A Systematic Review of Network Security Breaches and Solutions

Ravi Tomar, Yogesh Awasthi

Abstract*: Cyber Security is the protection of unauthorized access of the information. Different threat and issues are present in the network which stole unpredictable amount of data every year. For the information technology and computer systems, a cyber security rule is required to compel different group as well as businesses to secure their systems and information from cyber-attacks. In the healthcare sector huge amount of data can be theft every year which is dangerous for both government and personal view. The technical advancements have increased the risk's potential in the network in Cloud and Cyber. Security & privacy cracks are the vital issues which need to mitigate to maintain the dignity of the network. This paper conducted a review to secure the network from network security issues. There are various attacks which are vulnerable to the network like DoS, DDoS and Spoofing. These attacks have been described to identify the attacker's capability. In order to facilitate this, networks such as cloud, ad-hoc, cyber has been described to determine the security, a paradigm. A literature from past studies has been conducted to identify the threats and their behavior. Different types of attacks and their behavior is also studied, and a tabular structure is also presented for better understanding.

***Keywords* : Security, Attacks, Breaches, DDoS**

I. INTRODUCTION

Network security is the most crucial element in information security, as it is accountable for ensuring all data transmitted via networked computers. It has both hardware part and software technologies. Network security incorporates various layers of edge and network defenses. Each network safety layer establishes regulations and monitoring. Authorized consumers have access to network services, but the performance of exploits and threats against malicious performers. There are various types of network:

- Ad-hoc Network
- Cloud Network
- Cyber

An ad-hoc network is a decentralized local area network. Ad-hoc network implies a system that is constructed spontaneously without any pre-define infrastructure. An ad-hoc network is of mainly three types:

- Mobile Ad-hoc Network (MANET)
- Wireless Mesh Network
- Wireless Sensor Network

Revised Manuscript Received on September 05, 2020.
***** Correspondence Author
Ravi Tomar, School of Engineering & Technology (Department of CS), Shobhit Institute of Engineering & Technology, Meerut, India. Email: ravistc1@gmail.com
Yogesh Awasthi, School of Engineering & Technology (Department of CS), Shobhit Institute of Engineering & Technology, Meerut, India. Email: yogesh@shobhituniversity.ac.in

A mobile ad-hoc network (MANET) is a sort of multiple hop wireless network and can be described as a set of self-configuring and self-organizing wireless mobile devices. MANET systems can interact directly to each other inside their transmission range without the need for any base station, i.e., there is no need for any core coordination. The MANET can therefore also be defined as a decentralized network, meaning a system where there is no base station to coordinate the message flow. The primary goal behind the MANET is to enable networking anywhere and at any moment. Wireless mesh networks (WMNs) are made up of different routers and multiple clients with relatively low mesh router mobility and creating the important content of WMNs. They provide both mesh and standard customers with network access. A WMN is differently auto-organized and auto-configured, with network nodes automatically establishing and retaining mesh connectivity between each other (creating an ad hoc network in effect).This function gives many benefits to WMNs, including low upfront costs, simple network upgrade, automation and secure service coverage. Wireless Sensor Networks (WSN) are emerging as both an important new level in the IT ecosystem and a rich field of active studies that incorporate structure and system design, networking, distributed a technique, programming structure, data management, security, and social variables. Security is a widely used word that includes authentication, integrity, privacy, non-repudiation, and anti-playback features.

II. CLOUD NETWORK

Cloud computing have various unique security challenges and challenges. In the cloud, Information is stored by a third-party service distributer and accessed over the Internet. Cloud service distributer take cloud security threat as a common responsibility. In this technique, the cloud service provider fulfills the security of the cloud and the privacy of the customer. The cloud network has some issues related to IaaS, PaaS, and SaaS:

A. Software-as-a-service (SaaS):

- Minimum of visibility into what information is within cloud applications
- Malicious actor information removal from the cloud implementation
- Unfinished control over who can access confidential information
- Cloud apps delivered outside IT visibility (e.g. shadow IT)

B. Software-as-a-service (SaaS):

- Cloud architectures and accounts generated outside IT visibility (e.g. shadow IT)
- Incomplete governance over who can access delicate information
- Lack of cloud infrastructure abilities
- Lack of awareness of what information is in the cloud.

III. CYBER ATTACKS

A cyber-attack is an offensive manoeuvre that aim is computer data systems, infrastructures, computer networks, or personal computer devices. An intruder is a individual or process who tries to access information, features or other limited regions of the scheme without permission, possibly with malicious intent. Based on the context, cyber-attacks can be part of cyber-warfare or cyber terrorism. National states, people, groups, community, or organisations can employ a cyber-attack. A cyber-attack may come from different resources.

A cyber-attack can rob, change, or ruin a designated destination by logging into a vulnerable system. Cyber-attacks can variety from placing different element on a computer to trying to destroy all countries facilities. Legal specialists seek to restrict the access of the word to events that cause physical harm, distinguishing it from more routine information breaches and wider hacking operations.

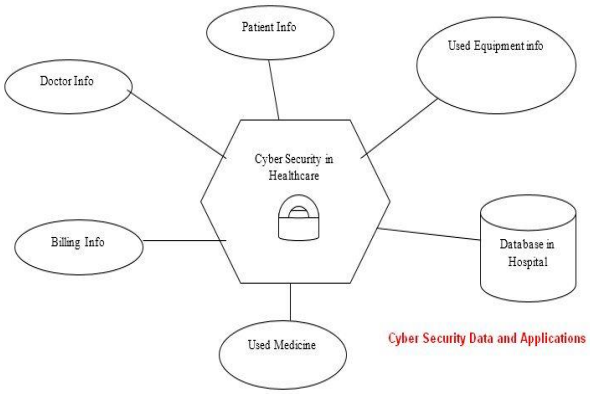

Fig. 1.Cyber Security in Health Care

IV. SECURITY THREATS

If Threats are described in the network security using threat models that can be further classified into the following categories:

A. DoS

DoS attacks are active attacks where malicious nodes produce fake messages to interrupt the activities of the network or eat the funds of other nodes. A Denial-of-service attack (DoS assault) is a security breach in which the offender tries to make a computer or network resource inaccessible to its desired purpose customers by momentarily or permanently disrupting Internet-connected host services. A DoS or DDoS threat is comparable to a bunch of people crowding the entrance of a shop, making it hard for legitimate customers to enter, interfering with trade.

B. DDoS

DDOS attack is known as dispersed, a huge-scale effort by mean of malicious users for flood the victim network by a massive number of packets and kills the sufferer network for resources like computing power, bandwidth, etc. The victim later is incapable of providing the facility to its legitimate clients, because of which the network performance is deeply affected. In short, since a malicious user sends huge amount of unwanted packets to the network or a separate computer, legitimate users' services are denied. Decentralized arrangements have increased "many-to-one" measurements, making it difficult to prevent attacks. DDS attacks consists of four elements. The important point is that the victim is the target host that needs to choose to receive the main attack. Second, it has a daemon agent attack and has attacked the target victim. The attacking agent is installed on the host. The attacker agent/secondary victim affects the target as well as the host. These attack daemons 'implementation functions involve an attacker for access and penetrate the host. The dispersed third element denial of service assault termed as the control master method. It is intended to coordinate the attack. In the last, there is the real attacker known as the real mind behind the attack. With the use of a access master technique, the actual attacker could stay behind the attack scenes. The components and procedure are of a DDOS attack are shown in Fig. 1. Below are the steps that take places for a distributed attack:

- The real attacker transfers an “execute” alert for controlling the master program.
- The program of control master then obtains the “execute” alert and broadcasts the command for attacking the daemons under their control.
- When the attack command is being received, the agent machine starts on the victim.

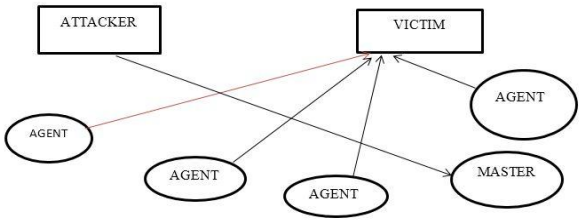

Fig. 2.DDoS Attack

C. Spoofing Attack

A spoofing activity is when a malicious party impersonates another machine or user on a node to launch attacks on network hosts, steal data, spread malware, or bypass access controls. Spoofing can be used for access private data of a target, spread malware through infected connections or attachments, bypass controls on network access, or redistribute traffic to perform a denial-of-service attack.

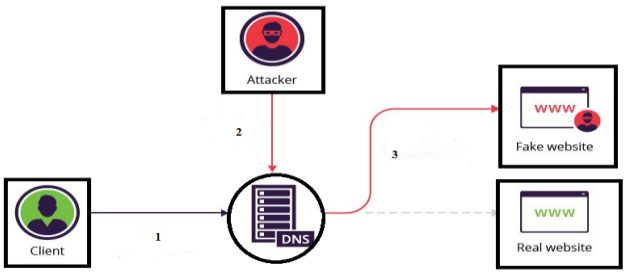

Fig. 3.Spoofing Attack

Table- I: Difference Between DoS, DDoS and Spoofing Attack

S.N.	***DoS***	***DDoS***	***Spoofing***
1.	An attack made by a single machine.	An attack made by many machines also known a botnet.	Vulnerable to the users work in the cyber network.
2.	It can be quickly discontinued the right security.	There may be a real headache to prevent it.	Spoofing attacks are difficult to detect so preventable measures have to be considered.
3.	The danger is low because they are rarely used to cover the attempt to violate the law.	It is at a moderate and high-risk level because it can be used for damage networks and even systems severely.	Spoofing attacks are hazardous as confidential information may be leaked.
4.	Malware is not included.	A botnet generally consists of thousands of infected PCs.	Spoofing includes millions of pc attacked by the fraudulent.
5.	Attacks mostly on website or server.	Attackers enhance, which mostly targeted are the websites.	Cyber-attacks frequent, in such phase as the number of attacks, increased.

V. RELATED WORK

He et al. (2019) provide an overview of the security demands of a space-based wireless network. As an instance, in the space-based wireless network, this paper researched the information link layer safety of satellite systems oriented on the 1553B network protocol. The space-based wireless network has various mechanisms like key management and also an intrusion detection is an important means to make sure space-based wireless network. These techniques usually require important resources for computing, communicating, and storing [1]. **Palanisamy et al. (2019)** describe the overall framework engineering and examine three notable plan problems: age and reproduction of the mystery message shares, the optimal part of the message shares in multiple respects as far as security, and the multi-path revelation schemes in a specially designated flexible scheme. This study presents a reliable data conveyance (SPLIT) Secure Protocol tool used to upgrade safe data conveyance in a versatile, specially designated scheme. The result legitimizes the SPLIT methodology's plausibility and viability [2]. **Donno et al. (2019)** evaluated cloud computing safety from a particular view: cloud computing as a key element of the IoT architecture. The motive behind this job lies in the proof that IoT systems today depend heavily on the cloud, where data analytics and intelligence live. The result provides a well-structured and current study of cloud computing security problems in the IoT age [3]. **Di et al. (2019)** propose an IDS based on cloud computing. Intrusion detection technology is an important means of maintaining computer network security. It gathers and analyses computer system files and information, detects intrusions that violate computer network safety, and alarms and blocks such intrusions. The intrusion detection system finished reaction and detection, performed a complete defensive function, addressed network security incidents, made the shift from post-discovery to pre-warning and automatic reaction, and also supplied more efficient proof to explore the intruders ' legal liability [4]. **Desai et al. (2019)** propose an AODV protocol predictive method based on linear regression. The proposed strategy tries to define adversaries during the route discovery stage to enhance QoS in MANETs, particularly for apps for which packet delivery rate is a critical parameter. In future, there is also a scope in the area of ad-hoc networks and their variants to improve their efficiency by integrating new, safe routing alternatives, energy conservation systems, authentication, and main distribution systems and performance optimization techniques [5]. **Wu et al. (2019)** demonstrate the cyber-physical attacks in Cyber Manufacturing systems with machine learning methods. Cyber-physical assaults in Cyber Manufacturing Systems are unique but critical to safety. To detect Cyber Physical assaults in CMS, physical information machine learning methods are created and incorporated in this study. Two examples are proposed with computation and testing: malicious 3D printing invasion and malicious CNC milling machine assault. The result shows that anomaly detection algorithm achieved 96.1 % accuracy in identifying cyber-physical assaults in the 3D printing system by applying machine learning techniques in physical information; random forest algorithm achieved an average 91.1 % accuracy in identifying cyber-physical assaults in the CNC milling system [6]. **Patil et al. (2019)** developed an effective security structure for monitoring VM network traffic. It utilizes both signature and anomaly detection methods and is therefore capable of identifying both recognized and unknown attacks. Hypervisor Distributed Network Security (HLDNS) is suggested to be deployed on each cloud computing customer. The proposed safety framework will be evaluated for efficiency and optimization evaluation on the cloud network tested at NIT Goa using the recent UNSW-NB15 and CICIDS-2017 intrusion information sets [7]. **Hyun et al. (2018)** Present an I2NSF architecture capable of providing effective and flexible security service in cloud-based safety services. The main input of the architecture of I2NSF is to standardize the interfaces of various suppliers to the NSFs to simplify the management of these NSFs. The result shows the feasibility and efficiency of the I2NSF architecture embedded with SDN [8]. **Senyo et al. (2018)** present A Meta-discovery of cloud services research in information technology intended to take company shares of literature and its accompanying data analysis structures, research methods, geographical distribution, level of analysis and trends over seven years.

The outcome demonstrates that the current literature on cloud computing tends to skew towards the technological dimension to the detriment of other under-investigated aspects such as company, scientific understanding, and application domain [9]. **Han et al. (2018)** propose a double-sided ring signature algorithm to protect both the transferring of messages with the secure transmission. The performance of these algorithms is theoretically analysed and compared to the standard ring signature algorithm in a real tool environment. The results show that the double-ring ring algorithm is superior to standard ring signatures in terms of security, call probability, and communication efficiency and is satisfactory for reliable communications and confidentiality requirements [10]. **Wang et al. (2018)** describe three protocols to address MCS privacy issues in ad hoc networks, regardless of third parties. It provides the Privacy Protection Protocol (PPS) protocol to protect SSCs' privacy. Subsequently, to ensure the confidentiality of the MDOs, they present the Privacy Protection Protocol (PPDRC) protocol. Finally, both MD and DECs offer a Neighbourhood with Privacy Protection (KN2P2) to identify nearby neighbours without leakage [11]. **Jain et al. (2018)** propose a new approach based on a dual-link fuzzy reliability model, which is measured in the demand distance vector (AODV) protocol to reduce blackhole attacks in ad hoc. It uses a reliable computational approach, which is supposedly fuzzy. A direct confidence calculation method identify malicious nodes and thus, the safe route in MANETs. The results indicate the performance improvement of the suggested protocol on the AODV protocol [12]. **Wang et al. (2018)** discuss the problem of coordinating routing together and transmitting power optimization for multiple hop namespaces in the presence of randomly distributed headphones after the Poisson point process. In this privacy, messages are delivered from one source to many hop routes that are connected to many legitimate relays on the network. Our motive is to minimize the possibility of end-to-end communication by optimizing the routing path and the transmit power of each hop and limiting the possibility of secrecy. This problem can be solved optimally by iterative external poly block approximation with the 1-D search algorithm. The simulation results show improved performance of the algorithms proposed for both clogging and blocking scenarios and point to a non-significant trade-off between each hop and the transmission power of secure hops [13]. **Liu et al. (2017)** discuss the concept and specification of CPS and figure out the current scenario of CPS research. CPS will cover different aspects of real life and economic life, will have wide influence and will lead to the comprehensive improvement of informatics and other subjects. CPS development also faces major difficulties. Finally, in creating CPS, it analyses the primary barriers and important research [14]. **Tomar et al. (2019)** emphasizes the various aspects of ad-hoc networks. The different types of attacks that affect the system and are prevented by various algorithms mentioned. Since ad-hoc wireless networks have no basis and are consistently unreliable, therefore a large number of strikes are subject. The black hole attack is seen as one of the riskiest conditions of them. In this attack, the malicious node usually absorbs each data packets that are similar to separate holes in all things. Likewise, all packets have been dropped in the network. For this reason, various prevention measures should be employed in the form of routing finding first then the optimization followed by the classification [15]. **Tomar et al. (2019)** discuss research on cybersecurity has gained more attention and interest outside the availability of computer security experts. Cybersecurity is not a single issue, but a series of highly different issues involving multiple threats. The data accommodation in health care system is growing continuously, which demanded a highly efficient and intelligent system to deal with the health records. The increase in the data increases the probability of affecting data by the cyber attacker. Therefore, it becomes essential to deal with cyber-attacks. This research focused on the utilization of cybersecurity for healthcare organization using machine learning approach. Our aim is to detect Distributed Denial of Service (DDoS) attack, which is one of the most commonly present cyber-attacks. This type of attack is designed to prevent genuine user from the required network resources. By using the concept of Artificial Neural Network (ANN), the system is trained based on the database related to the clinical record, financial record, individual record etc. During the data communication process, cross-validation is performed using ANN approach, which matched the data with the database and at last check the performance parameters. The experiment results indicate that there is an increase in the True Positive Rate (TPR) and False Positive Rate (FPR) of 0.27 % and 8.79 % respectively has been observed [16].

VI. CONCLUSION

The present transition to health care organization is based on the flow of information in real-time, the integration of information and communication technologies with physical equipment to provide a coherent system that can better track the patient's health in real-time and improve overall health services. As data communication is performed through wireless means therefore, the tendency to affect or steal data by an unauthorized person increases. Therefore, security plays an important role in any kind of established network. If the network is not secured, the data communication cannot settle down and high transmission loss will be faced. This paper deals with the types of established network over a large scale and the detailed security issues in the network. This paper also discussed the types of breaches and some of the obnoxious security threats in the network. A detailed literature survey is conducted, and the advantages and disadvantages of prevention measures are also discussed.

REFERENCES

1. He, D., Li, X., Chan, S., Gao, J., and Guizani, M. “Security Analysis of a Space-Based Wireless Network.” In *IEEE Network*, 33(1), 2019, pp. 36-43.
2. Palanisamy, B., Karthik, N., Chandrakumar, K., Thirunavukkarasu, K., and Jayasudha, R. (2019). “Improving Network Security in Mobile Ad Hoc Networks.” in *Journal of Computational and Theoretical Nanoscience*, 16(5-6), 2019, pp. 2299-2301.

3. De Donno, M., Giaretta, A., Dragoni, N., Bucchiarone, A., and Mazzara, M. "Cyber-Storms Come from Clouds: Security of Cloud Computing in the IoT Era." in *Future Internet*, 11(6), 2019, pp. 127.
4. Di, M. "Design of the Network Security Intrusion Detection System Based on Cloud Computing." in The International Conference on Cyber Security Intelligence and Analytics, Springer, Cham., Feburary 2018, pp. 68-73.
5. Desai, A. M., and Jhaveri, R. H. "Secure routing in mobile Ad hoc networks: A predictive approach." in *International Journal of Information Technology*, 11(2), 2019, pp. 345-356.
6. Wu, M., Song, Z., and Moon, Y. B., "Detecting cyber-physical attacks in Cyber Manufacturing systems with machine learning methods." In *Journal of intelligent manufacturing*, 30(3), 2019, pp. 1111-1123.
7. Patil, R., Dudeja, H., and Modi, C. "Designing an efficient security framework for detecting intrusions in a virtual network of cloud computing." in *Computers & Security*, 85, 2019, pp. 402-422.
8. Hyun, S., Kim, J., Kim, H., Jeong, J., Hares, S., Dunbar, L., and Farrel, A. "Interface to network security functions for cloud-based security services." in *IEEE Communications Magazine*, 56(1), 2018, pp. 171-178.
9. Senyo, P. K., Addae, E., and Boateng, R. "Cloud computing research: A review of research themes, frameworks, methods, and future research directions." in *International Journal of Information Management*, 38(1), 2018, pp. 128-139.
10. Han, Y., Xue, N. N., Wang, B. Y., Zhang, Q., Liu, C. L., and Zhang, W. S. "Improved dual-protected ring signature for security and privacy of vehicular communications in vehicular ad-hoc networks." In *IEEE Access*, 6, 2018, pp. 20209-20220.
11. Wang, Z., and Huang, D. "Privacy-preserving mobile crowdsensing in ad hoc networks." in *Ad Hoc Networks*, 73, 2018. pp. 14-26.
12. Jain, A. K., Tokekar, V., and Shrivastava, S. "Security Enhancement in MANETs Using Fuzzy-Based Trust Computation Against Black Hole Attacks." In *Information and Communication Technology, Springer, Singapore*, 2018, pp. 39-47.
13. Wang, H. M., Zhang, Y., Ng, D. W. K., and Lee, M. H. "Secure routing with power optimization for ad-hoc networks." in *IEEE Transactions on Communications*, 66(10), 2018, pp. 4666-4679.
14. Liu, Y., Peng, Y., Wang, B., Yao, S., and Liu, Z. "Review on cyber-physical systems." in *IEEE/CAA Journal of AutomaticaSinica*, 4(1), 2017, pp. 27-40.
15. Tomar, R., and Awasthi, Y. "Prevention Techniques Employed in Wireless Ad-Hoc Network." In *2nd International Conference on Advanced Science and Engineering*, April 2019.
16. Tomar, R., and Awasthi, Y. "Analysis Against DDOS Flooding in Healthcare System using Artificial Neural Network." In *International Journal of Advanced Trends in Computer Science and Engineering*, 8(1.5), November 2019, pp. 405-410.

AUTHORS PROFILE

Ravi Tomar is a research scholar at Shobhit Institute of Engineering & Technology, Meerut and also serving as one of the key promoter for various educational institutes under the banner Shivam Group of Institutions. He has received his Bachelors of Technology from Shobhit Deemed University in 2012, Masters in Technology from Swami Vivekanand Subharti University in 2014 with specialization in Computer Science Engineering. Presented a paper on Prevention Techniques in Wireless Ad-Hoc Networks in ICOASE 2019, IEEE, Research Paper Published in IJATCSE Vol 8, No.1.5, 2019 on Analysis against DDOS flooding attacks in Healthcare Systems using Artificial Neural Network and author or co-author of few scientific papers on international reviews. Currently working on Optimization of Route Identification and Alleviate Effects of Attacks in MANET using Soft Computing.

Yogesh Awasthi has joined the Africa University, Mutare, Zimbabwe in July 2020. He has also served in various academic institutions at International and National Level. Milestones of the service career includes, Lebanese French University, Erbil (2018-2020), Shobhit Institute of Engineering and Technology (Shobhit Deemed University) (2004-2018), Teerthanker Mahaveer University (2002-2004) and Delhi University. He has received his B.Sc. degree from Lucknow University in 1997, Master of Computer Applications (MCA) degree in 2002 from Rajiv Gandhi Technical University (RGTU), Bhopal, Second Master Degree i.e. Master of Technology (M.Tech.) in Computer Science Engineering in 2011 from Dr. A.P.J. Abdul Kalam Technical University (AKTU), Lucknow and Doctor of Philosophy (Ph.D.) in Computer Engineering & Information Technology from Shobhit Deemed University, India in 2015. He is member of various academic and administrative bodies. He has published 23 papers and articles in International and National Journals/Conferences. His area of research includes Artificial Intelligence, Watermarking Techniques, Cloud Computing and IoT. He has written a book on Java Programming titled as "Lets Play with JAVA". He was the Chairman and Head of various academic and administrative position in the university. He is a member of Computer Society of India, Member of International Association of Engineers, Hong Kong, and Member of Editorial Board of peer reviewed journals. He has guided more than 50 Master's and Graduate projects.