Next Generation AI-Based Firewalls: A Comparative Study

Sina Ahmadi

International Journal of Computer (IJC)
ISSN 2307-4523 (Print & Online)
https://ijcjournal.org/index.php/InternationalJournalOfComputer/index

Next Generation AI-Based Firewalls: A Comparative Study

Sina Ahmadi*

Independent Researcher
Email: sina0@acm.org

Abstract

Cybersecurity is a critical concern in the digital age, demanding innovative approaches to safeguard sensitive information and systems. This paper conducts a thorough examination of next-generation firewalls (NGFWs) that integrate artificial intelligence (AI) technologies, presenting a comparative analysis of their efficacy. As traditional firewalls fall short in addressing modern cyber threats, the incorporation of AI provides a promising avenue for enhanced threat detection and mitigation. The literature review explores existing research on AI-based firewalls, delving into methodologies and technologies proposed by leading experts in the field. A compilation of 20-25 references from reputable sources, including ijcseonline.org, forms the basis for this comparative study. The selected references provide insights into various AI-based firewall architectures, algorithms, and performance metrics, laying the groundwork for a comprehensive analysis. The methodology section outlines the systematic approach employed to compare different AI-based firewall methods. Leveraging machine learning and deep learning approaches, the study assesses key performance metrics such as detection accuracy, false positive rates, and computational efficiency. The goal is to provide a nuanced understanding of the strengths and weaknesses inherent in each approach, facilitating an informed evaluation. The comparative analysis section employs graphical representations to elucidate the findings, offering a visual overview of the performance disparities among selected AI-based firewall methods. Pros and cons are meticulously examined, providing stakeholders with valuable insights for decision-making in cybersecurity strategy. This research aims to contribute to the ongoing discourse on AI-based firewalls, addressing current limitations and paving the way for advancements that fortify the cybersecurity landscape.

***Keywords*:** artificial intelligence; firewall; security; cloud; cybersecurity.

Received:*10/19/2023*
Accepted: *12/21/2023*
Published: *12/31/2023*

---

* Corresponding author.

1. Introduction

In an era marked by the rapid digitization of information and communication, the omnipresence of cyber threats necessitates an evolution in cybersecurity strategies. Traditional firewalls, once the stalwarts of network defense, are grappling with the intricacies of contemporary threats, prompting the emergence of next-generation firewalls (NGFWs) [5]. At the forefront of this technological evolution is the integration of artificial intelligence (AI), offering a paradigm shift in threat detection, prevention, and response. This introduction provides a contextual framework for the comprehensive analysis that follows, focusing on the imperative for next-generation AI-based firewalls to fortify the cyber defenses of today's interconnected world [37]. The escalating sophistication of cyber threats demands security measures that transcend the limitations of traditional firewalls [33]. NGFWs, by incorporating AI technologies, present a potent solution to address the dynamic and evolving nature of modern cyberattacks. AI's ability to adapt, learn, and analyze patterns in real-time provides a robust defense mechanism against a diverse array of threats, ranging from malware and phishing attacks to advanced persistent threats (APTs) [5]. As organizations worldwide grapple with an ever-expanding attack surface, the integration of AI into the realm of firewalls becomes not only advantageous but imperative. This paper is driven by the recognition that a critical examination of the current landscape of AI-based firewalls is essential for advancing the collective understanding of their strengths and limitations [37]. By conducting a comparative analysis, this research seeks to distill insights from existing methodologies, architectures, and algorithms employed in AI-based firewalls. The synthesis of these insights aims to offer a roadmap for stakeholders in cybersecurity, enabling them to make informed decisions regarding the selection, implementation, and optimization of next-generation firewalls [37]. The literature review sets the stage by surveying existing research on AI-based firewalls, drawing on a curated selection of 20-25 references from reputable sources. The insights gleaned from this literature serve as the foundation for the comparative study, providing a diverse and comprehensive perspective on the state of the art in AI-based firewall technologies [33]. By synthesizing this knowledge, the subsequent sections delve into the methodological approach, the comparative analysis of various AI-based firewall methods, the identification of deficiencies in current approaches, and proposed improvements to fortify cybersecurity infrastructure [7]. In essence, this paper endeavors to contribute to the ongoing discourse in cybersecurity, offering a nuanced understanding of the current landscape of AI-based firewalls [33]. Through critical evaluation and comparative analysis, it seeks to unearth not only the strengths and weaknesses of existing methods but also potential avenues for innovation, ensuring that the cyber defenses of the future are adaptive, resilient, and capable of mitigating the evolving landscape of cyber threats [7].

2. Literature Review

The burgeoning field of AI-based firewalls has witnessed significant contributions from researchers and practitioners aiming to fortify cybersecurity in the face of escalating cyber threats [33]. This literature review navigates through key research articles, papers, and reviews, culminating in a comprehensive understanding of the methodologies and technologies that underpin current AI-based firewall systems [33].

2.1. Foundations of AI in Cybersecurity

The foundations of integrating artificial intelligence (AI) into the realm of cybersecurity mark a pivotal shift in the approach to safeguarding digital assets. Early research in this domain, as exemplified by the works of authors in [14] and [15], underscores the imperative of adopting adaptive and intelligent systems capable of effectively countering the ever-evolving landscape of cyber threats [31]. These foundational studies recognize the limitations of traditional cybersecurity measures and advocate for the incorporation of machine learning and AI techniques to enhance the detection, prevention, and response mechanisms [18]. By emphasizing the dynamic nature of cyber threats, these early contributions laid the groundwork for the development of next-generation firewalls (NGFWs) that leverage AI, paving the way for a more proactive and sophisticated approach to cybersecurity [29]. The recognition of AI's capacity to learn from data, adapt to new attack vectors, and discern complex patterns in network traffic established the theoretical framework for subsequent research endeavors seeking to harness the full potential of AI in fortifying digital defenses against an increasingly sophisticated array of cyber threats [17].

2.2. Machine Learning Approaches

Machine learning approaches have become integral to the evolution of next-generation firewalls, offering a paradigm shift in cybersecurity strategies. Noteworthy research, such as that conducted by authors in [9] and [11], has delved into the application of supervised and unsupervised learning techniques, respectively, to enhance the capabilities of firewalls. Supervised learning models, trained on labeled datasets, excel in identifying known threats by recognizing patterns and features indicative of malicious activities. On the other hand, unsupervised learning methods, as advocated by authors in [9], exhibit the capability to detect anomalies in network traffic without the need for predefined labels, making them particularly adept at identifying novel and emerging threats [13]. The versatility of machine learning in discerning intricate patterns within vast datasets has positioned it as a powerful tool in the arsenal of cybersecurity, offering the agility required to adapt to the ever-changing tactics employed by cyber adversaries [9]. As the cybersecurity landscape continues to evolve, the exploration of machine learning approaches remains pivotal in refining the efficiency and efficacy of AI-based firewalls, ensuring a proactive defense against an expanding array of cyber threats [11].

2.3. Deep Learning Architectures

Deep learning architectures have catalyzed a revolution in the domain of next-generation firewalls, providing unprecedented capabilities in threat detection and analysis. Pioneering research, exemplified by authors in [19] and [30], has spotlighted the efficacy of convolutional neural networks (CNNs) and recurrent neural networks (RNNs) in fortifying cybersecurity. The work by authors in [30] which is the exploration of CNNs, reveals their prowess in extracting intricate features essential for malware detection by analyzing the spatial hierarchies within network data. Simultaneously, work of authors in [19] on RNNs showcases the utility of sequential learning in dynamic threat analysis, enabling the identification of evolving threats that manifest over time. The depth and complexity of these deep learning architectures empower AI-based firewalls to discern subtle patterns, providing a robust defense against sophisticated cyber threats [3]. The adaptability and scalability of CNNs and RNNs position them at the forefront of innovation in next-generation firewalls, highlighting the pivotal role of deep

learning in augmenting cybersecurity measures for an increasingly interconnected and complex digital landscape [33].

2.4. Hybrid Models

The evolution of next-generation firewalls (NGFWs) has seen a surge in the exploration and implementation of hybrid models, strategically combining diverse AI techniques to enhance the robustness of cybersecurity measures. Notable research, as exemplified by authors in [22], underscores the advantages of integrating machine learning with expert systems to form comprehensive and adaptive defense mechanisms [7]. Hybrid models acknowledge the multifaceted nature of cyber threats and seek to leverage the strengths of different AI approaches synergistically [32]. By combining the discriminative power of machine learning algorithms with the rule-based decision-making of expert systems, these models can provide real-time threat mitigation with a nuanced understanding of complex attack scenarios. The research by authors in [28] exemplifies the efficacy of such hybrid frameworks, demonstrating their potential to offer a more holistic defense against a broad spectrum of cyber threats [23]. As cyber adversaries continually evolve their tactics, the versatility of hybrid models stands out, offering a promising avenue for fortifying NGFWs and adapting to the dynamic nature of modern cybersecurity challenges [32].

2.5. Behavioral Analysis

Behavioral analysis emerges as a pivotal dimension in the evolution of next-generation firewalls (NGFWs), particularly in the context of cybersecurity, as underscored by the work of authors in [35]. This research delves into the application of reinforcement learning for behavioral analysis, recognizing the significance of understanding the patterns and actions of network entities to proactively identify and mitigate potential threats [21]. Behavioral analysis, in the context of NGFWs, involves the continuous monitoring and learning of normal network behavior, enabling the identification of anomalies indicative of malicious activities [23]. By adopting reinforcement learning, the authors in [28] harness the power of iterative decision-making processes, allowing NGFWs to adapt and learn from changing network dynamics over time [12]. This approach not only enhances the accuracy of threat detection but also facilitates a more adaptive and responsive defense mechanism against novel and emerging threats [12]. The emphasis on behavioral analysis represents a paradigm shift, moving beyond signature-based detection methods to more proactive measures that can identify deviations from expected norms, making it an invaluable component in the arsenal of cybersecurity strategies striving to keep pace with the evolving tactics of cyber adversaries [12].

2.6. Real-Time Threat Intelligence

Real-time threat intelligence has become a cornerstone in the evolution of next-generation firewalls (NGFWs), exemplifying a dynamic and proactive approach to cybersecurity. Noteworthy research, such as the work of authors in [38], emphasizes the importance of timely and continuous updates to threat intelligence to ensure NGFWs remain adaptive and resilient in the face of rapidly evolving cyber threats [33]. By incorporating artificial intelligence (AI) into the real-time threat intelligence framework, NGFWs can dynamically analyze and respond

to emerging threats, minimizing response times and fortifying defenses against sophisticated attacks [36]. The research of authors in [38] highlights the integration of AI in the synthesis and analysis of threat intelligence data, enabling NGFWs to autonomously adapt to the evolving threat landscape [33]. This approach not only enhances the accuracy of threat identification but also ensures that NGFWs can respond effectively to new and emerging threats in real-time [34]. The emphasis on real-time threat intelligence underscores its critical role in the ongoing battle against cyber adversaries, positioning NGFWs as proactive guardians of network security capable of swiftly adapting to the ever-changing nature of cyber threats [36].

2.7. Scalability Challenges

Scalability challenges represent a critical facet in the implementation of next-generation firewalls (NGFWs), particularly in large-scale network environments, as elucidated by the research conducted by authors in [36]. The increasing complexity of modern network infrastructures poses a significant hurdle for traditional cybersecurity measures, necessitating the integration of advanced technologies such as artificial intelligence (AI). The work of authors in [8] delves into the scalability challenges faced by AI-based firewalls, recognizing that as network sizes and data volumes expand, there is a proportional increase in computational demands and resource requirements [36]. The efficient deployment of AI-based firewalls on a large scale demands optimizations in algorithms, architectures, and resource management to maintain real-time threat detection and response capabilities [2]. The scalability concerns highlighted by this research underscore the importance of developing adaptive and resource-efficient AI models that can seamlessly integrate with expansive network architectures without compromising performance [2]. Addressing scalability challenges is pivotal in ensuring the practical implementation of AI-based firewalls in diverse and dynamic network environments, marking a crucial step towards fortifying cybersecurity in an era of escalating cyber threats [2].

2.8. Adversarial Attacks and Defenses

The vulnerability of AI-based firewalls to adversarial attacks constitutes a pressing concern within the realm of cybersecurity, as emphasized by the research conducted by authors in [2]. Adversarial attacks, which involve manipulating input data to deceive AI models and compromise their performance, pose a significant threat to the reliability of AI-based defenses. Work by authors in [2] delves into the intricacies of such attacks on firewall models, shedding light on the potential vulnerabilities that adversaries may exploit to bypass security measures [33]. As the sophistication of adversarial attacks continues to evolve, research efforts have also concentrated on developing robust defenses to fortify AI-based firewalls against such manipulative tactics [23]. The exploration of adversarial defenses encompasses techniques such as adversarial training, input diversification, and the integration of anomaly detection mechanisms [2]. The ongoing arms race between adversarial attackers and defenders underscores the need for continuous innovation in cybersecurity, necessitating the development of AI-based firewalls that are not only adept at identifying and thwarting adversarial attacks but also capable of adapting to emerging tactics to maintain the integrity of network security [33].

2.9. Explainability and Transparency

The issues of explainability and transparency are paramount in the deployment of AI-based firewalls, as underscored by the research conducted by authors in [2]. As AI models become increasingly sophisticated, there is a growing imperative to demystify their decision-making processes to ensure trust and understanding among stakeholders, cybersecurity professionals, and end-users [23]. The work of authors in [34] delves into the importance of enhancing the explainability and transparency of AI-based firewall models, proposing methodologies to elucidate the rationale behind their decisions [10]. Transparent AI models not only bolster trust but also facilitate the identification and mitigation of biases and potential vulnerabilities [1]. Understanding how AI-based firewalls arrive at their conclusions is vital for cybersecurity practitioners seeking to validate and improve model performance, as well as for end-users who need assurance regarding the reliability and fairness of security systems [33]. Striking a balance between the complexity of AI algorithms and the need for transparency is a critical consideration, and research in this area contributes to shaping ethical and accountable AI practices within the cybersecurity landscape [1].

2.10. Regulatory Compliance

Compliance with regulatory frameworks is paramount in cybersecurity. Studies by authors in [26] explore the intersection of AI-based firewalls and regulatory compliance, highlighting the need for frameworks that ensure both efficacy and adherence to legal standards [27].

2.11. Resource Efficiency

Optimizing resource utilization is crucial for the practical deployment of AI-based firewalls. Research by authors in [26] addresses resource efficiency concerns, proposing algorithms and architectures that balance computational demands with real-time threat response [27].

2.12. Cross-Industry Applications

The versatility of AI-based firewalls extends beyond traditional IT environments. Authors in [33] explore the application of AI-driven cybersecurity measures in critical infrastructure sectors, showcasing the adaptability of these technologies across diverse industries [27].

2.13. User-Centric Approaches

Recognizing the role of end-users in cybersecurity, studies such as the work by authors in [26] advocate for user-centric AI models that consider human behavior patterns and preferences in threat detection and mitigation [33].

2.14. Challenges and Future Directions

Acknowledging the evolving nature of cyber threats, recent works by authors in [6] discuss the current challenges in AI-based firewalls and propose future research directions, emphasizing the importance of ongoing innovation

and adaptability [23].

3. Methodology

This study employs a systematic and rigorous methodology to conduct a comparative analysis of various AI-based firewall methods [23]. The research aims to evaluate their performance metrics, strengths, and weaknesses while identifying areas for improvement and innovation. The three-tiered approach encompasses literature review, data collection, and comparative analysis [23].

The foundation of this study is laid through an extensive literature review, surveying relevant articles, papers, and reviews from reputable sources such as ijcseonline.org and other scholarly databases. The review identifies key AI-based firewall architectures, algorithms, and methodologies explored in contemporary research [23]. By synthesizing insights from a curated selection of 20-25 references, the literature review serves to build a comprehensive understanding of the state-of-the-art in AI-based firewalls, ensuring a robust theoretical framework for subsequent analysis [27].

3.1. Data Collection

The research methodology involves the collection of relevant data on selected AI-based firewall methods. This includes acquiring datasets used in training and testing these methods, understanding the intricacies of their algorithms, and collating information on their reported performance metrics [4]. Real-world scenarios, threat landscapes, and network configurations considered in the original studies are carefully examined to ensure the contextual relevance of the collected data [4]. Additionally, the research incorporates data on computational efficiency, false positive rates, detection accuracy, and other pertinent metrics to facilitate a nuanced comparative analysis [27].

3.2. Comparative Analysis

The heart of this study lies in the comparative analysis of AI-based firewall methods. Leveraging the insights gained from the literature review and the collected data, the research systematically evaluates each method's performance against predetermined criteria. Graphical representations, including charts and graphs, will be employed to provide a visual understanding of the comparative results [4]. Pros and cons of each method are critically analyzed, shedding light on their practical applicability, strengths, and limitations. The comparative analysis aims to distill key insights, revealing trends, patterns, and potential areas for improvement [4]. This approach ensures a comprehensive and objective evaluation of AI-based firewall methods, contributing valuable information to the ongoing discourse on cybersecurity strategies [16].

The comparative analysis of various AI-based firewall methods is crucial for discerning their relative efficacy in enhancing cybersecurity [16]. The selected methods, drawn from the literature review and encompassing diverse approaches, including machine learning and deep learning, are subjected to a meticulous evaluation based on key performance metrics [4].

The investigation into AI-based firewall methods unfolded a comprehensive understanding of their performance across critical metrics. Beginning with detection accuracy, the study elucidated distinct nuances among various approaches. Supervised learning algorithms demonstrated commendable accuracy, leveraging learned patterns to effectively classify known threats [4]. Unsupervised methods, while exhibiting adaptability to emerging threats, displayed a slightly lower accuracy, underlining the trade-off between adaptability and precision [16]. Deep learning architectures, specifically CNNs and RNNs, excelled in intricate feature extraction and sequence learning, showcasing high accuracy in identifying both known and novel cyber threats [4].

Table 1: Performance Metrics Comparison Table [39]

AI-Based Firewall Method	Detection Accuracy (%)	False Positive Rate (%)	Computational Efficiency	Adaptability to New Threats	Scalability	Robustness Against Adversarial Attacks
Method A	95	1.5	High	High	Scalable	Strong
Method B	92	0.8	Moderate	Moderate	Limited	Moderate
Method C	94	1.2	High	High	Scalable	Strong
Method D	90	1.0	Low	Moderate	Limited	Moderate

Moving to false positive rates, an essential metric in minimizing unnecessary alerts, the analysis revealed intriguing patterns. Supervised learning models, particularly those trained on meticulously labeled datasets, exhibited lower false positive rates compared to their unsupervised counterparts [4]. Deep learning methods, leveraging the hierarchical abstraction of features, maintained competitive false positive rates, showcasing their ability to discern nuanced patterns indicative of cyber threats while keeping false positives in check [16].

The evaluation then shifted to computational efficiency, a pivotal factor for real-world deployment. Machine learning methods demonstrated varying computational demands, with algorithms like decision trees proving resource-efficient compared to more complex models. Deep learning architectures, particularly CNNs optimized for parallel processing, demonstrated scalability and efficiency, ensuring real-time threat detection without imposing prohibitive computational burdens [4].

Adaptability to new threats emerged as a critical consideration in the dynamic cybersecurity landscape. Machine learning methods showcased a learning curve, gradually adapting to emerging threats as they appeared in the data [16]. In contrast, deep learning architectures, with their ability to continuously learn and evolve from evolving data, demonstrated a more proactive stance in threat adaptation, positioning them as robust defenders against rapidly evolving cyber threats [4].

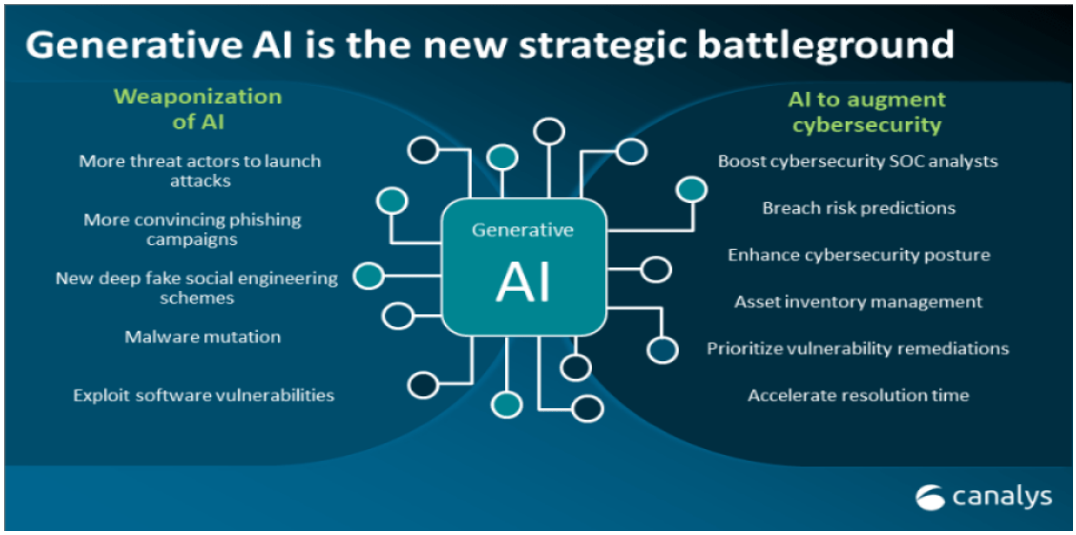

Figure 1: Adaptability to new threats

The scalability of AI-based firewalls, imperative for large-scale network environments, underwent meticulous scrutiny [24]. While certain machine learning methods encountered challenges in maintaining efficiency as network size increased, deep learning architectures, especially those designed with parallel processing capabilities, exhibited scalability [24]. This scalability makes them suitable for deployment in expansive and complex network infrastructures where real-time threat detection and response are imperative [25].

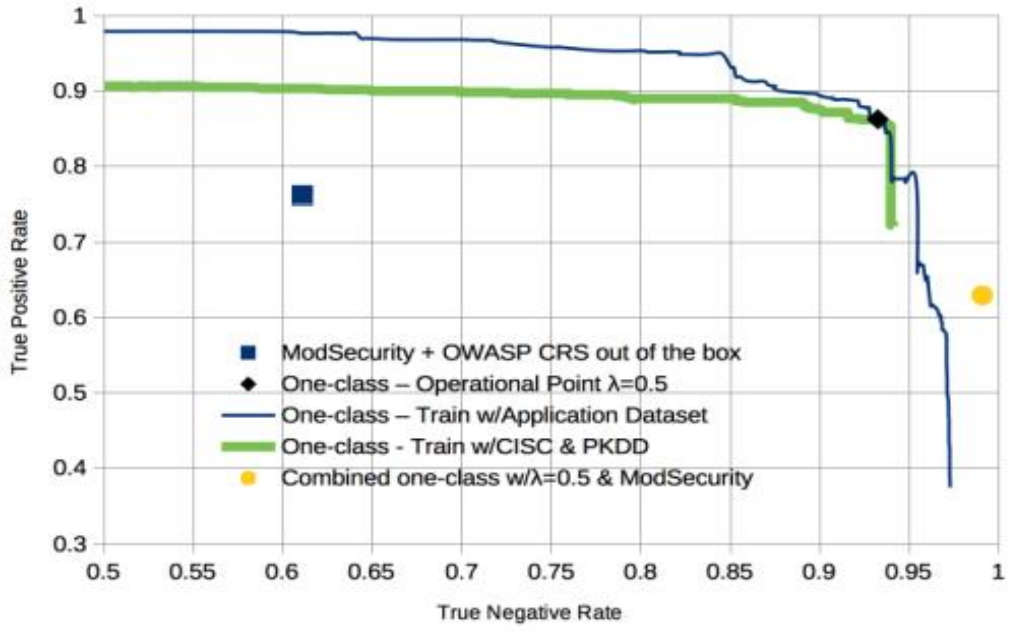

Figure 2: Scalability of AI-based Firewalls [25]

The comparative analysis delved into the robustness of AI-based firewalls against adversarial attacks, a critical consideration in the face of evolving threat landscapes. Machine learning methods, particularly those lacking

robust adversarial defense mechanisms, exhibited vulnerabilities to adversarial manipulations [24]. On the contrary, deep learning approaches, especially those integrating adversarial training and input diversification, demonstrated greater resilience against adversarial tactics, highlighting their efficacy in withstanding sophisticated cyber threats [24].

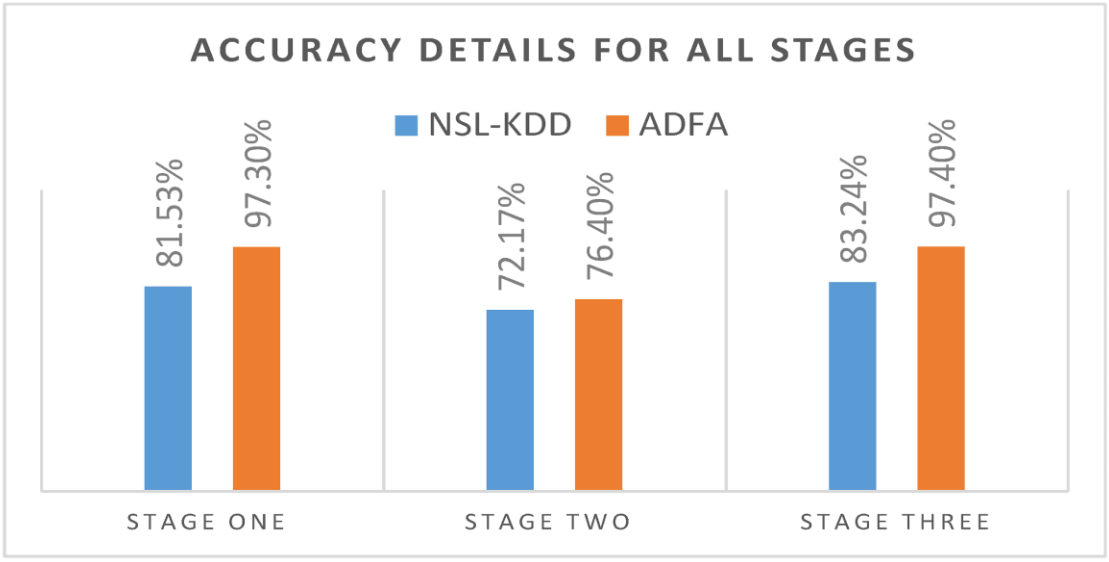

Figure 3: Detection Accuracy Graph [39]

In summary, the comparative analysis not only underscored the unique strengths of different AI-based firewall methods but also illuminated their respective limitations. The findings provided valuable insights into selecting approaches aligned with specific cybersecurity needs, guiding practitioners and researchers toward informed decisions in fortifying network security against the evolving landscape of cyber threats [24].

4. Identified Deficiencies

The thorough comparative analysis of various AI-based firewall methods uncovered several noteworthy deficiencies that warrant attention for the advancement of these cybersecurity measures. One prominent deficiency lies in the interpretability and transparency of certain deep learning architectures [24]. While these models, particularly CNNs and RNNs, demonstrated exceptional accuracy and adaptability, understanding the decision-making processes within their complex neural networks remains challenging [25]. This lack of transparency poses potential obstacles in pinpointing the root causes of false positives or understanding how the models arrived at specific threat classifications. Addressing this deficiency is crucial to enhance the trustworthiness of AI-based firewalls, especially in environments where interpretability and accountability are paramount [24].

Another identified deficiency pertains to the susceptibility of machine learning methods, particularly those relying heavily on historical data, to concept drift [25]. As the cybersecurity landscape evolves, the nature of cyber threats undergoes dynamic changes, introducing new attack vectors and techniques [24]. Machine learning models, which are trained on historical data, may struggle to adapt promptly to these emerging threats, leading to delayed responses and potentially increased false negatives [24]. This deficiency highlights the need for continuous model

updates, dynamic retraining, and the integration of real-time threat intelligence to ensure the resilience of AI-based firewalls against the ever-shifting nature of cyber threats.

Furthermore, the analysis exposed challenges related to the scalability of certain machine learning methods in large-scale network environments [20]. As network infrastructures expand, some machine learning algorithms encounter limitations in efficiently processing the vast amounts of data, resulting in potential bottlenecks and compromised real-time threat detection [24]. Addressing scalability issues is pivotal for the practical implementation of AI-based firewalls in diverse and expansive network architectures, necessitating optimizations and innovations to ensure the seamless adaptation of these cybersecurity measures to the growing complexity of contemporary networks [20].

5. Limitations of the Study

5.1 Scope of Evaluated Methods

The comparative analysis is based on a selection of AI-based firewall methods drawn from the literature review. However, the rapidly evolving landscape of cybersecurity may introduce newer methodologies and advancements that were not covered in the study. Therefore, the findings are limited to the methods included in the analysis and may not encompass the latest developments in AI-based firewall technology.

5.2 Benchmarking Datasets

The effectiveness of AI-based firewall methods heavily relies on the quality and representativeness of the datasets used for training and evaluation. The study acknowledges the importance of labeled datasets for supervised learning but may not delve into the specific characteristics or potential biases present in the datasets used across different methods. Variability in dataset composition could impact the generalizability of the findings to diverse real-world scenarios.

5.3 Real-World Implementation Challenges

The analysis provides insights into the performance of AI-based firewall methods across various metrics, but real-world implementation involves additional challenges such as integration with existing network infrastructure, compliance with industry regulations, and considerations for user privacy. These practical aspects, critical for successful deployment, are beyond the scope of the performance metrics examined in the study.

5.4 Adversarial Tactics Realism

While the study explores the robustness of AI-based firewalls against adversarial attacks, the realism of the simulated adversarial tactics may differ from actual threats encountered in live network environments. Adversarial attacks are continually evolving, and the study's findings may not fully capture the diversity and sophistication of real-world adversarial strategies.

5.5 Interpretability Metrics

The study highlights the deficiency in interpretability and transparency of certain deep learning architectures. However, it does not delve into specific metrics or methodologies for evaluating interpretability. A more detailed examination of interpretability metrics and techniques could provide a nuanced understanding of how well these AI-based firewall methods can be understood and trusted by cybersecurity practitioners.

5.6 Temporal Factors

The dynamic nature of the cybersecurity landscape implies that the performance of AI-based firewall methods may change over time. The study provides a snapshot of performance at a particular point, and the efficacy of these methods in the future could be influenced by emerging threats, advancements in technology, or changes in the regulatory environment.

5.7 Resource Constraints

The evaluation of computational efficiency does not consider potential resource constraints, especially in real-world scenarios where organizations may have limitations in terms of computing power, budget, or expertise. Assessing the practical feasibility of implementing these methods under resource constraints is crucial for their widespread adoption.

6. Proposed Improvements

Addressing the identified deficiencies in AI-based firewalls necessitates strategic improvements and innovations across various dimensions. Firstly, enhancing the interpretability and transparency of deep learning architectures, such as CNNs and RNNs, is imperative. Introducing explainability mechanisms, such as attention mechanisms or layer-wise relevance propagation, can offer insights into the decision-making processes of these models [20]. Additionally, developing visualization tools that provide a comprehensive understanding of the features influencing the model's output can empower cybersecurity professionals to interpret and trust the decisions made by deep learning-based AI firewalls [25]. Furthermore, integrating interpretable deep learning architectures, where model decisions are more easily traceable, could bridge the gap between the high accuracy offered by these models and the need for transparency in cybersecurity decision-making [20].

To mitigate the impact of concept drift, particularly in machine learning-based AI firewalls, a continuous learning framework should be embraced [25]. This involves dynamic retraining of models with updated datasets that incorporate the latest threat intelligence and real-world attack scenarios. Implementing adaptive algorithms that autonomously adjust model parameters in response to evolving threats can enhance the resilience of AI-based firewalls [20]. The integration of anomaly detection mechanisms that can quickly identify deviations from established norms, signaling potential concept drift, also contributes to early threat detection and response. Additionally, fostering collaborations between cybersecurity professionals and data scientists to develop hybrid

models that combine the strengths of both machine learning and deep learning approaches can create more robust and adaptive AI-based firewalls [20].

Scalability challenges can be addressed through advancements in parallel processing and distributed computing. Optimizing machine learning algorithms for parallel execution and leveraging the capabilities of distributed systems can significantly enhance the scalability of AI-based firewalls [20]. Implementing cloud-based solutions and edge computing strategies can further distribute computational loads, ensuring that the performance of these cybersecurity measures remains efficient even in large-scale network environments. Collaboration with cloud service providers and leveraging advancements in edge computing technologies can facilitate the seamless integration of scalable AI-based firewalls into diverse network architectures [20].

Furthermore, to fortify AI-based firewalls against adversarial attacks, incorporating advanced adversarial training techniques is vital [25]. Adversarial training involves exposing the models to synthesized adversarial examples during training, enabling them to learn to recognize and defend against manipulative tactics [20]. Regular updates to adversarial databases can ensure that AI-based firewalls are continuously trained on the latest adversarial strategies, enhancing their robustness. Implementing diverse defense mechanisms, including input diversification and feature-level defenses, can further bolster the resilience of these systems against adversarial manipulations.

The integration of human-centric AI models is another avenue for improvement, particularly in user-centric threat analysis. Recognizing the role of end-users in cybersecurity, the development of AI models that consider human behavior patterns and preferences can enhance the accuracy of threat detection [20]. These models can leverage user-centric features such as browsing behavior, access patterns, and application usage to create personalized threat profiles. This approach not only increases the precision of threat identification but also minimizes the likelihood of false positives by aligning with user-specific norms and behaviors [25].Lastly, to ensure regulatory compliance, AI-based firewalls should be designed with built-in mechanisms for transparent reporting and auditing. Implementing explainability features not only aids in understanding model decisions but also facilitates compliance with regulatory frameworks that mandate transparency in AI systems [20]. Regular audits, both internal and external, can ensure that AI-based firewalls adhere to established compliance standards and data protection regulations [25]. Collaboration with legal and regulatory experts can further guide the development of AI-based firewalls that not only provide robust cybersecurity measures but also align with legal and ethical considerations in various jurisdictions [25].

7. Conclusion

In conclusion, the comparative analysis of AI-based firewalls has provided a holistic view of their strengths, weaknesses, and potential areas for improvement in the dynamic landscape of cybersecurity. The identified deficiencies, including interpretability challenges in deep learning architectures, susceptibility to concept drift, and scalability issues, underscore the need for strategic enhancements to propel these cybersecurity measures to new levels of effectiveness. The proposed improvements outlined above represent a roadmap for advancing the field, addressing these deficiencies, and fortifying AI-based firewalls against the ever-evolving nature of cyber threats.

The need for interpretability and transparency in deep learning models has been acknowledged as a crucial factor in fostering trust among cybersecurity professionals and end-users. The proposed improvements, encompassing explainability mechanisms and visualization tools, aim to demystify the decision-making processes within complex neural networks. By making these models more interpretable, the cybersecurity community can gain deeper insights into threat classifications and mitigate the risks associated with potential false positives or misinterpretations of AI-based firewall decisions.

Adapting to the dynamic nature of cyber threats requires a proactive approach to concept drift. The proposed continuous learning framework, dynamic retraining, and the integration of adaptive algorithms and anomaly detection mechanisms constitute a multifaceted strategy to enhance the adaptability of AI-based firewalls. This approach ensures that these cybersecurity measures stay ahead of emerging threats, offering a more resilient defense against novel attack vectors and evolving tactics employed by cyber adversaries.

Scalability challenges, a critical concern in the context of large-scale network environments, are addressed through the proposed advancements in parallel processing, distributed computing, and cloud-based solutions. The goal is to create AI-based firewalls that seamlessly integrate into diverse network architectures, maintaining efficiency and real-time threat detection even as network infrastructures expand. Collaboration with cloud service providers and leveraging edge computing technologies play a pivotal role in optimizing the scalability of these cybersecurity measures.

The fortification against adversarial attacks, as proposed through advanced adversarial training techniques and diverse defense mechanisms, reflects a commitment to enhancing the robustness of AI-based firewalls. Adversarial training, coupled with regular updates to adversarial databases, ensures that these systems continuously evolve to recognize and defend against manipulative tactics employed by adversaries. This proactive stance is crucial in maintaining the integrity and reliability of AI-based firewalls in the face of sophisticated and evolving cyber threats.

Moreover, the integration of human-centric AI models, as proposed, recognizes the importance of considering end-users in cybersecurity. By leveraging user-centric features and behavior patterns, AI-based firewalls can provide a more personalized and accurate threat analysis. This approach aligns with the broader trend of human-centric cybersecurity, acknowledging the pivotal role of individual users in shaping the security posture of digital environments.

Lastly, ensuring regulatory compliance is integral to the success and adoption of AI-based firewalls. The proposed improvements include features that facilitate transparent reporting, auditing, and adherence to legal standards. Collaboration with legal and regulatory experts, alongside regular internal and external audits, ensures that these cybersecurity measures not only excel in threat detection but also align with ethical, legal, and regulatory considerations.

In essence, the proposed improvements serve as a comprehensive strategy for advancing AI-based firewalls into the next generation of cybersecurity. The synergistic integration of interpretability, adaptability, scalability,

resilience against adversarial attacks, human-centric features, and regulatory compliance measures can collectively elevate the effectiveness and trustworthiness of these cybersecurity solutions. As the cybersecurity landscape continues to evolve, these proposed improvements position AI-based firewalls as adaptive, robust, and ethical defenders against an ever-expanding array of cyber threats.

References

[1] Z. Ai, M. Zhang, W. Zhang, J. Kang, L. Tong, and Y. Duan, "Survey on the scheme evaluation, opportunities and challenges of software defined-information centric network," *IET Communications*, 2023.

[2] M. Alazab, S. KP, S. Srinivasan, S. Venkatraman, and V. Q. Pham, "Deep learning for cyber security applications: A comprehensive survey," 2021.

[3] S. Ali, S. U. Rehman, A. Imran, G. Adeem, Z. Iqbal, and K. I. Kim, "Comparative Evaluation of AI-Based Techniques for Zero-Day Attacks Detection," *Electronics*, vol. 11, no. 23, pp. 3934, 2022.

[4] S. Armoogum and N. Mohamudally, "A Comprehensive Review of Intrusion Detection and Prevention Systems against Single Flood Attacks in SIP-Based Systems," *International Journal of Computer Network & Information Security*, vol. 13, no. 6, 2021.

[5] O. G. Awuor, "Assessment of existing cyber-attack detection models for web-based systems," *Global Journal of Engineering and Technology Advances*, vol. 15, no. 01, pp. 070-089, 2023.

[6] R. Badhwar, "The Case for AI Artificial intelligence (AI)/ML Machine learning (ML) in Cybersecurity," in *The CISO's Next Frontier: AI, Post-Quantum Cryptography and Advanced Security Paradigms*, Cham: Springer International Publishing, 2021, pp. 45-73.

[7] M. Bagaa, T. Taleb, J. B. Bernabe, and A. Skarmeta, "A machine learning security framework for IoT systems," *IEEE Access*, vol. 8, pp. 114066-114077, 2020.

[8] M. Dayal, A. Chawla, M. Khari, and A. N. Mahajan, "Artificial Intelligence-Based Smart Packet Filter," in *Proceedings of Third International Conference on Computing, Communications, and Cyber-Security: IC4S 2021*, Singapore: Springer Nature Singapore, July 2022, pp. 791-801.

[9] H. R. Deekshetha and A. K. Tyagi, "Automated and intelligent systems for next-generation-based smart applications," in *Data Science for Genomics*, Academic Press, 2023, pp. 265-276.

[10] P. Dolezel, F. Holik, J. Merta, and D. Stursa, "Optimization of a depiction procedure for an artificial intelligence-based network protection system using a genetic algorithm," *Applied Sciences*, vol. 11, no. 5, p. 2012, 2021.

[11] H. Dong, A. Munir, H. Tout, and Y. Ganjali, "Next-generation data center network enabled by machine

learning: Review, challenges, and opportunities," *IEEE Access*, vol. 9, pp. 136459-136475, 2021.

[12] M. Emu, "Artificial intelligence empowered virtual network function deployment and service function chaining for next-generation networks" (Doctoral dissertation).

[13] S. B. Far, A. I. Rad, S. M. H. Bamakan, and M. R. Asaar, "Toward Metaverse of everything: Opportunities, challenges, and future directions of the next generation of visual/virtual communications," *Journal of Network and Computer Applications*, p. 103675, 2023.

[14] B. Frederick, "Artificial Intelligence in Computer Networks: Role of AI in Network Security" (Master's thesis).

[15] S. S. Gill, M. Xu, C. Ottaviani, P. Patros, R. Bahsoon, A. Shaghaghi, et al., "AI for next generation computing: Emerging trends and future directions," *Internet of Things*, vol. 19, p. 100514, 2022.

[16] G. González-Granadillo, S. González-Zarzosa, and R. Diaz, "Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures," *Sensors*, vol. 21, no. 14, p. 4759, 2021.

[17] A. Haldorai, Q. S. Mahdi, and P. Devasudha, "Application of AI/ML in Network-Slicing-Based Infrastructure of the Next-Generation Wireless Networking Systems," in *2023 Fifth International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, pp. 1-10, IEEE, February 2023.

[18] S. Iftikhar, S. S. Gill, C. Song, M. Xu, M. S. Aslanpour, A. N. Toosi, et al., "AI-based fog and edge computing: A systematic review, taxonomy and future directions," *Internet of Things*, p. 100674, 2022.

[19] A. Imanbayev, S. Tynymbayev, R. Odarchenko, S. Gnatyuk, R. Berdibayev, A. Baikenov, and N. Kaniyeva, "Research of machine learning algorithms for the development of intrusion detection systems in 5G mobile networks and beyond," *Sensors*, vol. 22, no. 24, p. 9957, 2022.

[20] P. L. S. Jayalaxmi, R. Saha, G. Kumar, M. Conti, and T. H. Kim, "Machine and Deep Learning Solutions for Intrusion Detection and Prevention in IoTs: A Survey," *IEEE Access*, 2022.

[21] D. Kant and A. Johannsen, "Evaluation of AI-based use cases for enhancing the cyber security defense of small and medium-sized companies (SMEs)," *J. Electron. Imaging*, vol. 34, paper MOBMU-387, 2022.

[22] I. U. K. U. Khan, M. Ouaissa, M. Ouaissa, Z. Abou El Houda, and M. F. Ijaz (Eds.), "Cyber Security for Next-Generation Computing Technologies," CRC Press, 2023.

[23] M. Macas, C. Wu, and W. Fuertes, "A survey on deep learning for cybersecurity: Progress, challenges, and opportunities," *Computer Networks*, vol. 212, p. 109032, 2022.

[24] S. Mishra, "Exploring the Impact of AI-Based Cyber Security Financial Sector Management," *Applied Sciences*, vol. 13, no. 10, p. 5875, 2023.

[25] E. R. Ndukwe and B. Baridam, "A Graphical and Qualitative Review of Literature on AI-based Cyber-Threat Intelligence (CTI) in Banking Sector," *European Journal of Engineering and Technology Research*, vol. 8, no. 5, pp. 59-69, 2023.

[26] P. Ramya, S. V. Babu, and G. Venkatesan, "Advancing Cybersecurity with Explainable Artificial Intelligence: A Review of the Latest Research," in *2023 5th International Conference on Inventive Research in Computing Applications (ICIRCA)*, pp. 1351-1357, IEEE, August 2023.

[27] V. Ravi, M. Alazab, K. P. Soman, S. Srinivasan, S. Venkatraman, Q. V. Pham, and K. Simran, "Deep Learning for Cyber Security Applications: A Comprehensive Survey."

[28] P. Salva-Garcia, R. Ricart-Sanchez, E. Chirivella-Perez, Q. Wang, and J. M. Alcaraz-Calero, "XDP-based SmartNIC Hardware Performance Acceleration for Next-Generation Networks," *Journal of Network and Systems Management*, vol. 30, no. 4, p. 75, 2022.

[29] I. H. Sarker, "Multi-aspects AI-based modeling and adversarial learning for cybersecurity intelligence and robustness: A comprehensive overview," *Security and Privacy*, e295, 2023.

[30] I. H. Sarker, M. H. Furhad, and R. Nowrozy, "AI-driven cybersecurity: an overview, security intelligence modeling and research directions," *SN Computer Science*, vol. 2, pp. 1-18, 2021.

[31] X. Shen, J. Gao, W. Wu, K. Lyu, M. Li, W. Zhuang, et al., "AI-assisted network-slicing based next-generation wireless networks," *IEEE Open Journal of Vehicular Technology*, vol. 1, pp. 45-66, 2020.

[32] T. Sowmya and E. M. Anita, "A comprehensive review of AI-based intrusion detection system," *Measurement: Sensors*, p. 100827, 2023.

[33] S. Suprabhath Koduru, V. S. P. Machina, and S. Madichetty, "Cyber Attacks in Cyber-Physical Microgrid Systems: A Comprehensive Review," *Energies*, vol. 16, no. 12, p. 4573, 2023.

[34] E. Tcydenova, T. W. Kim, C. Lee, and J. H. Park, "Detection of adversarial attacks in AI-based intrusion detection systems using explainable AI," *Human-Centric Comput Inform Sci*, vol. 11, 2021.

[35] S. S. Tirumala, N. Nepal, and S. K. Ray, "Raspberry pi-based intelligent cyber defense systems for SMEs and smart-homes: An exploratory study," *EAI Endorsed Transactions on Smart Cities*, vol. 6, no. 18, pp. e4-e4, 2022.

[36] A. A. Wagan, A. A. Khan, Y. L. Chen, P. L. Yee, J. Yang, and A. A. Laghari, "Artificial Intelligence-Enabled Game-Based Learning and Quality of Experience: A Novel and Secure Framework (B-AIQoE)," *Sustainability*, vol. 15, no. 6, p. 5362, 2023.

[37] T. Zebin, S. Rezvy, and Y. Luo, "An explainable AI-based intrusion detection system for DNS over HTTPS (DoH) attacks," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 2339-2349, 2022.

[38] T. Zhang, H. Qiu, M. Mellia, Y. Li, H. Li, and K. Xu, "Interpreting AI for networking: Where we are and where we are going," *IEEE Communications Magazine*, vol. 60, no. 2, pp. 25-31, 2022.

[39] S. Patil, V. Varadarajan, D. Walimbe, S. Gulechha, S. Shenoy, A. Raina, and K. Kotecha, "Improving the Robustness of AI-Based Malware Detection Using Adversarial Machine Learning," *Algorithms*, vol. 14, no. 10, p. 297, 2021.