Asian Journal of Engineering and Applied Technology
ISSN: 2249-068X (P) Vol.12 No.2, 2023, pp.24-28

DOI: https://doi.org/10.51983/ajeat-2023.12.2.3965

A Review of Network Attacks and Security Solutions in a Networked Environment

O. D. Okeh[1], O. F. Ajayi[2], E. A. Emuobonuvie[3] and D. A. Ekokotu[4]
[1,2]Babcock University, Ilesia, Ogun State, Nigeria
[3,4]University of Delta, Agbor, Delta State, Nigeria
E-mail: okeh0054@pg.babcock.edu.ng, ajayioluwa@babcock.edu.ng, andy.emuobonuvie@unidel.edu.ng, esmond.ekokotu@unidel.edu.ng
(Received 2 September 2023; Revised 23 October 2023, Accepted 21 November 2023; Available online 28 November 2023)

***Abstract* - The advancement in technology has led to the interconnectivity of devices referred to as networking. Not only that computers are networked, but the technology also now incorporates all devices giving rise to Internet of Things (IoT). The wide range of connectivity calls for security and protection of data and information as malicious users of the internet have taken advantage of the system. In this paper, we reviewed most of the common threading types of network attack. The paper has x-rayed the different challenges accompanying a network and how they could be detected and handled accordingly. Moreso, the different types of attacks have been looked into with a view to understanding the emerging attacks and how they could be curbed as well. Different security solutions such as cryptography, firewall and blockchain technology were discussed. Obviously, while implementing these security strategies, we are aware that our data and information cannot be fully secured but measures can be put in place to minimize the extent of attack and damages.**
Keywords: **Network Security, Internet of Things (IoT), Cryptography, Firewall, Blockchain**

I. INTRODUCTION

Networking in the twenty first century has emerged as a bedrock to information dissemination. The world would have been something else if not for the interconnectivity of devices. This has not only facilitated fast transfer of data and information but has also made communication easy and to every nook and cranny of the world. Individuals have taken this novel opportunity to collaborate with each other most. This has gone across different institutions, parastatals and organizations. Moreover, some drawbacks do exist in the use of this great technology. The wide connectivity of computers and other Internet devices have given rise to malicious users of the network whether local or international as the case may be. The constant invasion of the internet and network devices by these hoodlums and fraudsters has become a major challenge and must be looked into. This is the idea behind network security.

Network security is a way of protecting a network and its services against unauthorized user [2]. This could occur e in the form of data compression, extraction, modification, destruction, or disclosure. Network security kicks against malicious attackers of a network by offering quality protection and corresponding services to its users. This encompasses unauthorized modification, destruction, or disclosure, creating safety environment for the users of the network [1].

Security has a way of ensuring that the legitimate users and organizations have absolute protection, and the applied techniques are not injurious in any way. The massive involvement of people in use of the internet has attracted has led to proliferation of different kinds of network attacks such as spoofing, smishing, phishing, zero-day, Malware, and other forms of security breaches [3].

With respect to the proliferation of Internet of Things (IoT), network connectivity is currently experiencing different types and kinds of attacks. Most of these attacks violate humans' fundamental rights to information usage as well as transfer of data amongst institutions. This dissemination of information involves transfer confidentiality, integrity, accessibility, denial of services and the likes [4].

Every communication system has a way of managing and securing data and information, which is a primary goal of the organization involved in the network. Communication becomes a necessary weapon upon which many activities now drive. This in turn as given rise to techniques like cryptography and blockchain technologies in the domain of networking for proper and secured handling [16, 17].

II. REVIEW OF RELATED LITERATURE

A. Overview

Despite the fact that much work had been carried in the past in line with network security, a lot intrinsic techniques inherent in its use are yet to be exposed. The necessity to constantly report current security breaches in computer network stands on the verge of constant monitoring based on the fact that new threats are always emerging. This paper intends to review observed security gaps in types of security attacks, use of tools and techniques, as well as security solutions involved in the transmission of data and information in a network, in recent times [13].

B. Types of Attacks

1. Cyber Attacks

According to [18, 19] different network threats are organized into three fundamental themes known as the three D's (Disruption, Distortion, and Deterioration). The rate of attack on computer networks in recent times is alarming, and it needs serious intervention in order to curb the menace caused by such attacks. This act has caused a lot of theft and other forms of data breaches in recent times. Statistics shows a high projection that would likely occur in the near future. The reason being that most organizations are currently facing technological transformation thereby giving room to hackers [5].

2. Network Attacks

Network security has always attracted a high interest in its workability most especially now that Internet of Thing has become the order of the day. Network and Internet of Things (IoT) devices are recognized as sources of network disruption. Most hackers utilizes this current technology in accomplishing dubious and selfish purposes knowing fully well that most users of the Internet are not conversant with threading hazard to the device they use. [6] opined that the addition of more devices into a network aggravate the security breaches.

3. Wireless Network Wormhole Attacks

In a given network, a wormhole scenario is seen as a dangerous attack whereby two attackers positioned themselves in a strategic position while acquiring vital information. Traces of this malicious act is not easily noticed because of the already established position in the network. This scenario goes on unless there is a strong security technique to detect such act [7].

4. Eavesdropping Attacks

An eavesdrop and wormhole attacks are similar in nature. These types of attacks are targeted towards a specific kind of network (wireless network). The malicious users acquire secret information from a network that is loosely connected. The attackers capitalize on the loose nature of the connectivity and as such gains advantage on the network.by installing network monitoring software that captures and extract useful information from the system. Emanating factor such as physical security and other factors capable of affecting a network security was discussed by [8].

III. SECURITY TOOLS AND TECHNIQUES

The responsibility of most network administrators is to protect the establishment data and information. Organizational network security encompasses staff data, information and equipment. This is also extended to customers alike. The needed tools, procedures and techniques to handle these perceived attacks are carefully selected to take care of security challenges. It is highly advised that organization adopt and implement more than one technique in trying to curb security challenges as one tool or technique is incapable of solving security attacks on a network [14, 15].

A. Cryptography

Cryptography is deployed in protecting the protection of data and information in a network. This technique has the ability to encrypt and decrypt data. Cryptography is used to encrypt data moved from one computer stand point to another. It operation involves encoding and decoding of data as it moves from one node to another. This process is capable of handling data breaches in the process of data communication [9]. Cryptography involves the act of using symmetric and asymmetric key algorithms. Asymmetric key algorithms is a process that utilizes a special technique of manipulating big prime numbers, which eventually produces high level of security. Though this technique takes a long time to compute. [5] looked at security of data and information as a primary concern of any communication system.

Cryptography attracts so much benefit when adopted in a network. Cryptographers utilize this technique to ensure that data and information are transferred in the proper way thereby establishing confidentiality and integrity. Cryptography establishes the use digital signatures which prevents hackers from intercepting organizational data. Companies in turn use hash function techniques to maintain the integrity in the flow of data. There are three types of cryptography as identified by [10].

These are
1. Secret Key Cryptography.
2. Public Key Cryptography.
3. Hash Functions.

B. Firewall

Firewall could appear in the form of hardware or software used in protecting data. It has established itself in the network community as a strategic tool used in the security of data. This router setting permits data to freely flow within the network. The firewall setting determines different access or login details. Packet filtering witnesses a drawback because of the difficulty to confirm its source address usage which needs to multiple layers of packet filtering [11]. Identified benefits of firewall security entails its ability to monitor network traffic which include hacking prevention, spyware stoppage, virus attack stoppage and promotes privacy.

C. Blockchain Technology

A blockchain is seen as a decentralized, distributed and public digital ledger. This form of ledger records transactions in a computer system in such a way that the record cannot be easily manipulated retroactively without the alteration of all subsequent blocks and the consensus of the network.

Meanwhile, blockchain is still largely confined to use in recording and storing transactions for cryptocurrencies such as Bitcoin. Blockchain as a database tool has a lot of benefits.. The following are identified business benefits of a blockchain.

1. It saves time. Transaction time is drastically reduced by blockchain technology which is measured by minutes. Transaction is easily accomplished and is faster because they don't require verification by a central authority.
2. It saves cost. Participants are able to exchange items of value directly because the technology eliminates duplication of effort as participants only privileged access to a shared ledger.
3. It offers tighter security. Blockchain's security features cut across diverse sectors where hackers a predominant such as data tampering, fraud, and cybercrime.

IV. NETWORK SECURITY SOLUTIONS

A. Cryptography Implementation

To establish data confidentiality, integrity, authentication, and non-repudiation, there is the need to implement cryptography in a secure network environment. This implementation entails the application and use of secret keys, public keys, and hash functions alike [12]. Cryptography has abroad area coverage in its implementation in managing and taking care of security issues. It is a major technique approach deployed in handling specific security issues. Cryptographic technique has the ability to encrypt and decrypt information using strategic pattern. These features make it a useful tool for security implementation. Some of the mechanisms utilized by encryption mechanisms are encipherment, digital signature and access control.

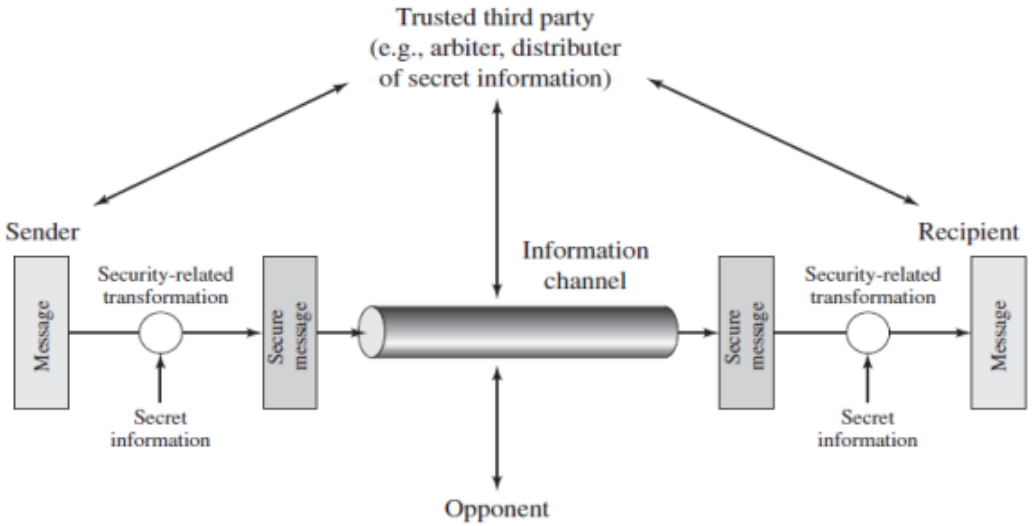
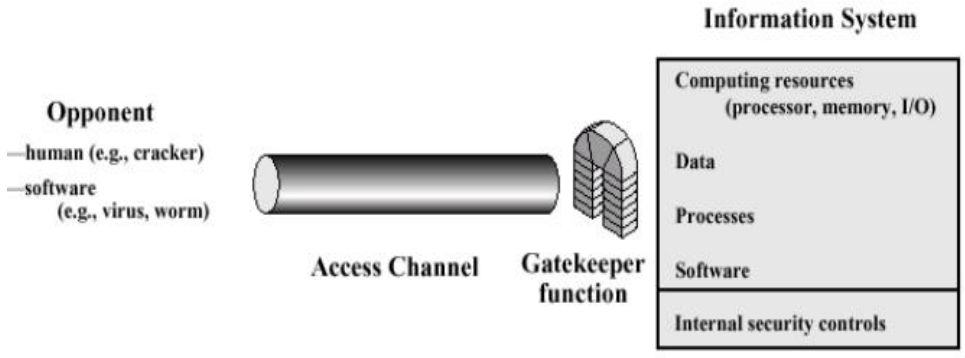


Fig. 1 Model for Combating Security Breaches

The security model indicted by Fig. 1, demonstrates the passage of message from one party using connected devices. The concerned parties must work together for the exchange to take place. Deploying this model requires designing a suitable algorithm for the security transformation. The generation of secret information (keys) activated by the algorithm is used to establish methods that will allocate the secret information in the network. Moreso, a protocol enabling the two parties to use the transformation and secret information for a security service is established.



Source: Science Direct

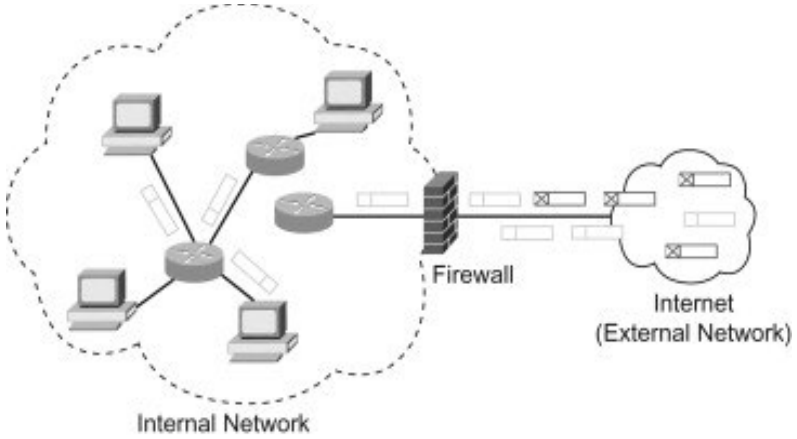
Fig. 2 Network Access Security Model

This model requires selecting right control functions in the identification of users. It also implements security controls to ensure only authorized users gain access to specified information and resources.

This approach validates the fact that only computers that are not compromised are used in the implementation of the model.

B. Firewall Implementation

Firewalls is primarily used in Internet security. Its implementation extends to network environments to handle tasks like restricting connectivity across internal network environments which involves sensitive data. This act is capable of preventing unauthorized access to internal systems and resources.



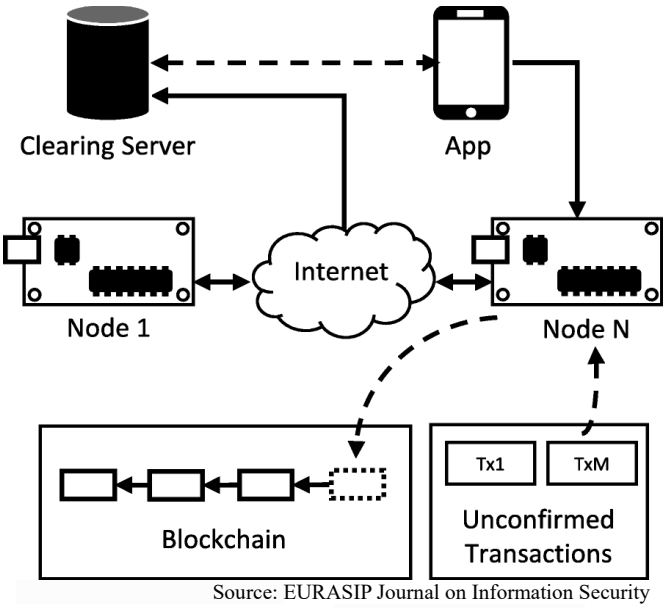
Source: Science Direct

Fig. 3 Firewall setup

Network security employs the implementation of a firewall such as the one shown in fig3. Its configuration needs to be properly configured in order to keep its organization properly protected from data leakage and cyberattacks. Firewall works at different types of environments ranging from a simple packet filtering to combination of several firewalls.

C. Blockchain Implementation

Blockchain technology is a current and dynamic technology being used in the network environment to handle data immutability and integrity and it also provides safe and effective workflow automation.



Source: EURASIP Journal on Information Security

Fig. 4 A Blockchain System showing its main Components

Fig. 4 demonstrates the connectivity inherent in a blockchain system whereby nodes are interconnected via the Internet within a Virtual Private Network (VPN). This connectivity promotes communication among the nodes despite the fact that it does not involve the use of public IP addresses. A clearing server is installed at each utility's premises. This server is also connected to a client listening on the blockchain and noting each customer in order to calculate the net energy consumption of each participant. The application also disseminates the information as a feedback to each user.

V. CONCLUSION

It is obvious that network activities are growing so also the likelihood of security issues and challenges. Internet of Things has to a great extent complicated the issues of securities since its emergence, as almost every gadget around the globe is being connected in one form or the other. The wide connectivity giving room for breaches both within and outside a given network. Deploying defensive measures in solving network issues is very important. This deployment is capable of reducing the chances of data being lost or stolen by malicious users of the network. It will also enhance the productivity of the network and its security. A network is expected to deploy all available tools and methodologies to handle its security challenges without relying on one technique or instrument only. In the same vain, while deploying the tools, techniques and procedures, organization are expected to position their employees and customers in the know, thereby informing them about the current security dangers.

REFERENCES

[1] S. Pandey, "Modern network security: Issues and challenges," *International Journal of Engineering Science and Technology*, vol. 3, no. 5, pp. 4351-4357, 2011.

[2] J. X. Wu, "Cyberspace endogenous safety and security," *Engineering*, 2021, DOI: 10.1016/j.eng.2021.05.015.

[3] J. X. Wu, *Cyberspace Endogenous Safety and Security: Mimic Defense and General Robust Control* (in Chinese). Beijing: Science Press, 2020.

[4] L. Caviglione *et al.,* "Tight arms race: Overview of current malware threats and trends in their detection," *IEEE Access*, vol. 9, pp. 5371-5396, December 2020.

[5] S. Bhattacharya *et al.,* "A novel PCA-firefly based XGBoost classification model for intrusion detection in networks using GPU," *Electronics*, vol. 2, no. 19, pp. 219, 2020.

[6] K. T. Nguyen *et al.,* "Survey on secure communication protocols for the internet of things," *Ad Hoc Netw.*, 2015.

[7] M. Alazab *et al.,* "Malicious spam emails developments and authorship attribution," in *2013 Fourth Cybercrime and Trustworthy Computing Workshop*, IEEE, pp. 58-68, 2013.

[8] R. Rammanohardas, "Artificial Intelligence in Cyber Security," *Journal of Physics, Conference on Artificial Intelligence and modern applications*, 240-ECS Meeting, 2021.

[9] K. D. B. Utama *et al.,* "Digital signature using MAC address based AES-128 and SHA-2 256-bit," in *Proc. 2017 International Seminar on Application for Technology of Information and Communication (iSemantic)*, Indonesia, pp. 72-78, 2017.

[10] Md. Shafiur Rahman *et al.,* "An Efficient Hybrid System for Anomaly Detection in Social Networks," *Springer,* vol. 4, DOI: https://doi.org/10.1186/s42400-021-00074-w, 2021.

[11] S. Namasudra, "Fast and secure data accessing by using DNA computing for the cloud environment," *IEEE Transactions on Services Computing*, 2020.

[12] S. Kumari and S. Namasudra, "System reliability evaluation using budget-constrained real d-mc search," *Computer Communications*, vol. 171, pp. 10-15, 2021.

[13] S. Kumari *et al.,* "Intelligent deception techniques against adversarial attack on the industrial system," *International Journal of Intelligent Systems*, vol. 36, no. 5, pp. 2412-2437, 2021.

[14] P. Pavithran *et al.,* "A novel cryptosystem based on DNA cryptography and randomly generated Mealy machine," *Computers & Security*, vol. 104, pp. 102160, 2021.

[15] M. Humayun and M. Niazi, "Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study," *Arabian Journal of Science & Engineering*, DOI: 10.1007/s13369-019-04319-2, pp. 1245-1250, 2020.

[16] Alex Mathew, "Machine Learning in Cyber-Security Threats," *International Conference on IoT Based Control Networks & Intelligent Systems*, DPI: 10.2139/ssrn.3769194, 2020.

[17] M. Coutinho *et al.,* "Learning perfectly secure cryptography to protect communications with adversarial neural cryptography," *Sensors*, vol. 18, no. 5, pp. 1306, 2018.