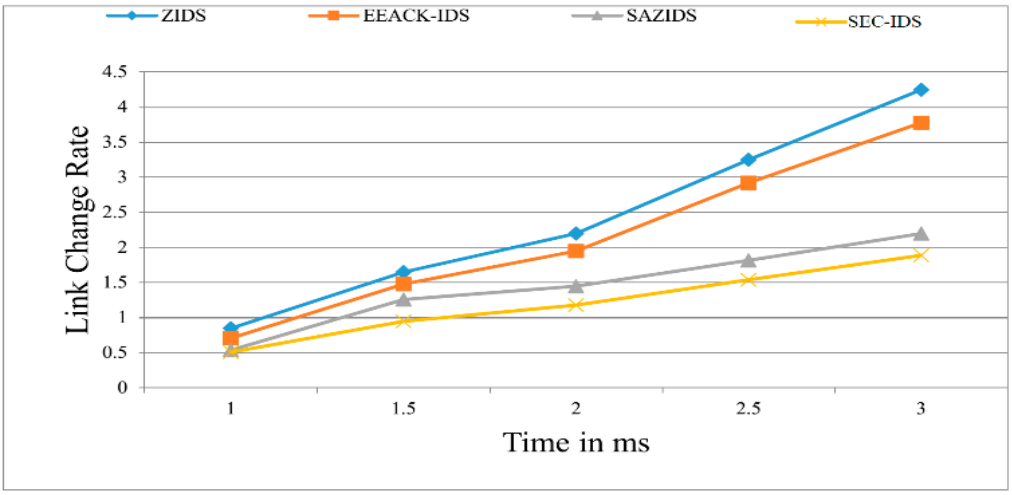

Figure 5. Link change rate of the proposed model compared with existing models.

The intrusion detection system (IDS) designed for edge computing and leveraging certificate authority introduces a robust security framework. This system capitalizes on certificate authority mechanisms to enhance the security posture of edge computing environments. The use of certificates ensures the authenticity and trustworthiness of entities within the edge network. By employing certificate-based validation, the IDS can effectively identify and respond to potential intrusions, safeguarding the integrity and confidentiality of edge computing resources. This approach establishes a secure foundation for edge computing operations, addressing the unique security challenges posed by decentralized and distributed computing environments. Further, the proposed IDS model has some pros and cons as follows:

Pros of the proposed SEC_IDS Model:

Comprehensive Detection Mechanisms: The integration of both signature-based and anomaly-based detection mechanisms enhances the overall effectiveness of intrusion detection. This comprehensive approach allows the system to detect known attack patterns as well as abnormal behaviors that may indicate novel threats.

Adaptability: The SEC-IDS framework is designed to be adaptable to evolving threats. The combination of signature-based and anomaly-based detection mechanisms ensures flexibility in identifying both known and unknown intrusion attempts, making it resilient to emerging attack vectors.

Edge Computing Utilization: Leveraging edge computing resources is a significant advantage. By distributing detection tasks closer to the data source within the MEC environment, the framework minimizes latency. This not only improves the real-time responsiveness of the intrusion detection system but also optimizes resource utilization.

Reduced Latency: The distribution of detection tasks at the edge reduces latency in the intrusion detection process. This is crucial for MEC environments where low latency is essential for ensuring timely responses to security threats.

Realistic Validation: The extensive experiments conducted in a simulated MEC environment provide a realistic validation of the SEC-IDS framework. Simulating MEC conditions allows for a controlled and replicable assessment of its performance under various scenarios.

Cons of proposed SEC_IDS Model:

Simulation Limitations: While the simulated MEC environment offers controlled experiments, it may not fully replicate the complexities and nuances of a live MEC deployment. Real-world conditions, such as network variability and dynamic user behavior, could introduce factors not accounted for in the simulation.

Resource Intensiveness: Implementing both signature-based and anomaly-based detection mechanisms may demand significant computational resources. In resource-constrained MEC environments, this could potentially lead to performance bottlenecks or increased energy consumption.

Dependency on Edge Infrastructure: The effectiveness of the SEC-IDS framework is contingent on the availability and reliability of edge computing resources. In scenarios where the edge infrastructure is limited or unstable, the system's performance may be compromised.

Ongoing Maintenance: To stay effective against evolving threats, the SEC-IDS framework may require regular updates and maintenance. Keeping signature databases up to date and refining anomaly detection models could introduce operational overhead.

Limited Generalization: The framework's performance may be optimized for the specific conditions of the simulated MEC environment, and its generalization to diverse MEC deployments may require additional validation and customization.

6. Conclusions

This study has illuminated a multitude of challenges in intrusion detection, causing disruptions in the operation of mobile edge networks and posing threats to availability, integrity, and confidentiality. Conventional firewalls and established machine learning-based methods encounter hurdles in adeptly discerning new or unfamiliar intrusive traffic. In response to these challenges, this paper introduces the Secured Edge Computing Intrusion Detection System (SEC-IDS), meticulously designed for mobile edge computing environments. The proposed framework incorporates distinct detection modules geared towards identifying unknown or novel attacks with a minimal false alarm rate (FAR) within the mobile edge infrastructure. The results of the implementation underscore the effectiveness of the SEC-IDS framework, achieving an impressive accuracy of 95.25% and an exceptionally low FAR of 1.1%. In contrast, the ZIDS demonstrates an accuracy of 86.04% with a FAR of 8.4%, while the SAIDS attains an accuracy of 86.94% with a FAR of 2.1%. These findings, when compared with prior works, signify a substantial enhancement in performance, with accuracy elevated by up to 10.78% and FAR reduced by up to 93%. The paper delves further into a security analysis grounded in game theory principles.

Funding: King Abdulaziz University (DSR) & Ministry of Education: IFPDP-269-22.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data is contained within the article.

Acknowledgments: The authors gratefully acknowledge technical and financial support from Ministry of Education and Deanship of Scientific Research (DSR), King Abdulaziz University (KAU), Jeddah, Saudi Arabia.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Abbas, N.; Zhang, Y.; Taherkordi, A.; Skeie, T. Mobile Edge Computing: A Survey. *IEEE Internet Things J.* **2017**, *5*, 450–465. [CrossRef]
2. Rehman, A.; Abdullah, S.; Fatima, M.; Iqbal, M.W.; Almarhabi, K.A.; Ashraf, M.U.; Ali, S. Ensuring Security and Energy Efficiency of Wireless Sensor Network by Using Blockchain. *Appl. Sci.* **2022**, *12*, 10794. [CrossRef]
3. Bukhsh, M.; Ali, M.S.; Alourani, A.; Shinan, K.; Ashraf, M.U.; Jabbar, A.; Chen, W. Long Short-Term Memory Recurrent Neural Network Approach for Approximating Roots (Eigen Values) of Transcendental Equation of Cantilever Beam. *Appl. Sci.* **2023**, *13*, 2887. [CrossRef]

4. Alzubi, O.A.; Alzubi, J.A.; Alazab, M.; Alrabea, A.; Awajan, A.; Qiqieh, I. Optimized Machine Learning-Based Intrusion Detection System for Fog and Edge Computing Environment. *Electronics* **2022**, *11*, 3007. [CrossRef]
5. Naqvi, M.R.; Iqbal, M.W.; Ashraf, M.U.; Ahmad, S.; Soliman, A.T.; Khurram, S.; Shafiq, M.; Choi, J.-G. Ontology Driven Testing Strategies for IoT Applications. *Comput. Mater. Contin.* **2022**, *70*, 5855–5869. [CrossRef]
6. Ali, S.S.D.; Zhao, H.P.; Kim, H. Mobile Edge Computing: A Promising Paradigm for Future Communication Systems. In Proceedings of the TENCON 2018—2018 IEEE Region 10 Conference, Jeju, Republic of Korea, 28–31 October 2018; pp. 1183–1187.
7. Vimal, S.; Suresh, A.; Subbulakshmi, P.; Pradeepa, S.; Kaliappan, M. Edge computing-based intrusion detection system for smart cities development using IoT in urban areas. In *Internet of Things in Smart Technologies for Sustainable Urban Development*; Springer Nature: Cham, Switzerland, 2020; pp. 219–237.
8. Ashraf, M.U.; Hannan, A.; Cheema, S.M.; Ali, Z.; Alofi, A. Detection and tracking contagion using IoT-edge technologies: Confronting COVID-19 pandemic. In Proceedings of the 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), Istanbul, Turkey, 12–13 June 2020; pp. 1–6.
9. Liang, C.; Shanmugam, B.; Azam, S.; Karim, A.; Islam, A.; Zamani, M.; Kavianpour, S.; Idris, N.B. Intrusion Detection System for the Internet of Things Based on Blockchain and Multi-Agent Systems. *Electronics* **2020**, *9*, 1120. [CrossRef]
10. Cao, X.; Fu, Y.; Chen, B. Packet-based intrusion detection using Bayesian topic models in mobile edge computing. *Secur. Commun. Netw.* **2020**, *2020*, 8860418. [CrossRef]
11. Eskandari, M.; Haider Janjua, Z.; Vecchio, M.; Antonelli, F. Passban IDS: An intelligent anomaly-based intrusion detection system for IoT edge devices. *IEEE Internet Things J.* **2020**, *7*, 6882–6897. [CrossRef]
12. Mumtaz, G.; Akram, S.; Iqbal, W.; Ashraf, M.U.; Almarhabi, K.A.; Alghamdi, A.M.; Bahaddad, A.A. Classification and Prediction of Significant Cyber Incidents (SCI) using Data Mining and Machine Learning (DM-ML). *IEEE Access* **2023**, *11*. [CrossRef]
13. Shinan, K.; Alsubhi, K.; Ashraf, M.U. BotSward: Centrality Measures for Graph-Based Bot Detection Using Machine Learning. *Comput. Mater. Contin.* **2023**, *74*, 693–714. [CrossRef]
14. Ahmed, M.; Usman, S.; Shah, N.A.; Ashraf, M.U.; Alghamdi, A.M.; Bahadded, A.A.; Almarhabi, K.A. AAQAL: A Machine Learning-Based Tool for Performance Optimization of Parallel SPMV Computations Using Block CSR. *Appl. Sci.* **2022**, *12*, 7073. [CrossRef]
15. Bashir, R.N.; Bajwa, I.S.; Iqbal, M.W.; Ashraf, M.U.; Alghamdi, A.M.; Bahaddad, A.A.; Almarhabi, K.A. Leaching Fraction (LF) of Irrigation Water for Saline Soils Using Machine Learning. *Intell. Autom. Soft Comput.* **2023**, *36*, 1915–1930. [CrossRef]
16. Almogren, A.S. Intrusion detection in Edge-of-Things computing. *J. Parallel Distrib. Comput.* **2020**, *137*, 259–265. [CrossRef]
17. Alexopoulos, N.; Vasilomanolakis, E.; Ivánkó, N.R.; Mühlhäuser, M. Towards blockchain-based collaborative intrusion detection systems. In Proceedings of the Critical Information Infrastructures Security: 12th International Conference, CRITIS 2017, Lucca, Italy, 8–13 October 2017; pp. 107–118.
18. Li, Q.; Hou, J.; Meng, S.; Long, H. GLIDE: A Game Theory and Data-Driven Mimicking Linkage Intrusion Detection for Edge Computing Networks. *Complexity* **2020**, *2020*, 7136160. [CrossRef]
19. Kozik, R.; Choraś, M.; Ficco, M.; Palmieri, F. A scalable distributed machine learning approach for attack detection in edge computing environments. *J. Parallel Distrib. Comput.* **2018**, *119*, 18–26. [CrossRef]
20. Bandecchi, S.; Dascalu, N. Intrusion Detection Scheme in Secure Zone Based System. *J. Comput. Nat. Sci.* **2021**, *1*, 19–25. [CrossRef]
21. Rivera, A.O.G.; White, E.M.; Tosh, D.K. Robust Authentication and Data Flow Integrity for P2P SCADA Infrastructures. In Proceedings of the 2021 IEEE 46th Conference on Local Computer Networks (LCN), Edmonton, AB, Canada, 7 September 2021; pp. 557–564.
22. Tyagi, A.K. *Data Science and Data Analytics*; Taylor & Francis Ltd.: London, UK, 2021; ISBN 9781003111290.
23. Fatima, F.; Ali, S.; Ashraf, M.U. Risk Reduction Activities Identification in Software Component Integration for Component Based Software Development (CBSD). *Int. J. Mod. Educ. Comput. Sci. IJMECS* **2017**, *9*, 19–31. [CrossRef]
24. Bhatt, T.; Kotwal, C.; Chaubey, N. Implementing and examination of eigrp ospf rip routing protocol in AMI network for DDoS attack using OPNET. *Int. J. Recent Technol. Eng.* **2019**, *8*, 3.
25. Schuchard, M.; Mohaisen, A.; Foo Kune, D.; Hopper, N.; Kim, Y.; Vasserman, E.Y. Losing control of the internet: Using the data plane to attack the control plane. In Proceedings of the 17th ACM Conference on Computer and Communications Security 2010, Chicago, IL, USA, 4–8 October 2010; pp. 726–728.
26. Gu, Q.; Liu, P. Denial of service attacks. In *Handbook of Computer Networks: Distributed Networks, Network Planning, Control, Management, and New Trends and Applications*; Wiley: Hoboken, NJ, USA, 2007; Volume 3, pp. 454–468.
27. Chen, Y.; Trappe, W.; Martin, R.P. Detecting and localizing wireless spoofing attacks. In Proceedings of the 2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, San Diego, CA, USA, 18–21 June 2007; pp. 193–202.
28. Bendovschi, A. Cyber-Attacks—Trends, Patterns and Security Countermeasures. *Procedia Econ. Finance* **2015**, *28*, 24–31. [CrossRef]
29. Ranjan, I.; Agnihotri, R.B. Ambiguity in cloud security with malware-injection attack. In Proceedings of the 2019 3rd International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 12–14 June 2019; pp. 306–310.
30. Ashraf, M.U.; Jamb, K.M.; Qayyum, R.; Ejaz, H.; Ilyas, I. IDP: A Privacy Provisioning Framework for TIP Attributes in Trusted Third Party-based Location-based Services Systems. *Int. J. Adv. Comput. Sci. Appl.* **2020**, *11*, 604–617. [CrossRef]

31. Ashraf, M.U.; Naeem, M.; Javed, A.; Ilyas, I. H2E: A Privacy Provisioning Framework for Collaborative Filtering Recommender System. *Int. J. Mod. Educ. Comput. Sci. (IJMECS)* **2019**, *11*, 1–13. [CrossRef]
32. Alsubhi, K.; Imtiaz, Z.; Raana, A.; Ashraf, M.U.; Hayat, B. MEACC: An energy-efficient framework for smart devices using cloud computing systems. *Front. Inf. Technol. Electron. Eng.* **2020**, *21*, 917–930. [CrossRef]