Fifth Generation Cyber Attacks and Security: A Review

Mukesh Kumar and Sukhjinder Kaur[*]

Department of Computer Science Engineering, Rayat Bahra University Mohali-140104, India

***Abstract**: Cyber attacks are growing more sophisticated and massive in this modern world and the harm is becoming more severe. Due to the COVID-19 pandemic, cybercriminals now have a larger attack surface, which could result in a cyber pandemic. One particularly vulnerable sector is the healthcare sector. Because of the speedy adoption of additional cloud servers, the proliferation of network-connected smart phones, and the transition to remote work, organizations have to quickly adapt their security procedures to ensure that they are secure at all times, from whatever remote regions they might connect from. The new security perimeter is now this. Fifth- generation cyber attacks have increased in sophistication due to the changing environment. As businesses adapted to remote work and all of its digital ramifications, cyber criminals took advantage of the world crisis to conduct several sophisticated cyber attacks. In this digital age, protecting security against cyber attacks becomes crucial. However, providing cyber security is a very complex undertaking that calls for expertise in assaults and the ability to assess potential risks. The constantly changing nature of assaults is the major problem with cyber security. This paper presents the various fifth-generation cyber attacks and the significance of cyber security. In addition to machine learning methods that can be employed to identify cyber attacks, many cyber security dangers are described. It is also discussed in this paper how important the fifth-generation cyber security architecture is.*

Keywords: Cyber attacks, Cyber security, COVID-19, Cyber threats, pandemic, Fifth Generation.

*Corresponding Author: Ms. Sukhjinder Kaur
e-mail: *sukhjinder.17978@rayatbahrauniversity.edu.in*

1. Introduction

Almost every industry, the government, and even financial institution have moved their operations to cyber infrastructure as a result of the growing trust and use of the Internet. This increases the cyber system's susceptibility to attacks. An intentional attempt to compromise the information system of another person or organization is known as a cyber attack [1]. Cyber attacks most frequently target businesses, the military, the government, or other financial institutions like banks, either to hack into secured information or to demand a ransom. Cyber attacks have advanced to a new degree of complexity, encompassing anything from large-scale internet disruption to big data breaches involving personal information and foreign espionage.

Due to the release of sophisticated "weapons-grade" hacking tools, attackers are now able to spread quickly and infect numerous organizations across a wide range of geographical areas. Mega-attacks on a large scale with several vectors are driving the demand for unified and integrated security structures.

Security from the second or third generation that simply protects against viruses, application attacks, and payload delivery only, is still the norm for most enterprises. All of the networks, cloud environments, virtualized data centers, and mobile devices are vulnerable. Organizations must upgrade to fifth-generation security, which uses sophisticated prevention of threats to consistently thwart attacks on a company's complete IT infrastructure, to ensure a cyber-secure organization. Fig.1. described the generations of cyber security.

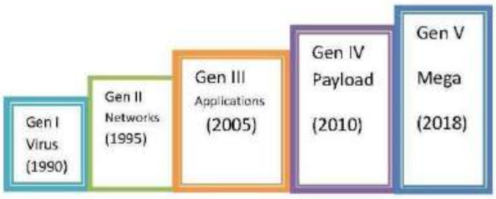

Fig. 1: Cyber Attack Generations

The frequency and sophistication of cyber attacks are rapidly expanding with the passage of time. This developed as one of the main risks to the online world. The Global Security Report 2015 from Trust wave indicated that 98% of tested web applications were susceptible to cyber attacks [2].

Cybercriminals are becoming more sophisticated, though, and they employ new tools and techniques to launch effective attacks. They usually identify the security gaps and weaknesses in the protected system, which allows them to steal data or damage the system in less time [3]. Since most daily activities are now conducted online in this digital age, there is a pressing need for improved cyber security using new techniques.

An equal increase in cyber security as attacks is necessary to counteract cyber attacks. Although many existing tactics and several new ones have been proposed by various academics, the impact of an assault is continually growing. Any government, personal, or private data must be protected from cyber attacks [4, 5].

Numerous nonprofit initiatives and projects have been carried out in recent years to address security threats. The most well-known group is Open Web Application Security Project (OWASP), which is a global nonprofit charitable group that specializes in application security [6]. Each year, they discover and publicize several software flaws, highlighting the ten most critical in their top ten projects. The top 10 vulnerabilities cited by OWASP include XML, External Entities (XXE), broken access control, security mis-configurations, cross-site scripting (XSS), unsafe deserialization, employing components with known vulnerabilities, and insufficient logging and monitoring for the year 2018 [7].

As a result, the term "cyber security" has emerged as the most important area of study. Information availability, confidentiality, and integrity are all preserved through cyber security. Despite being a single phrase, cyber security requires the coordination of several different domains to provide security. Fig. 2. shows various cyber security domains. The short description of these domains is given below:

- Application security enacts many procedures to enhance an application's security. This is frequently accomplished by keeping an eye on the application and identifying, resolving, and avoiding security flaws.

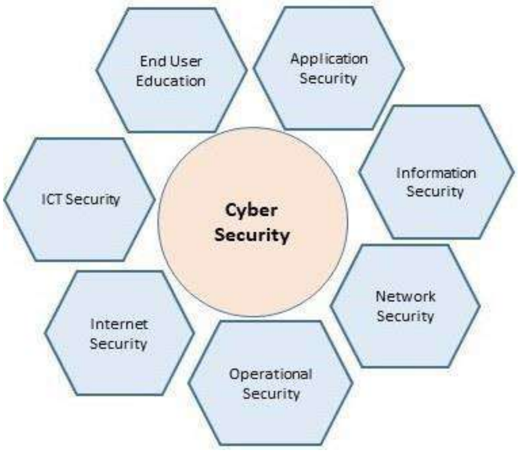

Fig. 2: Cyber Security domains

- Network security is a procedure created to protect the network's usability, integrity, and data as well as to offer secured access to the network. Hardware and software tools are always used for network security.
- Information security refers to a collection of guidelines or best practices for preserving the privacy, accuracy, and accessibility of company data and information in various formats.
- Operations security is the process of locating and defending unclassified important information that is frequently appealing for the rival or enemy to obtain

accurate information.

- Various security procedures are used to ensure the security of online transactions as part of internet security. Establishing exact rules and regulations entails defending browsers, networks, operating systems, and other applications from attacks.
- ICT security is the capacity to safeguard an organization's digital information assets' availability, confidentiality, and integrity.
- The weakest link in the cyber security chain is people. 50% of cyber attacks are the result of user ignorance, and nearly 90% of cyber attacks are brought on by human behavior.

2. Cyber Security Challenges

In this modern fast-growing digital world, billions of devices are connected, and increasing the count, efficient internet penetration, and widespread digitization of multiple sectors, including education, finance, healthcare, retail, and even agriculture and logistics, brings the threat of cyber-attacks, this can lead to not just financial losses but also data privacy breaches, putting the economy and people's lives in jeopardy. [8] Data leakage, use of insecure Wi-Fi networks, phishing attempts, ransom ware, malware, and apps with poor encryption are just a few of the prevalent cyber hazards we face. Data breaches have also increased as a result of IoT and connected devices.

3. Cyber Security Threats

Cyber attacks often aim to disable or obtain access to the target system. The objective can be accomplished by using a variety of attacks against the target system. There are many cyber attacks, and they even change daily. The following list of typical cyber attacks is explained:

3.1. Malware

Malicious Software is known as Malware. It is instruction or program or a file that is created to harm your devices or computers. Examples of malware are spyware, viruses, worms, and adware. Malware spreads through the attachment of an email, instant messaging, peer-to-peer downloads, phishing, and misleading websites [9, 10]. Malware is a common occurrence, producing varying degrees of disruption. Virus outbreaks inflict harm by removing data on infected systems. Malware increased the network traffic by sending virus-attached e-mail messages to all e-mail addresses which are in the contact or address book or a random combination of addresses.

3.2 Phishing

As the name suggests it is a cyber-attack by sends a tempting message to the users. The goal of this particular social engineering approach is to obtain sensitive information, such as login passwords, banking details, etc. from users [11]. When an attacker acts as a reliable source and persuades a victim to open an infected or misleading instant message, email, or text message. The recipient is subsequently tricked into opening a risky link, which may install malware, cause the computer to freeze as part of a ransom ware assault, or reveal private data.

3.3 Denial of Service (DoS) attack

A malicious actor can disrupt a computer's or another device's regular operation to prevent it from being used by its intended users through a denial of service (DoS) attack. This type of attack is carried out by overloading a targeted device with requests until regular traffic can no longer be processed, causing other users to experience a denial of service.

3.4 Man in Middle Attack

A man-in-the-middle attack is one in which the attacker gets caught in the middle means catching a conversation or data transfer that is in progress. The attackers act as both valid parties after inserting themselves in the "middle" of the data transfer. The attacker creates separate connections with the victims and sends messages between them, giving the impression that they are communicating directly through a secure network connection. The attacker has complete control of the conversation.

3.5 Crypto-jacking

Customized attacks where the target is made to generate crypto-currency on another person's computer. To carry out the necessary calculations, the attackers either use malware installed on the victim's machine or, occasionally, JavaScript code that runs in the victim's browser.

3.5 Sql Injection

An attack known as a "SQL injection" takes place when a server using SQL has malicious code inserted by an attacker, forcing the server to divulge information that it normally wouldn't. By entering malicious code into a search box on a susceptible website, an attacker could execute a SQL injection.

3.6 Zero-Day Exploit

A zero-day exploit happens after a net work vulnerability is revealed but before a patch or fix is implemented. During this window, attackers focus on the publicly revealed vulnerability. Threat detection from zero-day vulnerabilities necessitates ongoing monitoring.

3.7 Spam

It's an undesired email message [12]. Receiving spam emails can take recipients a lot of time, and some of them contain Java applets that run when the message is opened [13].

4. Fifth-Generation Cyber Attack

4.1 The Supply-Chain Attack

The most notable attack of the year in 2020 was the Solar Winds cybercrime incident, which showed highly skilled multi-vector attacks with traits of a cyber- pandemic where damaging behavior spreads swiftly within the business. This was a fifth-generation cyber attack in action [14].

When Solar Winds, a well-known IT management tool, was hacked a few days later, Microsoft, Fire Eye, Solar Winds, and the US government all acknowledged they had been the targets of an attack, and the extent of the situation became more obvious. Further analysis found that the attackers modified a Solar Winds system component, adding a backdoor known as Sunburst, which was then made available to users via an automatic software update. One of the most successful supply-chain hacks ever seen, that allowed remote access to numerous prestigious firms. The Solar Winds supply-chain attack is unique in many ways in the constantly changing cyber-landscape. The majority of Fortune 500 companies were among the estimated 18,000 Solar Winds clients that were impacted by its unusually broad scope (Check Point Research Blog).

5. Cyber-Pandemic in Covid-19

Organizations were compelled by COVID-19 to abandon their current business and strategic strategies and immediately change course to provide secure remote access for their workforces at scale. Security teams had to deal with increasing threats to their new cloud deployments as hackers attempted to take advantage of the disruption created by the outbreak: Since lockdowns began, 71% of security experts have noticed an increase in cyber threats.

As COVID-19 continues to dominate headlines in 2021, news of vaccine advancements or new national limits will continue to be leveraged in phishing campaigns, as they have through 2020. Furthermore, malicious attacks from criminals or nation states looking to take advantage of the situation will continue to target the pharmaceutical companies that created the vaccines.

According to recent research, the US healthcare sector is currently the most frequently attacked, with attacks up 71% from September 2020. Over 45% more attacks have occurred in the sector since November 2020, which is double the global increase in attacks during the same period (22%).

6. Remote Vulnerabilities

The COVID-19 pandemic's social distancing rules caused a significant movement in business from corporate offices to employees' homes as the corona virus swept throughout the world. Network administrators have to establish remote-access platforms in their businesses and quickly adapt to the demands of working remotely. Sadly, this frequently led to incorrect configurations and weak connections, which attackers could use to gain access to corporate data.

As a result, in the first half of 2020, attacks against remote access technologies like VPN and RDP (Remote Desktop Protocol, developed by Microsoft to provide an interface for remote connection) escalated.

Due to the large-scale adoption of e-learning platforms by schools, colleges, and universities, it may not come as a surprise that the sector saw a 30% spike in weekly cyber attacks in August 2020, just before the beginning of new semesters. If and when the pandemic spread reaches its apex, attacks initiated by these online "class clowns" will continue to obstruct remote-based learning efforts over the next year. (Check Point Research Blog)

7. Machine Learning Contribution to Cyber Security

To detect dangers in cyberspace, a variety of techniques and procedures have been developed in the literature. Machine learning has recently made significant contributions to cyber security. When it comes to spam detection, filters are essentially employed to analyze the content and determine whether or not the communication is spam.

7.1 Cyber-Defense Strategies

Password Security and access control: The usage of a username and password has long been seen as an important means of protecting personal information. This could be one of the initial steps toward implementing cyber security.

Data authentication: Before downloading anything, always be validated, which means They must be examined to discover if they come from a reliable source and if they have not been tampered with. To authenticate these papers, anti-virus software installed on the devices is commonly used. As a result, powerful anti-virus software is required to keep the gadgets safe and virus-free.

Anti-malware scanners: The software that scans or examines all of the computer's files and documents for viruses or infected code. Viruses, worms, and Trojan horses are all examples of malicious software that are frequently employed together.

Firewall: A firewall is a piece of software or hardware that assists in the filtering of undesirable data or traffic. It blocks hackers, viruses, and worms from accessing your devices and computers through the Internet. All messages pass through the firewall on the internet, which examine every message and block those message that does not identify the security requirements. As a result, firewalls are critical in discovering malware.

Anti-virus software: It is a sort of computer software that detects, stops, and removes potentially harmful software programs like worms and viruses. Many antivirus products have an auto-update capability that allows them to automatically download new virus characteristics as they are found so that they can be checked for. Every computer system should have anti-virus software installed.

7.2 Fifth Generation Cyber Security Architecture

Security is under more pressure than ever due to the business world's fast digital transition. The most frequent cause of failure and security issues is the use of outdated security architectures to manage all of this. As a result, businesses must implement the fifth-generation architecture, which incorporates cloud computing and the Internet of Things. However, single points of failure can be removed by providing businesses with the strength and resilience they need to maintain operations and security in any situation.

To defend against and stop the fifth-generation cyber attacks, and to manage and integrate with mobile, cloud, and networks, this security architecture must build consolidated, unified security architecture. Additionally, integrated threat prevention requires a dynamic security policy that applies to all the platforms, reflects business requirements, supports cloud requirements with auto- scaling, and has the flexibility to interface with third-party APIs. Additionally, a unified and advanced multi-layered threat protection environment must include CPU-Level sandbox prevention, anti-phishing, threat extraction, and anti-ransom ware solutions to combat both known and unknown "zero-day" attacks. Accordingly, the only method to provide a single, unified wall of defense to thwart fifth-generation cyber attacks is to have the proper architecture upon which the entire security infrastructure is based [15].

7.3 Fifth-Generation Solutions

This new environment presents a chance to rethink cyber security's role and make sure that every firm is implementing the fifth generation of security. Three guiding principles are listed below: (Check Point Research Blog)

8. Real-Time Prevention

We now know that immunization is much preferable to medical intervention. This also holds for your cyber security. Defending against the next cyber- pandemic is made easier for your business with real-time attack prevention before they invade.

8.1.Consolidation and Visibility

There will likely have security gaps, fragmented visibility, difficult management, and few scalability alternatives if solutions are applied to individual attack areas. You will be guaranteed the security efficacy required to thwart complex cyber attacks by consolidated security architecture. Your security posture is completed by unified management and risk visibility.

8.2 Continually Update Our Threat Intelligence

Organizations require comprehensive, real-time threat intelligence that offers the most recent information on the newest attack vectors and hacking tactics to avert zero-day assaults. All attack surfaces, including those in the mobile, cloud, network, endpoint, and IoT, must be covered by threat intelligence.

9. Conclusion

Due to tremendous technological improvement over the past 20 years, cyber security and cyber attacks have both developed and advanced significantly. Even though this is the case, the majority of firms, even after the development of the fifth generation of cyber security, are still using second or third-generation cyber security because they have not improved. Due to their size and speed, these fifth-generation assaults are known as mega attacks. The majority of today's firms utilize traditional, static detection-based security measures, yet these sophisticated attacks can easily get past them. Therefore, enterprises should build the fifth-generation security architecture to safeguard their network infrastructure, cloud infrastructure, and mobile infrastructure to defend against the most recent assaults.

As a result, it is important to raise awareness among businesses and individuals about cyber attacks, their effects, and security measures.

Everyone should only use technology after weighing the benefits and drawbacks, as well as security flaws, and after taking precautions to protect their data. Future work will provide a fifth-generation security architecture to safeguard the cloud, network, and mobile infrastructure that makes up the online digital infrastructure.

Acknowledgments

No specific grant for this research has been given by funding organizations in the public, private, or nonprofit sectors. The authors say they have no conflict of interest.

References

[1] D. Schatz, R. Bashroush, and J. Wall, (2017), Towards a more representative definition of cyber security, J. Digital Forensics, Security and Law, **12(2)**, pp.53-74.

[2] Trustwave's Global Security report; https://www2.trustwave.com/rs/815-RFM693/images/2015_TrustwaveGlobalSecurityReport.pdf.

[3] A. Chowdhury, Recent cyber security attacks and their mitigation approaches: An Overview, Int. Conf. on Applications and Techniques in information.

[4] R. Moore, (2014), Cybercrime: Investigating high-technology computer crime, Routledge.

[5] Cybercrime Definition, Statistics, and Examples, Encyclopedia Britannica, Retrieved 25 May 2021.

[6] The Open Web Application Security Project (OWASP) (2018), Available online: https:// www.swasc an.com/owasp.

[7] OWASP Top 10 Vulnerabilities, veracode, https://www.veracode.com/security/owasp-top-10

[8] B. Hamid, N. Jhanjhi, M. Humayun, A. Khan, and A. Alsayat, (2019), Cyber Security Issues and Challenges for Smart Cities: A survey, 13th Int. Conf. on Mathematics, Actuarial Science, Computer Sc. and Statistics (MACS), IEEE, pp.1-7.

[9] http://technet.microsoft.com. Retrieved 2009-09-10

[10] technet.microsoft.com, Retrieved on 10 September 2009.

[11] An Undirected Attack Against Critical Infrastructure, United States Computer Emergency Readiness Team (Us-cert.gov), Retrieved 28 September, 2014.

[12] Ramzan and Zulfikar, (2010), Phishing attacks and countermeasures, Stamp, Mark; Stavroulakis, Peter (eds.), Handbook of Information and Communication Security, Springer; ISBN 978-3-642-04117-4.

[13] H. Drucker, Wu D. Vapnik, (1999), Support vector machines for spam categorization, IEEE Trans Neural Netw Publ IEEE, **10(5)**, pp.1048-54.

[14] L. F. Cranor and B. A. Lamacchia, (1998), Spam Commun. ACM, **41(8)**, pp.74-83.

[15] https://www.checkpoint.com/downloads/product-related/genv-survey-study.pdf

[16] Security Report (2018) Check point, https://www.checkpoint.com/downloads/product-related/report/2018-security-report.pdf.