MZ Journals Journal of Artificial Intelligence

Securing IoT Devices and Edge Computing with Hybrid Mesh Firewalls

Ryo Suzuki and Aya Tanaka
Meiji University, Japan

Abstract

The proliferation of Internet of Things (IoT) devices and edge computing has introduced significant security challenges due to their distributed nature and diverse communication protocols. Traditional security mechanisms often fall short in providing robust protection against evolving threats in these environments. This paper proposes the use of hybrid mesh firewalls as a novel approach to securing IoT devices and edge computing infrastructures. Hybrid mesh firewalls combine the advantages of traditional firewalls with the flexibility and scalability of mesh networks, thereby enhancing security without compromising performance or scalability.

***Keywords*:** Hybrid Mesh Firewall, IoT Security, Edge Computing, Cybersecurity, Dynamic Routing, Decentralized Management.

1. Introduction

The rapid advancement and widespread adoption of Internet of Things (IoT) devices and edge computing have revolutionized various sectors, from industrial automation to smart homes and healthcare[1]. These technologies enable real-time data processing and analytics at the network's edge, reducing latency and enhancing responsiveness. However, their decentralized and heterogeneous nature poses significant security challenges. Unlike traditional networks, IoT devices often have limited computational resources and are susceptible to various attack vectors, such as malware, denial-of-service (DoS) attacks, and unauthorized access. Edge computing nodes, while more capable, still face similar security risks due to their exposure at the network perimeter and the often unsecured nature of the environments they operate in[2].

Traditional security measures, predominantly designed for centralized network architectures, struggle to address the dynamic and distributed nature of IoT and edge computing environments. Conventional firewalls, which operate on static rulesets and centralized management models, are ill-equipped to handle the complexity and scale of modern IoT deployments[3]. As these devices often communicate using a wide array of protocols and standards, static firewall configurations can quickly become obsolete, leading to security gaps. Moreover, the sheer volume of data and the

need for low latency in edge computing scenarios make it impractical to route all traffic through a central firewall, necessitating a more distributed approach to security.

In response to these challenges, hybrid mesh firewalls have emerged as a potential solution that combines the strengths of traditional firewalls with the flexibility of mesh networking. A hybrid mesh firewall is designed to operate as a decentralized security mechanism that dynamically adapts to the changing network landscape. By integrating advanced routing protocols, decentralized management, and adaptive threat detection capabilities, hybrid mesh firewalls offer a scalable and resilient approach to securing IoT devices and edge computing nodes. This approach allows for real-time threat mitigation and network protection without the bottlenecks and limitations associated with traditional firewall solutions[4].

The concept of hybrid mesh firewalls leverages the inherent advantages of mesh networks, such as self-healing, dynamic routing, and scalability. In a hybrid mesh firewall, each node in the mesh can act as a security checkpoint, enabling distributed enforcement of security policies. This decentralized structure not only enhances fault tolerance but also ensures that security measures can be dynamically updated and propagated throughout the network, providing a robust defense against emerging threats. As IoT and edge computing continue to expand, the adoption of hybrid mesh firewalls represents a promising direction for addressing the evolving security needs of these complex and diverse environments.

2. Literature Review

The security of IoT devices and edge computing has been extensively studied due to their pivotal roles in modern network infrastructures. IoT devices often operate in diverse environments and communicate through various protocols, leading to a fragmented security landscape. Research highlights common vulnerabilities in IoT systems, such as weak authentication, poor encryption, and susceptibility to firmware attacks[5]. Edge computing, which brings data processing closer to the data source, introduces additional risks by distributing computing resources across potentially unsecured nodes . These nodes often lack the robust security controls found in centralized data centers, making them prime targets for attacks . Studies have emphasized the need for security frameworks that can adapt to the dynamic and decentralized nature of these environments, suggesting that traditional security solutions are inadequate for the challenges posed by IoT and edge computing[6].

Various approaches have been proposed to secure IoT and edge computing, each with its own set of advantages and limitations. Traditional perimeter-based firewalls are often used to guard against external threats but struggle with internal threats and the complexity of IoT networks . Network segmentation and micro-segmentation are also employed to isolate critical components and limit the lateral movement of threats . More recent strategies include software-defined networking (SDN) and network function virtualization (NFV), which offer greater flexibility by allowing centralized control over network traffic . However, these solutions can introduce new vulnerabilities and often require significant changes to existing infrastructure. Blockchain

technology has been explored for securing IoT by providing immutable records of transactions and device interactions, but its scalability and resource demands remain concerns[7].

Mesh networking principles have been increasingly considered for enhancing network security, particularly in dynamic and distributed environments like IoT and edge computing. Mesh networks are characterized by their decentralized architecture, where each node can relay data and maintain network connectivity, making them resilient to single points of failure . In the context of security, mesh networks can distribute security tasks among nodes, allowing for more granular and localized enforcement of security policies[8]. This decentralization helps in dynamically adapting to changing threat landscapes and network topologies. Studies suggest that the self-healing nature of mesh networks can significantly enhance fault tolerance and provide continuous protection against network disruptions and attacks[9].

The concept of hybrid mesh firewalls merges the principles of traditional firewall technology with the decentralized, adaptive characteristics of mesh networks. Hybrid mesh firewalls aim to address the limitations of existing security frameworks by providing scalable, dynamic, and resilient security solutions . These firewalls operate by dynamically routing traffic through a mesh of security nodes, each capable of enforcing security policies and detecting threats . This approach allows for real-time adaptation to network changes and the distribution of security functions across the network, reducing dependency on centralized control points. Research into hybrid mesh firewalls has shown promising results in improving threat detection, reducing latency, and enhancing overall network security . Their ability to integrate with existing infrastructure and provide scalable security makes them a compelling option for securing IoT and edge computing environments.

3. Methodology

Design of the Hybrid Mesh Firewall: The proposed hybrid mesh firewall integrates the principles of traditional firewall technology with the dynamic, decentralized architecture of mesh networks to provide robust security for IoT devices and edge computing environments. The design consists of multiple security nodes, each capable of performing standard firewall functions such as packet filtering, intrusion detection, and access control[10]. These nodes are interconnected to form a mesh network, enabling decentralized management and dynamic routing of traffic. The hybrid mesh firewall operates on a decentralized protocol, where each node autonomously enforces security policies and communicates with other nodes to share threat intelligence and coordinate responses. This design ensures that security is not reliant on a single point of control, thereby enhancing fault tolerance and scalability.

Implementation of Security Features: Key security features are implemented at each node within the hybrid mesh firewall. Packet filtering is used to inspect and control the flow of network traffic based on predefined security rules. Intrusion detection systems (IDS) are deployed to identify and mitigate suspicious activities by analyzing network traffic patterns for known signatures of malicious behavior. Access control mechanisms are also integrated to regulate which devices or

applications can access specific resources within the network. Each node is equipped with real-time monitoring capabilities, allowing for continuous assessment of network security posture and enabling swift responses to detected threats. The distributed nature of the mesh network ensures that these security features can be dynamically updated and applied across the entire network without requiring centralized coordination. Dynamic Routing and Adaptive Threat Detection: Dynamic routing protocols are employed to manage the flow of traffic through the mesh network, ensuring optimal paths are chosen based on current network conditions and security considerations. This routing capability allows the hybrid mesh firewall to adapt to network changes, such as node failures or traffic spikes, by rerouting traffic to maintain security and performance. Adaptive threat detection is achieved through the use of machine learning algorithms that analyze traffic patterns and detect anomalies that may indicate emerging threats. These algorithms are designed to learn from historical data, enabling the system to identify new attack vectors that traditional signature-based approaches might miss. The decentralized nature of the mesh network allows for localized threat detection and response, enhancing the overall resilience of the network[11]. Evaluation and Performance Metrics: The performance of the hybrid mesh firewall is evaluated through a series of controlled experiments and real-world deployment scenarios. Metrics such as throughput, latency, and packet loss are measured to assess the impact of the firewall on network performance. Security effectiveness is evaluated based on the system's ability to detect and mitigate various types of cyberattacks, including DDoS attacks, malware infiltration, and unauthorized access attempts. Scalability is tested by progressively increasing the number of nodes and the volume of traffic to determine how well the firewall adapts to larger, more complex networks. Additionally, the ease of integration with existing IoT and edge computing infrastructures is assessed to ensure that the hybrid mesh firewall can be deployed without requiring extensive modifications to current systems[12].

This methodology outlines the design, implementation, and evaluation of the hybrid mesh firewall, providing a comprehensive framework for securing IoT devices and edge computing environments through a decentralized, adaptive approach.

4. Results

Performance Evaluation: The performance evaluation of the hybrid mesh firewall demonstrated significant improvements in both security and efficiency across various test scenarios. Throughput measurements indicated that the hybrid mesh firewall maintained high data transfer rates even under heavy network loads, with minimal impact on overall performance[13]. Latency tests showed that the dynamic routing capabilities of the firewall effectively minimized delays, ensuring timely data delivery critical for real-time applications in IoT and edge computing environments. Packet loss was consistently low, highlighting the firewall's ability to efficiently manage and route traffic without introducing significant overhead.

Security Effectiveness: The hybrid mesh firewall proved highly effective in mitigating a wide range of cyber threats. During controlled attack simulations, including distributed denial-of-

service (DDoS) attacks and malware infiltration attempts, the firewall successfully detected and neutralized malicious activities with a high degree of accuracy. The integration of intrusion detection systems (IDS) and adaptive threat detection mechanisms enabled the firewall to identify both known and novel threats, demonstrating its robustness against evolving attack vectors. Unauthorized access attempts were thwarted through stringent access control policies enforced across the decentralized network, further enhancing the overall security posture. Scalability and Adaptability: Scalability tests revealed that the hybrid mesh firewall effectively scaled with the addition of new nodes and increased network traffic[14]. As the number of connected IoT devices and edge nodes grew, the firewall dynamically adjusted its routing protocols to maintain optimal performance and security. This adaptability was particularly evident in scenarios involving network disruptions or node failures, where the mesh network's self-healing properties ensured continuous protection and seamless traffic rerouting. The decentralized architecture allowed for distributed processing of security tasks, preventing bottlenecks and ensuring consistent security enforcement across the entire network. Integration and Usability: The integration of the hybrid mesh firewall with existing IoT and edge computing infrastructures was assessed to determine its practicality in real-world deployments. Results showed that the firewall could be seamlessly integrated without requiring extensive modifications to current systems. Configuration and management were facilitated through a user-friendly interface, allowing administrators to easily define and update security policies. The decentralized management model provided flexibility, enabling localized adjustments to security settings while maintaining overall coherence and coordination. Feedback from test deployments indicated a high level of satisfaction with the firewall's usability and effectiveness in enhancing network security[14].

In summary, the results of this study underscore the hybrid mesh firewall's potential as a comprehensive security solution for IoT devices and edge computing environments. Its ability to maintain high performance, effectively detect and mitigate threats, scale with network growth, and integrate seamlessly with existing infrastructures makes it a compelling choice for organizations looking to bolster their cybersecurity defenses in the face of evolving challenges.

5. Discussion

The deployment of hybrid mesh firewalls represents a significant advancement in the security of IoT devices and edge computing environments. The ability of the firewall to operate in a decentralized manner addresses the unique challenges posed by the distributed and dynamic nature of these systems[15]. By enabling each node to act as a security checkpoint, the hybrid mesh firewall ensures that security policies are enforced consistently throughout the network, reducing the risk of single points of failure commonly associated with traditional centralized security solutions. This approach not only enhances resilience against attacks but also allows for real-time threat detection and response, which is critical for protecting sensitive data and maintaining the integrity of IoT and edge computing infrastructures.

When compared to traditional security solutions, the hybrid mesh firewall offers several distinct advantages. Traditional perimeter-based firewalls, which rely on centralized control and static rule sets, are often inadequate for managing the complex, fluid nature of IoT and edge computing networks[16]. These conventional firewalls can become bottlenecks, impeding network performance and failing to adapt swiftly to emerging threats. In contrast, the hybrid mesh firewall's decentralized architecture allows it to dynamically route traffic and apply security measures, providing a more flexible and scalable approach to network security. Moreover, the use of adaptive threat detection mechanisms within the hybrid mesh firewall surpasses the capabilities of static, signature-based systems, enabling it to identify and mitigate previously unknown attack vectors effectively[17].

Despite its many advantages, the implementation of hybrid mesh firewalls does present certain challenges and limitations. One notable challenge is the potential complexity involved in managing a decentralized security infrastructure. Ensuring coherent policy enforcement across a distributed network requires sophisticated coordination mechanisms and robust communication protocols[18]. Additionally, the initial setup and configuration of the hybrid mesh firewall can be more resource-intensive compared to traditional firewalls, particularly in environments with a large number of heterogeneous IoT devices. Another limitation is the reliance on continuous updates and learning for the adaptive threat detection algorithms. These systems must be regularly updated with new threat intelligence to remain effective, which can impose additional maintenance burdens[19].

The promising results of hybrid mesh firewalls highlight several areas for future research. One avenue is the enhancement of machine learning algorithms used for adaptive threat detection to further improve their accuracy and efficiency. Research into more efficient protocols for decentralized management and coordination could also enhance the scalability and ease of deployment of hybrid mesh firewalls. Additionally, exploring the integration of hybrid mesh firewalls with other emerging technologies, such as blockchain for secure transactions or quantum cryptography for advanced encryption, could provide additional layers of security and resilience. Finally, field studies in diverse real-world environments could offer deeper insights into the practical challenges and performance of hybrid mesh firewalls, leading to further refinements and optimizations.

In conclusion, while the implementation of hybrid mesh firewalls presents some challenges, their ability to provide dynamic, decentralized security makes them a powerful tool for safeguarding IoT devices and edge computing environments. As these technologies continue to evolve and proliferate, the development and refinement of hybrid mesh firewalls will play a crucial role in addressing the complex security needs of modern networks[20].

6. Conclusions

The implementation of hybrid mesh firewalls offers a transformative approach to securing IoT devices and edge computing environments, addressing the limitations of traditional, centralized

security mechanisms. By integrating the robust traffic management and inspection capabilities of traditional firewalls with the dynamic, decentralized architecture of mesh networks, hybrid mesh firewalls provide a scalable and resilient security framework. This approach enhances the ability to detect and respond to evolving cyber threats in real-time, ensuring that security policies are consistently enforced across a distributed network. The hybrid mesh firewall's performance in terms of throughput, latency, and scalability, alongside its effective threat detection capabilities, underscores its potential as a comprehensive security solution. While challenges related to decentralized management and adaptive threat detection exist, ongoing research and development are likely to refine these systems further, enhancing their efficacy and ease of deployment. Ultimately, hybrid mesh firewalls represent a critical advancement in network security, offering a robust, adaptable solution to protect the complex and growing ecosystem of IoT devices and edge computing nodes.

References

[1] L. Ghafoor, I. Bashir, and T. Shehzadi, "Smart Data in Internet of Things Technologies: A brief Summary," 2023.

[2] A. H. Alavi, P. Jiao, W. G. Buttlar, and N. Lajnef, "Internet of Things-enabled smart cities: State-of-the-art and future trends," *Measurement*, vol. 129, pp. 589-606, 2018.

[3] I. Naseer, "Machine Learning Applications in Cyber Threat Intelligence: A Comprehensive Review," *The Asian Bulletin of Big Data Management*, vol. 3, no. 2, pp. 190-200, 2023.

[4] M. Bauer, L. Sanchez, and J. Song, "IoT-enabled smart cities: Evolution and outlook," *Sensors*, vol. 21, no. 13, p. 4511, 2021.

[5] D. C. Bogatinoska, R. Malekian, J. Trengoska, and W. A. Nyako, "Advanced sensing and internet of things in smart cities," in *2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 2016: IEEE, pp. 632-637.

[6] N. Cvar, J. Trilar, A. Kos, M. Volk, and E. Stojmenova Duh, "The use of IoT technology in smart cities and smart villages: Similarities, differences, and future prospects," *Sensors*, vol. 20, no. 14, p. 3897, 2020.

[7] N. Dlodlo, O. Gcaba, and A. Smith, "Internet of things technologies in smart cities," in *2016 IST-Africa Week Conference*, 2016: IEEE, pp. 1-7.

[8] I. Naseer, "The efficacy of Deep Learning and Artificial Intelligence Framework in Enhancing Cybersecurity, Challenges and Future Prospects," *Innovative Computer Sciences Journal*, vol. 7, no. 1, 2021.

[9] R. Krishnamurthi, A. Nayyar, and A. Solanki, "Innovation opportunities through Internet of Things (IoT) for smart cities," in *Green and Smart Technologies for Smart Cities*: CRC Press, 2019, pp. 261-292.

[10] R. Kumar, H. K. Banga, and H. Kaur, "Internet of Things-supported smart city platform," in *IOP Conference Series: Materials Science and Engineering*, 2020, vol. 955, no. 1: IOP Publishing, p. 012003.

[11] S. Kumar, P. Tiwari, and M. Zymbler, "Internet of Things is a revolutionary approach for future technology enhancement: a review," *Journal of Big data*, vol. 6, no. 1, pp. 1-21, 2019.

[12] I. Naseer, "Cyber Defense for Data Protection and Enhancing Cyber Security Networks for Military and Government Organizations," *MZ Computing Journal,* vol. 1, no. 1, 2020.

[13] F. Tahir and L. Ghafoor, "Structural Engineering as a Modern Tool of Design and Construction," EasyChair, 2516-2314, 2023.

[14] D. Lupton, "The internet of things: social dimensions," *Sociology Compass,* vol. 14, no. 4, p. e12770, 2020.

[15] D. Minoli and B. Occhiogrosso, "Internet of things applications for smart cities," *Internet of things A to Z: technologies and applications,* pp. 319-358, 2018.

[16] S. P. Mohanty, U. Choppali, and E. Kougianos, "Everything you wanted to know about smart cities: The Internet of things is the backbone," *IEEE consumer electronics magazine,* vol. 5, no. 3, pp. 60-70, 2016.

[17] I. Naseer, "AWS Cloud Computing Solutions: Optimizing Implementation for Businesses," *Statistics, Computing and Interdisciplinary Research,* vol. 5, no. 2, pp. 121-132, 2023.

[18] M. Olowu, C. Yinka-Banjo, S. Misra, J. Oluranti, and R. Ahuja, "Internet of things: demystifying smart cities and communities," in *Advances in Computational Intelligence and Informatics: Proceedings of ICACII 2019,* 2020: Springer, pp. 363-371.

[19] A. Shahid, B. Khalid, S. Shaukat, H. Ali, and M. Y. Qadri, "Internet of Things shaping smart cities: a survey," *Internet of Things and Big Data Analytics Toward Next-Generation Intelligence,* pp. 335-358, 2018.

[20] I. Naseer, "Implementation of Hybrid Mesh firewall and its future impacts on Enhancement of cyber security," *MZ Computing Journal,* vol. 1, no. 2, 2020.