Section A-Research paper
ISSN 2063-5346

Security Threats in Traditional Firewall and Their Mitigation Using Next Generation Firewall

Simarpreet Singh[1], Dr. Jagroop Kaur[2]
Department of Computer Engineering, Punjabi University, Patiala, simarpreeet23@gmail.com
Department of Computer Science and Engineering, Punjabi University, Patiala, jagroop_ce@pbi.ac.in
DOI: 10.48047/ecb/2023.12.si4.1532

***Abstract*—The author of this paper conducts a comprehensive analysis of firewall systems for network security. In some cases, a firewall is unable to completely protect against all risks brought on by unauthorised access to a network. The author gave a brief overview of attacks that still take advantage of networks after firewall implementation. As a result, NGFW Pfsense is used to build a secure network employing a variety of infrastructure types. By utilising the three stages of the firewall and thoroughly inspecting each data packet to determine whether any were tampered with during transmission, NGFWs offer policies for the network's protection. A thorough investigation of several firewalls has previously been conducted and is briefly presented in this paper.**

Keywords— ***Firewall, Network Security, Next Generation firewall, pfsense.***

I. INTRODUCTION

Everyone is aware that the firewall is a network security technology that defends the network and makes an effort to control both valid and hostile traffic using some of its rules. The firewall regulates the data packets' validity and offers defence against both incoming and outgoing traffic. A firewall necessitates both outbound and incoming rules in order to guarantee the security of data packets and traffic. One antivirus programme cannot ensure a device's integrity. It will have a competitive advantage thanks to the firewall. Antivirus software protects a device's assets, but a firewall also guards its network-based services. Machines within the network that are less protected are more likely to have security flaws, and because of these vulnerabilities, there is a danger of cyber-attacks increases [1][2].

Cyberattacks frequently target sensitive data, putting both the security and integrity of the data at risk. As an illustration, suppose that on November 23, 2022, hackers gain access to five of AIIMS Delhi's physical servers, compromise data, and briefly shut down online services [3][4].

Firewalls are necessary to protect and provide access to medical equipment connected to the network and electronic health data from both inside and outside the network. In reality, the first line of defence for the security of healthcare systems has always been firewalls. An effective firewall must always act as a filter for both incoming and outgoing traffic. Two environmental considerations that affect a firewall system's effectiveness are where it is located and the type of data that needs to be protected[1]. Users should never encounter any issues while trying to access resources that the firewall has blocked. More specifically, in comparison to other systems, smart healthcare designs must take into account a patient's life-critical data, financial implications, and data governance compliance rules, all of which call for additional resources [2] [5][6][7].

Cybersecurity threats are constantly growing in scope. The effective and efficient use of firewalls reduces the impact of cyber threats on network infrastructures. It's critical to correctly implement firewalls if you want to defend yourself from attacks and dangers [8][9].

Despite having a number of advantages and benefits, firewalls remain open to attacks. This article examines the most common firewall types and their applicability for network environments. We also provide a quick overview of different firewall types, their operational principles, and vulnerabilities. We conclude by listing the problems with conventional firewalls that have not yet been fixed and making recommendations for securing networks with Next-Generation firewall. The ideal firewall will increase security and trust while preserving the confidentiality and privacy of patient data [10][11][12].

II. SECURITY CHALLENGES OF ENTERPRISES & MEDICAL INSTITUTES

The security issues that businesses and medical facilities encounter are explained in this section. As we all know, modern hospitals and businesses are very well furnished with a wide range of high-tech equipment that is either used to monitor the patient's condition or while carrying out any type of surgery. Businesses also employ high-tech infrastructure for storing data from various users. In

Section A-Research paper
ISSN 2063-5346

hospitals, these devices provide a lot of data that is essential for diagnosing patients; if this data is altered by a criminal, a patient's life could be at risk. The utmost importance must be given to maintaining the data's security and integrity. Lack of or inadequately implemented security in healthcare facilities has a detrimental impact on patient data, privacy, and vulnerability to numerous attacks [2] [13][14].

One of the most significant and difficult issues facing the healthcare system and businesses today is cyber-attacks. Healthcare devices must maintain full service availability since any service interruptions pose a risk to the patient's life. Common dangers to the networks of businesses and medical facilities include: [15][16].

A. SQL Injection:

SQL injection is one of the most widely used hacking techniques. The "SQL injection" technique is used to access user credentials from web page inputs by adding SQL instructions as statements[3]. In essence, malicious individuals can use these assertions to affect the application's web server and harm any of the specified organizations or users Table 1.[17][18]

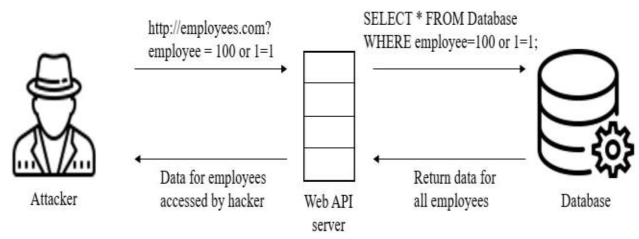

Fig I. SQL injection attack

The use of this code injection technique could destroy any database. Input from a web page can be used to inject malicious code into SQL statements, as seen in figure. [4] [19][20].

Table 1. Real life cases of SQL Injection attack

Date	Target	Impact
2017	Equifax (credit bureau company)	In this attack personal data of around 143 million customers get compromised. This is one of the Major data breach occurred during that time in America.
2015	Vtech (toy manufacturing company)	In this, data of 200000 children and around 5 million adults have been compromised to the attacker. Attacker didn't leak that data anywhere but warns the company about loopholes.
2008	Myspace	Data of 360 million customers get stolen which include emails, names of the customers and their passwords.

B. Man in the middle attack (MITM):

Three players are necessary for a man-in-the-middle attack. There is the victim, the application victim is attempting to interact with, and the "man in the middle" who is listening in on their conversations as listed in Figure 2. This type of attack allows perpetrator to intercept, send, and receive data that was meant for someone else.[4][21][22].

MITM attacks are broken down into various categories as listed in Table 2.

Table 2. Types of MITM attacks

Sr.No	Types	Purposes
1	Eavesdropping	1. A hacker watches how users behave. 2. Access to a user's machine is possible for perpetrator.
2	DNS Spoofing	Information about and access to the user's sensitive data.
3	Email Hijacking	1. To deceive a user into downloading malicious software, they might use spear-phishing. 2. Spoof an online acquaintance with the use of data from a hacked email account.
4	Session Hijacking	1. A session cookie is acquired by the attacker. This may possible when user's machine is exploited by any malicious code.

Section A-Research paper
ISSN 2063-5346

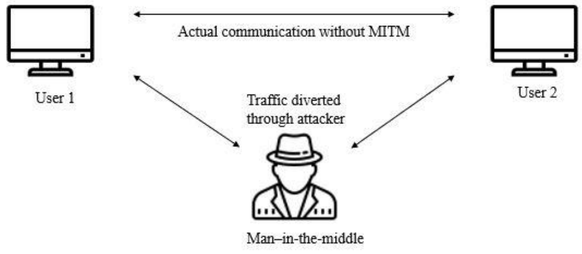

Fig 2. Man in the middle attack

C. DDOS (Distributed Denial of services):

DDOS occurs when legitimate users are unable to access a website because of traffic congestion. Online services are the target of attacks that result in a distributed denial of service[4]. As seen in Figure 3, the goal is to overwhelm them with traffic that the server or network cannot handle. Access to the website or service is intended to be blocked. Because they exploit a huge number of openly vulnerable computer systems as attack traffic sources, DDOS attacks are especially effective. Machines that are being misused include computers and other connected resources, such as Internet of Things (IoT) devices. A DDOS assault results in denial of service, which is similar to unforeseen traffic jams obstructing the road and preventing regular traffic from reaching its destination. There are many real-life cases in which DDOS attack is used to disrupt the accessibility of web services. Some of those cases are listed in Table 2 [23][24][25].

DDoS attacks are broken down into several categories:

- *Volume-based attacks:* Attacks are carried out by saturating the network bandwidth with traffic '[26][27].

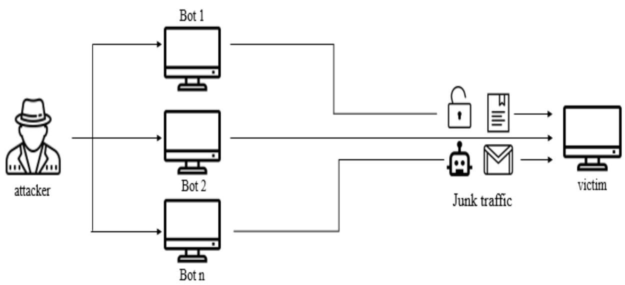

Fig 3. DDOS attack

- *Protocol attacks:* These are more focused and take advantage of resource issues in a server [28][29].
- *Application attacks***:** This kind of attack is thought to be the most harmful and effective because it targets web applications [30][31].

Table 2. Real life cases of DDOS attacks

Date	Target	Impact
October 2020	Google	The attacker tricked 180,000 vulnerable CLDAP (Connectionless Lightweight Directory Access Protocol), DNS, and SMTP servers over several networks at a rate of 167 Mpps causing those servers to give large responses
February 2020	Amazon web services	In this Connectionless Lightweight Directory Access Protocol (CLDAP) reflection technique is used. The three-day attack peaked at an astonishing 2.3 terabytes per second with disruption of services all over the world damaging revenue and value of brand.
February 2018	GitHub	GitHub attack used memcached DDoS, no botnets were utilized. Instead, the attackers took advantage of the memcached database caching system's amplifying impact. The hackers were able to amp up their assault by a factor of around 50,000 times by saturating memcached servers with bogus queries. It lasts about 20 minutes.

D. Ransomware

Access to files on a computer is restricted by malware known as ransomware[5]. This kind of attack encrypts the victim's files, and the attacker then demands payment from the victim to decrypt those files, as seen in Figure 4. The simplest option to recover those encrypted files is to pay money in order to obtain the decryption key because those files are crucial to the user or the operation of an organization. This is the rationale driving an increasing number of criminals to employ ransomware to demand money from businesses. Many varieties of ransomware have added other features, like data stealing, to provide victims additional incentive to pay the ransom. Recent ransomware

ISSN 2063-5346

attacks have negatively impacted hospitals' ability to provide care, disrupted public services, andseriously hurt a number of different enterprises as listed inTable 3.

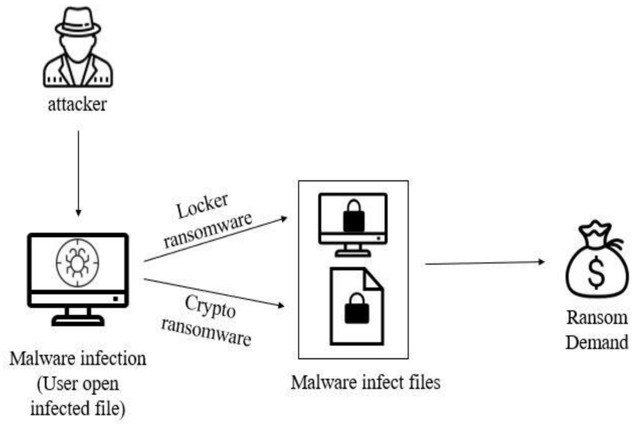

Fig 4. Ransomware attack

There are two types of ransomwares:

- *Locker ransomware:* Locker ransomware makes computer systems completely inaccessible. This variation infiltrates systems using social engineering strategies and credentials that have been compromised. Attacker prevent users from using it until a ransom is paid. Generally, a pop up message appears which tells the victim to pay the ransom amount in order to get access to their system[6][7].

- *Crypto ransomware:* Compared to locker ransomware, crypto ransomware is more prevalent and common. It encrypts all or portion of the computer's files and asks the victim to pay a ransom in exchange for the decryption key. Some more recent variations also infect networked, cloud, and shared storage. Various channels, such as phishing emails, rogue websites, and downloads, are used to distribute crypto ransomware[6][7].

Table 3. Real life cases of ransomware attacks

Date	Target	Impact
August 2021	Accenture	In this attack, perpetrators from Accenture's network stole around six terabytes of data. After that attacker allegedly demanded 50 million dollars from the company in order to give access of data back to company.
April 2021	Apple	Perpetrators stole blueprints of new apple devices from company. Attacker pledged to keep disseminating files taken from Apple until business paid a $50 million ransom demand.
June 2021	JBS (Food processing company)	The attack caused interruption at all JBS USA plants, including those that were devoted to producing pork and poultry. All JBS-owned beef processing plants in the US were temporarily shut down. Around 7000 Australian employees of JBS were "stood down". Finally, JBS paid 11 million dollars to the attackers.

III. PREVENTIVE MEASURE FROM SECURITY THREATS

As we know there are many security threats to aur networks. These threats can cause severe damage to our networks so the best way to save our network from these attacks by preventing those attacks from happening to our systems. Some of the preventive measures for these attacks are listed in Table 4. [32][33][34].

Table 4. Network attacks and their preventions

Attack	Description	Prevention
SQL Injection	Attacker uses dynamic queries concatenated with strings to get access the database of user	1. cease using string concatenation in dynamic queries. 2. Utilizing Stored Procedures That Are Properly Built 3. stop harmful SQL in user-supplied input from changing the logic of the executing query.
Man in the middle	Offender intervenes in a chat between a client and a program to either listen in on the conversation or act as one of the parties.	1. only visit websites having secure connection i.e.https://. 2. Use of Virtual private networks (VPN). 3. Endpoint security must be up-to-date. 4. Multi-factor Authentication (MFA) can be used to increase level of security.

ISSN 2063-5346

Distributed Denial of Service (DDOS)	when perpetrator's actions prevent legitimate users from accessing information systems, network resources or devices by overflowing the traffic handling capacity of attacked web service.	1. using multi-level protection techniques that make use of threat management and intrusion prevention systems. 2. use of micro-segmentation to protect zones independently. 3. Conduct a network vulnerability assessment
Ransomware	It is malware that restricts or disables user access to the system, either by locking the system's screen or by encrypting the user's files, in exchange for a ransom.	1. Backing up of data on cloud servers or external hard drives. 2. use of antivirus software and firewall. 3. use of network segmentation. 4. Application Whitelisting and endpoint security.

IV. FIREWALL TYPES FOR ENTERPRISES

The first line of defence against serious threats is a firewall, which separates internal networks from external networks and affects both traditional and new networks. By putting in place a strong set of security policies and rules, it is feasible to keep those systems secure and protect entire companies. By filtering, regulating, and managing all traffic sent and received from PCs, Local Area Networks, or Wide Local Area Networks, firewalls play a significant part in protecting against unauthorised intrusions and external attacks. Firewalls are either hardware or software devices that filter and control the data that is delivered from the internet to a private network or a single computer[8]. Only data deemed safe and harmless is permitted through firewalls to inbound or outbound. Each computer is given an IP address, which is used in a series of internet protocols to facilitate the transfer of data. That data is also known as "data packets".

A received packet is often compared to a predetermined rule, and depending on what is specified in the rule, it may be discarded or sent. Also referred to as packet filtering, this technique. This method permits dynamic packet filter rule generation, in contrast to stateful inspection firewalls, which build packet filter rules statically and show an expiry time. The choice of a firewall with a clear set of rules and the proper setup considerably reduces the impact of an attack on the institute's network.

A. Packet filtering:

A packet filtering firewall is the most basic kind of firewall.in this, set of rules are constructed and implemented on the network connection to allow or reject the traffic using the Internet Protocol (IP). This firewall is very simple to set up and may assist in filtering out all unwanted traffic, including malicious packets sent across risky ports and the origin of a potential assault. However, this does not guarantee complete network security because the protocol rules of packet filtering firewalls are largely reliant on IP addresses[9]. Another issue is that IP packet filters are often stateless, which prevents the packets from remembering and preserving any prior traffic data. This is bad because we can't manage and protect our network properly if there is no packet memory. Due to these factors, this form of firewall is only successful when fundamental network rules are used to allow or block specified hosts, such as business partners [35].

B. Stateful Inspection

Stateful Inspection firewalls function at the OSI model's session layer. In order to manage risks from packet to packet simultaneously, Stateful Inspection may maintain all previously processed packet information and examine information of incoming and outgoing packets.[10] Because of this, this firewall is frequently referred to as a dynamic packet filtering firewall. The easy modification of the internal network, which enables network managers to define certain ports they want to remain open, is one possible advantage of using this firewall[11]. This eliminates the potential for spoofing and some hacking methods, including port scanning, but it does not protect against the possibility of SQL injections or buffer overflows at the application layer. Nevertheless, despite the fact that SI firewalls provide effective network security, some possible problems include the poor network performance when they are not regularly overseen and managed.

C. Application proxy firewalls

Nowadays, this kind of firewall is the most effective. It works at application layer of OSI model. It adheres to the Stateful Mechanism and also has the ability to operate as a gateway for the network, operating as a man-in-the- between the server and the client. To put it another way, this firewall forbids any packets from being transferred directly from a program to a user or vice versa. As a result, before permitting a connection to the server, the application proxy can interpret addresses and carry out any extra controls[10]. Deep packet inspection is a feature offered by the Application proxy that guards against spoofing attacks and other hacking attempts while maintaining acceptable network performance. Additionally, application proxy can prevent harmful SQL statements and other malicious web application assaults, adding a strong layer of security for various network topologies, optimum security isolation, and high degrees of anonymity. Application proxies, even though they need less upkeep than Stateful inspection firewalls, may nevertheless result in bottleneck issues and other poor network performances if they are middle not routinely examined and updated. E-commerce websites are typical examples of applications that fall within this category of firewalls[11].

D. Next Generation Firewalls (NGFW)

The term "next-generation firewall" (NGFW) refers to a system security architecture built on hardware or software that can detect and thwart complex attacks by enforcing security controls at the application or port levels.

A system component known as a next-generation firewall (NGFW) combines a conventional firewall with additional filtering features. Due to the growing number of sophisticated apps, the negative risks they bring, and the inability of traditional firewalls to adapt to various forms of online activity, this sort of firewalls have become more and more popular. NGFW is a powerful firewall because it employs intricate intrusion prevention systems (IPS) and has the capacity to operate independently of OSI layer levels 2 through 7.[12].

Next generation Firewalls also allows website filtering, bandwidth analysis and antivirus inspection. There is no doubt that NGFW provides very flexible way to secure our network and it is currently the best class of firewalls but it must include some extra features like URL filtering, stronger QoS optimization, data leak protection. NFGW has frequently been viewed as a very sophisticated system that necessitates large expenditures to be effective and has several features that are not required by many enterprises.

Each type of firewall has its certain advantages and disadvantages which are listed in Table 5.

Table 5. Advantages and Disadvantages of various firewalls

Sr.no	Type	Advantages	Disadvantages
1	Packet filtering	Simple to configure efficient packet processing	It is impossible to secure the whole network. Attack potential due to false firewall settings. cannot filter at the application layer.
2	Stateful inspection	fewer open ports and the ability to manage multiple packets. effective threat management and the capacity to thwart assaults, particularly DDoS attacks, on data packets and memory.	high level of expertise in configuring it Risk of network problems if routine maintenance is neglected. Ineffective in protocols with no state.
3	Application proxy	able to act as a "man-in-the-middle" for the network. Detailed packet analysis.	Network slowdown risk if not regularly maintained
4	Next generation firewall	compatibility with intrusion detection and prevention systems, access control list functionality, and cutting-edge threat intelligence	Complexity is so high and a need for large investments. Some features are not designed for use in typical network situations.

How NGFW is better than other prominent firewall?

There are many weaknesses in different firewalls mentioned in Table 6. Perpetrators exploit those weaknesses to achieve their motives. Due to this, NGFW are used because they are very flexible and have ability to use wide variety of techniques to secure any network from hostilities mentioned in Table 7.

Table 6. Weaknesses associated to different firewalls for various network attacks.

Sr.No.	Attack	Firewall	Weakness
1	SQL Injection	Packet filtering	Only source and destination IP address is checked. If source is trusted, it allows data to pass otherwise not.

Section A-Research paper
ISSN 2063-5346

			But malicious data come from trusted source easily passes the firewall.
		Application proxy firewall	We can bypass application firewall by: 1. integrate malicious command with comments 2. insertion of special character
2	DDOS attack	Stateful inspection	Perpetrator send SYN message for connection for which server acknowledge it by sending SYN-ACK message but because user is not legitimate it never responds back with ACK led to TCP state table remain open for certain period.
		Application proxy firewall	Flooding attacks using botnets. Each request from bot seems legitimate.
3	Ransomware	Packet filtering	Perpetrator uses fragmentation of packets and by showing itself as legitimate source, sends malicious packets to the destination.
		Application proxy	Spear fishing emails technique is used to get access to the victim's machine

Table 7. Solutions for preventing network threats in NGFW

Sr.No.	**Attack**	**Next Generation Firewall (Ngfw)**	**Solution Proposed**
1	SQL injection		Deep packet inspection (DPI) [13]
2	DDOS attack	Pfsense	Utilizing clever rulesets that dynamically examine data packets in accordance with the set of specified rules
3	Ransomware		Content filtering.

After comparing Table 6 with Table 7 we can say that NGFW is far superior than other firewall. This is because NGFW are type of firewall which act as a complete package in which we can use multiple techniques to overcome almost all kind of security threats. This kind of flexibility is not available in any other kind of firewall. Hence, if we use NGFW to improve the security of any network it works more effectively to perform its operations because now network engineer has more option which are readily accessible by him, either in the form of software or by writing policies. Author mentions only pfsense NGFW because it is open source. Anyone can use this firewall to protect its network with all the advantages it has without paying any money.

V. DISCUSSION AND FUTURE SCOPE

In order to defend against network attacks, this article offers a complete taxonomy of network risks as well as various different kinds of firewalls. Packet filtering is a technique used by firewalls that is simple to install but has numerous vulnerabilities that are open to abuse. We can utilize several forms of firewalls, including application proxies or stateful inspection, to get around those issues. The complexity of these methods exceeds that of packet filtering. Although these methods can safeguard our network more effectively than packet filtering, the integrity and availability of data must still be maintained, therefore these methods do not yet provide the level of security that is necessary. As organizations become more digitally oriented, a growing volume of data is generated, necessitating the need for ever-more secure networks to prevent any unauthorized users from having an adverse impact on our operations or our data. Because of this, next-generation firewalls enter the picture, which are better than any other method at protecting and maintaining the integrity, confidentiality, and availability of data. NGFW are extremely complicated systems, and because of their intricate design, it is quite challenging for criminals to get past them. Even though NGFW are more expensive than other kinds of firewalls, a lot of people and businesses are moving towards using them these days. NGFW are adaptable by nature and may do so because of their flexibility.

Firewall makes the difference when it comes to the robust network security. NGFWs comes with the concept of Unified Threat Management (UTMs) which work as router combination with firewall policies. The author discussed about the Challenges, Type of attacks and Threats. In future if anyone wants to continue in this field of area, they may proceed with the manual policies created by the administrator so the policies cover the most of loopholes and inspect the every single packet from outside the network. Tightly coupled firewall also plays the prime role in security tightening of network. So, at last, if anyone wants to proceed in this area try to combines the tightly coupled firewall the custom-made policies firewall by which the most of the security aspects will be cover to make any network robust and secure.

VI. CONCLUSION

This reviews paper tells us that network security is crucial. It is very easy for people to get dependent on the Internet. The web is alluring; we aren't sure when we started browsing and when we finished. We need to know before we act. Cybercrime is caused by a small number of organizations that use the Internet for illicit activities; depending on the local laws and their misconduct, they may face jail time or fines.

For maintaining the network Security, we can use firewall. Different types of firewalls provide wide range of securities that they are capable of. Some firewalls are better than others but with the increase in security, complexity for developing and maintaining that firewall also increases. Currently, Next Generation Firewall are in trend and widely accepted by the businesses because the level of security provide by it is much greater than any other type. Hence in this paper author mentions certain techniques to overcomes the disadvantages of traditional firewalls by using next generation firewall.

VII. REFERENCES

[1] R. W. Anwar, T. Abdullah, and F. Pastore, “Firewall best practices for securing smart healthcare environment: A review,” Applied Sciences (Switzerland), vol. 11, no. 19. MDPI, Oct. 01, 2021. doi: 10.3390/app11199183.

[2] J. Beavers and S. Pournouri, “Recent cyber attacks and vulnerabilities in medical devices and healthcare institutions,” in Advanced Sciences and Technologies for Security Applications, Springer, 2019, pp. 249–267. doi: 10.1007/978-3-030-11289-9_11.

[3] Z. C. Su, S. Hlaing, and M. Khaing, “A Detection and Prevention Technique on SQL Injection Attacks.”

[4] J. M. Biju, N. Gopal, and A. J. Prakash, “Cyber Attacks And Its Different Types,” International Research Journal of Engineering and Technology, 2008, [Online]. Available: www.irjet.net

[5] B. A. S. Al-rimy, M. A. Maarof, and S. Z. M. Shaid, “Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions,” Computers and Security, vol. 74. Elsevier Ltd, pp. 144–166, May 01, 2018. doi: 10.1016/j.cose.2018.01.001.

[6] H. J. Chittooparambil, B. Shanmugam, S. Azam, K. Kannoorpatti, M. Jonkman, and G. N. Samy, “A review of ransomware families and detection methods,” in Advances in Intelligent Systems and Computing, 2019, vol. 843, pp. 588–597. doi: 10.1007/978-3-319-99007-1_55.

[7] I. A. Chesti, M. Humayun, N. U. Sama, and N. Z. Jhanjhi, “Evolution, Mitigation, and Prevention of Ransomware,” in 2020 2nd International Conference on Computer and Information Sciences, ICCIS 2020, Oct. 2020. doi: 10.1109/ICCIS49240.2020.9257708.

[8] A. Hussain, “Use Of Firewall And Ids To Detect And Prevent Network Attacks,” International Journal of Technical Research & Science, vol. 3, no. IX, Oct. 2018, doi: 10.30780/ijtrs.v3.i9.2018.002.

[9] A. Chaudhary Muzammil and R. Nandan, “Comparative Analysis of Packet Filtering Firewall,” 2019. [Online]. Available: www.ijsrcsams.com

[10] P. Priya Mukkamala and S. Rajendran, “A Survey On The Different Firewall Technologies,” 2020. [Online]. Available: http://www.ijeast.com

[11] R. Alsaqour, A. Motmi, and M. Abdelhaq, “A Systematic Study of Network Firewall and Its Implementation,” IJCSNS International Journal of Computer Science and Network Security, vol. 21, no. 4, 2021, doi: 10.22937/IJCSNS.2021.21.4.24.

[12] Institute of Electrical and Electronics Engineers, SoutheastCon 2018 : St. Petersburg, FL., Apr 19th - Apr 22nd, 2018.

[13] J. Liang and Y. Kim, "Evolution of Firewalls: Toward Securer Network Using Next Generation Firewall," 2022 IEEE 12th Annual Computing and Communication

Workshop and Conference (CCWC), 2022, pp. 0752-0759, doi: 10.1109/CCWC54503.2022.9720435

[14] Narayan, Vipul, et al. "Severity of Lumpy Disease detection based on Deep Learning Technique." 2023 International Conference on Disruptive Technologies (ICDT). IEEE, 2023.

[15] Chaturvedi, Pooja, Ajai Kumar Daniel, and Vipul Narayan. "Coverage Prediction for Target Coverage in WSN Using Machine Learning Approaches." (2021).

[16] Narayan, Vipul, A. K. Daniel, and Ashok Kumar Rai. "Energy efficient two tier cluster based protocol for wireless sensor network." 2020 international conference on electrical and electronics engineering (ICE3). IEEE, 2020.

[17] Narayan, Vipul, et al. "Enhance-Net: An Approach to Boost the Performance of Deep Learning Model Based on Real-Time Medical Images." Journal of Sensors 2023 (2023).

[18] Narayan, Vipul, et al. "To Implement a Web Page using Thread in Java." (2017).

[19] Narayan, Vipul, A. K. Daniel, and Pooja Chaturvedi. "E-FEERP: Enhanced Fuzzy based Energy Efficient Routing Protocol for Wireless Sensor Network." Wireless Personal Communications (2023): 1-28.

[20] Narayan, Vipul, et al. "Deep Learning Approaches for Human Gait Recognition: A Review." 2023 International Conference on Artificial Intelligence and Smart Communication (AISC). IEEE, 2023.

[21] Narayan, Vipul, and A. K. Daniel. "CHHP: coverage optimization and hole healing protocol using sleep and wake-up concept for wireless sensor network." International Journal of System Assurance Engineering and Management 13.Suppl 1 (2022): 546-556.

[22] Narayan, Vipul, et al. "FuzzyNet: Medical Image Classification based on GLCM Texture Feature." 2023 International Conference on Artificial Intelligence and Smart Communication (AISC). IEEE, 2023.

[23] Narayan, Vipul, and A. K. Daniel. "Energy Efficient Protocol for Lifetime Prediction of Wireless Sensor Network using Multivariate Polynomial Regression Model." Journal of Scientific & Industrial Research 81.12 (2022): 1297-1309.

[24] Narayan, Vipul, and A. K. Daniel. "CHOP: Maximum coverage optimization and resolve hole healing problem using sleep and wake-up technique for WSN." ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal 11.2 (2022): 159-178.

[25] Narayan, Vipul, and A. K. Daniel. "IOT based sensor monitoring system for smart complex and shopping malls." International conference on mobile networks and management. Cham: Springer International Publishing, 2021.

[26] Narayan, Vipul, and A. K. Daniel. "A novel approach for cluster head selection using trust function in WSN." Scalable Computing: Practice and Experience 22.1 (2021): 1-13.

[27] Gupta, Sandeep, Arun Pratap Srivastava, and Shashank Awasthi. "Fast and effective searches of personal names in an international environment." Int J Innov Res Eng Manag 1 (2014).

[28] Awasthi, Shashank, Naresh Kumar, and Pramod Kumar Srivastava. "An epidemic model to analyze the dynamics of malware propagation in rechargeable wireless sensor network." Journal of Discrete Mathematical Sciences and Cryptography 24.5 (2021): 1529-1543.

[29] Tyagi, Neha, et al. "Data Science: Concern for Credit Card Scam with Artificial Intelligence." Cyber Security in Intelligent Computing and Communications. Singapore: Springer Singapore, 2022. 115-128.

[30] Kumar, Neeraj, et al. "Parameter aware utility proportional fairness scheduling technique in a communication network." International Journal of Innovative Computing and Applications 12.2-3 (2021): 98-107.

[31] Srivastava, Arun Pratap, et al. "Fingerprint recognition system using MATLAB." 2019 International conference on automation, computational and technology management (ICACTM). IEEE, 2019.

[32] Awasthi, Shashank, et al. "A New Alzheimer's Disease Classification Technique from Brain MRI images." 2020 International Conference on Computation, Automation and Knowledge Management (ICCAKM). IEEE, 2020.

[33] Ojha, Rudra Pratap, et al. "Controlling of Fake Information Dissemination in Online Social Networks: An Epidemiological Approach." IEEE Access 11 (2023): 32229-32240.

[34] Srivastava, Swapnita, and P. K. Singh. "Proof of Optimality based on Greedy Algorithm for Offline Cache Replacement Algorithm." International Journal of Next-Generation Computing 13.3 (2022).

[35] Srivastava, Swapnita, and P. K. Singh. "HCIP: Hybrid Short Long History Table-based Cache Instruction Prefetcher." International Journal of Next-Generation Computing 13.3 (2022).