REVIEW OF NETWORK SECURITY MEASURES AND THREATS: RECENT DEVELOPMENTS AND FUTURE RESEARCH DIRECTIONS

Anuj Kumar Dwivedi
Assistant Professor, Ajay Kumar Garg Engineering College, Ghaziabad, UP, India
dwivedianuj@akgec.ac.in

***Abstract*—Remote access and data communication render networks vulnerable to various threats. Thus, network security is essential for data sharing and communication. This article emphasises network security in IT systems and reviews contemporary network threats and security remedies. The main goal is to prevent hackers from accessing secured data and provide a secure communication device for consumers. The review also examines network threats and data web security procedures. The report proposes new research directions to advance research. This paper discusses network security for secure data communication.**

***Keywords*—Remote access, security measures, network hazards, Research Directions**

I. INTRODUCTION

The rapid incorporation of computer technology in a variety of disciplines and the continuous development of automation systems are gradually reshaping the traditional labour landscape. As modern office environments adopt paperless and networked systems, conventional methods of work face increasing difficulties. Particularly, the commercialization of the Internet has propelled the Internet industry forward, resulting in extraordinary progress.[1].

As companies rely more on IT infrastructures, network security is crucial. Organisations risk irreparable system and reputation damage without adequate security. Layered security, which incorporates hardware, software, and user education to prevent multiple types of network attacks, is essential. Firewalls, intrusion detection systems, antivirus programmes, security updates, and employee education and training on best practises are all part of this. By implementing these safeguards, organisations can safeguard their networks from danger and keep their data secure and private. The risks to network resources' confidentiality, availability, and integrity are discussed in this section. Different types of network threats can arise from different sources, such as malware, unauthorized access, phishing attacks, denial-of-service (DoS) attacks, and man-in-the-middle (MitM) attacks. Effective security measures are critical to preventing these network threats. Network security prevents data misuse by properly implementing security measures. To remain competitive, companies must safeguard their sensitive data. Data loss, manipulation, and confidentiality breaches can lower a company's production and marketing value. Therefore, network administrators must set strict policies and monitor network resource access, misuse, and manipulation. We categorise and analyse network threat and security research issues in this paper to help researchers. We identify literature gaps and propose future research to advance this important field. Section II covers the literature review, while Section III concludes and suggests future research.

II. LITERATURE REVIEW

Numerous studies and researches have been conducted on security because it is one of the mostfundamental requirements of IT infrastructures. The various dangers to a network and the precautions that must be taken against them are discussed here.

Let's take a closer look at some of the most common network threats and the corresponding measures to prevent them.

A. Threats and Attacks to Network Security

To secure network data, It is critical to comprehend the various kinds of attacks that can happen. Network attacks can be classified into three main categories:

i) Unauthorized access to resources and information,
ii) Unauthorized manipulation of information,
iii) Attacks that cause service delivery to be disrupted (also referred to as "Denial of Service" attacks).

Illegal attempts to access password-protected networks and informational areas are considered unauthorised access to resources and information. Passwords can be cracked, false identities can be created, and malware can be used to accomplish this. Another type of attack is information

destruction, which involves trying to delete specific data by using database commands. This could have disastrous effects on the network. The attacker must enter the user or management area to carry out prohibited commands, such as writing, editing, sending emails, copying, or deleting specific information. These attacks result in service delivery disruption.

Threats to network security can also be grouped under Logic Attacks or Recourse Attacks. Logic attacks seek to compromise the system or gain unauthorised access by taking advantage of security flaws or software vulnerabilities in the code. Attacks known as "recourse" are designed to deplete network resources and may involve spamming the server with requests for services or infecting the network with malware.

Additionally, there are various categories for attacks on secured networks. Monitoring the organization's network for vulnerabilities constitutes a passive attack. Active attacks directly target the organization's servers and can be observed by security programmes like firewalls and intrusion prevention systems (IPS). Physical security can stop internal attacks from occurring because they require physical access to systems. Focusing on authentication and ensuring physical security will help prevent insider attacks, which are conducted by internal users with access to systems and data.

Implementing effective security measures to safeguard the network and its data requires understanding the various network security threats and attacks.

B. Security Measures

Network security is a key component of ensuring the security of the data and resources in the web of data. It is important to defend against all types of attacks on a variety of resources, including firewalls, routers, switches, network operation information, intangible network resources, information and information resources, terminals, and user operations.

The security measures of networks should be designed using appropriate designing methods and principles in order to implement an advanced security system in the web of data.

In order to defend networks, there are many essential steps that make up network security. Among the most important security precautions are firewalls, intrusion detection systems, web application firewalls, intrusion detection and prevention systems, virtual private network (VPN) protections, and content review systems like antivirus, anti-malware, anti-spam, and URL filtering. Together, these procedures are extremely important for defending networks against potential threats and unwanted activity.

After conducting a risk analysis in the web of data, the security policy should be constructed to reduce both risk and damage to a minimum. What and why the data needs to be protected, who is in charge of it, and setting up a framework to settle any potential conflicts are all part of the security policy. Permissive and restrictive security regulations can be broadly categorised into each other. In general, tightening security policies is a better and more suitable approach to enhancing network system security.

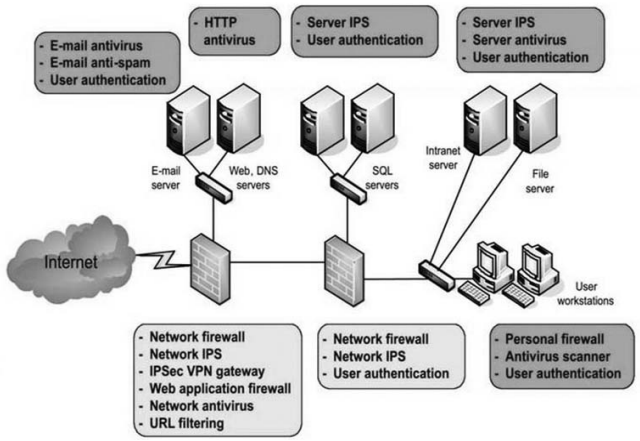

Figure 1: Comprehensive defense principle[3]

The protection of various IT system resources using a number of complementary security layers is the basis for the comprehensive defense strategy shown in Fig.1.Implementing network security entails making sure a network is completely ready for potential threats. To ensure that network security is implementedeffectively, there are a number of guidelines toremember. First, all network components need to have valid licenses and authentication and protection proceduresin place. The second recommendation is to regularly track and review network activities and the continuity of protection activities. Thirdly, a trusted individual should simulate an attack in order to evaluate the weaknesses of the security policies intended for the network. Finally, data should be gathered to improve security measures based on all the previous steps.

A successful network security strategy requires ongoing monitoring and upkeep. Network administrators must stay current with these updates because attackers are always refining their methods for gaining access to secured data. In order to remove danger, risk assessment is also crucial. After identifying the network assets and the threats to them, different risks should be evaluated. The most significant risks will be determined by a thorough assessment of the different types of risks, along with the sources that need to be protected from them.

Another crucial component of implementing network security is network layering. Each network activity can be protected separately thanks to the classification of security levels, and

the security parameters of one level are unaffected by the security policies of the other level. By classifying network activities and assigning them to various levels of security, network security levels enable the examination of the securityof each activity independently. This makes it possible to manage security measures accurately at each level. Examplesof using the network security level in network security measures include VoIP service at the service security layer, service management security, independent of service control security, and independent of user-side data security.

At all levels and layers of enterprise IT architecture, related security solutions will be applied to raise the security level of a comprehensive IT infrastructure. A hierarchical solution for network security is proposed after three layers of security are taken into account and defined. The security of transmission network infrastructure as well as specific network tools is covered by the infrastructure security layer. The security of the services that service providers offer to their customers is the main focus of the service security layer. The final layer, application security, focuses on the web-based applications that are accessible to users. Application Service Providers (ASPs), the service provider itself as an ASP, or their host companies with a separate data centre can all offer network applications. Application users, application providers, sub-providers, and service providers can all be seen as threats in this layer.

The network security's application security layer's organisational structure and each section's duties are shown in Fig.2[8].

- **Control security level:** This layer supports operations that are in charge of communicating data about services or network applications. This level typically includes network-wide machine-to-machine communication, which frequently includes control messages [8].
- User-side security level: This level covers securing user-side access to and utilisation of the services offered by the provider. End users can access extension services like VPNs, application-based networks, or the service provider's network directly [8].
- Information segmentation IT system resources should be divided into different security zones according to their degree of sensitivity, risk tolerance, and susceptibility to threats. In order to ensure that IT systems only provide data required to carry out their intended functions, the principle of "hiding information" is regarded as one of the extended cases of this rule. For Internet service providers who are only registered in public DNS, the system can be made available as servers. According to the minimum points principle, users and system administrators who are connected to an IT system should only have the minimal access rights required for optimum organization-wide performance. This also holds true for information and services that are offered to outside users. The "necessity to know" principle, which states that users and managers of IT systems only have access to information relevant to their roles and tasks, is one of the extensions of this rule [4].

The weakest part of an IT system determines its security. The Single Point of Failure (SPOF) idea is strongly related to this theory, especially addressing network service availability. According to this approach, all network cables, equipment (including network and security devices), and servers along the network channels linking users to key IT resources should be redundantly configured. This assures system performance

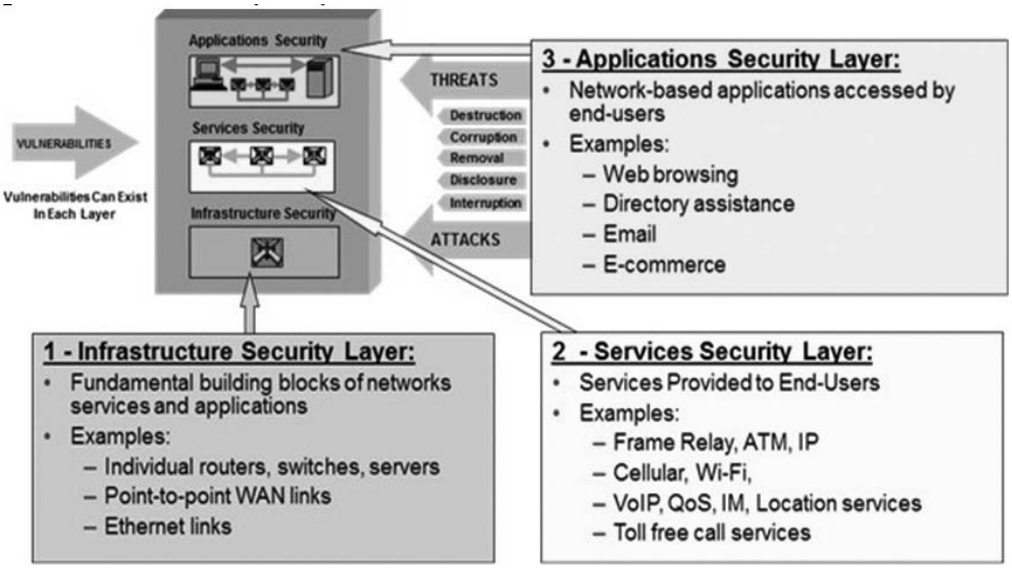

Figure 2: The network security with Application of securitylayer[8]

is unaffected by component failures or disturbances. The "segregation of duties" and "workflow" principles, as well as other organisational security principles, should be taken into account when designing a network security system. These rules are intended to restrict employees' ability to disobey and transgress IT system security regulations. Separation of duties refers to the requirement that significant tasks and duties be carried out by two or more employees [9]. Regarding the security measures of networks, it is also important to take job turnover into account for important job positions. Different security areas should house IT system resources with varying degrees of sensitivity. Contrary to computer systems and internal network equipment, computer equipment and services providers for external networks (suchas Internet service providers) should be located in different locations (such as the De-Militarized Zone). To be secure, strategic IT system resources must be situated in designated security zones . Specificsecurity zones should also includelow-reliability computer hardware and software, such as wireless network access points and remote access servers. Resources for various IT systems should be kept in separate security zones. In contrast to servers, workstations for users must be situated in separate security zones. Systems for network management and security must be installed in designated security locations. Contrary to systems related to the production phase, systems in the development phase must be situated in a different industry.

C. Firewalls and Intrusion Prevention

Firewalls safeguard network users from external threats. They're usually installed at the Internet-network interface. Hardware firewalls can monitor network traffic. They regulate data transfer between our network and the Internet.

Firewalls determine which data can enter and leave a system and which cannot [9]. Software firewalls provide basic threat supervision by examining patterns and content. Hardware firewalls are more efficient and can be employed more often [10], [1121]. The firewall controls network traffic flow through dedicated firewall equipment, firewall functionality in IPS equipment, and access control lists in network switches and routers. Secure architectures, security domains, and communication can be regulated by properly implementing and configuring firewalls [11].

Built a sophisticated Intrusion Detection System (IDS) to protect sensitive data from cyberattacks12. This research proposes a sophisticated cyber-attack model to prevent unauthorised network data access. Viruses, worms, and trojans spread through networks by staying dormant on infected devices. We must take proactive security measures to prevent such malware from infiltrating, including potential access points.

Figure 3 [3] demonstrates the implementation of network security measures to prevent intrusion by restricting users' access to the internal network. The illustration depicts that internal users are only permitted to access specific Internet services, namely corporate email and HTTP Proxy servers. This restricted access helps in maintaining a secure network environment.

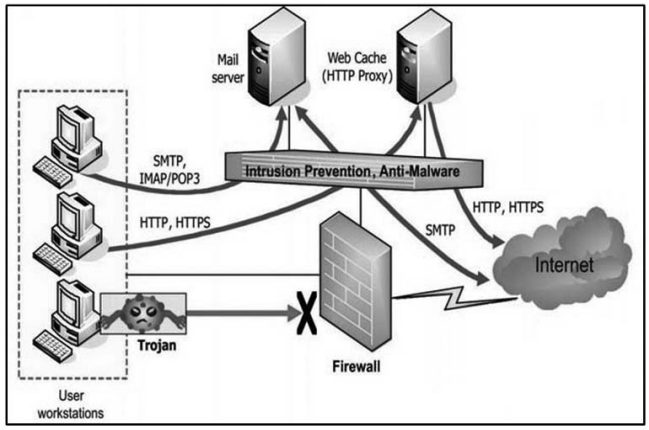

Figure 3: Prevent intrusion by controlling users' limited access to the internal network [3]

D. Effective Considerations in Network Security

Three steps make up the plan in this scenario. In fact, the following are part of network security:

1. Protection: Our systems and network need to be properly configured.
2. Detection: We must keep a close eye on the network to spot any alterations and the use of resources that indicate an intrusion.
3. Reaction: As soon as a problem is identified, we must act quickly to fix it and create a safe network environment [12].

A thorough strategy is necessary to repel attacks. Security professionals all agree that using just one line of defence can be dangerous since determined attackers can find ways to get around any defensive measure. It is crucial to understand that a network is an area rather than just a line or a point. Therefore, even if some of the encrypted data is hacked, deploying a well-designed security system with strong defence tactics can provide a safeguard. In these circumstances, it might still be viable to save and recover data resources [13].

To improve overall protection, a variety of network security methods are available. Some of these choices consist of:

1. Evaluating risks and vulnerabilities and considering the choice of suitable controllers.
2. Improving the network environment of the company and its servers, clients, and websites.
3. Networks for caching, NAT, proxies, Internet Protocol (IP) addresses, and routing are optimised.

4. Suggestions for picking the appropriate security standards.
5. Guidance on formulating and implementing rules and directives for information security.
6. Periodic or on-site training at different levels.
7. Attempting to defeat security systems to gauge their robustness.

Table 1. Recent developments in network threats and security measures.

Research Domain	***Papers***	***Findings and Discoveries***
Network Threats	[1]	Various types of attacks are presented to increase the security levels in the data network.
	14	Presenting existing tools and systems to defend secured data from hacker attacks
	15	The discussion of countermeasures to raise network security levels.
SecurityMeasures, Security policy	[2]	Attack graphs model is presented to provide an advanced security policy in the networks.
	[3]	presented in an effort to raise the level of security in the data web.
	[16]	The security policy is discussed in order to provide dependable network security in various organisations..
SecurityMeasures, network Security Implementation	[4]	An advanced flowchart is presented to implement security systems in complex networks.
	[5]	As a way of access limitation to improve network security, an advanced access control list is introduced.
	[17]	To improve security in the data web, a cutting-edge security protocol for wireless sensor networks is presented.
SecurityMeasures, Network layering	[6]	In order to stop hackers from obtaining the secured data, a deep neural network application in the intrusion detection technique is presented.
	[7]	Assist the network layering process with security measures.
	[18]	The use of network layering techniques is being researched to improve data web security.
SecurityMeasures, firewalls	[9]	Web firewall traffic filtering models are presented.
	[19]	To improve the caliber of cloud network security systems, the study develops a tree-rule firewall.
	[20]	The effectiveness of network security systems is discussed in relation to the quality of policy configured in firewalls.

III. CONCLUSION

Network security is essential to safeguard networks from internal and external attacks. It prioritises data confidentiality, integrity, and availability. To achieve these goals, several steps have been suggested and approved: identifying the areas that need protection, determining the specific threats to address, devising strategies to counter these threats, implementing cost-effective security measures, and continually reviewing and strengthening the security process.

A well-defined network security policy includes many parts. These include using firewalls, VPN solutions for remote access, intrusion detection systems, AAA security servers, and other related services, as well as access control and restriction mechanisms for different network devices.

Connecting advanced security systems improves system security. This lets systems share benefits and knowledge across sites. Advanced monitoring systems and keeping up with security trends can also reduce data breaches. New protocols and guidelines to address network threats are needed to secure organisations and their data.

Network security hardware modifications can enhance data network security. New firewall software that addresses emerging hacking methods can also help data protection systems. An innovative hardware processor and software communication system model may identify and prevent network threats, improving network security.
An effective network security system prevents unauthorised access and protects data. These ideas are useful for future studies on data protection and network security.

REFERENCES

[1] S.Tayal,N.Gupta,P.Gupta,D.Goyal,andM.Goyal, "AReview-paperon Network Security and Cryptography." *Advances in Computational Sciences and Technology*, vol.10 (5), pp.763-770,2017.

[2] R. Khan, and M. Hasan, "Networkthreats, 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.421 pp.43-69,2017.

[4] S.Gao,Z.Li,B.Xiao,andG.Wei,"Securitythreatsinthedataplaneofsoftware-defined networks." *IEEE network*, vol. 32 (4), pp. 108-113,2018.

[5] 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.

[6] 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.

[7] 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.

[8] H. I. Kobo, A. M. Abu-Mahfouz, and G. P. Hancke, "A survey on software-defined wireless sensor networks:Challenges anddesignre quirements." IEEE access, vol.5 pp.1872-1899, 2017.

[9] D. Barrera, I. Molloy, and H. Huang "Standardizing IoT network security policy enforcement, "In: Workshop on Decentralized IoT Security and Standards (DISS). p6, 2018.

[10] S. Zheng, Z. Li, and B. Li "Implementation and application of ACL in campus network, "In: AIP Conference Proceedings. vol1. AIP Publishing LLC, p090014, 2017.

[11] T. Hayajneh, S. Ullah, B. J. Mohd, and K. S. Balagani, "An WLAN security system with FPGA implementation formultimedia applications." IEEE Systems Journal, vol.11(4), pp.2536-2545, 2015.

[12] P.Sinha, V.Jha, A.K. Rai, and B. Bhushan "Security vulnerabilities attacks and counter measures 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.

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

[14] J. Singh, Y. Bello, A. Refaey, and A. Mohamed, "Five-Layers SDP-Based Hierarchical Security Paradigm for Multi-access Edge Computing." arXivpreprintar Xiv:200701246, vol. pp., 2020.

[18] N. Wagner, C.Ş. Şahin, J. Pena, J. Riordan, and S. Neumayer "Capturing the security effects of network segmentation via a continuous-time mark ovchain model, " In: Proceedings of the 50th Annual Simulation Symposium. Society for Computer Simulation International, p17, 2017.

[19] M.Oqaily, Y. Jarraya, M. Mohammady, S. Majumdar, M. Pourzandi, L. Wang, and M. Debbabi, "Seg Guard: Segmentation-based Anonymization of Network Datain Clouds for Privacy-Preserving Security Auditing." IEEE Transactions on Dependable and Secure Computing, vol. pp., 2019.

[20] S. Bazrafkan, S. Thavalengal, and P. Corcoran, "An end to end deepneural network for iris segmentation in unconstrain edscenarios." Neural Networks, vol.106 pp.79-95, 2018.

[21] 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.

[22] A.B. Achballah, S.B. Othman, and S.B. Saoud "FW_IP: Aflexible and light weight hardware firewall for NoC-based systems, "In: 2018 International Conference on Advanced Systems and Electric Technologies (IC_ASET). IEEE, pp.261-265, 2018.

[23] 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.

ABOUT THE AUTHOR

Anuj Kumar Dwivedi completed his B.Tech. degree from CSJM University, Kanpur. He further obtained an M.Tech in IT from IASE deemed University, Rajasthan. Currently, he is pursuing a Ph.D. in Computer Science & Engineering at Galgotias University in Greater Noida. Anuj Kumar Dwivedi currently holds the position of Assistant Professor in the Computer Science & Engineering Department at Ajay Kumar Garg Engineering College in Ghaziabad, Uttar Pradesh, India.