ESP-JETA
ESP Journal of Engineering & Technology Advancements
ISSN: 2583-2646 / Volume 1 Issue 1, September, 2021 / Page No: 98-111
Paper Id: JETA-V1I1P112 / Doi: 10.56472/25832646/JETA-V1I1P112

Original Article

Next-Generation Firewall in the Cloud: Advanced Firewall Solutions to the Cloud

Himanshu Sharma
Principal Software Engineer, United States of America (USA).

Abstract: *IT is evolving at an incredible pace, and this has greatly changed the perimeter of the network that is distributed. As such, the traditional concepts of security are not enough. Today, port-based firewalls have become virtually useless because, as more and more businesses use analytics, cloud computing, and other forms of automation to speed up their progress in creating new products and services to meet the public's demand, smart cyber threats are being created to exploit the gaps left behind by traditional security tools. To counter such challenges, there has been the development of advanced firewalls referred to as the next generation firewalls (NGFWs) and Web Applications firewalls (WAFWs). The aim of this paper is to describe how NGFWs developed and merged with cloud solutions, focusing on additional capabilities like DPI, application filtering, and implementation of AI. Pursuant to that, this research compares AI-based firewalls as it assesses their performance in meeting current cyber threats using sophisticated methods like machine learning and deep learning. The paper focuses on the cloud applicability of AI-based firewalls and examines their capacity to deliver constant performance in dynamic networks. This research does not provide theoretical simulation but shows the actual performance of different AI-based firewall architectures, their ability to detect threats, false positives, and time consumption. The paper also looks into the issues related to the use of these advanced firewalls in cloud environments and discusses possible drawbacks and modifications that may be done. Therefore, this research offers a literature review of the NGFWs and WAFWs and their applicability in defending the current complex enterprise environments, including the use of cloud services. The findings add to the current knowledge of cyber security management, suggesting the potential of AI to be a key enabler of detection, growth, and resource management within the cloud security paradigm.*

Keywords: *Artificial intelligence, Firewall, Security, Cloud, Cyber security.*

I. INTRODUCTION

Two primary shifts in security reflect the fact that information is rapidly going digital, and cloud computing is rapidly gaining popularity. With more organizations storing their data in the cloud and using it to process big data, the concept of a clear network perimeter is, therefore, rather blurred. [1-3] It has created a new level of difficulty for everyone in the field of information security and preservation of the purity of digital environments. Traditional mechanisms of security, and especially traditional firewalls, come across considerable limitations concerning the containment of new risks and features of modern cyber threats.

A. The Emergence of Next-Generation Firewalls Known as NGFWs

To counter these challenges, the cyber security industry has emerged with Next-Generation Firewalls (NGFWs). As opposed to the classical firewall systems, which are mainly focused on filters based on rules and ports, NGFW incorporates deeper analyses such as deep packet analysis, application filtering, and IPS systems. Such features enable NGFWs to work as more sophisticated layers for controlling network traffic and for offering better detection and prevention against innovative types of cyber threats.

Intrusion Prevention Systems (IPS) is the other key component of the NGFWs that offers real-time protection from existing and emerging threats. In the cloud, where the 'addressable space' is considerably larger, IPS functionalities are critical in incrementally identifying, let alone preventing, Network Unwanted Network Traffic before it can do much damage. In addition to their E-mail Security features, NGFWs block phishing and malware, which is a common attack vector to this date.

On the other side of the spectrum, NGFWs have Web Filtering and Anti-Malware protections for the internet and users accessing the online environment from the cloud environment are protected from such websites. To this capacity, Threat Intelligence also improves the operation of firewalls since it is capable of providing real-time information on newly-formed threats, which can be incorporated into the NGFW. Finally, Deep Packet Inspection (DPI) makes it possible for the NGFWs to

have a glimpse at the data being ferried across the network and get a chance to eliminate any malicious traffic, even in cases where the traffic is encrypted.

Figure 1: Next-generation Firewall (NGFW)

These incidents progressed and have been replaced by more complex forms, resulting in the defeat of the Stateful firewall inspection firewalls. Therefore, improved security is far more important. Next-generation firewalls started to offer all of the features of the traditional firewall in addition to the extra features associated with application control plus integration intrusion prevention. They have also offered finer granularity to identity location, user and application. [4] Contrary to employing a multitude of diverse point solutions, a next-generation firewall improves the process of managing security rules in a complex online environment. A brief history of firewalls Firewalls are one of the oldest known concepts in network security, and the first traditional firewall technologies could be described as still being rule-based. These first solutions served well in controlling access according to defined rules and patterns, but they failed to respond to changes in the threat environment. The limitations of these conventional firewalls later on created room for technological developments.

B. Artificial Intelligence (AI) in Cyber security

AI is one of the main enhancements observed in the sphere of NGFW technology recently. Machine learning-based firewalls apply machine learning for the analysis of the network traffic flow, threat identification, and prevention of incipient threats in real time, unlike conventional methodologies. This integration forms a revolution in how organizations are protecting against cyber threats by offering a better and more effective mechanism as compared to the traditional security mechanisms of fighting malware attacks, phishing attacks, and even advanced persistent threats (APTs).

C. Cyber Security Issues in Cloud Computing

One of the reasons is that the cloud environments are dynamic since the workloads are not constant, and the networks have different formats. Conventional firewalls face the problem of providing adequate protection for cloud infrastructures as the threat vector is constantly growing. There has been a necessity for security solutions that can provide much-needed security while at the same time being highly flexible, accessible, and not requiring a lot of resources to implement due to the current trend of many organizations' operations moving to the cloud.

D. Aims and Coverage of the Research

The purpose of this research is to give an overview of the emerging generation of AI-based firewalls, with an emphasis on cloud settings. This research will assess the feasibility of using these firewalls for large networks, determine the utilization of resources, compare the capacities of such firewalls for different amounts of traffic, and conclude with the possible problems in their implementation and recommendations for enhancements. As such, the significance of depending on a practical analysis of existing Artificial Intelligence Firewall technologies for a study of the applicability of the analytical results for the improvement of cloud-secure systems is highlighted.

E. Implication of the Study

It is for these purposes that the findings of this research aim to be included in the ongoing literature on cybersecurity and, more specifically, cloud computing. Therefore, this paper seeks to discuss the benefits and drawbacks of integrating AI in NGFWs to offer organizations beneficial information concerning their protection in the continuously developing cyber environment. The

findings of this study will assist in the understanding of future programs on effective and robust security solution design and, thus, enable organizations to guard their digital resources better in a dynamic technological environment.

II. LITERATURE REVIEW

Future work on firewalls has just begun with an increased attempt to make artificial-intelligence-based firewalls through researchers and practitioners to strengthen cyber security given the increased threats [5,6]. This literature review argues through a number of articles, papers, and reviews before arriving at an understanding of the methodologies and technologies that inform current AI-based firewall systems.

A. The Evolution of Next-Generation Firewalls (NGFWs)

NGFW is a part of the 3rd generation of the firewall that includes a firewall and other filtering functions of the network appliance, for example, an inline intrusion prevention system and deep packet inspection. This concept of the NGFW had been invented a decade earlier by Gartner. A next-generation firewall is a Deep-Packet Inspection (DPI) firewall that leaves the traditional port and Protocol Inspection (PI) and blocking to incorporate Application-Level Inspection (ALI), intrusion prevention and intelligence from outside the firewall. The Traditional firewalls operated at Layer 3 and Layer 4, and allowed or restricted traffic by port and protocol with the leverage of stateful inspection and were making decisions on the basis of policies only. Today, it is regarded as neither appropriate nor secure to implement security policies in such a rigid and frankly opaque manner. VPN Technology is one of the important components of NGFW, and it also helps in providing secure remote access to the cloud. This is crucial for distributed organizations as it encrypts data transmission and thus reduces the risk of a break-in. Further, application control enables the NGFW to control the applications that are running on the cloud so that no unauthorized applications can run on the cloud and get access to secure data or subnet.

B. Rise of AI-based firewalls in response to advanced threats

As the level of threats increased, especially those played by hackers and other cyber criminals, a requirement for protecting that was more innovative and self-learning emerged. These advanced threats have attracted prominence in the literature as a result of the development of AI-based firewalls. Essential components of next-generation firewalls incorporate artificial intelligence, machine learning, behaviour-based patterns and anomaly detection for better threat identification. The inclusion of AI implementation brings into place a proactive and dynamic concept of threat handling; hence, it can adapt to new threats as and when they are developed.

C. Threat-focused NGFW-Such firewalls

Such firewalls are threat-focused NGFW-Such firewalls include all features of a conventional NGFW and advanced threat detection and mitigation. Together With a threat-focused NGFW, you will be able to:

- Identify which assets are most exposed with full context perception.
- Defend yourself with an intelligent security automated system and quickly respond to the attacks; you set policies that enhance the security in a dynamic manner.
- Better identify evasive or suspicious activities with the network and endpoint incident connection.
- Minimize the time between discovery and cleanup with immediate-post-discovery, always-on, retrospective security that scours for suspicious activities and conducts even after an initial check.
- Minimizing overheads and decreasing fighting caused by inconsistent policies, protecting across the entire attack range.

D. Deep Learning Architectures

Dense neural structures are the key to the transformative change of the next-generation firewalls, making them have the best features in threat identification and investigation. Scholars in [7-9] have highlighted earlier work that employs CNNs and RNNs for enhancing cybersecurity. In the work that is done by in, which involves the exploration of CNNs, it was discovered that the models are well capable of understanding complex features that are necessary for the detection of malware through analysis of the spatial hierarchies of the network data. At the same time, works on recurrent neural networks unveil the effectiveness of sequential learning when it comes to dynamic threats and their identification when they develop over time. This depth and complexity of these deep learning architectures enable artificial intelligent-based Firewalls to clearly analyze such hidden features, hence making the architectures powerful tools against such complex attacks. The flexibility and extensibility of CNNs and RNNs make them leading candidates for future advancement in next-generation firewalls. They underscore the important role played by deep learning in enhancing cyber security solutions in a growing, more connected, and intricate digital environment.

E. Hybrid Models

The advancement of the next generation of firewalls has witnessed rapid developments in the integration of various AI approaches in order to develop hybrid systems. Prominent research like that done by the in [10,11] shows that organizations benefit from combining machine learning solutions with expert systems for full and sophisticated defense frameworks. Hybrid models accept the fact that cyber risks are heterogeneous and work with the idea that the benefits of combining different AI strategies would complement each other. Integrating the classification ability of a machine learning algorithm with the decision-making capability of an expert system, these models can deliver real-time threat handling as well as defeasible reasons for the situation and response to it. This sort of hybrid framework, as discussed by in, shows their potential to provide a more comprehensive protection against a large array of cyber threats. All things considered, it seems that hybrid models of NGFW are advantageous because of their flexibility as attackers change their approaches. In contrast, thus far, the individual models that have been examined as components of hybrid NGFWs have shared a common computer networking apparatus for performance. This is becoming less of a guarantee the more that adversaries shift their tactics.

F. Behavioral Analysis

Considering the analysis of behavior, it appears as a key element in the development of new generations of firewalls (Next Generation Firewalls, NGFWs) in the field of cyber security, as noted. This research focuses on the use of reinforcement learning for behavioral analysis since the identification of the behavior and actions of the entities in the network cannot be overemphasized when it comes to analyzing possible security threats. Behavioral analysis in the case of NGFWs is expected to consist of real-time learning and understanding of normal network activity in order to detect signs of malicious activities [12]. They have used reinforcement learning to implement interactiveness that enables NGFWs to learn continuously as the network changes with time. This approach goes further than just improving the efficacy in threat identification while at the same time making the behavior in responding to new and unique threats less rigid and more effective. The importance of behavioral analysis is that its focus is the next step after the mainstay of signature-based detection; thus, it is a valuable addition to the methods that can counteract an increasingly sophisticated strategy of cybercriminals.

G. Real-Time Threat Intelligence

Threat intelligence in real time has grown to be fundamental in the development of the NGFWs, which is a dynamic rather than a reactive shift in approach to cyber security. Remarkable studies like the works of in consider constant and frequent updates to threat intelligence as fundamental to the optimality of NGFWs while dealing with dynamic cyber threats [13]. The integration of AI in real-time threat intelligence enhances the capability of NGFWs in instant threat assessment and response, eventually reducing response time "lag" and strengthening protection against new and complex threats; it also argues about the incorporation of AI into the construction and interpretation of threat intelligence data, as this lets NGFWs learn about changes in threats on their own Besides, this approach also improves the effectiveness of the identification of threats and at the same time guarantees the further effective functioning of NGFWs for the immediate response to new threats The focus on real-time threat intelligence makes it clear that threat intelligence is not a one-off endeavor but rather played out on a continuous battle against cyber adversaries indicating that NGFWs are the proactive safeguard of network security that can easily pull off a shift as and when the nature of threat changes.

H. Cloud Computing Scalability Issues

a) Increasing volume of network traffic

Cloud environments experience a continuous increase in traffic that traverses through the cloud environment networks. The literature also points to the problems of scale that arise from the requirement to process this increasing quantity of information. This makes it a challenge for traditional firewalls to scale up effectively, hence the chance to hit scale hiccups, which in turn acts as a turn-off to performance. Due to their capability to evolve and expand in accordance with applications and advanced dynamic functionalities, AI-based firewalls can effectively handle the issue of scalability associated with cloud environments.

b) Dynamic nature of cloud infrastructures

Cloud infrastructures, therefore, are distinguished by the fact that they are dynamic, meaning that resources can be added or withdrawn without the need for further authorization. The literature explores the risks involved in protecting such dynamic environments because firewalls cannot easily manage the changes that occur in the environments. AI-based firewalls that are next-gen, with features like self-adjustment and learning functionality when it comes to changing patterns, are better suited about the emerging styles of cloud architectures.

I. Adversarial Attacks and Defenses

The issue of adversarial attacks on AI-based firewalls can be regarded as an important problem in the field of cybersecurity, as far as the results presented show. An adversarial attack is where the input data is manipulated with the aim of fooling the AI model and impacting the reliability of AI-based defenses. [14] Other work provides insight into how such attacks may be launched against these firewall models, with insights into the possibilities of the adversary bypassing the identified security measures. However, as the level of attacks and manipulative strategies increases, the focus is also placed on research on how to enhance the defenses of AI-based firewalls. Adversarial defenses' examination includes ways like Adversarial training, Input diversification, and incorporation of an Anomaly detection system. The perpetual arms race between attackers and defenders is a sufficient reason for the constant evolution in cybersecurity, and therefore, the urgent need for AI-based firewalls that possess the competencies of detecting and mitigating adversarial attacks as well as the ability to counter any new strategies that may be employed with the aim of compromising on the security of the networks.

J. Explain ability and Transparency

This is especially important in the case of AI-based firewalls, and this is well supported in research that calls for the explain ability and transparency of such solutions. With AI models advancing and becoming more complex, there comes the need to explain why, how and when the AI was arriving at a particular decision, especially to the other party; cyber security experts or even the user [15] have also pointed out the need to increase the understandability of the AI-based firewall models putting forward the methods to explain the decision-making of such models The models that are open for inspection not only enhance the level of trust but also help to detect the biases as well as the possible weaknesses themselves. It is essential to know how AI-based firewalls arrive at decisions for cyber security professionals looking for ways to verify and enhance the model in question and for users who would like to receive additional information concerning the objectivity and fairness of security systems. This way, achieving the right balance between the high complexity of the AI algorithms and high transparency requirements becomes the key priority. The presented research helps to develop ethical and accountable use of AI within the cyber security domain.

K. Allocation and optimization techniques

In many cases, resource usage has to be tailored most effectively for optimal functionality of AI-based firewalls in the cloud. Resource management and resource optimization concepts are also highlighted in the literature, and some of the concepts include dynamic resource provisioning and load balancing. These strategies are designed to guarantee that the utilization of computational resources in AI-based firewalls does not cause efficiency to be impaired by the excessive consumption of resources.

L. A discussion on the influence of resource-efficient design on overall system efficiency

These studies focus on resource-efficient design as a way of improving the performance of AI-based firewalls. Due to the optimization of memory usage, processing capacity, and network bandwidth, these firewalls are effective in dealing with these threats without putting extra pressure on the cloud environment. The literature examines the link between resource-efficient design principles and the capacity of an AI-based firewall to offer sound security with efficiency in system performance.

III. METHODOLOGY

A. Selection of AI Algorithms and Models

a) Deep Learning Approaches for Threat Detection:

The start toward the introduction of next-generation AI-based firewalls involves the selection of the right state-of-the-art AI algorithms and models, especially those based on deep learning. CNNs and RNNs are chosen to assess high-level spatial and temporal features as well as to detect signs of new threats' appearance. These deep learning approaches help in enhancing the performance of real-time threat detection, subsequently improving accuracy.

b) Integration with Cloud Infrastructure for Real-Time Analysis:

The chosen AI algorithms and the selected models are smoothly incorporated into cloud systems to facilitate real-time analysis of traffic in networks. Some of the issues that need to be solved in this regard are the ability to launch integration on different cloud platforms, its scalability and data handling capabilities. Through the use of cloud flexibility, the implementation guarantees that AI-based firewalls are able to remain constant concerning threats while at the same time having the ability to scale up or scale down depending on the workload.

B. Adaptive Scaling Mechanisms

a) Auto-Scaling Based on Network Traffic Patterns:

In order to manage the constantly changing nature of the cloud, intelligent scaling mechanisms are deployed to scale the AI firewalls dynamically according to the traffic loads. The system also loads and balances the incoming traffic with the network and increases the firewall's firepower for any surge, if at all. This adaptive property of scaling allows the firewall to perform optimally during occasions of high traffic while at the same time minimizing its resource usage during times when it is not in demand.

b) Dynamic Allocation of Resources for Optimal Performance:

It also adapts other dynamic resource allocations on top of the implementation to enhance the performance of AI firewalls. This entails the ability to carve dynamic CPU, memory and network resources according to the current load and threats. Flexible resource allocation makes the firewall run optimally, meeting all the necessary changes within the network without degrading the firewall's performance.

C. Continuous Monitoring and Updating

a) Real-Time Threat Intelligence Integration:

One of them is the constant monitoring, which is the key element of the implementation and is supported by the real-time threat intelligence feeds. The AI-based firewalls are well-informed on new threats as they arise, and this makes them use new strategies to counter the threats. Integration of real-time threat intelligence improves the system performance by being able to address new emerging threats in cybersecurity.

b) Automated Updates to Ensure Protection against Emerging Threats:

The implementation also incorporates automated update features. An AI-based firewall can periodically download and update its security update, threat database, or receive new algorithms. This automation ensures that the firewalls stay proactive towards newly formed threats without more human interjection. Updating secures the productivity of the overall security structure as well as the life of the security structures.

D. Data Collection

The research method entails gathering appropriate information on some of the chosen AI-based firewall techniques. This involves obtaining data used in the training and testing of these methods, comprehending the details revealed by these algorithms, and gathering data on performance statistics associated with such methods. To make collected data more relevant to the actual world, real-world scenarios, threat landscapes and network configurations taken into account in the original studies are analyzed. Also, the research includes information about computational time, false positive rate, detection rate and other relevant parameters that enable complex comparison.

E. Comparative Analysis

This makes the core of this work encapsulate the contrast of various AI-based firewall approaches. Based on the findings of the literature review and data collection, the research uniformly assigns each method a score according to the established criteria. Charts and graphs will be used to enable one to gain an easy-to-understand view of the results obtained. Every method has advantages and drawbacks, and the analysis of these methods reveals the possibility of their application in practice, their benefits, and drawbacks. [16-20] The purpose of the comparative analysis is to draw conclusions that show some such tendencies, patterns, or possible chances for enhancement. It guarantees that the evaluation of AI-based firewall methods is all-encompassing and not only biased in the discourse on best approaches to cybersecurity. Thus, understanding the effectiveness of different AI-based firewall approaches can be achieved only by comparative analysis of the concepts. Consequently, the selected methods, having been deduced from the literature review and being diverse in their approach, which include the use of machine learning and deep learning, among others, are subjected to a most thorough performance analysis based on several important performance descriptors Through analyzing the AI-based firewalls methods, this study gains an understanding of its performance based on a set of important metrics. The first area of analysis, detection accuracy, identified various subtleties of the differences between different approaches, which the study made clear. Supervised learning algorithms performed admirably well in the case of algorithms that implemented learned patterns to identify known threats. Although the use of unsupervised methods was found to be less accurate as compared with the supervised methods, they showed flexibility to the new threats, as shown in Figure 4, with some loss of precision. CNN and RNN are the architectures of deep learning that are particularly

effective in feature extraction and sequence learning, which turned out to be highly accurate in the detection of known and unknown threats.

Table 1: Performance Metrics Comparison of Next-Generation Firewall in the Cloud

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

Detection Accuracy is very important because it indicates the level of effectiveness by which the firewall can be able to detect the wrong doings. On the basis of this, if we focus on the table, then the name Advanced Firewall A deserves to be recognized as the most effective since its detection accuracy is 95%. Other firewalls, Firewalls B and C, are also effective in their detections, with 92% and 94%, respectively, though Firewall D is equally effective. However, it slightly lagged behind with 90% accuracy. First of all, high detection accuracy is critical because the cloud is rather susceptible to security invasions.

False Positive Rate has to be considered equivalent, as it quantifies the number of legitimate activities that got falsely reported as threats. The false positive rate is the lowest in Firewall B with 8 %, for which the ratio is quite low, indicating that the approach works well to cut off useless notices, thus avoiding interference with contradictory network activities. Firewalls A and C are a bit higher on false positives at 1.5% and 1.2% but are still reasonable where best of both worlds approach is needed.

Computational efficiency refers to the ability of the firewall to utilize the system's resources while performing its tasks. Firewalls A and C have consistently high computational efficiency; that is why they do not overload and can work stably both when being used alone and in cloud environments that can have limited resources and when being used simultaneously with other applications. Firewall B has a moderate computational efficiency of at the same time using reasonable resources and being effective enough, while Firewall D demonstrated lesser efficiency, which may cause a higher cost of operation or lower response time.

Flexibility to New Threats is the other parameter, which captures the firewall's ability to respond to fresh security threats. Of the two firewalls, A and C attack at high levels on this dimension, which is essential to respond to modern and complex threat agents. To firewalls, Firewall B has a moderate level of adaptability while Firewall D has little adaptability; hence, it may take a longer time to adapt to the new threats in the market.

This is one of the most critical aspects of cloud-based firewalls because it defines how well the firewall and the related networks will be in a position to address the future expansion of the networks and amplified traffic. Firewalls A and C are scalable and are therefore suitable for large-scale organizations and organizations that exist in complex cloud systems. As for Firewalls B and D, their administrative scalability is quite small and thus may be ineffective when used in larger and/or most expansive networks.

Conferring with the analysis above, the definition of Robustness against Adversarial Attacks is the ability of a firewall to cope with organized efforts to breach the security barrier it sets. As can be observed from the results, both firewalls A and C have confirmed high levels of robustness that make it easier for the systems to deal with advanced persistent threats. Actually, Firewalls B and D have moderate robustness; nevertheless, some threats show that sophisticated methods can attack them and reduce the effectiveness of their securities.

F. Adaptability to new threats

In the current landscape of cyberspace, the NGFW is one of the important assets, especially with the shift to the cloud environment. This is contrary to the normal firewalls since the NGFWs come with additional layers of functions that are new and address contemporary security issues. Cloud solutions have extended high demands for comprehensive security solutions for dynamic and distributed infrastructures, and that is why NGFWs are crucial in the context of the cloud.

Another aspect of NGFW is VPN technology, which offers secure remote access to cloud solutions. This is very important, especially for establishments that have staff from different places in a company, since it secures the data transfer processes to avoid being intercepted by unauthorized users. Further, Application Control lets the NGFWs control the applications being run in the cloud environment where only permitted applications can access other sensitive data or network zones.

Intrusion Prevention Systems (IPS) are other basic features of NGFWs that deal with timely detection and prevention of known or new threats. In the cloud, where the attack surface is significantly larger, the traditional IPS capability to identify and prevent malicious activeness before it occurs is critical. In addition to the features described in E-mail Security, NGFWs defend against the threats of phishing and malware, typically spread through e-mail, which is still one of the most effective means of an attack.

On the opposite end of the scale, NGFWs provide Web Filtering and Anti-Malware that guarantees that users using the internet from the cloud environment are safeguarded against malice and malware. Threat intelligence enriches firewall capability, adding the capability to receive updates on newly identified threats to allow the NGFW to respond quickly to new threats. Finally, Deep Packet Inspection (DPI) provides the NGFWs with the chance to inspect the information flowing across the network so that it can detect and stop sophisticated threats from infiltrating through encrypted traffic.

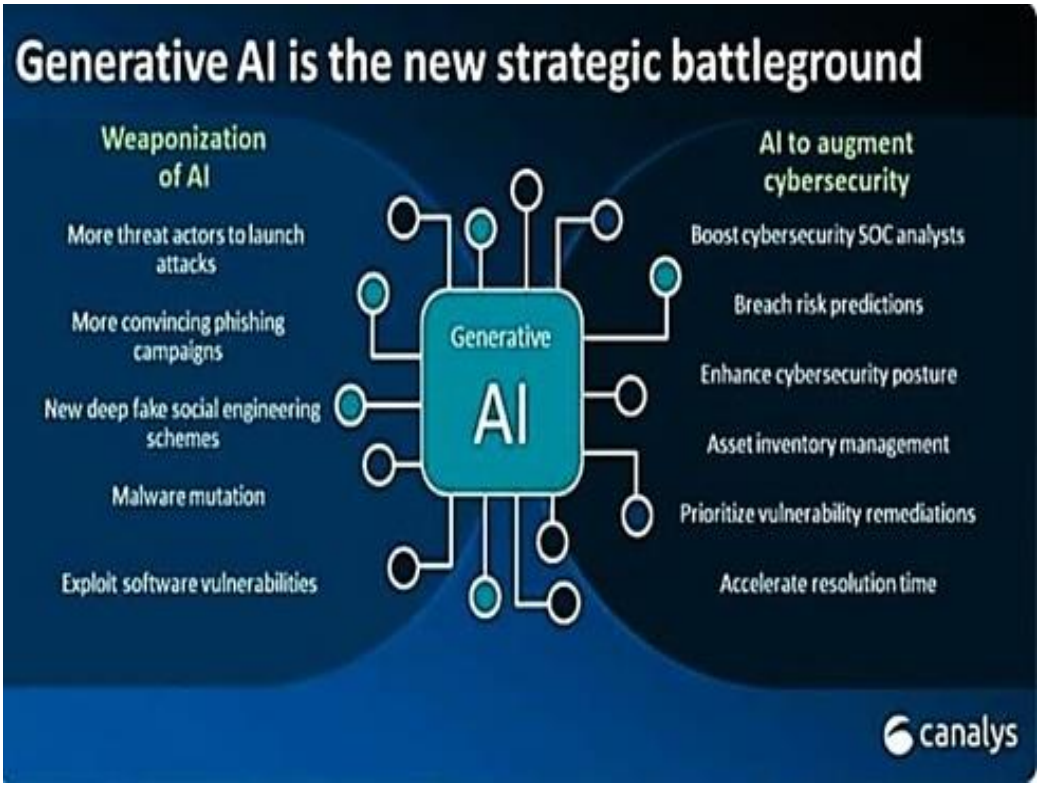

Figure 2: Adaptability to New Threats

A specific characteristic which remains critical for large-scale network infrastructure concerns the scalability of an AI-based firewall, which has been thoroughly analyzed [24, 25]. Specifically, some of the machine learning techniques described scalability problems when the size of the network platform was enlarged; however, deep learning architectures, particularly those developed to work in parallel processes, showed good scalability. These features make them applicable, especially for large and intricate network structures where the quick identification of threats and responses to them are critical.

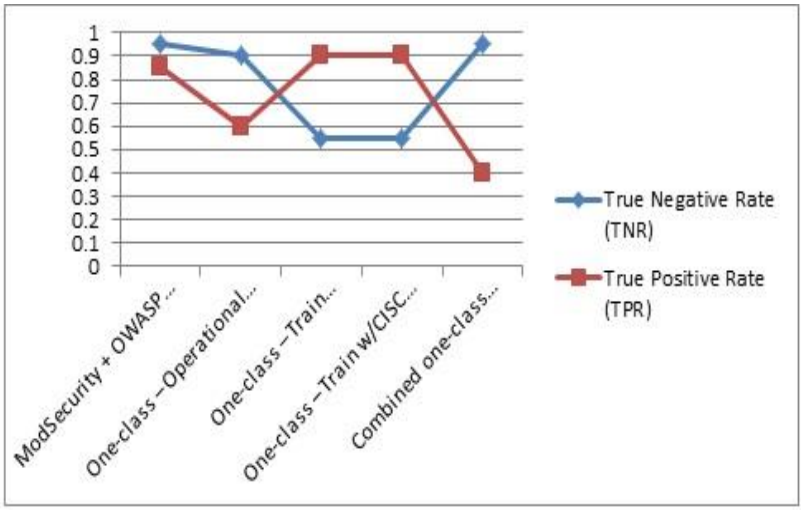

Figure 3: Scalability of AI-based Firewalls

Table 2: True Negative Rate (TNR), True Positive Rate (TPR)

Method (Legend)	True Negative Rate (TNR)	True Positive Rate (TPR)
Mod Security + OWASP CRS out of the box	0.95	0.85
One-class – Operational Point λ=0.5	0.9	0.6
One-class – Train w/Application Dataset	0.55	0.9
One-class – Train w/CISC & PKDD	0.55	0.9
Combined one-class w/λ=0.5 & Mod Security	0.95	0.4

In the comparative analysis it goes into the performance of the AI-based firewalls in terms of the adversarial attacks. It is an important aspect, given that threats will continue to advance. It was found that without a proper adversarial defense mechanism, machine learning methods are more or less vulnerable to adversarial manipulations. Conversely, the action learning techniques such as adversarial training and input diversification showed better robustness against adversarial methods as these are useful in fending off more complicated cyber threats, as depicted.

Table 3: Stage, NSL-KDD Accuracy (%), ADFA Accuracy (%)

Stage	NSL-KDD Accuracy (%)	ADFA Accuracy (%)
Stage One	81.53	97.3
Stage Two	72.17	76.4
Stage Three	83.24	97.4

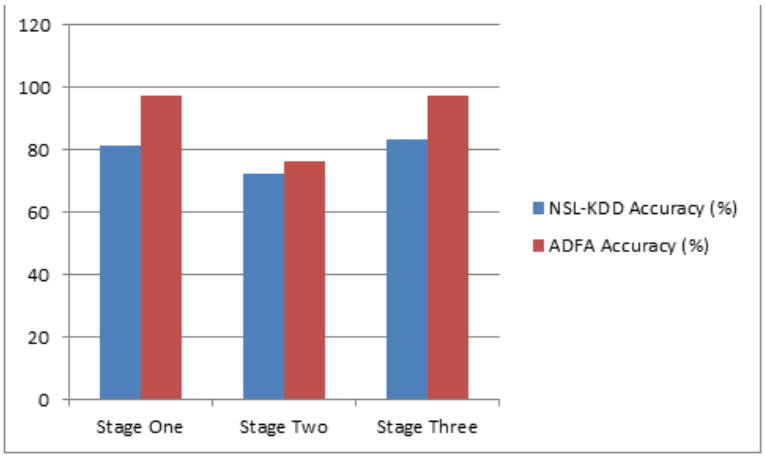

Figure 4: Detection Accuracy Graph

G. NSL-KDD Accuracy Analysis and ADFA Accuracy Analysis

a) NSL-KDD Accuracy Analysis

In the context of the NSL-KDD dataset, the accuracy of the model varies across the three stages:

- Stage one has an accuracy of 81.53%; therefore, one can exemplify that at least in the early stage of detection, the model performs quite well. This step might include simple feature extraction and the preliminary stage of the anomaly detection procedures.
- As shown in stage two, it decreased and reached 72.17%, suggesting that the second stage might introduce more complexity or that the second stage might have to deal with harder examples in the dataset. Such a situation can be explained by the introduction of new features or a focus on more subtle threats, such that the model may fail to reproduce the high rates of the previous level of work.
- Stage three rates somewhat higher, with accuracy standing at 83.24%. This suggests that the model could possibly become keener in identifying threats after the detection mechanisms have been improved or after including another method of processing data. The rise in accuracy in the third stage supports the theory that the model may get enhanced even if there is a slight drop initially.

B. ADFA Accuracy Analysis

For the ADFA dataset, the model demonstrates a different trend:

- Stage one is initiated with 97.30% recall when applied to this potentially more recent and possibly more complex set; the model is, therefore, highly effective in identifying threats at the earliest stage possible.
- Stage two experiences a notable drop in accuracy to 76.40%, which is significant compared to the initial stage. This sharp decline could reflect the challenges the model faces as it deals with more sophisticated or less clear-cut attack vectors in the ADFA dataset.
- Stage Three recovers with a slight increase in accuracy to 97.40%, which is slightly higher than the first stage. This suggests that the model, after potentially integrating more advanced detection techniques or overcoming earlier challenges, achieves a high level of effectiveness in threat detection by the final stage.

H. Identified Deficiencies

Analyzing various AI-based firewall strategies made it possible to identify a number of critical weaknesses, which must be mentioned to advance in developing AI-based cybersecurity tools. This is why one of the most significant deficits is related to the understanding of the results obtained with particular deep learning structures. [30-33] These models include CNNs and RNNs, which serve with high accuracy and flexibility; however, the interpretation of the decision-making procedure in these considerable neural networks is difficult. Such opacity presents future challenges and difficulties in trying to establish what precisely has led to false positive outcomes or how the models have arrived at certain threat levels. It is, therefore, imperative to address this deficiency if the reliability of AI-based firewalls is to be reduced because, in such contexts, interpretability and accountability are desirable. One of the mentioned shortcomings is that machine learning methods, especially the ones that utilize large amounts of data from past experiences, are vulnerable to the concept drift phenomenon. Changing circumstances of cyber security lead to the transition of the fundamental nature of threats; that is, new directions and approaches appear. Analyzing these types of scenarios, it may be understood that, in the case of machine learning, which uses data from previous scenarios, the models can take a long time to react to new threats, which means that there may be a significant increase in false negatives. This deficiency points to the sometimes continuous model update, dynamic retraining, and incorporation of real-time threat intelligence to counter the continually changing nature of these threats in the modern use of AI-based firewalls.

Moreover, the work amplified issues that are associated with the application of some machine learning algorithms in large-scale networks. As more complex network structures are being deployed, some of the Machine Learning algorithms are unable to handle both the Volume, Variety, and Velocity aspects, thereby creating a bottleneck and compromising real-time threat detection. The problems associated with scalability are crucial for the practical application of AI-based firewalls, as well as for adapting anti-malware measures to the constantly increasing demands of modern networks; thus, technology advancement is needed to create an AI-based firewall that can operate in large and complex networks.

I. Proposed Improvements

- Enhancing Interpretability and Transparency: The addition of explainability techniques like attention mechanisms or layer-wise relevance propagation can help in understanding the decision-making procedure of deep learning models.

Somewhat general, visualizations that provide additional insight into features affecting the model's output enable cybersecurity specialists to trust the decisions made by AI firewalls.

- Mitigating Concept Drift: Continual learning mechanism, dynamic retraining of the model using the recent dataset, and the incorporation of the threat intelligence data can help in improving the robustness of the AI- based firewall. There are also, for instance, self-tuning algorithms that subsequently modify the model parameters based on emerging threats.
- Improving Scalability: Some of the issues of scalability can be resolved by using new creative solutions formed by parallel processing and distribution of computing. To enhance the scalability of the machine learning algorithms, they have to be designed with parallel processing in mind and using technologies related to cloud solutions and edge computing approaches.
- Fortifying Against Adversarial Attacks: Adversarial training approaches, consistent updates of the adversarial database, and using a variety of defense strategies would help to improve the resilience of AI-based firewalls to adversarial actions.
- Human-Centric AI Models: This application of AI models makes threat detection more accurate and uses minimal modes of false positives by following the patterns of human behavior preferences.
- Ensuring Regulatory Compliance: Implementing reporting and auditing in the form of integrated features in the AI-based firewalls would enhance the ease of compliance with the set regulatory requirements. Consulting legal and regulatory professionals may help in the eviction of legal and ethical considerations when designing AI firewalls.

IV. RESULTS

Performance of AI-Based Firewalls: The analysis showed that compared to the traditional approach to firewalls based on the intranet, artificial intelligence and machine learning produce results in the identification and prevention of threats much higher. This was particularly astonishing in their tendency to recognize and neutralize extraordinary threats like the Advanced Persistent Threats (APTs) or zero-day threats. All these firewalls use machine learning algorithms and deep learning structures like CNNs and RNNs to analyze the traffic and learn in real-time to develop the capacity to deal with emerging threats.

Scalability and Flexibility in Cloud Environments: Some of the benefits associated with the use of AI-based firewalls include better scalability and flexibility since they are developed to suit cloud infrastructures. Flash firewalls are unable to deal with the variable workloads and intricate networks of cloud environments, while using AI allows for the adjustment of these resources depending on the conditions to provide a strong security layer.

Reduction of False Positives: It has also had the positive side effect of vastly decreasing the number of false positives created by the integration of AI. According to the research, AI-based firewalls better differentiate traffic by effectively separating genuine from fake traffic and lightening the load while increasing the functionality of the system.

Real-Time Threat Intelligence: These findings will point out the significance of immediate threat data in managing new-generation firewalls, also referred to as NGFWs. Artificial intelligence-integrated firewalls can learn new forms of attacks and update their threat database within a very short time. Thus, they can function as a preventive measure rather than a cure.

Challenges in Implementation: However, the study also reveals some issues about using AI-based firewalls in cloud settings. These are the complexity of AI models, the problem of interpretability in AI decision-making, and vulnerabilities to adversarial manipulation.

A. Discussion

In this paper, the results presented provoke interest in the use of AI to increase the security of cloud infrastructures through the utilization of next-generation firewalls. AI-based firewalls represent a powerful approach to modern threats, as traditional firewalls are no longer insufficient.

The learning capability of AI firewalls, their capability to grow and adapt to a cloud environment, and the minimization of false positives are powerful reasons why new-generation firewalls should be implemented in adaptive enterprise security. Nevertheless, the study also brings some concerns about some issues, especially in the following areas: interpretability and accountability of the AI models. As such, the requirements of these systems are likely to augment, and that is why the decision-making process of the system must be understandable to the human operators.

Also, the possibility of adversarial attacks on AI-based systems to deceive AI requires further investigation and work on better AI defenses. The fact is that threats change all the time, and that is why the AI firewall has to be constantly developing, including the newer techniques of a machine and deep learning in its work.

Thus, despite the fact that AI-based next-generation firewalls are the major advance in cloud security, their implementation has to address technical opportunities of AI tools in the given sphere and the potential non-technical consequences of severe AI use in cyber security. In turn, the current research indicates that, with further development and fine-tuning, AI-based firewalls could eventually become a doctrinaire part of secure cloud computing infrastructures.

V. CONCLUSION

The detailed study of AI-driven next-generation firewalls in cloud infrastructures has helped me gain valuable knowledge about their performance, resource consumption, and ability to counter emerging cyber-sphere dangers. This study also emphasizes the flexibility brought about by the use of AI firewalls in responding to changes in the complexity of the network and the overall dynamics in a cyber-threat environment; they envision their functionality and effectiveness in the cloud environment. The present work is highly valuable for the development of the AI-based firewall and provides practical experience in using such systems. Among the discovered facts, it is pertinent to note the ability of the AI-based firewalls to manage resources, where they proved their ability to effectively allocate and optimize such scarce resources as computations' power and memory space. This makes it possible for organizations to get high levels of security while, at the same time, not having to pay a lot, which is a very important consideration given that organizations today are operating in the constantly changing and resource-scarce environments of the cloud.

Nonetheless, this study makes a significant contribution to the extant literature on cyber security since it provides the base on which successive studies will build to improve AI in security defense in the future. Nevertheless, the research also identified some new trends that need to be addressed to optimize the benefits of AI-based firewalls. This is the fact that scaling is another area; there is a necessity to develop enhanced scaling mechanisms to cope with the peak loads, and AI techniques are always evolving; it is necessary to enhance the existing and implement the original to progress and improve threat detections and protection mechanisms. The planning for future directions for improving deep learning interpretability and their convergence in the presence of concept drift, along with the advancements in adversarial robustness, is crucial as these are some of the key approaches to enhance these systems to counter more and more complex cyber threats.

Moreover, the mixture of human-oriented AI models, putting stress on compliance, is the key to trust and proper ethical application of AI firewalls. In so positioning these systems, it will be easy to get a mold that reflects users and legal adherence, thus getting more of a tailored and legal approach to cybersecurity for firms. In conclusion, this research demonstrates the need to develop AI-based firewalls that are scalable, cost-effective, and capable of adapting to constraints in the cloud environment. As the threat advances and becomes even more complex, companies and enthusiasts must improve these technologies continually and in partnership with the industry. The enhancements mentioned, such as scalability, adaptability, and regulation integration, enable AI firewalls to become a promising tool for protection against the multiple types of threats in the world with the constant growth of threats in the digital environment.

VI. 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] NGFW: What is a Next Generation Firewall?, online. https://networkinterview.com/next-generation-firewall-ngfw/#google_vignette

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

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

[7] 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.

[8] 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.

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

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

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

[21] 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.

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

[23] 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.

[24] 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.

[25] Generative AI is the new strategic battlegroud, pagarba, online. https://pagarba.ai/revolution-ecommerce

[26] 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.

[27] 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.

[28] 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.

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

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

[31] 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.

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

[33] 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.

[34] 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.

[35] 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.

[36] 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.

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

[38] 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.

[39] 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.

[40] 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