A Review in Recent Development of Network Threats and Security Measures

Roza Dastres, Mohsen Soori

A Review in Recent Development of Network Threats and Security Measures

Roza Dastres, Mohsen Soori

Open Science Index, Computer and Information Engineering Vol:15, No:1, 2021 waset.org/Publication/10011793

***Abstract*—**Networks are vulnerable devices due to their basic feature of facilitating remote access and data communication. The information in the networks needs to be kept secured and safe in order to provide an effective communication and sharing device in the web of data. Due to challenges and threats of the data in networks, the network security is one of the most important considerations in information technology infrastructures. As a result, the security measures are considered in the network in order to decrease the probability of accessing the secured data by the hackers. The purpose of network security is to protect the network and its components from unauthorized access and abuse in order to provide a safe and secured communication device for the users. In the present research work a review in recent development of network threats and security measures is presented and future research works are also suggested. Different attacks to the networks and security measured against them are discussed in order to increase security in the web of data. So, new ideas in the network security systems can be presented by analyzing the published papers in order to move forward the research field.

***Keywords*—**Network threats, network security, security measures, firewalls.

I. Introduction

NETWORK security is one of the most important considerations in the field of information security today with the expansion of business system dependencies on IT-based infrastructures. The lack of security measures in IT infrastructure can cause irreparable damage to organizations and companies which is not desirable for business and marketing process.

The purpose of network security is primarily to prevent damage from data misuse. There are a number of potential problems that can occur if network security is not implemented properly. Every business will need to keep some critical and classified information from the access of its competitors. The data loss can decrease the added value in the process of part production and marketing. Moreover, the true way of moving in the business and product marketing can be lost due to the data manipulation as a result of lack of security measures in the financial information. As a result, the lack of security measure in the web of data can cause violation of confidentiality in the different businesses and marketing of products. Therefore, it is vital for any network administrator to use strict policies to prevent potential losses, regardless of the size and type of network [1]. It is a set of policies, regulations, and arrangements developed by a network administrator or administrators to prevent and monitor unauthorized access, misuse, correction, prevent change, or restrict access to computer networks and network accessible resources [2].

In the present research work, different issues of research works in the network threats and security measures are categorized to provide a useful study for the researchers in the interesting field. As a result, new ideas for network security systems and gaps in the existing literature are obtained and future research works are also suggested in order to push forward this interesting research field. The literature review is presented in Section II. The conclusion and future research works are presented in Section III.

II. Literature Review

Due to the fact that security is one of the basic needs in information technology infrastructures, extensive studies and researches have been done by various research works. In this section, the different network threats and necessary security measures to prevent them are discussed.

A. Network Security Threats and Attacks

In order to provide the security measures in the network of data, the attacks should be clearly defined. An attack is a dangerous or non-dangerous attempt to modify or use a resource accessible through the network in a way that was not intended. The network attacks can be classified into three general categories:

1- Unauthorized access to resources and information through the network.
2- Unauthorized manipulation of information on a network.
3- Attacks that lead to disruption of service delivery and are called Denial of Service [3].

The key word in the first two categories is to perform actions illegally. Defining an authorized or unauthorized action is the responsibility of the network security policy which can be defined as an attempt by a user to view or modify information that is not allowed. Unauthorized access can be one of the most common attacks on any network. In this way, the attacker tries to access the restricted area of information and the network. Breaking passwords, creating sub-paths, creating fake identities or using malware are the main ways to carry out these attacks [4], [5].

Information destruction is one of the most destructive attack networks. In this way, the attacker tries to destroy certain information by performing commands in the database. This

R. D. is with the Department of Computer Engineering, Cyprus International University, North Cyprus, Turkey (e-mail: roza.dastres@yahoo.com).

M. S. is with the Department of Mechanical Engineering, Eastern Mediterranean University, Famagusta, Via Mersin 10, North Cyprus, Turkey (corresponding author, e-mail: Mohsen.soori@emu.edu.tr).

can be limited or very extensive. Depending on the type of attacker, the network can lose all your information in a matter of seconds. Attacks that lead to disruption of service delivery are another form of unauthorized access. In this method, the person enters the user or management area to execute the command or a set of commands which are normally prohibited. In this way, the attacker may write, modify, send email, copy information, or delete certain information in order to find a way to access to the restricted data. The extent of the attack depends on the capabilities of the attacker [6], [7].

Network security threats fall into one or two general categories as Logic Attacks or Recourse Attacks. Rational attacks, as the name implies, are a for-profit strategy used to eliminate any weakness in the system. Weaknesses can include software vulnerabilities such as backdoors and security errors in the code [8]. The purpose of the attack is to enter the system in order to corrupt or gain unauthorized access of the system [9]. Resource attacks are aimed at destroying resources of networks. The trick became more popular in the 1990s, but gradually declined in popularity. In this method, the network system is forced to be destroyed, which is therefore vulnerable. These attacks are carried out in different ways in order to apply forces to the web of data. The fastest way is for the server to face a huge flood of service requests that are out of its control. Also, some resource attacks involve installing malware on the network, which will make it vulnerable [10].

There is also another classification for the different attacks to the secured networks as,

- Passive attacks: Passive attacks are against the security of the organization's network, in order to identify the network; the intruder monitors the organization's network. Since in this attack the intruder does not do any malicious activity to detect this type of attack, it is very difficult, for example, one type of passive attack is that the attacker captures the internal network packets of the organization, the hope is that this type of attack can be easily prevented with proper encryption in the network infrastructure [11].
- Active attacks: In this type of attack, the attacker directly attacks the organization's servers. The attacks are visible for the security systems of the network in order to be monitored. Strategies to combat these attacks include setting up firewalls (software and hardware) as well as IPS systems [11], [12].
- Internal attacks: (Close-in) in this type of attack, intruders physically access to the systems. Unfortunately, with physical access to systems, almost any intruder can do a lot of work and cause irreparable damage to the organization. An appropriate and logical way to deal with this type of attack is to ensure the physical security of systems and servers [12].
- Insider attacks: These types of network attacks are usually carried out by internal users of organizations that have access to systems and information. According to the level of knowledge and awareness of the attackers to the computer networks, they can penetrate to the network systems. The solution of the attacks is to prevent this type of security attack in Layer 2 and focus on authentication, while physical security must be fully ensured [12], [13].

B. Security Measures

To provide basic knowledge of security measures in the web of data, some concepts in network security are presented in this section. In a modern network there are many resources for protection. The following is a list of network resources that should be protected against all types of attacks: 1- Firewalls routers and switches as network equipment, 2- Network operation information such as routing tables and access list configurations stored on the router. 3- Intangible network resources such as bandwidth and speed. 4- Information and information resources connected to the network, such as databases and information servers. 5- Terminals that are connected to the network to use different sources. 6- Information being exchanged on the network at any moment of time. 7- Keeping users' operations and using their network resources private to prevent user identification [14], [15].

On networked computers such as database and web servers, information is exchanged over the network and information about network components to perform tasks such as router routing tables. Network resources can also be terminal equipment such as routers and firewalls or connection mechanisms in order to prevent hackers to access the secured data [16].

Principles of network security design: To implement an advanced security systems in the web of data, a proper designing method and principles should be applied to the security measures of the networks. Network security protections are the first line of defense for Information Technology (IT) system resources against threats (such as intruders or malicious code) that arise from out-of-network flows. Key protection measures for network security include firewalls, intrusion detection and web Application Firewall, Intrusion Detection System (IDS) and Intrusion Prevention System (IPS), Virtual Private Network (VPN) protections and content review systems such as antivirus, anti-malware, anti-spam and Uniform Resource Location (URL) filtering [17]. These hardware and software solutions support and complement security mechanisms for operating systems, databases, and applications. To provide an efficient security system in the secured data of networks, advanced flowchart designing methods regarding the threats levels is applied [18]. Basic security principles of IT systems which should be considered in designing a network security system are as shown in Fig. 1 [19].

Security policy: The network security policy should be defined in such a way in order to minimize the risk and the amount of damage after the risk analysis in the web of data. Security policy should be general and in the field of general vision and not go into details. The details can change in a short time, but the general principles of security of a network that make up its policies remain the same [20].

Elements involved in security policy are: 1- What and why the data should be protected. 2- Who is responsible for data protection. 3- Creating a context that resolves any possible conflicts. Security policies can be broadly divided into two categories: 1- Permissive: Anything that is not specifically prohibited is allowed. 2- Restrictive: Anything that is not explicitly allowed is prohibited. Usually the idea of using restrictive security policies is better and more appropriate method in term of security enhancement of network systems. This selection is due to security problems of authorized policies in order to provide restriction to access of secured data [21], [22].

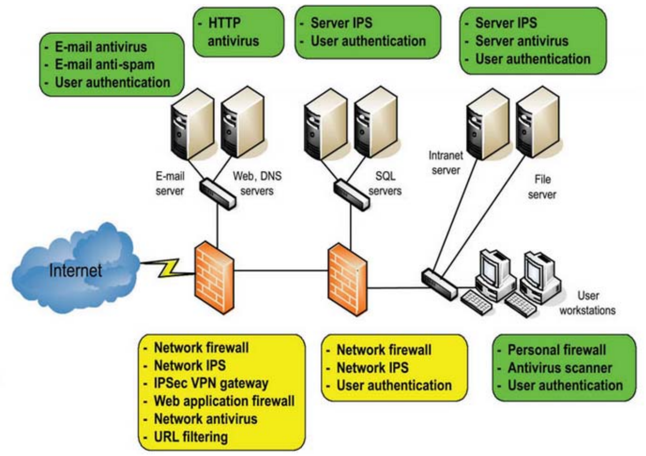

Fig. 1 The principle of comprehensive defense: protection of various IT system resources based on several complementary security layers [19]

Network security implementation: The best approach to implement a good network security is to have our network fully prepared for threats. Here are 4 tips for the network security implementation process: 1- Security: Ensure that all components are properly licensed and have authentication and protection policies. 2 - Review: Track network activities and continuity of protection activities. 3- Testing: Assess the vulnerabilities of the security policies intended for the network by simulating an attack by a trusted person. If it is possible to circumvent the prohibitions, it will be necessary to implement more sophisticated techniques. 4- Improving the situation: Based on all the previous steps, collect data and use them to create better measures [23], [24].

All network administrators should keep in mind that a good security strategy for the network involves constant monitoring and maintenance. It is certainly not enough for security policies to be created and abandoned to do its job. Attackers are constantly updating themselves to find a way to the secured data. So, network administrators need to keep up to date with these enhancements [25].

Elimination of danger: After determining the network assets and their threatening factors, various risks should be assessed. At best, the network should be able to protect against all kinds of errors, but cheap security is not achieved. Therefore, it is necessary to make a proper assessment of the types of risks in order to identify the most important ones, and on the other hand, to identify the sources that should be protected against these risks. The two main factors in risk analysis are: 1- The possibility of carrying out an attack and 2- Damage to the network in case of a successful attack [26], [27].

Network layering: Security levels are a classification of network activities so that each network activity can be protected separately and the security policies of one level do not affect the security parameters of the other level. For example, if a DOS attack in the field of network security occurs in the security layer on the user side, we do not seek to deal with this attack in the management layer [28]. Network security levels make it possible to examine the security of each activity separately by categorizing network activities and placing them at different levels. Since each activity is considered separately, the security measures in each level can be accurately managed. VoIP service at the service security layer, service management security (such as user security), independent of service control security (such as SIP protocol), and independent of user-side data security (such as user voice) are some examples of applying the network security level in security measures of networks [29], [30]. To increase the security level of the comprehensive IT infrastructure, related security solutions will be used at all levels and layers of enterprise IT architecture. To establish end-to-end security, it is necessary to apply security components related to different equipment and groups. The task of security layers, like network layers, is to provide service and activate the higher layer. Therefore, the need for network layering is felt in the web of data. Three layers of security are considered, and by defining different layers of security, a hierarchical solution for network security is proposed. Layering is done in such a way that each layer has its own vulnerabilities, which is done with the aim of facilitating dealing with threats [31].

"Infrastructure Security Layer" enables "Service Security Layer" and this layer also enables "Application Security Layer" in order to provide an advanced network security by Network layering. The following layers are explained as,

- Infrastructure security layer: The infrastructure layer covers the security of transmission network facilities as well as individual network tools. This layer provides a description of the main network implementation, services and applications of each [32].
- Service security layer: The security of the services that the service providers provide to the customers is provided in this layer. This range of services includes basic services (for example, Internet communication services such as Authentication Authorization Accounting (AAA) server, Domain Name System (DNS) service, etc.) to special services such as Voice Over Internet Protocol (VOIP), VPN etc. The task of this layer is to protect service providers and their customers from potential security threats [32].
- Application security layer: This layer focuses on the applications which are available for the users in the web. Network applications may be provided by the Application Service Providers (ASPs) as a third party provider, the service provider itself as ASPs, or their host companies having an independent data center. Accordingly in this layer, four targets can be considered as a threat: 1-

application users, 2- Application provider, 3-Sub-provider 4- Service provider [33]. The structure of application security layer in the network security and the task of each section is shown in Fig. 2 [33].

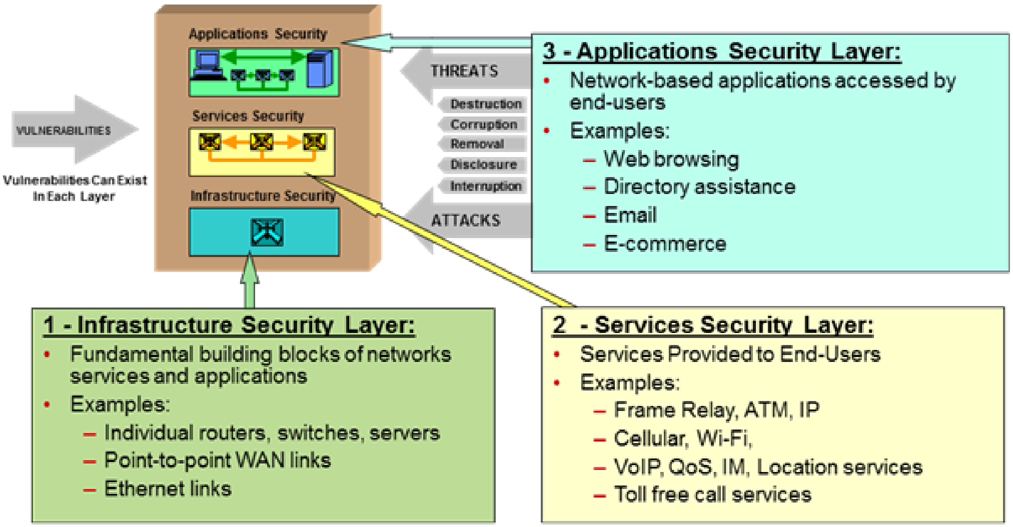
Applications Security
Services Security
Infrastructure Security
VULNERABILITIES
Vulnerabilities Can Exist In Each Layer
THREATS
Destruction
Corruption
Removal
Disclosure
Interruption
ATTACKS
3 - Applications Security Layer:
• Network-based applications accessed by end-users
• Examples:
– Web browsing
– Directory assistance
– Email
– E-commerce
1 - Infrastructure Security Layer:
• Fundamental building blocks of networks services and applications
• Examples:
– Individual routers, switches, servers
– Point-to-point WAN links
– Ethernet links
2 - Services Security Layer:
• Services Provided to End-Users
• Examples:
– Frame Relay, ATM, IP
– Cellular, Wi-Fi,
– VoIP, QoS, IM, Location services
– Toll free call services

Fig. 2 Application of security layer in the network security [33]

- Control security level: The function of this layer is to support activities that are responsible for transmitting information about services or network applications. This level generally includes the communication between machines in the network, which usually includes control messages [33].
- User-side security level: This level includes securing access to and using the services provided by the provider on the user side. End users may use the service provider network itself, or extension services such as VPNs, or on application-based networks [33].
- Information segmentation: IT system resources with different levels of sensitivity, including risk tolerance and vulnerability to varying degrees of threat, should be included in different security areas. The principle of "hiding information" is considered as one of the extended cases of this rule, so that IT systems only provide data that is necessary to perform the tasks of the IT system. The system can be provided as servers for Internet service providers which are registered only in public DNS. The principle of minimum points people connected to the IT system (such as users and system administrators) must have the minimum privileges necessary for optimal performance in the organization. This also applies to data and services that are made available to external users. One of the extensions of this rule is the principle of "necessity to know", according to which users and managers of IT systems have access only to information related to their roles and tasks [34].

The level of security of the IT system depends on the factor that has the least security. One of the extensions of this rule is the principle of Single Point of Failure (SPOF), which is related to the availability of network services, according to which all links, equipment (network and security) as well as servers on network routes between users and important resources IT system performance must be implemented in redundant configurations. When designing a network security system, the principles of organizational security should be considered, including the rules of "segregation of duties" and "workflow". The purpose of these principles is to limit the ability of employees to disregard and violate IT system security policies. Separation of duties means that important tasks and functions must be performed by two or more employees [35]. Also, job turnover should be considered for important job positions in terms of security measures of networks. IT systems resources with different levels of sensitivity should be located in different security areas. Computer equipment and services providers for external networks (such as the Internet provider companies) should be located in different areas (such as De-Militarized Zone), unlike computer systems and internal network equipment. Strategic IT system resources must be located in specific security areas to be secured [36]. Low-reliability computer equipment and systems, such as remote access servers and wireless network access points, should also be included in specific security areas. Different types of IT system resources should be placed in separate security areas. Workstations for users must be located in different security areas, unlike servers. Security and network management systems must be located in specific security areas. Systems in the development phase must be located in a different sector, unlike systems related to the production phase [37].

C. Preventing Intrusion and Firewalls

The firewalls in software or hardware systems act as a security wall between the users of networks and the world outside. Firewalls are usually located on the border between our network and the Internet. Hardware firewalls can monitor the content and communication paths of our network. Firewalls define the rules for how information enters and leaves our network and the Internet. In fact, we use firewalls to determine which data have the right to enter and exit and which should not [38], [39]. The software firewalls are cost-effective tools in the fire wall systems and they can examine patterns and content and can give a little oversight of the threats. In addition, hardware firewalls are very powerful and therefore can be used more than their software modes [40], [41]. At the user's discretion, the firewall is the main tool for maintaining or restricting the flow of network traffic in various situations such as dedicated firewall equipment, firewall function in IPS equipment and access control list in network switches and routers. With proper deployment and configuration, firewalls can help build secure architectures, split the IT network infrastructure into security domains, and control the communication between them [42].

To increase cyber-attack to the secured data, an advanced IDS is developed by [43]. In this paper, an advanced cyber-attack modeling is presented to prevent access of hackers to the secured data in the networks. Viruses, worms and trojans try to spread across the network and can remain on asymptomatic infected devices for days or weeks. Our job is to make a security effort to prevent the penetration of this type of malware as well as malware that opens the way for them.

The implementation of the network security process to prevent intrusion by controlling users' limited access to the internal network is shown in Fig. 3 [19]. In this example, Internet services for internal users are only available through corporate email and Hyper Text Transfer Protocol (HTTP) Proxy servers.

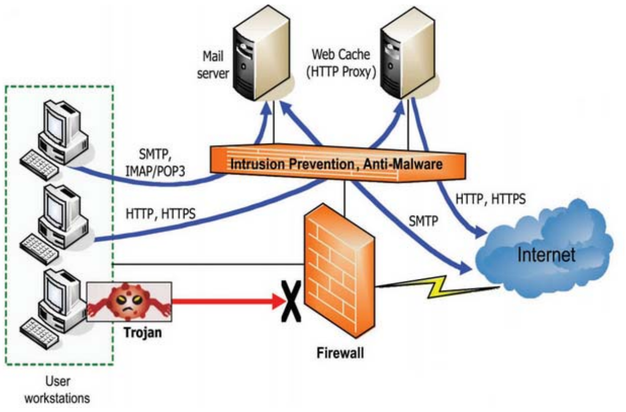

Fig. 3 Prevent intrusion by controlling users' limited access to the internal network [19]

D.Effective Considerations in Network Security

The overall strategy in this case consists of three steps. In fact, network security includes the following:

1- Protection: We need to configure our systems and network properly.
2- Detection: We must fully monitor the network and detect changes and the use of network resources that are signs of intrusion.
3- Reaction: Once identified problems, we need to respond to them quickly and quickly provide a secure environment on network [44].

This is a defense strategy against the attackers. If there is one common denominator among security experts, it is dangerous to rely on the first single line of defense. Because any defense tool can be defeated by the enemy. The network is not a line or a point which is really a territory. As a result, if an attacker has attacked part of the secured data, it is possible to save data resources and rescue them if the security system is properly organized for defense techniques [45]. The network security solutions can be presented as,

1- Assessing risks and vulnerabilities and analyzing the selection of appropriate controllers.
2- Optimizing servers, clients, websites and the organization's network environment.
3- Optimization of Cache, Network Address Translation (NAT), Proxy, Internet Protocol (IP) address and routing networks.
4- Advice on choosing the right security standards.
5- Advice on defining and applying guidelines and executive instructions for information security.
6- On-site training or periodically at various levels.
7- Testing the strength of security systems by trying to break them.

Recent development in the network threats and security measures are presented in Table I.

TABLE I
RECENT DEVELOPMENTS IN THE NETWORK THREATS AND SECURITY MEASURES

Topic of research work	Papers	Finding/ Discoveries
Network Threats	[12]	In order to increase the security levels in the network of data, different type of the attacks are presented.
	[46]	Existing tool and systems to protect the secured data against the hackers' attacks are presented.
	[47]	An advanced model of network attacks and security measures against them are discussed to increase security levels in the networks.
Security Measures, Security policy	[14]	To provide an advanced security policy in the networks, attack graphs model is presented.
	[19]	The methods and policies of the network security is presented in order to increase security levels in the web of data.
	[48]	To provide reliable network security in different organization, the security policy is discussed.
Security Measures, network security Implementation	[23]	To implement security systems in complex networks, an advanced flowchart is presented.
	[25]	An advanced access control list is presented to provide network security by using an access restriction method.
	[49]	An advanced security protocol foe the wireless sensor network is presented to increase security in web of data.
Security Measures, Network layering	[29]	Application of deep neural network in the intrusion detection technique is presented in order to prevent hackers to obtain the secured data.
	[32]	Network layer threats is discussed in the study to provide security measures for the Network layering process.
	[50]	Application of the cloud computing systems in the Network layering techniques is investigated to increase security levels in the web of data.
Security Measures, firewalls	[38]	To offer in depth security for the networks, an advanced traffic filtering models using web firewalls are presented.
	[51]	Tree-Rule Firewall is developed in the study to increase quality in cloud network security systems.
	[52]	The quality of policy configured in the firewalls is discussed to increase efficiency of network security systems.

III. Conclusion

Network Security is a process in which a network is protected against various types of internal and external threats. The purpose of network security is to protect the network against the above attacks, so the goals can be presented in three categories: 1- Proving data confidentiality, 2- Maintaining comprehensive data, 3- Maintaining data availability. The following steps have been suggested and approved for security: 1- Identifying the part that should be protected, 2- Deciding on the cases against which the section in question should be protected, 3- Deciding on how to make threats, 4- Implementing facilities that can protect your assets in a cost-effective way, 5- Continuous review of the process and strengthening it in case of weakness. By defining a security policy, we achieve its implementation in the form of a network security plan. The elements that make up a network security plan are: 1- Security features of each device such as managerial password or using Secure Shell (SSH), 2- Firewalls, 3- VPN integrators for remote access, 4- Intrusion detection, 5- AAA security servers and other AAA services for the network, 6- Access control and access restriction mechanisms for different network devices. In order to increase security of different systems, and advanced web of security systems can be connected together in order to share advantages of each system in different locations. Advanced monitoring system to the security techniques can be implemented to decrease the rate of intrusion to the secured data. New protocols and rules for the security measures of the different organization regarding the new levels of the attacks to the networks should be provided in order to secure the data. So, new solution regarding the developed threats should be presented to increase security levels in the networks. The hardware of network security systems can be modified in order to provide advanced security measures in the web of data. The new firewall software regarding the developed methods of hackers can be presented in order to provide a key tool in the data protection systems. An advanced model of hardware processor and software communication system to detect and prevent the network attacks can be implemented in terms of network security enhancement process. As a result, an advanced network security system can be presented in order to decrease the levels of data access by the hackers. These are suggestions for the future research works in order to develop the data protection methods and network security systems.

References

[1] S. Tayal, N. Gupta, P. Gupta, D. Goyal, and M. Goyal, “A Review paper on Network Security and Cryptography.” *Advances in Computational Sciences and Technology*, vol. 10 (5), pp. 763-770, 2017.

[2] R. Khan, and M. Hasan, “Network threats, attacks and security measures: A review.” *International Journal of Advanced Research in Computer Science*, vol. 8 (8), pp. 116-120, 2017.

[3] S. Rathore, P. K. Sharma, V. Loia, Y.-S. Jeong, and J. H. Park, “Social network security: Issues, challenges, threats, and solutions.” *Information sciences*, vol. 421pp. 43-69, 2017.

[4] S. Gao, Z. Li, B. Xiao, and G. Wei, “Security threats in the data plane of software-defined networks.” *IEEE network*, vol. 32 (4), pp. 108-113, 2018.

[5] T. Islam, D. Manivannan, and S. Zeadally, “A classification and characterization of security threats in cloud computing.” *Int J Next-Gener Comput*, vol. 7 (1), pp. 268-285, 2016.

[6] L. R. Bays, R. R. Oliveira, M. P. Barcellos, L. P. Gaspary, and E. R. M. Madeira, “Virtual network security: threats, countermeasures, and challenges.” *Journal of Internet Services and Applications*, vol. 6 (1), pp. 1, 2015.

[7] P. Sinha, A. kumar Rai, and B. Bhushan “Information Security threats and attacks with conceivable counteraction,“ *In: 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT). IEEE*, pp. 1208-1213, 2019.

[8] R. Dastres, and M. Soori, “Impact of Meltdown and Spectre on CPU Manufacture Security Issues.” vol. 18(2) pp., 62-69, 2021.

[9] A. Tayal, N. Mishra, and S. Sharma, “Active monitoring & postmortem forensic analysis of network threats: A survey.” *International Journal of Electronics and Information Engineering,* vol. 6 (1), pp. 49-59, 2017.

[10] Z. Lu, X. Lu, W. Wang, and C. Wang “Review and evaluation of security threats on the communication networks in the smart grid,“ *In: 2010-Milcom 2010 Military Communications Conference. IEEE,* pp. 1830-1835, 2010.

[11] A. Simmonds, P. Sandilands, and L. Van Ekert “An ontology for network security attacks,“ *In: Asian Applied Computing Conference. Springer,* pp. 317-323, 2004.

[12] M. V. Pawar, and J. Anuradha, “Network security and types of attacks in network.” Procedia Computer Science, vol. 48pp. 503-506, 2015.

[13] F. L. Greitzer, and R. E. Hohimer, “Modeling human behavior to anticipate insider attacks.” *Journal of Strategic Security,* vol. 4 (2), pp. 25-48, 2011.

[14] K. Kaynar, “A taxonomy for attack graph generation and usage in network security.” *Journal of Information Security and Applications,* vol. 29pp. 27-56, 2016.

[15] R. Khondoker, P. Larbig, D. Senf, K. Bayarou, and N. Gruschka “AutoSecSDNDemo: Demonstration of automated end-to-end security in software-defined networks,“ *In: 2016 IEEE NetSoft Conference and Workshops (NetSoft). IEEE,* pp. 347-348, 2016.

[16] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan “Internet of things (IoT) security: Current status, challenges and prospective measures,“ *In: 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST). IEEE,* pp. 336-341, 2015.

[17] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti, and M. Jo, “Design of secure user authenticated key management protocol for generic IoT networks.” *IEEE Internet of Things Journal,* vol. 5 (1), pp. 269-282, 2017.

[18] H. I. Kobo, A. M. Abu-Mahfouz, and G. P. Hancke, “A survey on software-defined wireless sensor networks: Challenges and design requirements.” IEEE access, vol. 5pp. 1872-1899, 2017.

[19] M. Stawowski, “The principles of network security design.” *ISSA Journal*, vol. pp. 29-31, 2007.

[20] D. Barrera, I. Molloy, and H. Huang “Standardizing IoT network security policy enforcement,“ *In: Workshop on Decentralized IoT Security and Standards (DISS).* p 6, 2018.

[21] J. Liu, Y. Li, H. Wang, D. Jin, L. Su, L. Zeng, and T. Vasilakos, “Leveraging software-defined networking for security policy enforcement.” *Information Sciences,* vol. 327pp. 288-299, 2016.

[22] R. Neisse, G. Steri, and G. Baldini “Enforcement of security policy rules for the internet of things,“ *In: 2014 IEEE 10th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). IEEE*, pp. 165-172, 2014.

[23] F. Hu, Q. Hao, and K. Bao, “A survey on software-defined network and openflow: From concept to implementation.” *IEEE Communications Surveys & Tutorials,* vol. 16 (4), pp. 2181-2206, 2014.

[24] B. Wang, K. Lu, and P. Chang “Design and implementation of Linux firewall based on the frame of Netfilter/IPtable,“ In: 2016 11th International Conference on Computer Science & Education (ICCSE). IEEE, pp. 949-953, 2016.

[25] S. Zheng, Z. Li, and B. Li “Implementation and application of ACL in campus network,“ *In: AIP Conference Proceedings.* vol 1. AIP Publishing LLC, p 090014, 2017.

[26] T. Hayajneh, S. Ullah, B. J. Mohd, and K. S. Balagani, “An enhanced WLAN security system with FPGA implementation for multimedia applications.” *IEEE Systems Journal*, vol. 11 (4), pp. 2536-2545, 2015.

[27] M. Ali, S. U. Khan, and A. V. Vasilakos, “Security in cloud computing: Opportunities and challenges.” *Information sciences,* vol. 305pp. 357-383, 2015.

[28] P. Sinha, V. Jha, A. K. Rai, and B. Bhushan “Security vulnerabilities,

attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey,“ *In: 2017 International Conference on Signal Processing and Communication (ICSPC). IEEE,* pp. 288-293, 2017.

[29] M.-J. Kang, and J.-W. Kang “A novel intrusion detection method using deep neural network for in-vehicle network security,“ In*: 2016 IEEE 83rd Vehicular Technology Conference (VTC Spring). IEEE*, pp. 1-5, 2016.

[30] R. Dastres, and M. Soori, “Secure Socket Layer in the Network and Web Security.” *International Journal of Computer and Information Engineering,* vol. 14 (10), pp. 330-333, 2020.

[31] S. Climent, A. Sanchez, J. V. Capella, N. Meratnia, and J. J. Serrano, “Underwater acoustic wireless sensor networks: advances and future trends in physical, MAC and routing layers.” *Sensors,* vol. 14 (1), pp. 795-833, 2014.

[32] V. Pruthi, K. Mittal, N. Sharma, and I. Kaushik “Network Layers Threats & its Countermeasures in WSNs,“ *In: 2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS). IEEE,* pp. 156-163, 2019.

[33] J. Singh, Y. Bello, A. Refaey, and A. Mohamed, “Five-Layers SDP-Based Hierarchical Security Paradigm for Multi-access Edge Computing.” *arXiv preprint arXiv :200701246*, vol. pp., 2020.

[34] N. Wagner, C. Ş. Şahin, J. Pena, J. Riordan, and S. Neumayer “Capturing the security effects of network segmentation via a continuous-time markov chain model,“ *In: Proceedings of the 50th Annual Simulation Symposium. Society for Computer Simulation International*, p 17, 2017.

[35] M. Oqaily, Y. Jarraya, M. Mohammady, S. Majumdar, M. Pourzandi, L. Wang, and M. Debbabi, “SegGuard: Segmentation-based Anonymization of Network Data in Clouds for Privacy-Preserving Security Auditing.” *IEEE Transactions on Dependable and Secure Computing,* vol. pp., 2019.

[36] R. Du, C. Zhao, S. Li, and J. Li, “Efficient weakly secure network coding scheme against node conspiracy attack based on network segmentation.” *EURASIP Journal on Wireless Communications and Networking,* vol. 2014 (1), pp. 1-9, 2014.

[37] S. Bazrafkan, S. Thavalengal, and P. Corcoran, “An end to end deep neural network for iris segmentation in unconstrained scenarios.” *Neural Networks,* vol. 106pp. 79-95, 2018.

[38] V. Clincy, and H. Shahriar “Web application firewall: Network security models and configuration,“ *In: 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC). IEEE,* pp. 835-836, 2018.

[39] Zerkane, D. Espes, P. Le Parc, and F. Cuppens “Software defined networking reactive stateful firewall,“ *In: IFIP International Conference on ICT Systems Security and Privacy Protection. Springer,* pp. 119-132, 2016.

[40] A. B. Achballah, S. B. Othman, and S. B. Saoud “FW_IP: A flexible and lightweight hardware firewall for NoC-based systems,“ *In: 2018 International Conference on Advanced Systems and Electric Technologies (IC_ASET). IEEE,* pp. 261-265, 2018.

[41] H. Yuan, L. Zheng, S. Qiu, X. Peng, Y. Liang, Y. Hu, and G. Deng “Design and Implementation of Enterprise Network Security System Based on Firewall,“ *In: The International Conference on Cyber Security Intelligence and Analytics. Springer,* pp. 1070-1078, 2019.

[42] M. N. Chowdhury, K. Ferens, and M. Ferens “Network intrusion detection using machine learning,“ *In: Proceedings of the International Conference on Security and Management (SAM). The Steering Committee of The World Congress in Computer Science, Computer …,* p 30, 2016.

[43] M. E. Kuhl, M. Sudit, J. Kistner, and K. Costantini “Cyber attack modeling and simulation for network security analysis,“ *In: 2007 Winter Simulation Conference. IEEE,* pp. 1180-1188, 2007.

[44] W. Saad, X. Zhou, B. Maham, T. Basar, and H. V. Poor, “Tree formation with physical layer security considerations in wireless multi-hop networks.” *IEEE Transactions on Wireless Communications,* vol. 11 (11), pp. 3980-3991, 2012.

[45] G. Dini, and M. Tiloca “Considerations on security in zigbee networks,“ *In: 2010 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing. IEEE,* pp. 58-65, 2010.

[46] N. Hoque, M. H. Bhuyan, R. C. Baishya, D. K. Bhattacharyya, and J. K. Kalita, “Network attacks: Taxonomy, tools and systems.” *Journal of Network and Computer Applications,* vol. 40pp. 307-324, 2014.

[47] V. Gorodetski, and I. Kotenko “Attacks against computer network: Formal grammar-based framework and simulation tool,“ *In: International Workshop on Recent Advances in Intrusion Detection. Springer,* pp. 219-238, 2002.

[48] J. G. Alfaro, N. Boulahia-Cuppens, and F. Cuppens, “Complete analysis of configuration rules to guarantee reliable network security policies.” *International Journal of Information Security,* vol. 7 (2), pp. 103-122, 2008.

[49] A. Sahana, and I. S. Misra “Implementation of RSA security protocol for sensor network security: Design and network lifetime analysis,“ *In: 2011 2nd International Conference on wireless communication, vehicular technology, information theory and aerospace & electronic systems technology (Wireless VITAE). IEEE,* pp. 1-5, 2011.

[50] C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, “A survey on security issues and solutions at different layers of Cloud computing.” *The journal of supercomputing,* vol. 63 (2), pp. 561-592, 2013.

[51] X. He, T. Chomsiri, P. Nanda, and Z. Tan, “Improving cloud network security using the Tree-Rule firewall.” *Future generation computer systems,* vol. 30pp. 116-126, 2014.

[52] H. Hu, G.-J. Ahn, and K. Kulkarni, “Detecting and resolving firewall policy anomalies.” *IEEE Transactions on dependable and secure computing,* vol. 9 (3), pp. 318-331, 2012.