International Journal of Safety and Security Engineering
Vol. 12, No. 1, February, 2022, pp. 77-82
Journal homepage: http://iieta.org/journals/ijsse

Effectiveness of Forensic Firewall in Protection of Devices from Cyberattacks

Bandr Fakiha

Department of Medical Health Services, Umm Al-Qura University, Al-Qunfudah 21955, Saudi Arabia

Corresponding Author Email: bsfakiha@uqu.edu.sa

https://doi.org/10.18280/ijsse.120110

Received: 29 October 2021
Accepted: 26 December 2021

Keywords:
ANOVA, computer network, experimental research, firewall, internet, user, WI-FI

ABSTRACT

Computers and networks serve a host of functions. As they provide the much-needed services, unscrupulous parties also make work difficult by promoting cyberattacks that could lead to sensitive data loss and inability to access a personal computer. The submission explores the use of firewalls in protecting users against network-driven attacks. Firewalls intercept malware attacks, phishing, and identity theft by denying access to certain suspicious sites. However, users must realize that some hardware firewalls cannot protect them from certain web attacks and software firewalls that are in-built fail to detect malicious attacks on some occasions. Therefore, some entities are forced to incorporate both hardware and software to get the desired level of protection. Using an experimental research method, the study explores the effectiveness of firewall protection by presenting more gains that demerits.

1. INTRODUCTION

Internet access is almost inevitable in the 21st century. As most people find easier ways of communication and working digitally, they meet various challenges, including cyber-related crimes. Most people familiar with daily computer usage over the internet or WI-FI often find notifications from the service provider concerning protection against threats. This refers to firewall protection, which protects users against cyberattacks [1]. Several people have fallen victim of privacy violations online because they lacked firewall protection. Others experienced phishing and some scammed for sharing data unconsciously over a common internet or WI-FI connection. Through firewall protection, one can restrict unwarranted access of personal information by others [2].

Firewalls prevent cyberattacks by deterring malicious network traffic that gives advantage to fraudulent parties. Often, a user receives an alert about a possible threat, including efforts of blocking data access from suspicious locations. For this reason, a user is less likely to experience a denial-of-service attack [3]. Firewall protection is undeniably necessary and users must know the right configuration settings to apply since this enables one to establish why they need security when browsing.

2. RELATED WORK

There are different levels of protection from external attacks while using computers. Some people use strong passwords to limit external access to personal space. While passwords can be configured and easily manipulated to gain access, firewalls prevent needless network traffic and suspicious software from accessing computers [4]. Through effective configuration, firewalls prevent malicious flow of data from ports, multiple locations or network addresses, and computer applications. For instance, when one plays a free internet game, the chances of being redirected to a different page is high. Often, the high-speed exercise takes a user to a malicious site, which could access personal data without one's knowledge [5]. Firewall protection identifies such as site unsafe or asks permission from the user to pursue the risky exercise.

Firewalls are in different categories, but the two broad ones are hardware and software. Hardware firewalls are physically placed between the internet and the computer, and this trend is common in small office settings. They are in the form of a broadband router that connects the gateway and network [6]. Often, the Internet Service Providers (ISPs) and offices agree on the best ways of protecting desktops from malware, and they device a network system that controls traffic by reducing data leakage to unsolicited parties. Thus, system maintenance is often scheduled.

However, hardware systems are being replaced by software firewalls that are inbuilt within the Operating System (OS). For instance, Microsoft offers added protection to users, but clients can still access the services separately from computer stores and vendors. Also, ISPs offer such services to ensure that clients only access secure sites [7]. The internal system, which is in the form of a computer program, operates using applications and port numbers [8]. Firewall as a Service (FWaaS) is equally popular among corporates because the cloud-based system is expandable and a business can grow with it as perimeter security [9]. Essentially, it is a virtual firewall. Often, the type of firewall chosen by an individual or business depends on the functionality, structure, needs, and size of the entity. Business can also opt for the packet-filtering firewall that blocks network traffic IP protocol, port numbers, and IP address. It is the best and the most basic, commonly used for blocking traffic on malicious sites. Users can also explore proxy service firewalls, which inspect and filter messages at the point of entry [10]. The network protection technology that analyses incoming traffic is popularly used on emails to stop spam messages from getting to the "inbox" section.

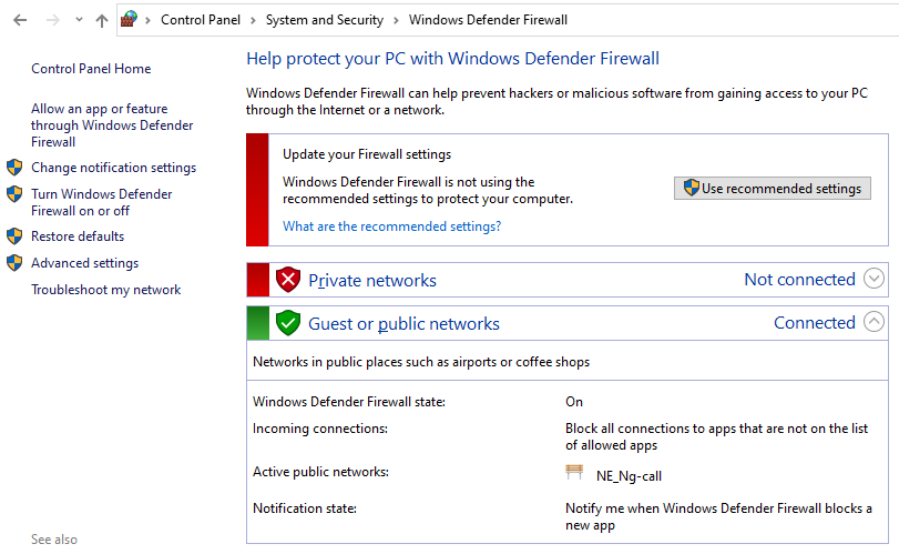

Figure 1. Using in-built system for establishing firewall protection

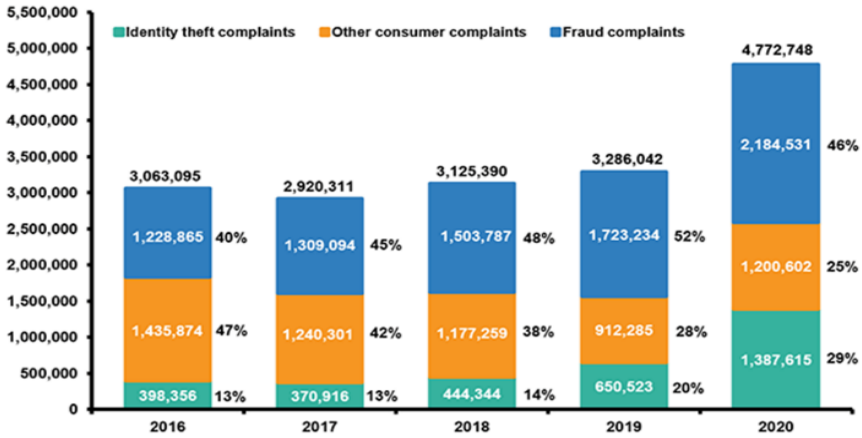

Figure 2. Identity theft data between 2016 and 2020

Users might also take interest in stately multi-layer inspection (SMLI) firewalls that often track already established connections [11]. Like broadband router, it filters traffic by focusing on protocol, port, and state while remaining with the context of rules. Often, it works on already functional connections, and needs support from software because of the challenges it faces in identifying web connections [12]. Also, a unified threat management (UTM) firewall can be used because it is a program that prevents virus intrusion and actions as an antivirus. It offers an umbrella support for the entire system, and is one of the best for modern computer users. Another firewall solution is the next-generation (NGFW), which offers an advanced security level for sophisticated users with more needs [13]. For instance, it can handle advanced malware and keeps evolving. Hence, it is safe than SMLI and packet-filtering firewalls. In addition, there is the network address translation (NAT) firewall that blocks unwanted communication over the internet, when the connected network is private [14]. The illustration in Figure 1 shows how a user can establish firewall protection from an in-built system.

Firewall protection is necessary because of the consequences of cyberattacks. In a 2020 study conducted by Aite Group, at least 47% of Americans faced identity theft in the same year [15]. Identity theft cost Americans $502.5 billion in 2019 and $712.4 billion in the subsequent year giving it a 42% rise. The research institution projects an increase in losses to $721.3 billion by the end of 2021 [16]. In 2020, most businesses went online and fraudsters found ways of using network connectivity and skills in machine learning to commit crimes [17]. They stole data from computers, especially for people who used public WI-FI or Local Area Network because these increase vulnerabilities of data. Hence, fraudsters easily used their information to build a profile and later engaged in crime. Figure 2 shows statistics of identity theft between 2016 and 2020.

Identity theft manifests in the form of tax and credit card frauds, business/personal loan theft, miscellaneous actions, and access to government benefits [18]. Firewall strives to prevent such crimes by alerting users that a different person might be accessing their information at a different location [19]. Often, the location is shared and the computer address also shown to make it easy for one to schedule an immediate follow-up on the incident. The history of firewalls explains the in-depth need for such devices in modern computing environments to address identity theft and other forms of cyberattacks.

3. METHODOLOGY

The research will use an experimental research design to draw a relationship between statistical data and real-life

solutions. Experiments are designed to test causal (cause-and-effect) relationships between variables. In this context, the research strives to establish the relationship between firewall protection and cybersecurity. The research depends on the assumptions that the statistical hypotheses will make. Statistical hypotheses assess the value the populace's parameters [20]. A null hypothesis (H0: μi = μj) refers to the statement that is subjected to the statistical test while the alternative hypothesis (H1: μi ≠ μj) is chosen is the null hypothesis cannot apply in the context. For instance, the expected null hypothesis is that firewall protection prevents cyberattacks for all populations. An alternative hypothesis would denote that not all groups are equal and that some people do not qualify firewall for complete protection from cyberattacks.

The experiment to be conducted to accept the alternative or fail to reject the null hypothesis is a case-controlled experimental design that makes use of a control experiment and test experiment. The experimental procedure will involve the use of information systems where firewall is used to protect the system while the control experiment will involve the use of non-protected information system [21]. Data regarding cybersecurity threats such as virus, phishing attacks, malware attacks, Denial of Service (DOS), SQL-injection, man-in-the middle attacks (MitM) will be examined and recorded over a long duration of time such as two years [22]. Data recording will involve recording the number of firewalls used in the information system every month and recording of the cases of cyber threats for that month. Data analysis will involve the use of statistical techniques such as correlation and significance analyses that measure the association between the number of firewalls used in the information system every month and cases of cyberattacks [23]. The results will be used to accept or reject the hypotheses.

Data collection will involve assessing the cause-and-effect relationship between firewalls and cybersecurity. There are different firewalls that work dissimilarly to achieve various effects. Therefore, the independent and depend variables' relationship is affected by an extraneous (control) variable [1]. In this study context, the independent variable is the firewall, and its dependent counterpart is the cyberattack. Different factors influence the relationship between the variables, and they include the various types of firewalls. Control variables for the research include a host of reasons why people chose hardware, software, or both firewalls [3]. Figure 3 shows the relationship between the variables.

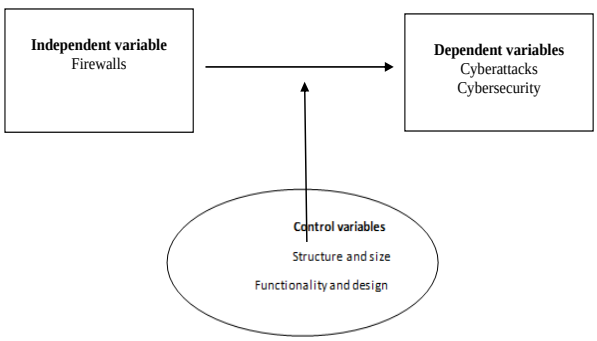

Figure 3. Conceptual framework for the study

The independent variables will be measured in terms of the number of firewalls used in the information systems every month for a duration of 6 months. For instance, if the number of firewalls used in the information system is 4 in January, the corresponding value of independent variable will be 4. The dependent variable will include the number of cyber-attacks and cyber threats recorded each month. For example if 20 cases of cyber threats and 10 cases of cyber-attacks are observed in January, these values will be entered into their corresponding columns. The process will be repeated for each month until a 12 month data is collected. The control variables will be the use of information system that has been designed without firewalls and collecting information in the same manner as the test experiment.

Based on the null hypothesis, the experiences of all populations are the same, and firewalls protect them. The alternative hypothesis is premised on the fact that human experiences are different.

H0: μi = μj

H0: Firewall protection is effective for cyberattacks

H1: μi ≠ μj

H1: Since not everyone has tried all firewalls, it is illogical to conclude that the network interception technology prevents cyberattacks

According to the null hypothesis, any firewall is effective in cyberattacks prevention, but the alternative hypothesis focuses on control variables and different types of the independent variable such as UTM, SMLI, NGFW, and NAT. this experimental research approach involves behavioral studies because it focuses on an observed set of traits in a natural environment [19]. The greatest advantage of the approach is that the reactions are genuine and not manipulated unlike in a forensic laboratory setting.

The best way to justify the veracity of the null hypothesis is through an ANOVA statistical analysis involving a two-group experimental design [6]. According to the research [2], there is a single independent variable tested against an independent variable amidst the control variable during a pretest and posttest exercise. In essence, a control variable such as capacity and design will explain why an organization would opt for a cloud-based firewall or an individual will take an in-built software system [7]. Both are software-based, yet some consumers prefer hardware firewall. In such designs, object R stands for a random assignment, O is the pretest or posttest while X refers to the treatment administered to the independent variable.

The relationship between R and O is that R stands for the number of firewalls used in the information system at the instance where a test is conducted to determine whether cyber-attack or cyber-threats has occurred while O represents the number of cyber-attacks or threats that have been recorded [9]. An example of such a case is when R (3 firewalls have been used) while O (the number of cyber-attacks is 10 in a month) X refers to the order in which the experiment has been carried out, such as 1st experiment, 2nd experiment, 3rd experiment, etc.

R	O_1	X	O_2	(Treatment group)
R	O_3		O_4	(Control group)

Another important component of the formula is the E (effect), which is calculated by measuring the different between posttest and pretest results. ANOVA applies in the context because of the regression analysis as summarized in the formula below

$$E = (O\,2 - O\,1) - (O\,4 - O\,3)$$

A two-way analysis of variance (ANOVA) analysis is a process of analyzing the statistical differences between the means of three or more independent groups. The steps involved in calculation of ANOVA include: the identification of significance level, selecting an appropriate statistical analysis technique such as ANOVA, setting up decision rule, and computing the test statistic [12]. In the present study, ANOVA analysis will be useful in getting insight into the statistical significance of the means of the control process and the test process during the analysis of the impact of firewall in enhancing security of the information system from cyber-attacks [3]. The statistical significance of the means of the control and experimental process will be calculated by getting the F-test results. F-test will enable comparison of the mean of cases of cyber-attacks or cyber-threats in the experimental situation with that of the control experiment. A high F-test value shows a small statistical significance of the variance between the groups.

The random experiment should take a firewall as a treatment group. R is achieved through O1 (hardware firewall and design of the organization) X O2 (software firewall and functionality) to get the treatment group. For the control group, the equation is, O1 (Broadband router and design of the organization) X O2 (UTM and functionality) because this takes an in-depth approach into the different types of the hardware and software firewalls. The mathematical expression that provides a relationship between the R and O will be the F-test result which will computed using Statistical Package for Social Scientist (SPSS) or Microsoft Excel. R is the sum of hardware firewalls and the software firewalls and is obtained using the equation:

R = number of hardware firewalls + number of software firewalls.

O is the number of cyber-attacks that have been successfully executed in the information system within a particular month while X is the sequence for months in which the tests have been conducted.

The study uses a two-way, randomized ANOVA (Y=Xij Constant elements=ɯ+eij Additional components = ai+bj). As shown in the formula, Y is the dependent variable and it remains unchanged throughout the research. Still, it significantly influences "E." In the two-way ANOVA, the attributes of the treatment group (independent variable) change depending on the pretest and posttest results of the control variable. There is no impact of the results of the pretest and posttest of the control variables on the attributes of the treatment group because they are independent groups. Therefore, the outcomes of the pretest and posttest of the test procedure are independent from those of the control procedure. Hence, this reduces generalizability of outcomes, and it makes the alternative variable more plausible.

4. RESULTS AND DISCUSSION

4.1 Cyberattacks and network vulnerabilities

According to the research, the greatest interest of infrastructure developers who work on networked systems is to improve security. Firewalls strive to address issues such as denial-of-service or cyberattacks, but occasionally fail to achieve the expected results. According to Mitchell [10], some cyberattacks cannot be protected by firewall. If the network utility system is flawed, firewall cannot shield a user from suspicious traffic occasioned by insider threats [11]. Essentially, some threats are in-built, and one requires an antivirus for additional protection even as they use UMT. Also, when people share USB devices, possibilities of malware attacks increase [13]. Often, a first instinct is that the in-built system will scan the device to ensure it is safe. While the device might be safe from virus, kit could be a potential data carrier across the network. As established, most hardware firewall cannot detect web-based problems, and even in such a case, a broadband router is less likely to prevent a cyberattacks [16]. Also, data leakage could occur from the equipment manufacturer. This hardware leakage problem increases a user's vulnerability to attacks because of the exposed IP address. This part responds mostly to the alternative hypothesis, which shares the skepticism of other groups over the effectiveness of firewall. Still, several others share in the thoughts of the null hypothesis, which conclude the firewall prevents cyberattacks.

Network attacks are classified into: snooping, Distributed denial of service (DDoS), man in the middle Attacks, Code and SQL Injection Attacks, Privilege Escalation, viruses, worms, Trojans etc. Snooping is the process where an attacker listens to traffic during data transfer between machines and accessing the network to read confidential information [3].

DDoS is a type of network attack where the attackers create botnets, compromise of devices, and use them as means through which false traffic is directed to network or servers [3]. An example of DDoS at the network level is when huge volumes of SYN packets are sent to overwhelm a server by performing a number of SQL queries that prevent the databases from functioning. Man in the Middle Attack occurs when traffic through a network is interrupted. This type of attack majorly occurs when the communication protocol is not secured or the attackers manage to go bypass the security, and access data that is transmitted, and access credentials of the user [1]. Code and SQL injection attacks occur when an attacker accesses a website that does not validate inputs and fill out a form or make an API call that enables passing of the malicious code rather than the expected information. After the code has been executed, the server allows the attackers to compromise it [7]. Viruses is the most likely form of network attack that occurs when the user clicks or copy media or a host. Most viruses undergo self-replication without the user being aware of their presence. Viruses tend to be spread into instant messaging, emails, removable media, and network connections. Worms have similar characteristics as viruses and have the ability to self-replicate and spread full copies and segments of itself through the network. Trojans are programs that occur in a similar manner as legitimate software and allow the attacker to spy on the legitimate user when the user calls upon the software [2]. Network vulnerabilities are classified into: hardware issues, physical device security issues, firewall issues, IoT devices, unauthorized devices, software vulnerability, etc. Hardware issues occur when network devices such as routers are not properly managed through upgrades or replacement [8]. Physical device security is a vulnerability that occurs when access to a device is unsupervised and an intruder gets the opportunity to download code from a prearranged location or copy it from a USB device. Firewall issues that cause vulnerability of a network include: the installation of unnecessary services, the use of few firewalls, etc. [10]. Wireless issues that lead to increased vulnerability of a network include poorly secured Wi-Fi network that enable connection of nearby devices that get past

the firewall. Access points that do not have passwords create the risks of anyone nearby being able to gain access and lack of encryption of a Wi-Fi with a password that make devices readily available to incoming and outgoing traffic.

4.2 Firewalls are effective

Firewalls are effective when chosen correctly and used for the intended purpose. They offer different layers of protection, and everything depends on utility. For instance, not everybody is in need of a filtering firewall such as packet-filtering, proxy, and inspection [15]. In packet-filtering, one's greatest interest should be cyberattacks such as eavesdropping and phishing that are directly linked to the ISP. Occasionally, ISPs engage in datamining exercises for their Know-Your-Customer research exercises and the possibility of creating loopholes for cyberattacks increase [12]. Therefore, a firewall protection technology that filters packets of data is required. A person opting for proxy should not that it protects users against external attacks on IP addresses. For the inspection filtering, the firewall protects one against spam emails [9]. Such levels of protection are excellent for individual level support even though companies also need them. However, conglomerates should opt for hardware and cloud-based systems that operate at a larger scale like NAT and SMLI.

According to the discourse, the alternative hypothesis is more feasible because it answers more questions in the research [7]. Indirectly, the alternative hypothesis establishes that firewall protection enhances system performance and occasionally protects users against viruses [20]. The alternative hypothesis is accepted when there is a positive correlation between the number of firewalls in the system and the number of cyber-attacks i.e. when the increase in the number of firewalls results into lower number of cyber-attacks on the devices.

Also, it educated users on acquiring more knowledge of in-built firewalls to establish that they are getting the right level of defense and the manufacturer of the computer does not propagate cyberattacks on clients [12]. According to [3], in the 5G network era, the possibility of manufacturer-driven cyberattacks is high. Additionally, the alternative hypothesis explains why firewalls are both hardware and software while emphasizing the undeniable need for protection from cyberattacks. The use of both hardware and software firewalls is effective towards achieving effective protection of devices from attack by complementing each other [16]. A hardware firewall protects devices such as printers and computers from unauthorized access by dangerous traffic. The act of combining hardware and software firewalls provide protection to computers and other devices in a network. The hardware firewalls regulate traffic coming in from and going into the internet while software firewalls ensure security of what is coming into or going out of a device such as a computer. The hypothesis expects users to learn about host-based intrusion, malware, and the need for developing critical infrastructure to manage phishing [5]. Generally, the alternative hypothesis is more comprehensive and offers sufficient room for future research.

5. CONCLUSION

Firewall protection is necessary for preventing cyberattacks. However, one must be knowledgeable on the required layer of protection to avoid depending on an in-built system that continues predisposing a computer to malicious sites. Based on the null hypothesis, firewall prevents all cyberattacks, but the alternative hypothesis argues that levels of protection differ depending on the problem one faces. Some people deal with spam mails, phishing, eavesdropping, and identity theft among other forms of cyberattacks. As such, it is important to treat every situation uniquely by proposing the use of different firewalls.

ACKNOWLEDGMENT

Big thanks to Umm Al-Qura University, for its support through this study.

REFERENCES

[1] Abdalrahman, G.A., Varol, H. (2019). Defending against cyber-attacks on the internet of things. In 2019 7th International Symposium on Digital Forensics and Security (ISDFS), pp. 1-6. http://doi.org/10.1109/ISDFS.2019.8757478

[2] Aite Group. (n.d). Facts + Statistics: Identity theft and cybercrime. https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime, accessed on 12 October 2021.

[3] Al-Shaer, E.S., Hamed, H.H. (2004). Modeling and management of firewall policies. IEEE Transactions on Network and Service Management, 1(1): 2-10. https://doi.org/10.1109/TNSM.2004.4623689

[4] Armstrong, R.A., Eperjesi, F., Gilmartin, B. (2002). The application of analysis of variance (ANOVA) to different experimental designs in optometry. Ophthalmic and Physiological Optics, 22(3): 248-256. https://doi.org/10.1046/j.1475-1313.2002.00020.x

[5] Clincy, V., Shahriar, H. (2018). Web application firewall: Network security models and configuration. In 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), 1: 835-836. http://doi.org/10.1109/COMPSAC.2018.00144

[6] Davis, C. (2020). The cyberattacks your firewall won't protect you from https://skyhelm.com/cyberattacks-your-firewall-wont-protect-you-from/, accessed on 12 October 2021.

[7] Demertzis, K., Iliadis, L. (2019). Cognitive web application firewall to critical infrastructures protection from phishing attacks. Journal of Computations & Modelling, 9(2): 1-26.

[8] Eden, D. (2017). Field experiments in organizations. Annual Review of Organizational Psychology and Organizational Behavior, 4: 91-122. https://doi.org/10.1146/annurev-orgpsych-041015-062400

[9] Eian, I.C., Yong, L.K., Li, M.Y.X., Qi, Y.H., Fatima, Z. (2020). Cyber attacks in the era of COVID-19 and possible solution domains. Preprints, 2020: 2020090630. http://doi.org/10.20944/preprints202009.0630.v1

[10] Mitchell, O. (2015). Experimental research design. The Encyclopedia of Crime And Punishment, 1-6. https://doi.org/10.1002/9781118519639.wbecpx113

[11] Morris, T.H., Pan, S., Adhikari, U. (2012). Cyber security recommendations for wide area monitoring,

protection, and control systems. In 2012 IEEE Power and Energy Society General Meeting, pp. 1-6. http://doi.org/10.1109/PESGM.2012.6345127

[12] Pak, S.I., Oh, T.H. (2010). The application of analysis of variance (ANOVA). Journal of Veterinary Clinics, 27(1): 71-78.

[13] Raju, S. (2019). 13 Most misunderstood facts about firewall. https://www.teceze.com/13-most-misunderstood-facts-about-firewall, accessed on 12 October 2021.

[14] Sobola, T.D., Zavarsky, P., Butakov, S. (2020). Experimental study of modsecurity web application firewalls. In 2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), pp. 209-213. http://doi.org/10.1109/BigDataSecurity-HPSC-IDS49724.2020.00045

[15] Song, X. (2020). Firewall technology in computer network security in 5G environment. In Journal of Physics: Conference Series, 1544(1): 012090. https://doi.org/10.1088/1742-6596/1544/1/012090

[16] Srinivas, J., Das, A.K., Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. Future Generation Computer Systems, 92: 178-188. https://doi.org/10.1016/j.future.2018.09.063

[17] Süzen, A.A. (2020). A risk-assessment of cyber attacks and defense strategies in Industry 4.0 Ecosystem. International Journal of Computer Network & Information Security, 12(1): 1-12. http://doi.org/10.5815/ijcnis.2020.01.01

[18] Touhiduzzaman, M., Hahn, A., Srivastava, A. (2018). Arcades: Analysis of risk from cyberattack against defensive strategies for the power grid. IET Cyber-Physical Systems: Theory & Applications, 3(3): 119-128.

[19] Tsuchiya, A., Fraile, F., Koshijima, I., Ortiz, A., Poler, R. (2018). Software defined networking firewall for industry 4.0 manufacturing systems. Journal of Industrial Engineering and Management (JIEM), 11(2): 318-333. http://dx.doi.org/10.3926/jiem.2534

[20] Ucar, E., Ozhan, E. (2017). The analysis of firewall policy through machine learning and data mining. Wireless Personal Communications, 96(2): 2891-2909. https://doi.org/10.1007/s11277-017-4330-0

[21] Upadhyay, D., Sampalli, S. (2020). SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations. Computers & Security, 89: 101666. https://doi.org/10.1016/j.cose.2019.101666

[22] Wendt, O., Miller, B. (2012). Quality appraisal of single-subject experimental designs: An overview and comparison of different appraisal tools. Education and Treatment of Children, 35(2): 235-268. https://doi.org/10.1353/etc.2012.0010

[23] Yost, W., Jaiswal, C. (2017). MalFire: Malware firewall for malicious content detection and protection. In 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), pp. 428-433. http://doi.org/10.1109/UEMCON.2017.8249075