Chapter-III

NEXT-GENERATION FIREWALLS: ARCHITECTURE AND EFFECTIVENESS

Dr. Meera Arvind, Professor of Information Security, Vellore Institute of Technology (VIT), Vellore, India.

Dr. Arjun Nair, Professor of Information Security, Vellore Institute of Technology (VIT), Vellore, India.

Abstract--- IT is developing at an astonishing rate, which has significantly altered the distributed network's perimeter. Therefore, the conventional ideas of security are insufficient. Port-based firewalls are now essentially worthless since smart cyber threats are emerging to take advantage of the weaknesses in traditional security tools as more and more companies use analytics, cloud computing, and other automation tools to accelerate the development of new goods and services to satisfy consumer demand. Advanced firewalls such as Web Applications firewalls (WAFWs) and next generation firewalls (NGFWs) have been developed to address these issues. With an emphasis on extra features like DPI, application filtering, and AI implementation, this article aims to explain how NGFWs evolved and integrated with cloud solutions. Accordingly, this study evaluates the effectiveness of AI-based firewalls in fending off contemporary cyberthreats by utilizing advanced techniques such as machine learning and deep learning. The study looks at AI-based firewalls' ability to provide consistent performance in dynamic networks and focuses on how well they work in the cloud. This study illustrates the real performance of various AI-based firewall architectures, including their capacity to identify threats, false positives, and time consumption, without any theoretical simulation. Along with discussing potential disadvantages and potential changes, the article also examines the problems associated with using these advanced firewalls in cloud systems. In order to defend the current complex enterprise environments, including the usage of cloud services, this research provides a literature evaluation of the NGFWs and WAFWs and their relevance. The results broaden our understanding of cyber security management and point to AI's potential as a crucial facilitator of resource management, growth, and detection in the context of cloud security.

Keywords--- Artificial Intelligence, Firewall, Security, Cloud, Cyber Security.

1. INTRODUCTION

The fast digitization of information and the growing popularity of cloud computing are reflected in two main changes in security. The idea of a distinct network border is thus becoming less evident as more businesses store their data in the cloud and use it to process big data. Everyone working in the fields of information security and maintaining the integrity of digital environments now faces a new level of difficulty as a result. Conventional security measures, particularly firewalls, have significant shortcomings when it comes to containing emerging dangers and characteristics of contemporary cyberthreats (Jaggernauth & Rocke, 2021). The cyber security sector has developed Next-Generation (NGFWs) to address these issues. NGFW integrates more in-depth analyses including deep packet analysis, application filtering, and IPS systems, in contrast to traditional firewall systems, which are primarily concerned with filters based on rules and ports. These characteristics allow NGFWs to function as more advanced layers for managing network traffic and providing improved detection and defence against cutting-edge cyberthreats (Liang & Kim, 2022). The other essential element of NGFWs that provides real-time defence against both known and unknown threats is an intrusion prevention system (IPS). IPS features are essential for gradually detecting, let alone stopping, network unwanted traffic before it has a chance to cause significant harm in the cloud, where the "addressable space" is much larger. Apart from their email security characteristics, NGFWs also prevent malware and phishing, which are still frequent attack methods (Gudimetla et al., 2017). On the opposite end of the spectrum, NGFWs contain anti-malware and web filtering features that safeguard people browsing the internet from websites that are harmful to cloud-based users. Because Threat Intelligence may provide real-time information on newly-formed threats that can be integrated into the NGFW, it also enhances the performance of firewalls. Last but not least, Deep Packet Inspection (DPI) enables NGFWs to see the data being transferred over the network and have an opportunity to remove any malicious traffic, even when it is encrypted. The entire world is now separated into different networks for communication, information sharing, financial transactions, and other purposes (Audin, 2004).

The enormous expansion of computer networks and systems has made people and businesses more reliant on the data that is saved and shared through these systems. As a result, it becomes essential to safeguard not only the computers, the data they contain, and the different resources that are connected to them, but also to guarantee legitimacy and prevent attacks on the network and computers (Thu et al., 2023). To put it simply, a computer network is an interconnection of digital telecommunications that allows the different nodes to share resources. Any device that can transfer data, such as computers, routers, switches, etc., can serve as a node. For data to flow between these nodes, a data link is necessary. Wireless media or a cable can be used to connect the nodes to one another. Another way to think of a network is as an anthology of connected entities (Lei, 2024).

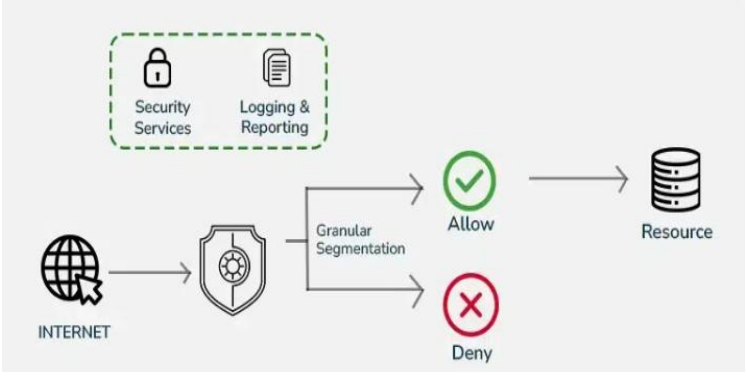

Figure 1: Next Generation Firewall

In a more straightforward manner, packets are sent over these established channels from one device to another. A packet is sent by one device and received by the other. If these packets are not interfered with, there is no issue; however, this is not always the case. Our concerns about the security of data packets and, consequently, networks from numerous dangers were heightened by the transmission of data across these communication channels. Using a firewall is the most fundamental and straightforward method of protecting our computer systems and network (Thu et al., 2023). Firewalls have been the first line of defines for the required safety and protection ever since we became concerned about protecting our networks and systems. A computer firewall is used to guard

against deliberate intrusions that could jeopardize confidentiality, cause data corruption, or cause a denial of service on a computer, whether it is networked or standalone. The security mechanisms known as firewalls are in charge of guarding our networks and personal computers against malicious malware, hackers, and intruders. They shield us and our networks against malicious malware that could infiltrate our computers or from snoopy hackers (Singh & Singh, 2023).

2. REVIEW OF LITERATURE

Yao, (2013) created a lightweight multicast authentication system for small-scale Internet of Things applications and updated the original Nyberg's fast one-way accumulator. SE-AKA, a safe and effective Authentication and Key Agreement (AKA) protocol, was suggested by Lai, (2013) and is compatible with all group authentication scenarios in LTE networks. In particular, SE-AKA implements an asymmetric key cryptosystem to safeguard user privacy and employs Elliptic Curve Diffie-Hellman (ECDH) to provide KFS/KBS (Fathia, 2024).

The extent of the DDoS flooding assault issue and efforts to mitigate it were examined by Zargar, (2013). Based on where and when they stop, identify, and react to DDoS flooding attacks, it categorized the attacks and ranked the current countermeasures. Thus, RSA, the most popular public key cryptography technique, serves as the foundation for Kothmayr's, (2013) suggested security strategy. It is intended to operate on common communication stacks for Low Power Wireless Personal Area Networks (6LoWPAN) using UDP/IPv6 networking.

The Fuzzy Attribute-Based Signcryption (FABSC), a unique security technique that appropriately balances security and elasticity, was created (Hu Chunqiang, 2013; Ilyasov, 2024).

Zhou, (2013) suggested a secure and effective routing system for WSNs that relies on authentication and encryption. By shifting routing-related responsibilities to the BS, BEARP specifically reduces the burdens on sensor nodes. This not only preserves network-wide energy equivalency and increases network lifetime, but it also enhances the security mechanism that the secure BS performs exclusively. Shin et al., (2015) suggested a simple method of authentication. Additionally, in order to fend against potential attacks in

ubiquitous networks, the technique offers secure password updates, session key agreement, and mutual authentication between entities (Islam et al., 2023).

Imran Memon et al. (2015) suggested using an asymmetric cryptographic approach to protect user privacy and provide safe connection. Because the asymmetric cryptography scheme is strong against this kind of attack by providing mutual authentication, the authors were able to tackle the wireless communication problem in the A3 algorithm, such as eavesdropping, and make the system more secure. Gope et al. (2015) suggested an enhanced protocol of Wen et al. (2013) that is resistant to a number of known attack types, including replay, forgery, known session key, backward, and forward secrecy, among others.

For safe data transmission in military heterogeneous wireless sensor networks (MHTWSN), Kumar et al. (2017) suggested a new secure multipath routing protocol (NSRP). To find trusted neighbour nodes and create secure multiple routes for dependable data delivery in MHTWSN, NSRP employs elliptic curve cryptography (ECC) (Freet & Agrawal, 2016).

A new method was presented by Pandi Vijayakumar et al., (2017) to enhance VANETs' current authentication functionality. The first privacy-preserving method in this suggested framework is anonymous authentication, which not only authenticates the vehicle user anonymously but also maintains the integrity of the communications being transmitted.

In order to implement Secure Multiparty Computation (MPC) and Fully Homomorphic Encryption (FHE) in Smart Grid (SG) Advanced Metering Infrastructure (AMI) networks that are constructed utilizing wireless mesh networks, SametTonyali et al. (2018) suggested new protocols. By encrypting the data (FHE) or calculating its shares on a randomly generated polynomial (secure MPC), the suggested methods hide the smart meters' (SMs') reading data (Kokko, 2017). The suggested approach by Sravani Challa et al. (2018) covers functionality aspects such the inclusion of dynamic sensor nodes, password and biometric updates, smart card revocation, and other standard capabilities needed for user authentication in wireless sensor networks.

Using intelligent software agents, neural networks, genetic algorithms, neuro-genetic algorithms, fuzzy techniques, rough sets, and particle swarm intelligence, Sannasi Ganapathy et al. (2013) conducted a survey on intelligent methods for feature selection and classification for intrusion detection in networks (Manda et al., 2023).

By identifying attack characteristics, Louvieris et al., (2013) introduced a novel anomaly detection technique that can be utilized to identify hitherto unidentified network attacks. To improve the situational awareness of cyber network operators, this effects-based feature identification technique integrates k-means clustering, Naive Bayes feature selection, and C4.5 decision tree classification in a unique way to identify cyberattacks with high accuracy.

3. DIFFERENT APPROACHES FOR THREATS

Deep Learning Approaches for Threat Detection:

Choosing the most cutting-edge AI models and algorithms, particularly those based on deep learning, is the first step towards the launch of next-generation AI-based firewalls. CNNs and RNNs are selected to evaluate high-level temporal and spatial characteristics and to identify indications of the emergence of new threats. These deep learning techniques aid in improving real-time threat detection capability, which in turn raises accuracy.

Integration with Cloud Infrastructure for Real-Time Analysis

The models and AI algorithms that have been chosen are seamlessly integrated into cloud platforms to enable real-time network traffic analysis. Its scalability, data processing skills, and capacity to start integration on various cloud platforms are some of the problems that need to be resolved in this regard. The deployment ensures that AI-based firewalls can maintain a continuous level of protection against threats while also utilizing cloud flexibility to scale up or down in response to demand.

Auto-Scaling Based on Network Traffic Patterns

Intelligent scaling techniques are used to scale the AI firewalls dynamically based on traffic volumes in order to handle the cloud's ever-changing nature.

Additionally, the system loads and balances incoming network traffic and boosts the firewall's power in case of a spike. This adaptive scaling feature enables the firewall to minimize resource consumption when not in use and operate at peak efficiency during periods of high traffic (Pavlović et al., 2023).

Dynamic Allocation of Resources for Optimal Performance

In order to improve AI firewall performance, it also adjusts additional dynamic resource allocations on top of the implementation. This means that CPU, memory, and network resources can be dynamically allocated based on the risks and load at any given time. The firewall operates at its best when resources are allocated flexibly, accommodating any network modifications without compromising its functionality.

Real-Time Threat Intelligence Integration

Among these is continuous monitoring, which is the implementation's main component and is aided by real-time threat intelligence feeds. As new threats emerge, the AI-based firewalls are aware of them and employ innovative tactics to combat them. By addressing newly developing cybersecurity risks, the integration of real-time threat intelligence enhances system performance.

Automated Updates to Ensure Protection against Emerging Threats

Automated update features are also included in the implementation. The threat database, security updates, and new algorithms can be downloaded and updated on a regular basis by an AI-based firewall. Without additional human intervention, this automation guarantees that the firewalls remain proactive in the face of emerging threats. Updating ensures both the longevity of the security structures and their general productivity.

Adaptability to New Threats

The NGFW is one of the most valuable resources in the current cyber environment, particularly with the move to the cloud. Since NGFWs have extra layers of functionality that are novel and solve current security challenges, this

runs counter to standard firewalls. NGFWs are essential in the context of the cloud because cloud solutions have increased the demand for all-encompassing security solutions for distributed and dynamic infrastructures. VPN technology, which provides safe remote access to cloud solutions, is another facet of NGFW. This is crucial because it protects data transmission procedures from being intercepted by unauthorized users, which is especially critical for businesses with employees from several locations. Furthermore, only authorized apps can access additional sensitive data or network zones thanks to Application Control, which enables NGFWs to regulate the apps running in the cloud environment. Other fundamental components of NGFWs that address the prompt identification and mitigation of known or emerging threats include Intrusion Prevention Systems (IPS). The typical IPS capability to detect and stop malicious activity before it happens is crucial in the cloud, where the attack surface is much greater. Along with the characteristics outlined in E-mail Security, NGFWs protect against malware and phishing attacks, which are commonly disseminated via email, which is still one of the most efficient attack vectors (Rao et al., 2022).

4. ANALYSING VARIOUS AI-BASED FIREWALL STRATEGIES

Numerous significant flaws were discovered through the analysis of different AI-based firewall tactics, which must be noted in order to progress the development of AI-based cybersecurity products. For this reason, comprehension of the outcomes of specific deep learning structures is one of the most notable deficiencies. These models include CNNs and RNNs, which are very accurate and flexible. However, it is challenging to understand how these large neural networks make decisions. Future problems and difficulty in determining the specific cause of false positive results or how the models arrived at particular hazard ratings are presented by such opacity. Because interpretability and accountability are essential in such circumstances, it is necessary to overcome this weakness if the trustworthiness of AI-based firewalls is to be decreased. One of the aforementioned drawbacks is that machine learning techniques are susceptible to the idea drift phenomena, particularly those that make use of substantial volumes of data from prior experiences. The underlying nature of threats has changed as a result of shifting cyber security conditions; new strategies and directions have

emerged. It is clear from analysing these kinds of situations that machine learning, which relies on data from earlier situations, can cause models to react slowly to novel dangers, potentially leading to a large rise in false negatives. This shortcoming highlights the need for dynamic retraining, sometimes continuous model updates, and real-time threat intelligence integration to combat the ever-evolving nature of these attacks in the context of contemporary AI-based firewalls (Neupane et al., 2018).

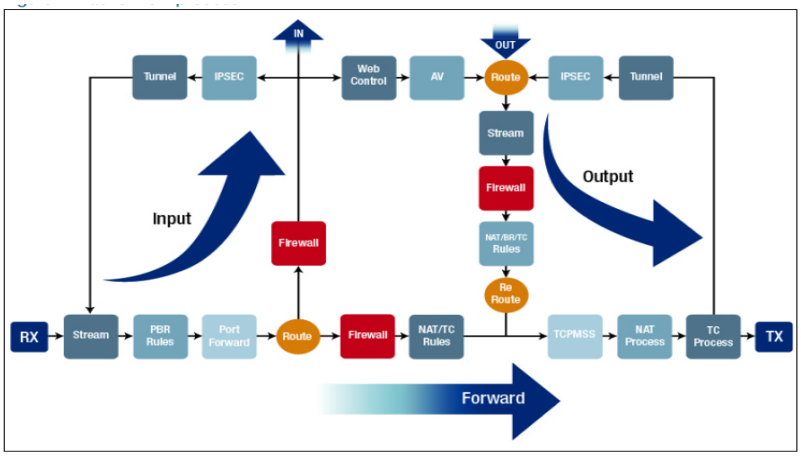

Figure 2: Packet Flow Process

Furthermore, the study exacerbated problems related to the use of specific machine learning algorithms in extensive networks. Some machine learning algorithms are unable to manage the Volume, Variety, and Velocity features of increasingly complex network structures, which results in a bottleneck and jeopardizes real-time threat identification. The practical implementation of AI-based firewalls and the adaptation of anti-malware measures to the ever-increasing demands of contemporary networks depend heavily on the issues surrounding scalability; therefore, technological advancement is required to create an AI-based firewall that can function in large and complex networks (Patel et al., 2024).

Proposed Improvements

Improving Interpretability and Transparency: Deep learning models' decision-making process can be better understood by incorporating explain ability

approaches like layer-wise relevance propagation or attention mechanisms. Generally speaking, cybersecurity experts can have confidence in the choices made by AI firewalls when they see visualizations that offer more information about the characteristics influencing the model's output.

Mitigating Concept Drift

The robustness of the AI-based firewall can be increased with the use of dynamic retraining of the model using recent datasets, continuous learning mechanisms, and the integration of threat intelligence data. Additionally, there are self-tuning algorithms that adjust the model parameters in response to new threats.

Improving Scalability

By utilizing innovative solutions created by parallel processing and computing dispersion, some of the scalability problems can be addressed. Machine learning algorithms must be developed with parallel processing in mind, utilizing cloud and edge computing technologies, in order to increase their scalability.

Fortifying Against Adversarial Attacks

AI-based firewalls would be more resilient to hostile activities if they used a range of defense techniques, regularly updated the adversarial database, and used adversarial training procedures.

Human-Centric AI Models

Through the use of AI models that mimic human behaviour patterns, threat detection becomes more accurate and employs fewer false positive modes.

Ensuring Regulatory Compliance

It would be easier to comply with the established regulatory standards if AI-based firewalls have integrated reporting and auditing functionalities. When constructing AI firewalls, legal and ethical considerations may be eliminated with the assistance of legal and regulatory experts.

4.1. Types of Attacks on a Network

Although they present some risks, networks—both intranet and internet—offer incredible opportunities. Information is vulnerable to various threats or attacks in the absence of appropriate controls. Viruses, worms, and trojans were major threats in the early days of computers, but these slowly developing threats have since been replaced by threats that spread quickly—within 15 minutes. Current attacks are far more covert than they were in the past due to the way that today's online threats are evolving. Attackers are drawn to the network's information and resources, which make them desirable targets. A network is considered secure if all of its systems and resources can withstand attacks of any kind. In the event of an attack, a system or network must be able to minimize the harm and quickly recover. Communication surveillance (passive attacks), active network assaults, close-in attacks, exploitation by the systems within the network, and attacks via the service provider are some examples of attack classifications. Below, many attack kinds are covered (Lamdakkar et al., 2024).

Passive Attacks

Unencrypted communication is watched for sensitive data and cleartext passwords in these types of attacks. Monitoring unsecured communications, traffic analysis, gathering authentication data, and decrypting traffic that has been inadequately encrypted are a few examples. Adversaries are able to predict future activities through passive interception of network processes. Without the user's consent, it could lead to the disclosure of data files or information to the attacker. Adversaries are able to predict future activities through passive interception of network processes. Such attacks are typically an effort to exploit the data that is accessible through the system. It won't negatively impact the system's resources.

Active Attack

In these types of assaults, attempts are made to get around or compromise the systems that are part of the secured networks. Trojan horses, worms, viruses, and stealth can all be used to do this. In order for the available information to be stolen or altered, attempts are made to circumvent the security measures and

install harmful code. These attacks attempt to intercept data while it is in transit or attempt to gain access to the target network by a remote user who has been granted permission. It could lead to data tampering, Denial of Service, or the distribution of data files. Usually, the goal of such assaults is to damage the system's resources and interfere with its functionality.

5. PROXY FIREWALL

In contrast to packet filter firewalls, which only examine packets without changing them, proxy firewalls serve as a mediator in all connections that are made through them between the internal and external networks. As a result, it prevents direct communication between the machine or device making the request and the one providing it. On behalf of the asking machine, the proxy server instead obtains the data from the providing machine. Additionally, it has the ability to store these data in its memory, allowing it to supply the same data upon request from another internal network device without physically visiting the computer in question. Stated differently, an internal network's systems are all represented by a single address. Other computer systems within a network can use a shared Internet connection thanks to a hardware device on the network. Clients generate requests, which are then accepted by the proxies and either sent to the server or handled by the cache. These proxies are also known as "gateway" or "server.".

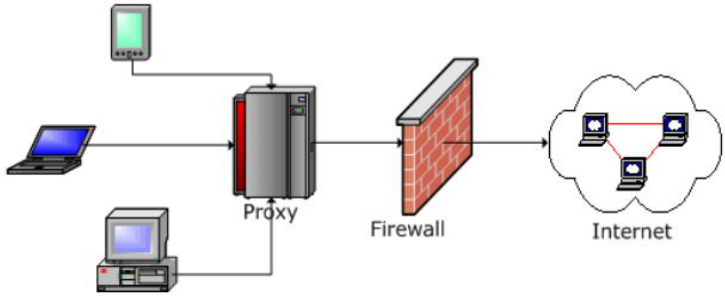

Figure 3: Proxy Firewall

Its primary purpose is to offer security from the outside network. It controls the packets entering and leaving the network. Client requests are filtered, cached, logged, and managed by firewall proxy servers. It is employed to limit connections

from a proxy to the source server within the local area network (LAN) or to the external network (internet). It differs from a traditional firewall in that it only offers one address and limits connections from the outside world. To put it simply, a proxy essentially performs the following tasks:

1) Sends the request to the server located in the external network or
2) non-trusted zone after receiving it from a system within the internal network or trusted zone (intranet).
3) Reads the server's answer to the request after receiving it.
4) Returns this response to the client if it is safe to do so.

The two primary operating layers of a proxy server are the application layer and the transport layer. As a result, they fall into two categories: circuit-level gateways, which are proxy servers that operate at the transport layer, and application gateways, which are proxy servers that operate at the application layer.

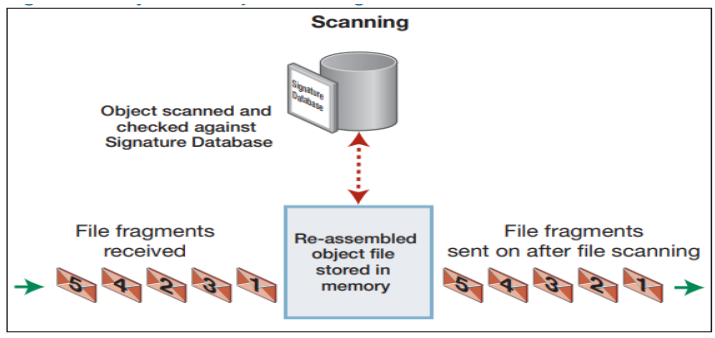

Figure 4: Proxy-based Object Scanning

5.1. Circuit Level Proxy

Similar to application-level proxy firewalls, they always establish a new connection after receiving connections from clients, rejecting some and accepting others in accordance with the policies. Although users perceive this procedure to be transparent, it is actually not as transparent as it may be. The circuit level proxy firewall was created to get around this and boost speed. Because the proxy establishes an end-to-end connection between the client and the target application, the connection between the client and the server is a virtual circuit. TCP connection relays are provided by circuit level firewall proxies. These circuit

level proxies finish the handshake procedure by intercepting the TCP connections being made to a host behind them. Traffic begins to move from the server to the client and vice versa as soon as the firewall allows a connection to be made. The firewall is in charge of making sure that only the authentic packets from the established connection pass through. Because circuit level firewalls don't verify any data or the packet's payload, they are sufficiently quick. In essence, circuit level firewalls make sure that the handshake procedure is correctly finished before the connection is established. These firewalls do not allow the use of payload data in the higher-layer conventions to restrict access, nor do they allow access confinements to be imposed on conventions other than TCP (Mukkamala et al., 2020).

5.2. Application-level Proxy

This particular proxy server firewall allows application-layer admission control. They capture the requirements that the network's applications are requesting and carry out the necessary actions to fulfil the request. All of the results are then returned to the application that made the request, verifying that it was handled correctly. As a result, the different apps are given a high degree of security without having to communicate directly with servers that are not part of the network. A separate proxy is required for service. It can thoroughly examine incoming and outgoing data packets even at the application level because it is there and functions at that level. Some apps may even be prohibited from accessing the computer network. Every communication and network action carried out by the apps is also recorded in a log. The application-level proxy flow scenario is shown in detail in figure 1.18. The firewall interprets any client request as though it were coming from the serving device.

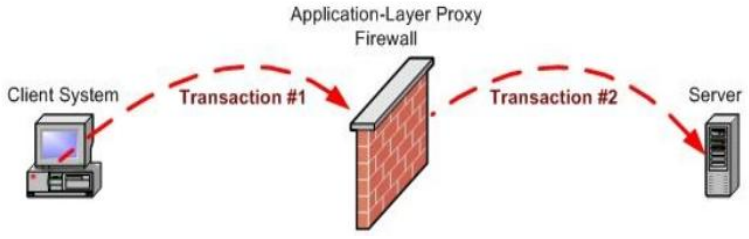

Figure 5: Application-Level Proxy Firewall

6. LATEST TECHNOLOGIES AND FIREWALL

We are no longer restricted to wired networks alone. Various technologies have been developed for network formation. Some of them have been covered below:

Wireless Sensor Networks

In order to monitor certain ecological, physical, or medical conditions, WSNs (Wireless Sensor Networks) are composed of specialized wireless sensor nodes that are spatially circulated throughout the environment. These nodes may include cameras for vision, mouthpieces for sound, and temperature sensors. WSN nodes are typically wireless, albeit they may or may not be mobile over time. A sensor, communication antenna, microprocessor, and power source make up a WSN node. A wireless sensor network is made up of these nodes that communicate with one another on the fly to send the data they have collected to a base station that serves as the network's command and control center. There are two possible modes of communication between the nodes and the base station: one-way, or simply from the nodes to the base station, or two-way. Since WSNs are frequently utilized in fields like environmental/earth sensing, air pollution monitoring, forest fire detection, health monitoring, etc., they are the most useful kind of ad hoc networks available today. WSNs serve as the foundation for many smart city initiatives and the Internet of Things which is thought to be the next major advancement in ICT after the creation of the internet, www, and smartphones. By combining data from multiple sensors, WSNs are able to gather accurate and varied environmental data across a vast area. Furthermore, the UC's scope zone and application domain are expanded by the combination of Smart WSNs with a larger network, such as the Internet. Any object that moves or is placed immobile could have sensors attached to it. Security has always been a fundamental concern in the field of networking, and wireless sensor networking scenarios are no exception. In actuality, security in this kind of setting necessitates greater emphasis than has been observed in conventional systems. Compared to typical computing scenarios, there is a far higher chance of security threats being introduced as wireless networks and other system scenarios have been integrated into computer processing environments. Security is risk management, according to. The assessment of threats, vulnerabilities, and attacks, the determination of

costs associated with the threats and the evaluation of all the different attacks given the vulnerabilities, and the development of appropriate safeguards and countermeasures are the primary areas of security attention. All of this is done based on the cost versus the likely loss that the risk will produce. The majority of experts categorize security issues into three groups. They are availability, integrity, and secrecy. Although it will take some work, it is very possible to secure these locations in distributed systems.

Cloud Computing

When data centers began offering web services like server hosting and storage, cloud computing was born. As the internet grew and increasingly large-scale client web administrations appeared, specialized cooperatives like Google, Microsoft, and Amazon realized that:

1) They are able to rent out storage that would otherwise be unnecessary.
2) Any designer can now create a dynamic biological system of uses thanks to open-source application programming interfaces (APIs), which are likely impossible for a single firm to create on its own.

The primary advantage of cloud computing is that users don't need any technical knowledge or experience with the supporting infrastructure. The goal of cloud computing is to enable the identification of computer resources (such as servers, networks, storage, apps, and services) that require little administrative work and can be rapidly and simply configured. "The National Institute of Standards and Technology (NIST) states that the service provider can also accomplish this by posting a shared pool of configurable, on-demand network access to interactive mode." Since they are the best single coherent computer with a computer server, cloud computing devices are connected to the network. Emphasis on cloud service providers in browser-based program versions to give clients total control, doing away with the requirement for ongoing computer equipment management or client licensing version upgrades.

Internet of Things

The term "ubiquitous computing" was originally used to describe what is now known as the "Internet of things." As a result, we use both terms interchangeably

in this work. One way to conceptualize ubiquitous computing is as though there are computers everywhere. After centralized computer registering and PC registering, which were introduced by at Xerox's Palo-Alto [Parc] research center in 1988, this is the third wave of processing. It is common to omit Mark Weiser as the originator of ubiquitous computing. Ubiquitous computing envisions a smart environment with autonomous computer systems and smooth communication between system entities. This processing mechanism can provide humanity with an unparalleled level of convenience and profitability. In a world known as ubiquitous computing (UC), computers are everywhere, but we are unaware of their existence. In order to allow machine-to-machine (M2M) communications and disseminate a wide range of protocols, places, and applications, ubiquitous computing is essential for recommending propelled amalgamation of devices, frameworks, and services. This idea can lead to a wide range of products, such as heart monitoring monitors, cars with built-in sensors, or field operation tools that assist firefighters in their search and protection. By making these processing devices invisible to the user, the concept of ubiquitous computing aims to promote constant collaboration with the atmosphere and available resources by making a large number of registering devices available throughout the physical world. All types of devices and sensors are seamlessly linked to wireless networks to provide users with communication and computing services. Security is primarily concerned with evaluating potential attacks in light of vulnerabilities and creating suitable defences and counters. The majority of this is carried out by weighing the cost against the possible harm that the risk could cause. The majority of experts categorize security issues into three groups. They are availability, integrity, and secrecy. Although it will take some work, it is very possible to secure these locations in distributed systems. There are restrictions on ubiquitous systems that do not apply to conventional computing. They drastically alter the security of ubiquitous computing. These limitations include energy as a source, computational power, and connectivity. Three security areas are reviewed below from the standpoint of ubiquitous computing. In the world of ubiquitous computing, most security solutions for portable devices now use a predefined configuration of algorithms and administration protocols that are insufficient.

7. IMPORTANCE OF FIREWALL

In the past, hackers were thought to be extremely talented programmers who knew every little element about the network. They succeeded in taking advantage of the weaknesses in the networks. Nowadays, though, anyone can become a hacker in a matter of minutes by using a variety of online tools. Because of this, the network had to be secured, necessitating the use of security policies that could be updated on a regular basis. Since those networks are still vulnerable to internal dangers, we cannot declare that a network that is isolated from the outside world is secure. Cutting off contact with the outside world is also not a solution. Given that firewalls are the first line of protection, security and dependability are crucial for analysing all network traffic. Networks and businesses are protected by the use of firewalls. As a result, it became the attackers' first option for investigating firewall vulnerabilities and fully exploiting them. To take advantage of its weaknesses, one must determine how the firewall, firmware, etc., is implemented. Understanding how attackers can fingerprint a firewall is essential for network security as it can aid in the development of countermeasures for firewall tactics. Additionally, how the administrator confirms that the high-level policy is enforced by the firewall policy. For instance, "the people of a department should not be able to access the database of other departments" could be the policy. This can help with firewall analysis and debugging. It is difficult to confirm that a firewall accurately verifies a policy. First, it makes sense that standards conflicts and the ensuing request affectability would ensnare the guidelines in a firewall setup. Second, a firewall approach could include innumerable components. In extreme circumstances, an Internet firewall may consist of hundreds or even thousands of standards. Third, an endeavour firewall strategy frequently includes historical decisions that were made by different chairmen for different reasons, at different periods, and for different causes. This makes it much more difficult to examine firewall arrangements. Humans are incapable of verifying several intricately linked rules. Therefore, effective methods and tools for validating firewall tactics are essential to firewall success. However, the lack of firewall arrangement checks devices severely under-assists firewall executives. The majority of firewalls on the Internet suffer from

strategy errors, according to quantitative studies. Firewall errors can be extremely costly and harmful. As a result, they might entice hackers to use these security flaws to target the network and result in large losses for companies. Firewalls have played a significant part in cloud environments as well as traditional networks. We must ensure that security and trust are upheld because cloud computing is also quickly growing in the commercial sector. In these kinds of situations, we must establish and preserve confidence. Nowadays, the majority of information is stored on the cloud and can be accessed via WSN or conventional networks. This has also drawn in hackers, who are constantly attempting to infiltrate networks and use their resources without permission, in addition to authorized users. It can occasionally result in issues for the network's authorized users. Since firewalls are the first line of defines in terms of security, security professionals have always been interested in their architecture and deployment.

8. CONCLUSION

Security is a basic concern for any computer system or network, particularly in this day and age when practically everything and everyone has some sort of network access. Unauthorized access must be prevented to host systems, network resources, user data, etc. Various firms are implementing security techniques in their computer systems for this reason. One of the simplest instruments in this section is a firewall. At the several entrance points, security policies are being established and put into effect. Their primary focus is on the availability, confidentiality, and integrity of user data and network resources. In order to guarantee the security of a network or isolated system, every incoming and departing data packet must adhere to the whole security policy or set of rules. If the data packet complies with all security regulations, it can pass over the security barrier; if not, it must be dropped. Basic firewall technology checks the source and destination IP addresses, as well as the port and packet numbers. However, as network requirements grow, firewall advancements also become essential. As a result, numerous firewall kinds have developed. such as NAT PAT VPN, stateful firewall, stateless firewall, etc. Because technology has advanced so rapidly, firewalls now play an important role. Because of this, firewalls have a lot of work to do. In some way, this has made firewalls less effective.

REFERENCES

[1] Jaggernauth, E., & Rocke, S. (2021). Effectiveness of Paired Next Generation Firewalls in Securing Industrial Automation and Control Systems: A Case Study. *West Indian Journal of Engineering*, 4-10.

[2] Liang, J., & Kim, Y. (2022, January). Evolution of firewalls: Toward securer network using next generation firewall. In *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 0752-0759). IEEE.

[3] Gudimetla, S., & Kotha, N. (2017). Firewall Fundamentals-Safeguarding Your Digital Perimeter. *Neuro Quantology*, *15*(4), 200-207.

[4] Audin, G. (2004). Next-gen firewalls: what to expect. *Business Communications Review.*, *34*(6), 56-61.

[5] Thu, S. L. (2023, November). Evaluation of the Next Generation Firewall with Breach and Attack Simulation. In *Conference on Innovative Technologies in Intelligent Systems and Industrial Applications* (pp. 253-271). Cham: Springer Nature Switzerland.

[6] Lei, S. (2024, June). Synergizing next-generation firewalls and defense-in-depth strategies in a dynamic cybersecurity landscape. In *International Conference on Computer Network Security and Software Engineering (CNSSE 2024)* (Vol. 13175, pp. 143-149). SPIE.

[7] Singh, L., & Singh, R. (2023). Comparative Analysis of Traditional Firewalls and Next-Generation Firewalls: A Review. *Latest Trends in Engineering and Technology*, 15-27.

[8] Fathia, A., & Blessing, E. (2024). Machine Learning Algorithms for Anomaly Detection in Next-Gen AI-Based Firewalls: A Performance Analysis.

[9] Ilyasov, I. (2024). Deploying Firewall Protection and Security Protocols. *Innovative Science*, (12-2-1), 50-52.

[10] Islam, M. S., Uddin, M. A., Hossain, D. M. D., Ahmed, D. M. S., & Moazzam, D. M. G. (2023). Analysis and evaluation of network and application security based on next generation firewall. *International Journal of Computing and Digital Systems*, *13*(1), 193-202.

[11] Freet, D., & Agrawal, R. (2016). Network security and next-generation firewalls. In *Proceedings of International Conference on Technology Management (ICTM 2016)* (p. 23).

[12] Kokko, K. (2017). Next-generation firewall case study.

[13] Manda, J. K. (2023). Next-Generation Firewall Technologies for Telecom: Evaluating Advanced Firewall Technologies and Their Role in Protecting Telecom Networks from Evolving Cyber Threats.

[14] Pavlović, M., Zajeganović, M., & Milivojević, M. (2023). Implementation of Next-Generation Firewalls in Modern Networks. *Recent Advances in Information Technology, Tourism, Economics, Management and Agriculture*, 19.

[15] Rao, S. D. P. (2022). Mitigating Network Threats: Integrating Threat Modeling in Next-Generation Firewall Architecture.

[16] Neupane, K., Haddad, R., & Chen, L. (2018, April). Next generation firewall for network security: a survey. In *SoutheastCon 2018* (pp. 1-6). IEEE.

[17] Patel, U. (2024). The role of next-generation firewalls in modern network security: a comprehensive analysis. *International Journal of Advanced Research in Engineering and Technology (IJARET)*, *15*(4), 135-154.

[18] Lamdakkar, O., Ameur, I., Eleyatt, M. M., Carlier, F., & Ait Ibourek, L. (2024). Toward a modern secure network based on next-generation firewalls: recommendations and best practices. *Procedia Computer Science*, *238*, 1029-1035.

[19] Mukkamala, P. P., & Rajendran, S. (2020). A survey on the different firewall technologies. *International Journal of Engineering Applied Sciences and Technology*, *5*(1), 363-365.