Proceedings of the 8th International Conference on Communication and Electronics Systems (ICCES 2023)
IEEE Xplore Part Number: CFP23AWO-ART; ISBN: 979-8-3503-9663-8

Machine Learning based Cybersecurity Technique for Detection of Upcoming Cyber Attacks

Dr Kanchi Lohitha Lakshmi
Department of Computer Science and Engineering, Vasireddy Venkatadri Institute Of Technology, Guntur
lohita.kanchi@gmail.com

S.Shobana
Department of IT
R.M.K Engineering College
ssh.it@rmkec.ac.in

Bathula Prasanna Kumar
Department of Computer Science and Engineering
KKR & KSR Institute of Technology and Sciences, Guntur, AP
prasannabpk@gmail.com

K.B.Glory
Department of Engineering English,
Koneru Lakshmaiah Education Foundation,
Vaddeswaram-522302, Andhra Pradesh State, India, kommalapatiglory@gmail.com

Bonda Kiran Kumar
Department of Architecture
KL school of Architecture
KL Deemed to be University, Vaddeswaram,
Guntur District -522302
architectkiranbonda@gmail.com

Sandya Rani
Dept. of IT
St. Martin's Engineering College
Secunderabad Telangana India.
sandhya.marri@gmail.com

***Abstract*— Cyberattacks are prevalent in the age of the Internet. Each year, both the quantity and severity of cybercrimes increase. Protection against cyber-attacks has become a primary responsibility, Significant in the internet society of today. However, providing cyber security is a highly difficult task that requires experience in the field of attacks and the ability to evaluate the possibility of threats. The continual evolution of cyberattacks is the biggest challenge in this industry. This article describes the significance of cyber security and enumerates the hazards that exist in the present digital environment. The statistics and evaluation of cyberattacks demonstrate the seriousness of these occurrences. Several sorts of cyber security threats are outlined, along with the machine learning approaches that may be used to detect these attacks.**

Keywords*— Cybersecurity, Cyberattack, Internet, Security, Technology, Challenge, Defence, Digital

I. INTRODUCTION

As more people depend on and use the Internet, companies, governments, and even banks have moved their activities online. Therefore, cyber defenses are weakened. Cyberattacks are defined as any intentional attempt to obtain unauthorized access to a target's computer network. Businesses, governments, and other financial institutions such as banks are regular targets of cyberattacks designed to steal valuable data or demand a ransom in return for access. Both the number and complexity of cyberattacks increase significantly over time [1]. The online community now confronts significant hurdles as a result. The Worldwide Security Report found that around 98% of online applications are vulnerable to hackers. According to a survey performed by the Department of Business, Technology, and Skills, ninety percent of major businesses and seventy-four percent of small businesses had experienced security breaches. As a result, "cyber security" has become the principal field of research. Cyber security is the protection of information in cyberspace, assuring its confidentiality, integrity, and accessibility. Despite being a distinct notion, cybersecurity requires the collaboration of several disciplines to guarantee safety.These regions are just briefly described [2].

- Application security is the practice of enhancing an application's safety via several techniques. Monitoring the application and searching for, repairing, and attempting to avoid security problems are typical approaches for doing this.
- Information security refers to a collection of rules and practices meant to safeguard the confidentiality, integrity, and accessibility of an organization's data and records.
- Networking security is a process that secures the confidentiality, availability, and authenticity of a network and its data while permitting authorized access to the network. Typically, both hardware and software technologies are employed to defend a network.
- Operational security is the practice of identifying and protecting unrestricted but vital data that may be enticing to a competitor or opponent seeking an advantage.
- To ensure the security of digital payments, Internet service providers use a variety of security procedures. It comprises defining stringent criteria for the Defence against the attack of browsers, networks, operational platforms, and other programs.
- Information and communication technology security is the ability to protect the C, I, and A of an organization's electronic data assets.
- Humans are the most vulnerable component of any cybersecurity system due to their inherent unreliability. Half of all cyberattacks are caused by user ignorance of cybersecurity risks, while more than 90 percent are the result of intentional human activity [3].

In contrast, cybercriminals are growing more skilled in their attacks and are increasingly using cutting-edge tools and methods. In a short period, they may identify and exploit security vulnerabilities in a system, enabling them to steal data or inflict system damage. In the present electronic age, there is an urgent need for increased cyber security via the use of creative tactics, since people perform all of their vital everyday activities online [4]. Cybersecurity expenditures must expand at the same pace as cyberattacks if they are to be addressed successfully. The research aimed to fulfil the following objectives:

- Study regarding cyberattack, cybersecurity, cyber security threat, and cost of cybercrime.
- Examine the cyber-attack for small and medium businesses.
- Study regarding Impact and severity of cyber-attacks.
- To study the move to next-generation cyber security design.
- Examine the resources of counter threats.

II. METHODOLOGY

Cyberattacks are common worldwide. Cybercrimes rise annually in number & complexity. Cybersecurity is becoming a priority. modern digital society. Cyber security is challenging and needs skills in assaults & threat assessment [5]. This industry's major problem is cyberattacking development. This article discusses cyber security & digital threats. Cyberattack data show their severity. Any hostile activity against a computer, server, network, or another internet-connected item would constitute a cyberattack [6]. Assault is the act of attempting to enter a system without authorization and maybe with malicious intent. Depending on the conditions, attacks on computer networks may be characterized as cyberwarfare or cyberterrorism. A cyberattack may be launched by any entity, including nation-states, individuals, groups, societies, and organizations, or even an unknown attacker. Occasionally, the phrase "cyber weapon" is used to describe a gadget that assists in launching an attack over the internet. In the last few years, the number of cyberattacks has increased at an alarming rate [7].

The objective of a cyberattack is to get access to a system to steal, change, or destroy data. There is a broad range of cyberattacks, ranging from the installation of malware on an individual's computer to the targeting of a whole nation's key infrastructure [8]. To distinguish between regular data breaches and bigger hacking operations, legal authorities are attempting to limit the scope of the term to incidents that result in physical injury. The complexity of cyberattacks has enhanced the threat they represent [9].

Cybersecurity

Cybersecurity refers to the practice of protecting from hostile cyberattacks from hardware, software, and data stored on or accessible over the internet [10]. Individuals and corporations alike use the technology to protect their data centers and other electronic assets against infiltration. A robust cybersecurity strategy can offer effective protection against attacks that aim to breach security and steal data. Cybersecurity is also essential for defending against attacks that seek to harm or otherwise disrupt the regular operation of a device or system [12]. In 2015, cybercrime cost companies $3 trillion worldwide. By 2025, annual expenditures are expected to exceed $10.5 trillion. Cybersecurity Technologies reports that the flow of money via cybercrime is the biggest in human history. This reflects an annual growth rate of 15%. Each sector is susceptible to cyber-attacks, but small & medium enterprises (SMEs) face the brunt of their rising frequency, complexity, and frequency. Accenture discovered that just 14% of businesses were prepared for cyber-attacks, even though 43% of cyber-attacks targeted small businesses.

In addition to disrupting corporate operations, a cyber-attack can damage vital information technology (IT) assets or infrastructure, making complete recovery impossible without considerable financial and human commitment. This makes Defence harder for tiny businesses. According to a recent study, small and medium-sized enterprises all across the globe have faced cyber-attacks.

- Inadequate security measures: 46% of respondents believe their security measures are ineffective against cyberattacks.
- Sixty-six percent have been the subject of a cyberattack during the last year, demonstrating the frequency of such attacks.
- Sixty-nine percent of respondents believe that the targeting of cyberattacks is becoming more specific.

When it comes to attacks against small businesses, the most common include:

- 57% of Phishing and social engineering.
- 33 percent of hacked or stolen devices have been reported.
- Identification theft, 30%

The chief executive officer of a firm may minimize risks, enhance returns on cybersecurity efforts, and even prevent future attacks by knowing more about the sorts of systems that are often targeted and their consequences .

Cyber Security Threat

The purpose of the majority of cyberattacks is to breach or get access to the target system. Multiple means of attack on the target systems will ultimately result in success and the mission's completion.

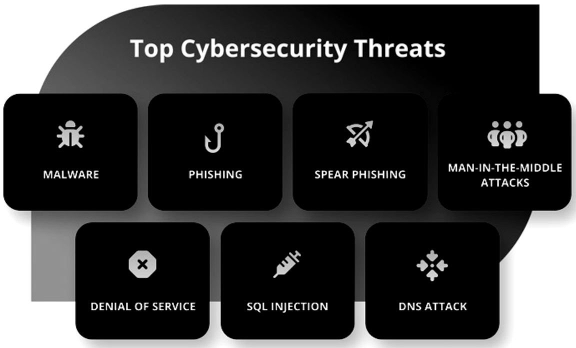

Figure 1: Top Cybersecurity Threats

There are several sorts of cyberattacks, and the number is increasing. The following are examples of common cyberattack types:

Cryptojacking

A unique kind of cyberattack employs a third-party computer to mine bitcoin on the victim's behalf. In some instances, hackers may utilize JavaScript code that runs in the victim's browsers, and in others, They would install malicious software on the victim's PC to do the required computations.

Phishing

"Phishing" refers to the act of sending emails that are constructed to seem as if they originated from a reputable organization. The purpose is either to gain unauthorized access to the victim's computer or to acquire sensitive information, such as passwords & credit card details.Presently, phishing emails are one of the most common internet security threats.

Denial-of-service Attack

A denial-of-service attack is an assault that employs a massive amount of traffic to overload a target's system, server, or network, preventing it from working properly. The system is overloaded and cannot process legitimate requests. This attack may be conducted using a network of compromised devices. Multiple attacks are made against the target as opposed to a single one. This kind of attack is technically referred to as a DDoS attack. 24 percent of firms have seen a distributed denial of service attack over the last year.

Malware

Malware, an abbreviation for "malevolent software," refers to software having malicious intent that may cause harm to a computer or an entire network. From the earliest worms and viruses to the most complex spyware and ransomware, malicious programs vary in sophistication. Infection of a system or network happens when a user activates a malicious link, opens a malicious file, or installs malicious software. Malware can only proliferate and spread when it interacts with other software or hardware. This is the most crucial point to know. Reasons include limiting network connectivity, installing harmful software, and gathering data.

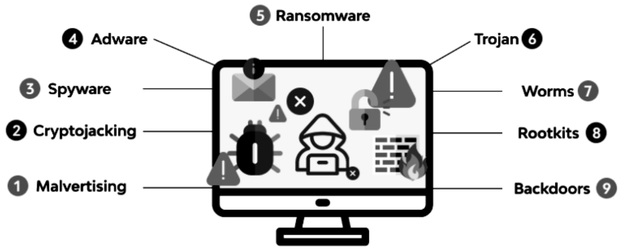

Figure 2: Malware Types

Spam

It is an unsolicited email that nobody requested. It may be necessary for recipients of spam e-mails to manually execute Java applets included inside the message. In addition to the aforementioned threats, the SANS Institute identifies the following harmful spyware behaviors as the most prevalent:

- Installing a rootkit or applying other system modifications to impede removal;
- Setting up a bit for use as a remote control by the attacker
- Exfiltrating or encrypting for ransom captured sensitive documents.
- Including modifications to the network settings,
- Deactivating security software, such as an antivirus application or a malware detector
- Disabling Microsoft's security and update functions
- Scanning websites for security flaws, taking information from online forms and capturing information from displays.
- Activating audio/video capture devices
- Falsely claiming to be an antivirus or anti-spyware application.
- Enhancing search results by modification,
- This involves the implementation of fake certificates,
- Viruses release files sequentially, in a cascade.
- The capture of typed text,
- Among other acts connected to spamming,
- Installing a snooper.

Man-in-the-middle Attack

A man-in-the-middle (MITM) attack is one in which the perpetrator interposes himself between two parties. After effectively disrupting communication, an intruder can filter and steal information. In this scenario, eavesdropping attacks are a common occurrence. Theft of passwords, the transmission of credentials, etc., are merely a few instances of MITM attacks. (Rahim, 2017). On an unprotected public Wi-Fi network, hostile actors may often place themselves between a guest's equipment and the network. The victim unknowingly grants the attacker access to all of his or her data. The attacker may place malware on the victim's PC to steal personal information.

III. INFLUENCE & SIGNIFICANCE OF CYBERATTACKS

The consequences of a cyberattack on a business might vary from relatively minor disruptions to catastrophic losses. Regardless of the origin of the hack, there will be consequences. Your business may continue to experience the consequences of the hack weeks or months after it occurred. I have developed a list of your company's five probable weak spots:

- Financial difficulties
- Loss of work time
- Reputational harm
- Legal responsibility
- Difficulties keeping the business going

The risk of a ransomware attack is increasing. Towards the end of 2016, the ransomware infected a business every forty seconds. Cybersecurity Innovations forecasts that this frequency will climb to once every 11 seconds by the year 2021. Utilizing malicious software, attackers hold information or systems, hostage, until a ransom is paid. As firms increasingly use digital technology, security issues continue to develop. The bulk of failures and security breaches may be attributed to archaic security architectures that are meant to manage all of this. Incorporating cloud computing and the Internet of Things, the architecture of the next generation enables businesses to eliminate single points of failure by providing the essential robustness and resilience to continue functioning or defend against any attack. This protection architecture will provide a single safety architecture that regulates and interacts with mobile, cloud, and networking to guard against and prevent the next generation of cyberattacks.(Langer, 2020). In addition to providing fluid safety rules across all systems that reflect business objectives, meet cloud needs with auto-scaling, or may interact dynamically with third-party APIs, unified risk detection must be able to scale to meet cloud requirements. In addition, to guard against both known and unknown "zero-day" attacks, a coherent and complex multi-layered risk avoidance ecosystem must include CPU-Level sandbox avoidance, threat extraction, anti-phishing, and anti-ransomware technologies. The only way to provide a single, cohesive wall of protection against upcoming generation attacks is to ensure that the whole safety network is based on the proper architecture.

Resources of Counter Threats

To better prepare yourself to combat cyberthreats, you may like to review the following helpful resources.

A. MITRE's Backing

MITRE, a non-profit research and development organization backed by the federal government, partners with public and private sectors to distribute knowledge about cyber threats to prevent ransomware. AI, smart information science, quantum data science, space defense, medical computing, cyber-threats, and cyber-resilience, among others, are all included in its body of knowledge.

B. Enhancing Internet of Things Cybersecurity Act

The government is taking efforts to prevent these cyberattacks. In 2020, the Internet of Things Cybersecurity Protection Act was signed into law. The National Institute of Standards and Technology (NIST) will provide government-level standards on edge technology security that will assist the corporate sector.

C. Protection of Machines

Hardware, particularly silicon-based components, is increasingly charged with defending against cyber-attacks. Security solutions like crypto acceleration, authentic random-number generation, memory encryption, and protected booting may counter side-channel and Row hammer attacks.

D. *Cybersecurity Landscape in the Era of 5G*

The advantages of 5G will not only be enjoyed by corporations, governments, and academic institutions, but also by cybercriminals. With the growth of speedier and much more ubiquitous wireless connections, criminal behaviors on the Internet are anticipated to increase. 5G Countries, an industry trade association, encourages the growth of 5G across the New World by sharing information about how to safeguard 5G-related innovations or system design. The group proposes a seven-layer approach to threat intelligence, with layers ranging from an IP address through unsupervised machine learning. The corporation has issued a white paper titled "Security Concerns for the 5G Era" that provides more recommendations. It provides practical recommendations about the design of 5G-related systems.

E. Developing a Cybersecurity Strategy Customized to Your Specific Requirements

The whole universe revolves around the premise of "zero trust." If you are in control of a company or network, you should never connect to a network node or device unless it has been properly authenticated or verified. If you are the designer of a device, your device's boot ROM must be safeguarded with the "root of trust." This indicates that the boot codes must be secure and incapable of being modified by a third party. Multiple examples of malicious malware successfully infecting boot ROMs have been documented. When a system is infected with malware, the malicious software either instantly seizes control of the system at boot-up or enters a dormant condition, ready to cause issues later. Consequently, it is necessary to cultivate the basis of trust properly. In such a scenario, the whole system's integrity is in danger. Find the proper resources and/or a reliable third-party consultant to help you accomplish your goals.

F. Exceptionally Valuable Cybersecurity Techniques

The process of establishing cybersecurity may be challenging due to the multiple aspects that must be addressed. To collect the findings of the Dark Readings 2020 Strategic Security Survey, 190 IT and cybersecurity specialists from organizations with at least 100 employees were interviewed. According to the survey results, the eight most effective cybersecurity techniques are endpoint protection, upcoming firewalls, virtual private networks (VPNs), data encryption, email security and spam detection, vulnerability assessment, and penetration testing, antivirus and anti-malware software, and identity management. As seen in the following table, there are many more technical considerations to consider.

IV. CONCLUSION

Both cyberattacks and cybersecurity have developed and evolved greatly during the last two decades due to technological advancements. Despite this, despite the introduction of upcoming generation approaches, many businesses remained trapped in the past, using cyber security measures from the second or third generation. The upcoming generation of attacks is appropriately dubbed "giant assaults" due to their vast size and quick tempo. The majority of firms still depend on outmoded security systems that rely only on static detection techniques, which these sophisticated attacks can readily defeat. Therefore, firms should use 5G security to protect their networks, clouds, and smart devices from the most current attacks. In conclusion, a larger effort must be made to educate organizations and individuals about the risks of cyberattacks and the measures they may take to defend themselves. Before committing to broad usage, everyone should assess the advantages and disadvantages of the technology, as well as the dangers connected with security breaches.

REFERENCES

[1] Eichensehr, K. (2018). Decentralized Cyberattack attribution. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3369808

[2] Trappe, W., &amp; Straub, J. (2018). Cybersecurity: A new open access journal. Cybersecurity, 1(1), 1. https://doi.org/10.3390/cybersecurity1010001

[3] Cybercrime costs 110bn a year – maybe more. (2012). Computer Fraud &amp; Security, 2012(9), 3–20. https://doi.org/10.1016/s1361-3723(12)70088-x

[4] Patayo, C. (2021). A preventive and detective model for a phishing attack in small and medium size businesses. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3777065

[5] Chidukwani, A., Zander, S., &amp; Koutsakis, P. (2022). A survey on the cyber security of small-to-medium businesses: Challenges, research focus and recommendations. IEEE Access, 10, 85701–85719. https://doi.org/10.1109/access.2022.3197899

[6] Kshetri, N., &amp; Voas, J. (2022). Cryptojacking. Computer, 55(1), 18–19. https://doi.org/10.1109/mc.2021.3122474

[7] Denial-of-service attack. (2013). Encyclopedia of Crisis Management. https://doi.org/10.4135/9781452275956.n91

[8] Moallem, A. (2021). Malware protection technology. Understanding Cybersecurity Technologies, 79–88. https://doi.org/10.1201/9781003038429-9

[9] Rahim, R. (2017). Man-in-the-middle-attack prevention using Interlock Protocol Method. https://doi.org/10.31227/osf.io/8txn7

[10] Espinoza-Zelaya, C., &amp; Moon, Y. (2022). Taxonomy of severity of cyber-attacks in cyber-manufacturing systems. Volume 2B: Advanced Manufacturing. https://doi.org/10.1115/imece2022-94492

[11] Langer, A. M. (2020). Cyber security in analysis and Design. Analysis and Design of Next-Generation Software Architectures, 181–199. https://doi.org/10.1007/978-3-030-36899-9_9

[12] Barkov, A. V., &amp; Kiselev, A. S. (2022). Legal support of information security: Tools to counter cyberthreats. Journal of Applied Research, 1(5), 91–96. https://doi.org/10.47576/2712-7516_2022_5_1_91

.