International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/IJSRCSEIT

Security and Performance Enhancement of Network by Integration of Firewall Mechanism with Advanced Encryption System

Dr. Dinesh Gupta[1], Er Krishan Kumar[2], Renu[3]
[1]Principal of JCDM College of Engineering, Sirsa, Haryana, India
[2] Assistant Professor, Department of CSE, JCDM College of Engineering, Sirsa, Haryana, India
[3] M.Tech. Scholar, Department of CSE, JCDM College of Engineering, Sirsa, Haryana, India

Article Info

Publication Issue :
Volume 8, Issue 6
November-December-2022

Page Number : 643-652

Article History
Accepted: 10 Dec 2022
Published: 30 Dec 2022

ABSTRACT

Due to growing demoing of networking there remains need of data security. There are different type of threat to data that is travelling over network. Different researcher have proposed firewall mechanism to filter the un authentic transmission while some researcher focused on data encryption to convert plain text in cipher text. Encryption makes the data secure from being understood by unauthentic user but it does not provide security to data at the time of denial of services or packet dropping. However firewall protects data in such cases but integration of firewall and encryption reduces the system performance. Thus there is need to focus of research where performance should be enhanced while integration of encryption and firewall.

Keywords : Firewall, Encryption, Decryption, Security, Performance

I. INTRODUCTION

1.1 Firewall

A firewall is a kind of network security software that is used to monitor incoming and outgoing network traffic and make decisions about whether or not to allow or refuse that traffic based on a predetermined set of security criteria. Since the beginning of the information technology age, firewalls have served as the first and most important line of protection for computer networks. It is possible to use either a firewall that is software-only or one that is hardware-based. Firewalls are used to prevent outside hackers from accessing a network by blocking potentially destructive or unwanted network activity. Firewalls prevent malicious software from accessing private information on computers and networks that are linked to the internet. The usage of proxy server firewalls, packet filters, and stateful inspection firewalls are three of the most prevalent kinds of firewalls that businesses use to secure their data and equipment from dangers originating from the outside world. First, we will provide you with a brief summary of each of them individually. A trustworthy computer system or network is shielded from untrusted connections from the outside world, such as the Internet. Although it is a physical barrier, a firewall functions more like an electronic filter, since it restricts the data that may travel through it to just that which can be trusted. Certain firewalls will allow traffic from any IP address, with the exception of IP addresses that are included on a blacklist.

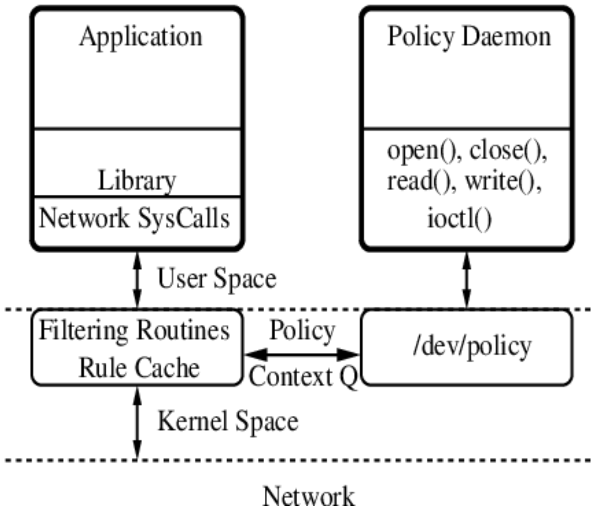

Fig 1 Block Diagram of Firewalls

1.2 Security of Digital Data In Cloud Using Encryption Mechanism

There have been many instances in which data stored in the cloud has been encrypted for security purposes. To put it another way, cryptography is the study of secure communication technologies that allow a message to be read only by its sender and its recipient. These technologies are studied under the umbrella term "cryptography." The origin of the term "kryptos" may be traced back to the Greek word "kryptos," which means "hidden." An intercepted signal may be decoded and interpreted by third parties that have access to all of the necessary information. In the course of the suggested research, polynomial encryption has been used, and it has been contrasted with various alternative encryption strategies, including RSA and AES.

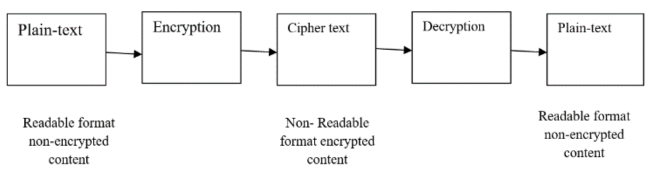

Fig 2 Data encryption

1.13 Threats to Security

It is imperative that companies be aware of the possible risks posed by the internet. According to study conducted by the Cloud Security Alliance, the following are some of the most significant risks associated with cloud computing:

a) **Data breaches:** Sensitive information may be primary target of an attack in which sensitive information is accessed, stolen, or exploited by an unauthorized user. Examples of sensitive data include health information, financial information, personal identification information, and intellectual property information.
b) **Insufficient identity, credential and access management:** If credentials are not securely safeguarded, they might be at risk of being compromised by an attack. Unauthorized users run the risk of having data viewed, updated, or destroyed without their knowledge.
c) **Insecure interfaces and APIs:** Companies make use of a collection of application programming interfaces, often known as APIs, which are supplied by cloud service providers in order to manage and interact with cloud services. In addition, customers and users of third-party applications commonly make use of these interfaces in order to provide services to the consumers they serve. Unauthorized users are able to access and make use of them in their own projects. They could be able to communicate data, get permissions, and retain records. It's also feasible that they might be able to keep records.
d) **System vulnerability:** Applications that are operating on a system might have vulnerabilities that can be exploited, which can lead to security breaches. By penetrating the system, an adversary might potentially get access to confidential information and cause disruptions to service operations.

e) **Account or service hijacking – using stolen passwords:** Abuse of high-level privilege accounts is possible via the use of account hijacking or the taking over of services. It is standard practise for fraudulent activities, such as phishing and other types of attack that exploit software security vulnerabilities, to make use of stolen passwords.

f) **Malicious insider:** It is possible for a malicious insider to get access to the sensitive data of the system administrator or even to take control of the cloud services at a higher level without being detected at any point. A malicious insider may be responsible for damage to the company's brand, as well as financial losses and productivity losses.

g) **Data loss:** The inherent hazards of the cloud, in conjunction with the architectural characteristics of cloud applications, might combine in ways that can result in the loss of data that is stored on the cloud. Anyone who has access to the data has the ability to remove or make changes to the records of the organisation.

h) **Lack of due diligence:** Most cloud service providers have a robust system set up for doing due diligence on cloud technologies. When businesses choose service providers without carefully evaluating the technology and the risks connected with it, they put themselves in harm's way and risk losing customers and revenue.

i) **Abuse and nefarious use of cloud services:** A "threat" occurs when someone uses cloud computing resources to launch an attack against users, companies, or other cloud service providers. DDoS attacks, email spam, phishing, and breaking into password databases are just a few of the most popular entry points.

j) **Shared technology vulnerabilities:** Cloud service companies provide their services by sharing hardware and software. Cloud infrastructure components may be insufficient to provide proper isolation. As an alternative explanation, flaws in a standard technology might be exploited in any distribution method.

II. Literature Review

Research on firewalls and other forms of online protection has been thoroughly examined. Researchers in several fields have used various approaches to achieve their respective goals. In this part, we will go through the results of some of the studies that were taken into consideration.

Several firewall systems, including hardware, software, and virtual solutions, were compared by Wojciech Konikiewicz (2017) in terms of performance and security. Maximum firewall throughput, additional delay, and Denial of Service attack resistance are all crucial factors to think about. In this study, we provide experimental results, conduct an analysis of the data, and make some conclusions with practical significance. Firewalls are essential to a network's security and must be present for maximum protection. They need to offer an adequate level of security without negatively impacting network speed in order to prevent packet delay from rising.

According to Richa Sharma (2017), the firewall's principal function is to protect and track the activities of its users. These modern times with their gift of the internet are lucky. Bedizens may do their jobs from anywhere with an Internet connection and at any time. E-tendering, e-commerce, and online banking are just a few examples of the many online transactions that may be conducted these days. However, as the internet expanded, people started wasting more and more time there doing pointless things like chatting, playing games, gambling, and so on. There's also the person who uses their time at the office to educate themselves in potentially harmful activities, like hacking, rather than doing actual job. Hackers can cause financial and reputational harm by breaking into a company's network and stealing sensitive information or destroying the company's infrastructure. It's bad news for the company and the founders. Therefore, the corporation has implemented a firewall in order to monitor the worker and the company's network. Firewalls are well-known as a crucial part of any network's defences. A firewall may be software, hardware, or a combination of the two, and it is used to secure networks and people all over the world. The device processes packets in both directions.

Shwetambari (2014) The purpose of this study is to investigate firewalls. You may build a firewall using either hardware, software, or a combination of the two. To prevent hackers from gaining access to private networks, firewalls are often used to secure intranets. In the context of networked computers, the term "firewall" describes more than simply a simple mechanism. It's come to be associated with certain meanings that are surprisingly grounded in reality. A firewall checks every file that enters and leaves a network for malicious code and other problems.

Name: Steven Thomason (2012) Your gateways' security might be bolstered by installing hardware and software like next-generation firewalls and sophisticated packet inspection devices. Traditional firewalls are no longer sufficient protection against modern Internet threats.

M. I. Kashefi (2013) This research classifies firewall vulnerabilities according to their natures and the various kinds of firewalls in order to provide a better perspective for future research. There is also discussion of modern approaches to preventing vulnerabilities such firewall fingerprinting, which may be used by attackers to learn more specifics about a firewall's faults in order to exploit them. Increased funding for network security devices and solutions is essential as the security threats to computer networks grow in tandem with their size. Firewalls are an essential first line of defence in keeping networks secure, and continuous improvements to this technology ensure that the internet is a safer place. It is not feasible to make changes or come up with fresh ideas unless the current methods and needs are carefully examined.

Damodharan (2018) (2018) the purpose of this article is to discuss the topic of network firewalls, which provide security for interconnected networks that wish to share data in a commercial setting. Therefore, a firewall is more permissive of both incoming and outgoing data, while also giving the impression of anonymity for FTP and website access via the internet (FTP). In recent years, there has been an increase in threats to the safety of computer networks and the internet as a whole. The constant evolution of cyber threats makes the development of adaptable and novel approaches to security a pressing issue. Protecting your digital assets is a top priority, and in this post we'll discuss some of the best practises for doing so. When properly configured, a firewall may prevent or severely limit the flow of any data over a network, whether it's destined for the inside or outside. Firewall software is the name for this kind of programme. To achieve the objectives of information security and free communication, which are crucial in a commercial setting, this kind of firewall is mostly ineffective.

In the words of Dr. Ajit Singh (2013) the authors conclude that a network firewall is beneficial for both the internal network of a corporation and any external networks that seek to exchange data over the network. A firewall's primary function is to prevent unauthorised access to private networks while still securing the flow of information over the Internet. A network's perimeter may be fortified with virtual walls to stop hackers from getting in and sensitive information from leaking out. The term "firewall" refers to a computer programme. Firewalls that prevent the free flow of information and ideas are often ineffective and unacceptable in corporate settings.

Bavithra.G.R (2018) This article discusses the importance of computer system security and provides examples of methods that may be used to protect data and hardware stored on computers. This article describes the problems and threats to network security, and shows how firewalls may be used to prevent assaults. Finally, based on a wide range of network topologies, a contrast is drawn between Packet Filter Submission Gateways and Individual Firewalls. In addition, a new approach to coercion, threat management, and network environment security is presented in the study. In recent years, there has been an increase in threats to the safety of computer networks and the internet as a whole. Because new forms of threats are always emerging, it is challenging to create security systems that are both flexible and adaptive.

According to Raed Alsaqour (2021), this investigation aims to assess the many firewalls available, their architectural design, and the security holes they may include. Reading this content may help you learn more about firewalls and their many designs. With the Internet growing at a dizzying rate, today's networks are just going to become larger. Companies are increasingly abandoning simple networks in favour of more advanced ones. Extremely private information is routinely sent via networks, making them an easy target for cybercriminals. All networks, no matter how large or little, are susceptible to a wide range of threats. Various security procedures are used by businesses to safeguard their systems against intrusion. These preventative measures are implemented throughout the board, beginning with the hardware and ending with the network. The safety of the network improves in tandem with the progress made in this area. An external firewall and an internal network firewall both provide security for the network. Firewalls' principal function is to prevent unauthorised access to networks and devices.

This is the work of Roumaissa Khelf (2018) In this research, we look at the different approaches to security policy management and how to spot and solve conflicts. In this study, we examine the pros and cons of the different approaches of verifying security policies in IPSec and firewalls. In light of this, network security has emerged as a major concern during the last decade. Hardware and software are both required for effective network security. Firewalls and IPSec gateways provide traffic control and network security by enforcing these rules. Nonetheless, security defects that risk the overall system's functioning may come from discrepancies in security policy rules, which are often hard or impossible to uncover.

It's Roza Dastres (2021) The goal of ensuring the safety and security of the internet's networks is to provide simpler communication and information sharing among its users. Due to the issues and dangers created by data in networks, IT infrastructures must take network security extremely seriously. Therefore, security measures on the network are considered so that hackers are less likely to obtain access to the confidential information. Ultimately, the goal of network security is to prevent unauthorised users from gaining access to or otherwise abusing the network and its resources. This research looks at the risks and safeguards of networks, as well as possible future research directions. Several types of network threats and the countermeasures put in place to stop them are investigated in order to make the transfer of data over the internet safer. Reading up on prior work in the field of network security systems might inspire new avenues of inquiry.

Chinese (Xinzhou) He (2021) Expansion in this era of ultra-fast networks. The safety of the system has been carefully considered. With the goal of strengthening the safety of the network. The firewall is a very useful piece of technology. The public is also curious in his development. In this article, we'll take a deeper look into firewalls. That this would inspire you in any way is my sincere wish.

S. G. Mihalos (2019) This research examines network security threats, rules, and procedures using Net filter/Iptables as a framework for implementing the firewall as a network concealing approach. The virtualization of a test-bed network happens in parallel with the creation of network security rules that are tailored to the specific services offered by the company and other factors. Finally, a network security policy is put into action using iptables technology, and its efficacy is put to the test through penetration testing. The industry as a whole now generally agrees that implementing security solutions on networking infrastructures is crucial. When business and government networks connect to the internet for the purposes of performing financial transactions and maintaining crucial data, it is critical that anti-hacking measures be put in place.

Lia Yuchong (2021) Researchers set out to take a thorough look at the various methods to cyber security and assess their advantages and drawbacks. Recent attacks by descendants are extensively analysed. Traditional security models are examined in tandem with cyber security's rich history and its first attempts to address the problem. Threats and issues in cyber security are covered, as well as developments and innovations in the field. Professionals in the fields of information technology and cyber security are likely to profit from this in-depth analysis. Cyberattacks are conducted with the intention of financially harming targets. In other cases, cyber assaults may have a military or political purpose. These losses may occur due to a number of different attack vectors, such as computer viruses, knowledge leaks, DDSs, and other similar services. In order to prevent cyber intrusions from causing havoc, many different types of organisations use many different strategies. Cyber security keeps a constant eye on the most recent IT data. Researchers from all around the world have developed a wide variety of approaches to cybercrime mitigation. Some of these methods are now in widespread usage, while others are in the exploratory stages of development.

Royal Anwar Waseem (2021) This article provides a comprehensive analysis of the merits and drawbacks of several firewall types, which may be used to the creation of rules for connected healthcare infrastructure. And there are many security risks, threats, and attacks that may occur in these environments. To prevent these problems from occurring and to keep sensitive data secure, a firewall is an essential first line of defence for smart healthcare networks. Firewalls that are hosted in the cloud and can be set up on any network may soon replace those that are housed on individual servers. Making the most of a firewall's potential advantages, however, is a complex process that calls for careful thought and implementation. Therefore, it is crucial to get an in-depth understanding of firewall types, services, and vulnerabilities before establishing a firewall in a smart healthcare setting.

Mr. Khaled Salah (2012) By incorporating a Markov chain into an analytical queuing model, rule-based firewalls may be put through their paces under realistic traffic circumstances and distributed denial of service (DoS) attacks on individual rule positions. Important aspects of design may be quantified with the help of equations we devise. When setting up a firewall, it's important to minimise data loss, packet delay, and processor load. Our analytic model is supported by both simulation and real-world data. Network security experts and designers depend on the ability to foresee overall firewall performance when evaluating the efficacy and resilience of firewalls against DDOS (Distributed Denial of Service) attacks, such as those often conducted by today's Botnets.

According to Mohammad Imran (2015), the number of network attacks has been on the rise, leading to the disclosure of sensitive information, the spread of malware, and a general weakening of network security. Our networks need security measures to defend themselves from intruders and restrict or block information from travelling between them. Firewalls are designed to filter outgoing traffic and stop hackers from gaining access to a network.

Professor Shikha Pandit, Ph.D. (2014) This study proposes a brand-new device to address the issue brought up in the preceding sentence. Computers can't function without the help of networks. Today's fast-paced environment makes networking crucial to the success of any business or field. Routers are used to pick a path, switches facilitate communication, and firewalls protect against unauthorised access. The prevalence of spoofing and eavesdropping attacks is increasing, making it more crucial than ever to take precautions. Therefore, engineers are now dealing with a backlog brought on by the necessity to implement security measures while keeping costs to a minimum.

This article by S.C. Tharaka (2016) discusses common firewall technologies used to secure networks. A firewall can't prevent all threats from the internet, especially those that come from unknown networks. To ensure the safety of the network, many firewall technologies are used. Several researches have been conducted on the topic of firewall technology. The primary focus of this research is on combining firewall capacity with other firewall technologies including packet filtering, NAT, VPN, and proxy services to block malicious intrusions. The connection between firewall capacity and firewall technology is understudied. The goal of the project is to build a more secure network by combining firewall capability with technology. The experimental findings confirm the feasibility of the suggested concept in safeguarding a computer network.

Thomason Steven (2012) there is some evidence that sophisticated packet inspection devices and next-generation firewalls may help fortify your network's entry points against malicious hacking attempts. Traditional firewalls are no longer sufficient protection against modern Internet threats.

The paper by Rahat Afreen and co-authors (2011) discusses PKC systems, sometimes known as public key cryptography (PKC). Using two completely separate keys, a PKC-related system is able to function. Since one key was divided into two and maintained open, PKC systems required a large key to function.

In their discussion on cloud computing, M.Georgescu and M.Matei (2013) point out that it is not just the IT sector that is benefiting from the rise of the cloud. They said that we could have access to very flexible and inexpensive computer resources in the cloud. A further benefit of cloud computing is its potential to forge a fresh link between IT and business divisions inside an organisation.

P.Pazowski (2013) has written an in-depth examination of cloud computing, including its essential features, definitions, and implementation methods. The authors want to draw attention to the differences between the traditional methods of managing and executing IS/IT in businesses and the newer, more innovative approaches. This has been accomplished by using cloud computing. According to Bhavani and Guruprasad, "cloud computing" is "the notion of enabling ubiquitous, convenient, on-demand networked access to a dynamically provided pool of configurable computing resources." Selecting and organising software for later execution is an example of resource provisioning.

III. Problem Statement

Even though networking is increasingly used, data security remains an issue. In the process of being sent through a network, data is vulnerable to a wide variety of threats. Some researchers have focused on developing data encryption processes to transform plain text into cypher text, while others have devised firewall systems to prevent unauthenticated transfers. While encryption helps ensure that sensitive information remains private from prying eyes, it is ineffective if the underlying service is blocked or packets are lost in transit. However, a firewall will protect the data in such a scenario; however, combining a firewall with encryption can slow down the system. It is necessary to include encryption and firewalls into the research focus in order to get better performance.

IV. Need of Research

Cloud-based, distant education continues to gain popularity. When it comes to digital information processing in the cloud, several different avenues of inquiry have been explored. However, there are caveats to be aware of with these studies. In the past, there have been insecure proposals for cloud-based systems dealing with digital material. Though some researchers have taken steps to tighten security, the problem of performance remains a concern due to the time spent ensuring data integrity. This study aims to investigate concerns related to cloud computing, such as safety and efficiency. There should be a solution that can protect digital data without negatively impacting performance. Previous studies pertaining to cloud-based online digital systems are reviewed, along with their methodology and limitations, and the Cloud system and the need of an online system are presented. A scope of such a system and the necessity for future research to keep up its security and performance are then outlined.

V. Conclusion

The integrated method was studied; it combines content substitution to shrink data packets with encryption to make them more secure. The suggested studies have enhanced the effectiveness and security of cloud-based learning environments. The simulation results show that the suggested cloud-based educational platform outperforms the more conventional methods. Since the information has been compressed and encrypted, it may be transferred fast without compromising security. The information is decrypted and decompressed at the receiving end. Because there is less data being sent, transmission errors and delays are less of a concern. Additionally, the number of lost data packets decreases. A number of assaults, such as a man-in-the-middle attack, denial of service attack, brute force attack, cloud service attack, malicious insider attack, and application layer attack, are mitigated by the suggested technique in compared to conventional security solutions. The provided solution is more secure than the alternatives, including methods based on RSA and DNA cryptography.

VI. Scope of Research

One possible outcome of future research is a more effective compression method. There may be techniques to increase safety that can be discovered in further research. Enhanced cloud services and optimization methods may be included into future studies to boost performance while decreasing error rates. Soft computing techniques may be used to improve service reliability and quality. To make the cloud more trustworthy in practical situations, researchers may look at its high availability and zero downtime.

VII. REFERENCES

[1]. Wojciech Konikiewicz & Marcin Markowski (2017), Analysis of Performance and Efficiency of Hardware and Software Firewalls, Vol. 9, No. 1, pp. 49

[2]. Richa Sharma & Chandresh Parekh (2017), A Study and Its Classification, Volume 8, No. 4, May – June 2017

[3]. Miss. Shwetambari G. Pundkar & Prof. Dr. G. R. Bamnote (2014), Analysis of firewall technology in computer network technology

in computer network security, Vol.3 Issue.4, April- 2014, pg. 841-846

[4]. Steven Thomason (2012), Improving Network Security: Next Generation Firewalls and Advanced Packet Inspection Devices, Volume 12 Issue 13 Version 1.0 Year 2012

[5]. RahatAfreen, S.C. Mehrotra, (2011). A Review on Elliptic Curve Cryptography for Embedded Systems. International Journal of Computer Science & Information Technology (IJCSIT), Vol 3, No 3, June 2011, Pp 84-103.

[6]. M.Georgescu and M.Matei 2013, the value of cloud computing in business environment, The USV Annals of Economics and Public Administration, vol.13, no.1, pp. 222--228, 2013.

[7]. P.Pazowski and Z.Pastuszak 2013, Cloud computing – a case study for new ideal of IS/IT implementation, in International Conference on Management, Knowledge and Learning, Zadar, Croatia, 2013, pp. 855--862.

[8]. B.H. Bhavani and H.S. Guruprasad 2014, Resource provisioning techniques in cloud computing environment: A survey, International Journal of Research in Computer and Communication Technology, vol.3, no.3, pp. 395--401, 2014.

[9]. J. Skrinarova, M. Povinsky 2015, Comparative Study of Simulators for Cloud Computing, IEEE, PP.1-8, 2015.

[10]. I. Kashefi, Maryam Kassiri, Ali Shahidinejad (2013). A Survey on Security Issues in Firewalls: A New Approach for Classifying Firewall Vulnerabilities.

[11]. Damodharan, Prabhat Kumar Srivastava (2018). A Review Paper on Computer Firewall. International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 5, Issue 2, February 2018

[12]. Dr. Ajit Singh, Madhu Pahal, Neeraj Goyat (2013), A Review Paper On Firewall, Vol. 1 Issue II, September 2013

[13]. Bavithra.G.R, Mahalakshmi.V, R.Suganya (2018), A Review on Firewall and its Attacks, Vol. 7, Issue 1, January 2018

[14]. Raed Alsaqour, 1 Ahmed Motmi, 2*Maha Abdelhaq (2021). A Systematic Study of Network Firewall and Its Implementation. IJCSNS International Journal of Computer Science and Network Security, VOL.21 No.4, April 2021

[15]. Roumaissa Khelf; Nacira Ghoualmi-Zine (2018). IPSec/Firewall Security Policy Analysis: A Survey. DOI: 10.1109/SIVA.2018.8660973

[16]. Roza Dastres, Mohsen Soori (2021). A Review in Recent Development of Network Threats and Security Measures. International Journal of Computer and Information Engineering Vol:15, No:1, 2021.

[17]. Xinzhou He (2021). Research on Computer Network Security Based on Firewall Technology. doi:10.1088/1742-6596/1744/4/042037

[18]. M. G. Mihalos1,*, S. I. Nalmpantis2 and K. Ovaliadis2 (2019). Design and Implementation of Firewall Security Policies using Linux Iptables. Journal of Engineering Science and Technology Review 12 (1) (2019) 80 – 86.

[19]. Yuchong Lia, Qinghui Liu (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. https://doi.org/10.1016/j.egyr.2021.08.126.

[20]. Raja Waseem Anwar 1,*ORCID,Tariq Abdullah 2 andFlavio Pastore (2021). Firewall Best Practices for Securing Smart Healthcare Environment: A Review. Appl. Sci. 2021, 11(19), 9183; https://doi.org/10.3390/app11199183

[21]. Khaled Salah, Khalid Elbadawi, Raouf Boutaba (2012), Performance Modelling and Analysis of Network Firewalls, Volume: 9 , Issue: 1 , March 2012

[22]. Mohammad Imran, Dr.AbdulrahmanA.Algamdi, Bilal Ahmad (2015), Role of firewall Technology in Network Security, Volume 4, Issue 12 December 2015

[23]. Er. Shikha Pandit, Er. Pritam Kumar, Er. Deepak Malik (2014), Fire-Router: A new secure inter-networking device, Vol. 3, Issue. 6, June 2014, pg.279 – 285

[24]. S.C. Tharaka, R.L.C. Silva, S. Sharmila, S.U.I. Silva, K.L.D.N. Liyanage, A.A.T.K.K. Amarasinghe, D.Dhammearatchi (2016), High Security Firewall: Prevent Unauthorized Access Using Firewall Technologies, Volume 6, Issue 4, April 2016

Cite this article as :

Dr. Dinesh Gupta, Er Krishan Kumar, Renu, "Security and Performance Enhancement of Network by Integration of Firewall Mechanism with Advanced Encryption System", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 8 Issue 6, pp. 643-652, November-December 2022.
Journal URL : https://ijsrcseit.com/CSEIT2286163