Journal of Management and Service Science, 2021,
Vol. 01, Iss. 01, S. No. 002, pp. 1-8

Cyber Security Methodologies and Attack Management

Sachin Kumar Tomar[1], Pawan Singh[2]

[1,2]Amity School of Engineering & Technology, Amity University Uttar Pradesh, Lucknow, India
sachintmr71@gmail.com[1], pawansingh51279gmail.com[2]

How to cite this paper: S. K. Tomar and P. Singh (2021) Cyber Security Methodologies and Attack Management. *Journal of Management and Service Science*, **1(1)**, 2, pp. 1-8.

https://doi.org/10.54060/JMSS/001.01.002

Received: 24/02/2021
Accepted: 08/03/2021
Published: 09/03/2021

Abstract

Cyber Security refers to the process of protecting data and systems from cyber-attacks. Any firm without security policies and systematic security systems is at large risk and the important data related to that firm is not safe without security policies. Payment Card Industry and Data Security Standard framework used to protect payment security credit card, debit card, etc. In maintaining access, the hacker inside the target system is used to exploit vulnerabilities and password cracking. In today's era, day by day cybercrimes rise so it raised the requirement of system Security or even the entire network. As more business exercises are being mechanized and an expanding number of PCs are being utilized to store important data, the requirement for secure PC frameworks turns out to be more evident. As a result, network safety issues have become public safety issues.

Keywords

Cyber Security, Terminologies, Attacks, Forensics, Steganography, Cryptography

1. Introduction

Cyber Security refers to the processes of protecting data and systems from cyber-attacks. Securing the data have become one of the biggest tasks today. Several Governments and companies are proceeding with many checks to stop these cybercrimes. Any firm without security policies and systematic security systems is at large risk and the important data related to that firm are not safe without security policies. A cyber assault is purposeful exploitation of PC frameworks, organizations, and innovation subordinate ventures [5]. These assaults utilize malicious code to alter PC code, information, or rationale. Coming full circle into ruinous results that can compromise your information and declare cybercrimes, such as, data and fraud [7]. A digital assault is otherwise called a PC network assault. Mounting a decent safeguard requires understanding the offense. As should be hackers have many choices, such as DDoS attacks, malware attack, man-in-the-center block attempt, and brute-forcing attack, to attempting to acquire unapproved admittance to basic frameworks and delicate information [1]. Measures to relieve

these dangers differ, yet security rudiments stay the equivalent: Keep your computer and anti-virus data sets updated, train your representatives, design your firewall to whitelist just the particular ports and has you need, keep your passwords solid, utilize a least-advantaged model in your IT environment, make daily backups, and continuously review your IT frameworks for any malicious activity.

2. Terminologies and Need of Security

2.1 Terminologies

There are many numbers of terminologies in Cyber Security like Hacking [3], It is used to attempt misuse and exploiting a system and other also like cracking. In cracking, attacker try to breach passwords, software, systems, and wi-fi security and Port Scanning. In port scanning, attacker try to determine the vulnerabilities and Spoofing, in spoofing, attacker tries to gain confidential data by faking it is used on email, websites, and phone calls.

2.2 Need for Security

In today's era, day by day cybercrimes rises so it is required to need Security of the system or even the entire network. And it protects our firms against phishing, malware, etc. from Hackers. So, in today's world security is used to observe and take precautions across these types of attacks. Cybersecurity is important as it contains everything that has to do with protecting our confidential material, identifiable data, protected health data, personal details, licensed innovation, data, and legal and industrial data frameworks from theft and damage. As more corporate processes become automated and a growing percentage of PCs are used to hold critical data, the need for protected PC systems becomes increasingly apparent. As a consequence, network security concerns have morphed into national security concern [3].

3. Cyber Security Methodology

Reconnaissance refers to gathering information about the target for the ex-Domain name, IP, Target personal information, Email, Subdomains, Job information, etc. Reconnaissance is also known as Foot-Printing. We have many tools to gather information about target tools are Netcraft, whois, HTT track-used to mirror the website, Firebug-data extractor, Recon-ng-reconnaissance of the network, sublist3r-for subdomains, etc. Scanning refers to identifying hosts, IP addresses, running service in the target system, open ports, and services in the target network. Usually in this phase, hacker tries to prepare a blueprint of the target. we have so many tools to know about the target tools are- Nmap-complete network scanner this is one of my favorite Network scanning tool, Angry IP scanner-pings each IP address and resolves it mac and port, Hping3/2-used for packet crafting for TCP/IP, Netscan pro-it helps to troubleshoot the network, ID serve-for Banner grabbing/OS Fingerprinting, Nessus /Open VAS/Qualys-for vulnerability scanning [10]. Gaining Access - It refers to the real hacking phase in this phase hacker takes place in the system. The hacker exposed vulnerabilities and information in the first and second phases are now exploited to gain the target computer. Now attacker cracking Password by Dictionary attack-create passwords word list and runs against the user account. Brute force-in this software combines all words it tries every combination. Hash injection attack: it converts normal text into the encrypted form, and it is not easy to decrypt the password. Windows Passwords are stored in (SAM) Security Account Manager. In Linux user's passwords are stored in (Shadow) file. In maintaining access phase, hackers inside the target system by exploiting vulnerabilities and password cracking. Now the attacker can easily download and upload anything in the target system and to gain system easily next time attacker installs some software like Trojan horses, Keylogger and Rootkits. Trojan horses are a malicious software user thinks it is legitimate software, but it steals all information. Keylogger records the movement of target keyboard keys. Rootkits is a software that hides its presence in the target system

and its compromised system. Clearing tracks Now here is the final phase once a hacker gained into the target system after that hacker covers all their tracks to prevent their presence in the system. Hacker uses Auditpool a tool to remove their presence Auditpool tool stores in the Windows Nt Resource kit for the system by this tool attacker can easily disable their auditing [2].

There are some security measures, and these will give you a **basic level security** against the most common IT risks, by **Use strong passwords, Control access, put up a firewall, use security software, Update programs and systems regularly, Moni**tor for intrusion. Strong passwords are vital to good online security. Make your password difficult to guess. Make sure that individuals can only access data and services for which they are authorized. Firewalls are effectively gatekeepers between your computer and the internet, and one of the major barriers to prevent the spread of cyber threats such as viruses and malware. You should use security software, such as anti-spyware, anti-malware, and anti-virus programs, to help detect and remove malicious code if it slips into your network. Updates contain vital security upgrades that help protect against known bugs and vulnerabilities. You can use intrusion detectors to monitor system and unusual network activity [2].

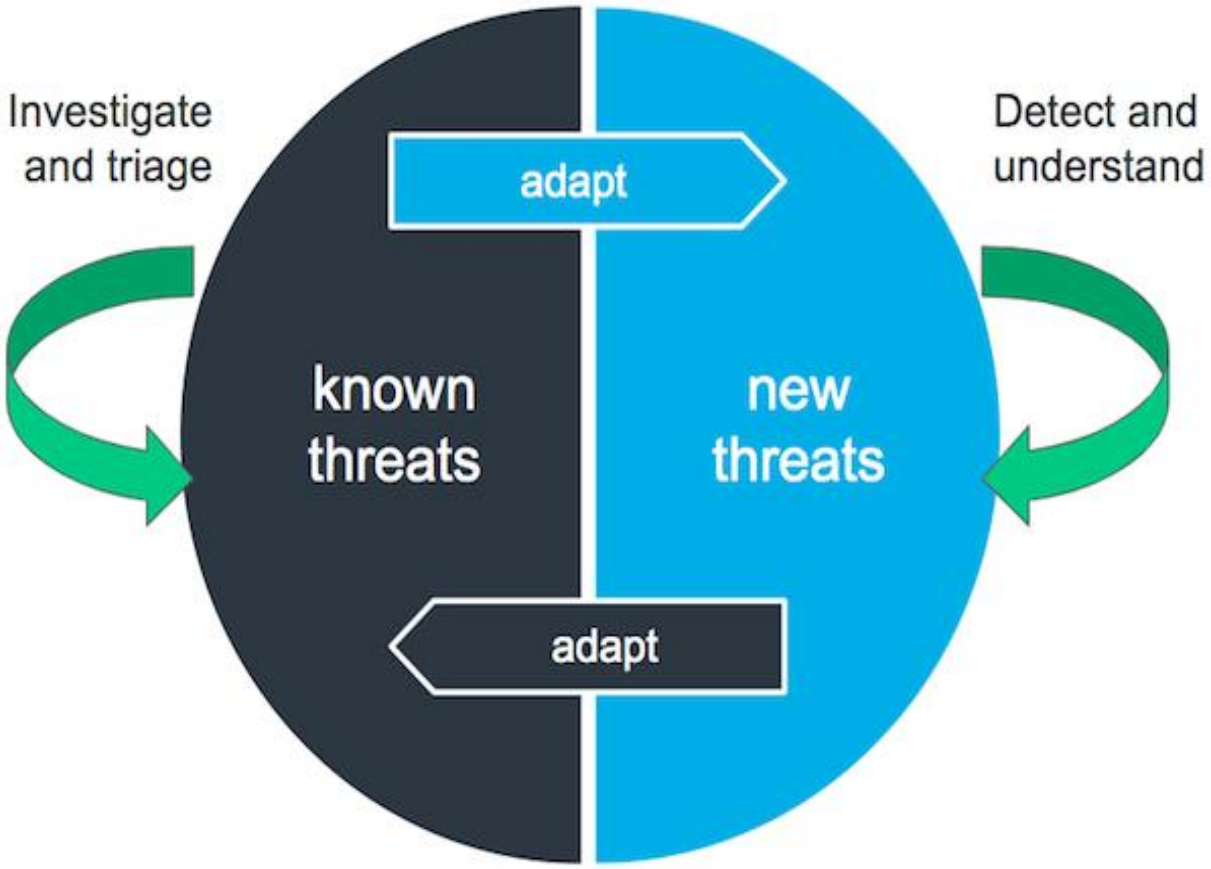

Figure 1. Threat Cycle

4. Deep web and Darknet

Surface Web contains WWW that is used for general purposes for the public and it is used to access by Google, Facebook, Yahoo, etc. Deep web contains 90% of information but it is not accessible by surface web search engines. It contains financial records, Govt resources, Legal doc, etc. The mainly deep web is not indexed by the normal browser or search engine like Google one should use TOR browser to access Deep Web [5]. Darknet is a part of the deep web it is accessed by the TOR browser it hides our identity. Darknet contains Illegal information, Drug trafficking sites. In this, users exchanged data anonymously.

5. Frameworks

There are certain basic frameworks used in Cybersecurity to lower overall risk of the firm's system vulnerabilities to reveal. It is known to as a security system. A cybersecurity study is a series of documents that describe the measures that an organization uses to cope with its internet security risk. Such frameworks reduce a company's vulnerability to flaws. Companies, initiatives, and commercial circumstances are all put to the test on a regular basis to ensure the protection of their essential structures and data. To help handle these issues, an organization need a critical, all-encompassing thinking network security plan to protect its systematic structure and data frameworks. As a result, companies should look for guidance from network safety systems. When used correctly, a network security framework enables IT security leaders to deal with their businesses' cyber-threats even more intelligently. An organization can either modify an existing cybersecurity program or build one from the ground up to solve its specific challenges [8].

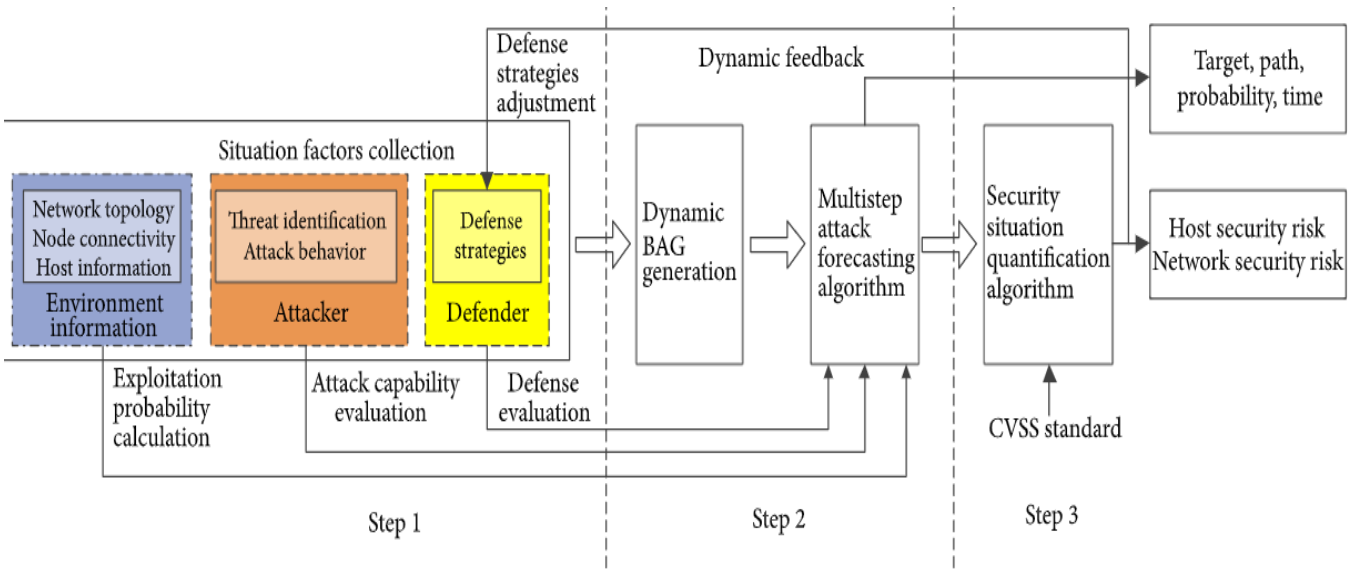

Figure 2. Framework of Security

6. Cyber Forensics

Cyber Forensic investigation is the recovery and investigation of the material found in computers and digital devices. Digital forensics is in today's era of forensic science which deals with a look-a-digital device. Here we follow the process of Digital Forensics is in the first phase we Identify where the crime happens and crime scenes. In the second phase, we Check warrant,

evidence, transport, etc. In the third phase, we extract the data and Check data in victims pen drive, laptop. In the fourth phase, we analyze all the evidence and in the last Generate a complete report [11].

7. Steganography

It is a method to hide any secret message inside any file. In steganography, our secret message is transmitted to undetectable by casual eyes.

8. Some Common Attacks

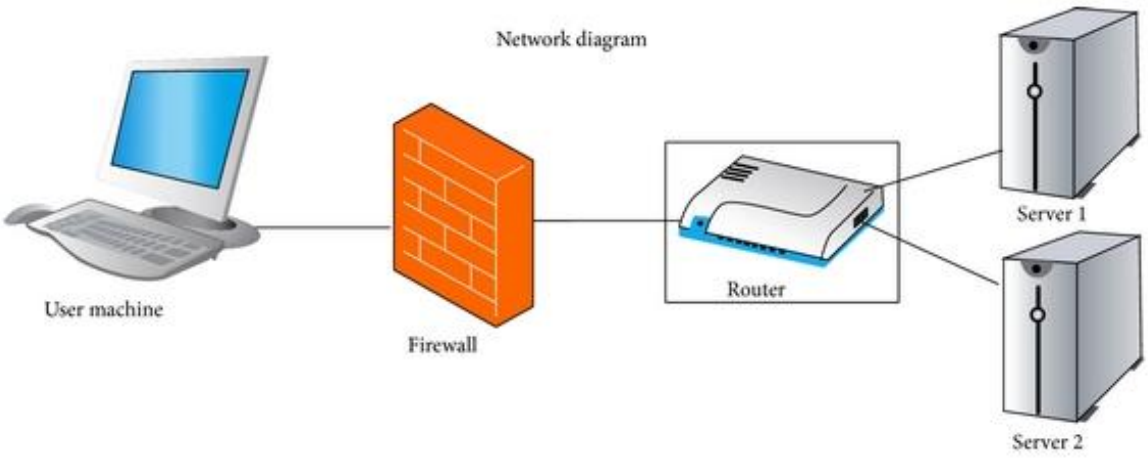

Figure 3. Attack System

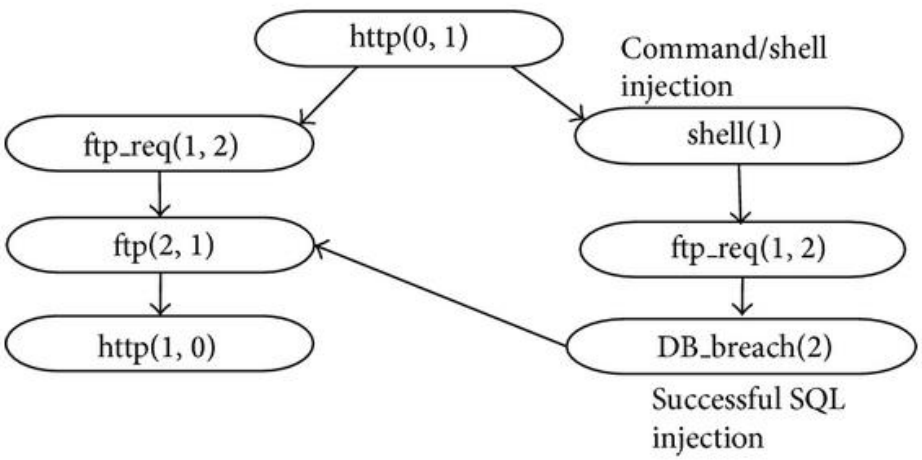

Figure 4. Attack Graph

8.1 Phishing

Phishing is a kind of Social Engineering attack frequently it is used to steal user information, as well as login credentials and atm card numbers.[5] It happens when an attacker, impersonates as a trusted individual or any organization, victim opening a malicious link, mail, etc. which can install the malware in the victim's system and steal his data.

8.2 DoS and DDoS

DoS attack is a Denial-of-Service attack in this attack attacker flood the server by sending lots of TCP and UDP packets. In DDoS Distributed Denial of Service attacker select single target and flood the server by sending lot request using multiple systems. In DDoS, the target is bombarded with a lot of packets from the different-different location. Ex-Buffer Overflow attack, Ping Death attack, SYN Flood attack [5].

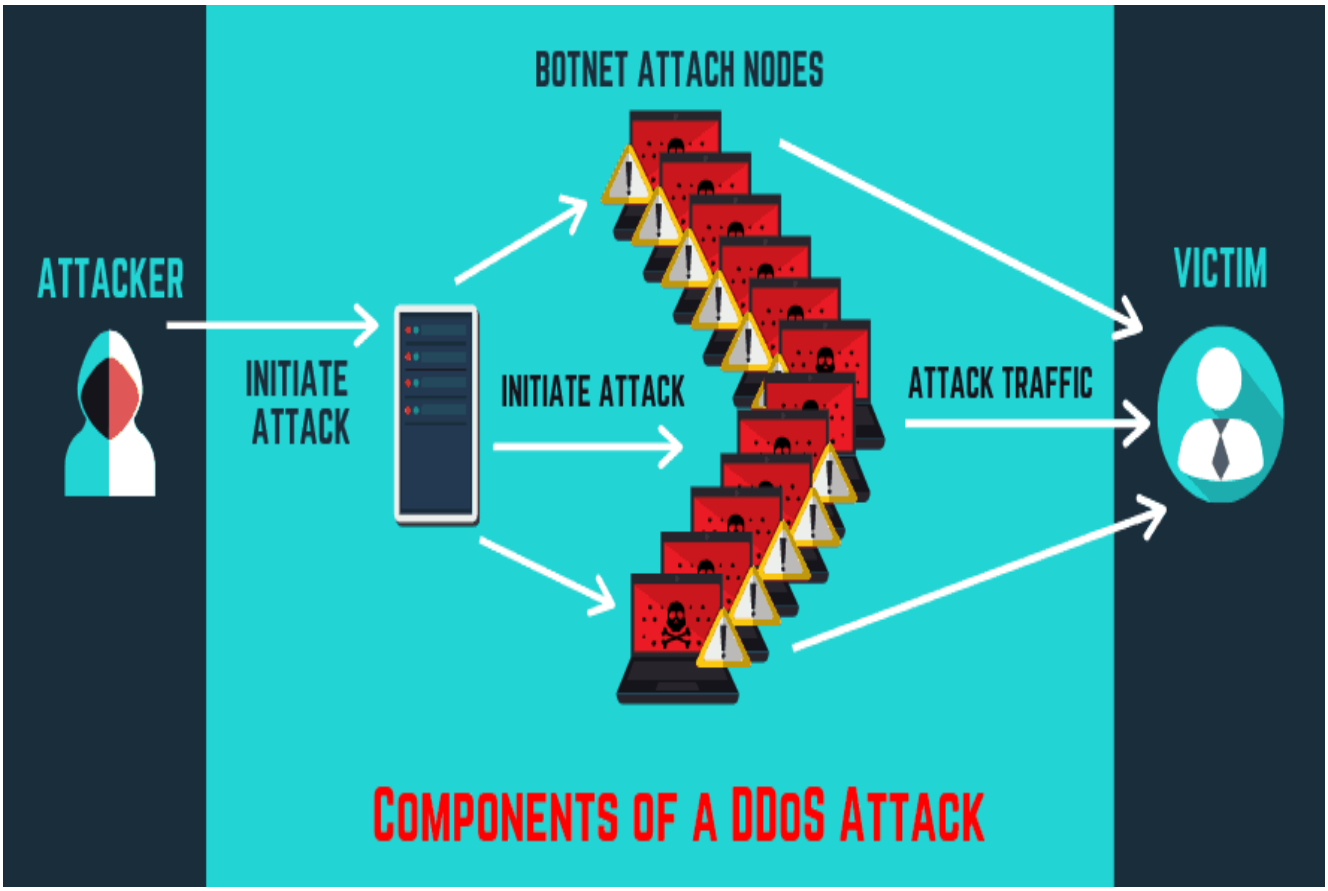

Figure 5. DDoS Attack Methodology

8.3 Malware

Malware is malicious software, and it is very harmful to systems because it damages or disables our computer system, and it also gives control of our system to the creator of that malware. E.g., Trojan horse, Virus, Backdoor, Rootkit, Ransomware.

9.Cryptography

In cryptography, plain text is converted to cypher text. Cryptography is used to keep our data and communications safe. The approach or practise of obtaining information and exchanges is known as cryptography. The act of cryptography dates back long before the advanced age and is now exclusively used in an inventive context. During World War II, Navajo code talkers developed a code that used the Navajo language to communicate secret communications. Cryptography is now used to keep confidential information, such as secret passwords, safe on the internet. Cryptography is used by network security experts to prepare computations, figures, as well as other security measures that categorize and protect the company's and clients' data [3].

Cryptography, the study of secure communication techniques, restrict access to a message's content to only the sender and intended recipient. Kryptos is comes from the Greek kryptos, which means "hidden." It has a strong link to encryption, which is the technique of altering plaintext into ciphertext and then presenting it back to plaintext. Cryptography also includes techniques like microdots and mixing that allow data to be mixed up in visuals. Ancient Egyptians were known to apply these strategies in complicated hieroglyphics, while Roman Emperor Julius Caesar is said to have employed one of several modern codes [3].

The most well-known application of cryptographic algorithms in electronic communication is to disguise and decipher email and other plain-text instantaneous communications. The symmetrical or "mystery key" architecture is the simplest method. Content is jumbled using a strange key, and then both the encoded message and the secret key are sent to the recipient to be decoded. What is the problem? In the event that the communication is blocked, an outsider has everything they need to decode and read it. Cryptologists devised the imbalanced or "public key" structure to overcome this problem. Every customer has pair of keys in this situation: one public and one private. Transmitters require the intended beneficiary's shared key, disguise the text, and transmit it on. When the message arrives, only the recipient's secret key can decipher it, implying that stealing is useless without the matching secret key.

10. Cyber Crime Preventions

Do not open a file from an unknown sender and do not use the same password everywhere and do not keep a copy of plain text login [6]. Try not login into your accounts on a public network and always Enable Multi-Factor Authentication and do not give personal information by phone or email and do not visit a fishy website. Always update yourself [4].

11. Conclusion

In the event of a cyber security incident, such as an attack, studies show that the greatest defense is a PC-savvy customer [4]. To consider is by far the most vulnerable, who are identified in this investigation as new employees inside an organization, as specifically, with the adversary seeking for personally identifiable information from people involved. Mental issues that contribute to customer and organization vulnerability are also addressed in this investigation. This study finds that cyber security threats and approaches have a role to play in reducing the impact of digital attacks, risk, and vulnerability, while creativity has a role to play in reducing the influence of digital attacks, threat, and lack of strength. Cyber-attacks can be mitigated, but there does not appear to be an absolute solution for overcoming such network security threats at this time. Later, when the company implements the system security design, the operation of the cyberattack, threat, and vulnerability decreases [4].

Acknowledgements

I would like to thank my university for giving me this golden opportunity to research such an interesting topic. I would also like to thank Dr. Anil Kumar, Assistant Pro-Vice-Chancellor & Director, ASET, and Dr. Deepak Arora, Professor & Head, Dept of CSE

& IT, ASET for encouraging students to indulge invaluable research activities to enhance their technical skills. Next, I want to thank my faculty guide, Dr. Pawan Singh, for guiding me throughout this domain of Cyber Security. I would also like to thank the internet, books, friends, and the institute for the knowledge I acquired with their help.

References

[1] H. Suryotrisongko and Y. Musashi, "Review of Cybersecurity Research Topics, Taxonomy and Challenges: Interdisciplinary Perspective," *2019 IEEE 12th Conference on Service-Oriented Computing and Applications (SOCA)*, Kaohsiung, Taiwan, pp. 162-167, 2019. doi: 10.1109/SOCA.2019.00031.

[2] Y. Liu, H. Qin, Z. Chen, C. Shi, R. Zhang and W. Chen, "Research on Cyber Security Defense Technology of Power Generation Acquisition Terminal in New Energy Plant," *2019 IEEE International Conference on Energy Internet (ICEI)*, Nanjing, China, pp. 25-30, 2019. doi: 10.1109/ICEI.2019.00011

[3] F. Alkhudhayr, S. Alfarraj, B. Aljameeli and S. Elkhdiri, "Information Security:A Review of Information Security Issues and Techniques," *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, Riyadh, Saudi Arabia, pp. 1-6, 2019. doi: 10.1109/CAIS.2019.8769504.

[4] C. Ten, G. Manimaran and C. Liu, "Cybersecurity for Critical Infrastructures: Attack and Defense Modeling," in *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, vol. 40, no. 4, pp. 853-865, 2010. doi: 10.1109/TSMCA.2010.2048028.

[5] K. Thakur, M. Qiu, K. Gai and M. L. Ali, "An Investigation on Cyber Security Threats and Security Models," *2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing*, New York, NY, pp. 307-311, 2015. doi: 10.1109/CSCloud.2015.71.

[6] J. Akram and L. Ping, "How to build a vulnerability benchmark to overcome cyber security attacks," in IET Information Security, vol. 14, no. 1, pp. 60-71, 1 2020. doi: 10.1049/iet-ifs.2018.5647.

[7] R. Dong, X. Li, Q. Zhang and H. Yuan, "Network intrusion detection model based on multivariate correlation analysis – long short-time memory network," in IET Information Security, vol. 14, no. 2, pp. 166-174, 2020. doi: 10.1049/iet-ifs.2019.0294.

[8] F. Yan, Y. Jian-Wen and C. Lin, "Computer Network Security and Technology Research," *2015 Seventh International Conference on Measuring Technology and Mechatronics Automation*, Nanchang, pp. 293-296, 2015. doi: 10.1109/ICMTMA.2015.77.

[9] Q. Meng, D. Li and Y. Ma, "Research and Application Based on Network Security Monitoring Platform and Device," 2019 IEEE Innovative Smart Grid Technologies - Asia (ISGT Asia), Chengdu, China, pp. 716-719, 2019. doi: 10.1109/ISGT-Asia.2019.8881520.

[10] T. Ohta and T. Chikaraishi, "Network security model," Proceedings of IEEE Singapore International Conference on Networks/International Conference on Information Engineering '93, Singapore, vol.2, pp. 507-511, 1993. doi: 10.1109/SICON.1993.515640.

[11] E. Morioka and M. S. Sharbaf, "Digital forensics research on cloud computing: An investigation of cloud forensics solutions," *2016 IEEE Symposium on Technologies for Homeland Security (HST)*, Waltham, MA, USA, pp. 1-6, 2016. doi: 10.1109/THS.2016.7568909.