RESEARCH ARTICLE OPEN ACCESS

Cybersecurity Attacks and Counter Measures- A Review

Dr.G.Brindha[1], Mrs.P.Sudha Juliet [2]
[1]Associate Professor, [2]Assistant Professor
[1,2]Department of EIE,
[1,2]Meenakshi College of Engineering.

ABSTRACT
Every system is vulnerable to attacks, as the current plague of data breaches demonstrates. Establishing and enforcing procedures to monitor their cyber environment, spot vulnerabilities, and promptly patch security gaps is critical for any business that handles, saves, transmits, or maintains data in any other way. Understanding the difference between cyber threats and vulnerabilities is essential before pinpointing specific risks to contemporary data systems. Common security threat categories include, for instance, phishing assaults that cause the installing malware that corrupts your data, a staff member neglecting data security procedure that results in a data breach, or even a tornado destroying the data center for your business, preventing access. The research investigates the many types of cyberthreats that exist today, such as advanced persistent threats, malware, ransomware, and social engineering scams. It examines the changing strategies and methods employed by cybercriminals and emphasizes the possible effects on several industries, including banking, healthcare, and essential infrastructure. The usefulness of technical developments like blockchain, AI, and machine learning in strengthening cybersecurity defenses is also assessed in this article. Lastly, it offers suggestions for future lines of inquiry and preventative actions to successfully counter new cyberthreats.

Keywords: Cybersecurity, Defense Strategies,EmergingThreats,Malware, Ransomware.

Date of Submission: 18-05-2024 Date of acceptance: 03-06-2024

I. INTRODUCTION

The growing interconnectedness of today's globe has made cybersecurity a top priority for all parties—individuals, corporations, and governments. The danger landscape has changed because of the internet's widespread use and technology's rapid growth, giving rise to new and evolving cybersecurity concerns that require our careful attention[1].Cybersecurity threats comprise a broad spectrum of malevolent actions undertaken by individuals, collectives, or even states with the aim of jeopardizing the availability, confidentiality, or integrity of digital systems and information. Our national security, financial stability, intellectual property, and privacy are all seriously threatened by these challenges.It is critical that we remain up to date on the newest developments in cybersecurity and the threats that could arise in the future and take advantage of holes in our digital infrastructure.We may create efficient defenses to safeguard our businesses, ourselves, and society at large by comprehending these threats [2].The most well-known new cybersecurity risks that have received attention recently are examined in this study. We will explore their traits, possible effects, and the underlying causes of these dangers. We will also go over the best practices and countermeasures that can help lower these risks and improve our overall cybersecurityposture.It is critical to understand that the cybersecurity industry is a dynamic one. As hackers continue to develop creative ways to take advantage of holes in our systems and networks, new risks will inevitably surface. Through cultivating a climate of consciousness, instruction, and readiness, we can adjust to these changing risks and remain one step ahead.

1.1 CYBER SECURITY VULNERABILITIES, THREATS

The attacker first identifies the list of possible nodes [15] and discovers the routes possible according to the location details of the nodes. Categories of vulnerabilities

- Corrupted (Loss of integrity)
- Leaky(Loss of confidentiality)
- Unavailable or veryslow (Loss of availability)

Threatsrepresentpotentialsecurityharmto an asset when vulnerabilities are exploited. Attacks are threatsthat have been carried out.

- Passive – Make use of information from the system without affecting system resources.

- Active – Alter systemresources or affect operation.
- Insider – Initiated byan entity inside the organization.
- Outsider – Initiated fromoutside the perimeter.

1.1.1 Types of Active attacks:

a) Masquerade attacks allow an attacker to obtain access to a system or higher privileges than they are permitted by posing as a certain user. One can attempt a masquerade by using passwords and login IDs that have been stolen, by looking for holes in software security, or by getting around the authentication process[3].

b) Session replay: In this kind of attack, the hacker obtains the session ID to obtain the login credentials of an authorized user. The unauthorized person gains access to the website and can do any action that an authorized user can.

c) Message modification: To change the data on a target system or route a message to a new location, an attacker modifies the packet header addresses in this attack.

d) A denial of service (DoS) attack prevents users from using a web resource or network. Usually, this is achieved by sending the target an excessive amount of traffic.Large numbers of hacked systems, also referred to as a botnet or zombie army, assault a single target in a distributed denial-of-service (DDoS) exploit.

1.1.2 Types of Passive Attacks:

Despite being very rare from a classification standpoint, passive attacks are quite simple to execute, especially if the traffic is not encrypted [4]. Different Passive Attack Types:

a) Eavesdropping, often known as tapping, is the act of an attacker listening in on two parties' messages. The traffic must not be encrypted for the attack to be effective. The attacker may be able to obtain any unencrypted data, including a password supplied in response to an HTTP request.

b) Traffic analysis: the hacker examines the metadata carried in the traffic to infer details about the exchange and the involved parties, such as the type of traffic that is being exchanged (rate, duration, etc.). When encrypted data is utilized, traffic analysis can result in cryptanalysis attacks, in which the attacker may be able to decrypt the traffic and get information.

c) Attacks using software: Software intended to take control of or harm a computer user's operating system without the user's knowledge or consent is known as malicious code, or malware. It can be highly harmful and challenging to get rid of.

1.1.3 Cyberthreats and Cyberwarfare:

Cyberwarfare is the use of digital attacks, such as computer viruses and hacking, by one nation to interfere with another's vital computer systems to cause harm, death, or destruction. In future conflicts, hackers will fight alongside soldiers with conventional weaponry like rifles and missiles, utilizing computer code to target an enemy's infrastructure.Cyberwarfare is the deployment of computer viruses or denial-of-service assaults, among other tactics, by a nation-state or international organization to target and try to compromise the computers or information networks of another country[5].

1.1.4 Cyber Crime:

Criminal action that either targets or makes use of a computer, computer network, or networked device is known as cybercrime.Hackers or cybercriminals who aim to profit from cybercrime commit it. Cybercrime is committed by people.

II. COUNTER MEASURES:

An organization issues security policies as a formal set of recommendations to make sure that users who are allowed to access corporate technology and information assets follow the rules and regulations pertaining to information security [6].A security policy is also referred to as a "living document," meaning that it is updated constantly in response to changes in personnel needs and technological requirements.To maintain the security of our network, we employ security policies. Most security policy types are generated automatically after installation. Additionally, we can alter policies to fit our unique setting.

2.1 Need for Security:

1) It boosts productivity.
2) It maintains responsibility and discipline.
3) A commercial agreement can be made or broken by it.
4) Educate employees on security literacy

The next section discusses some crucial recommendations for cyber security policies, including:

a) virus and spyware protection strategy:

It assists in identifying threads within files and identifying apps displaying questionable conduct.Using signatures, it eliminates and fixes the negative impacts of infections and security threats.

b) Firewall Policy:

It identifies cybercriminals' attacks and eliminates undesired sources of network traffic. It prevents unauthorized users from accessing systems and networks that link to the Internet.

c) Intrusion Prevention policy:

This policy automatically identifies and stops browser and network attacks. It also guards against weaknesses in programs, examines the contents of one or more data packages, and finds malware that enters the system legally.

d) Application and Device Control: This policy controls which external devices can connect to a system and safeguards its resources from apps. While the application control policy can only be applied to Windows clients, the device control policy is applicable to both Mac and Windows machines.

e) Encryption: The technique of encoding data to render it unreadable to unauthorized parties is known as encryption. Sensitive data is encrypted so that, even if it is intercepted, it cannot be decrypted without the right key.

f) Strong Authentication: Enforcing strong authentication methods, like biometric or two-factor authentication (2FA), gives user logins an additional degree of protection. This guarantees that systems and data are only accessible to those who are authorized.

g) Data Backup and Recovery: To recover from occurrences such as ransomware attacks or hardware malfunctions, it is imperative to routinely backup important data and confirm the files' integrity. A strong backup plan guarantees that in the event of a data loss or security incident, the data can be recovered [7].

h) Incident Response Plan: This document describes what should be done in case of a cybersecurity incident. It aids in organizations' quick and efficient response, reducing harm and promoting a speedy recovery.

III. CYBERSECURITY DEFENSE STRATEGIES

Institutions that want to put the Industry model into practice must take precautions against any actions that might result in an unfavorable situation regarding the confidentiality, availability, and integrity of their data in cyberspace.An investigation into the potential sources of cyberattacks within the company is necessary to stop this [8]. Two primary headings are used to assess the assaults on Industry systems. These hazards are both caused by nature and by humans.Human-induced hazards are the main things that might endanger the organization's cyberspace. Threats caused by humans might come from both the inside and the outside. Human dangers inside an organization might arise from inexperienced staff, spies, malevolent individuals, or mistakes made by IT managers [19]. External dangers include things like espionage and other illegal access to the institution's cyberspace from the internet environment.

Five basic approaches to defense of computing systems

1. Prevent attack:- Block attack / Close vulnerability
2. Deter attack:-Make attack harder
3. Deflect attack:- Make another target more attractive than this target
4. Detect attack:- During or after
5. Recover from attack

Systems in the future of manufacturing are more vulnerable to cyberattacks than those in previous industrial revolutions because of the reduced human component [9]. Attacks that target intelligent production systems in particular may negatively impact an institution's ability to produce. Figure 1 illustrates the layers at which businesses wishing to use the Industry architecture may be vulnerable to and affected by cyberattacks.

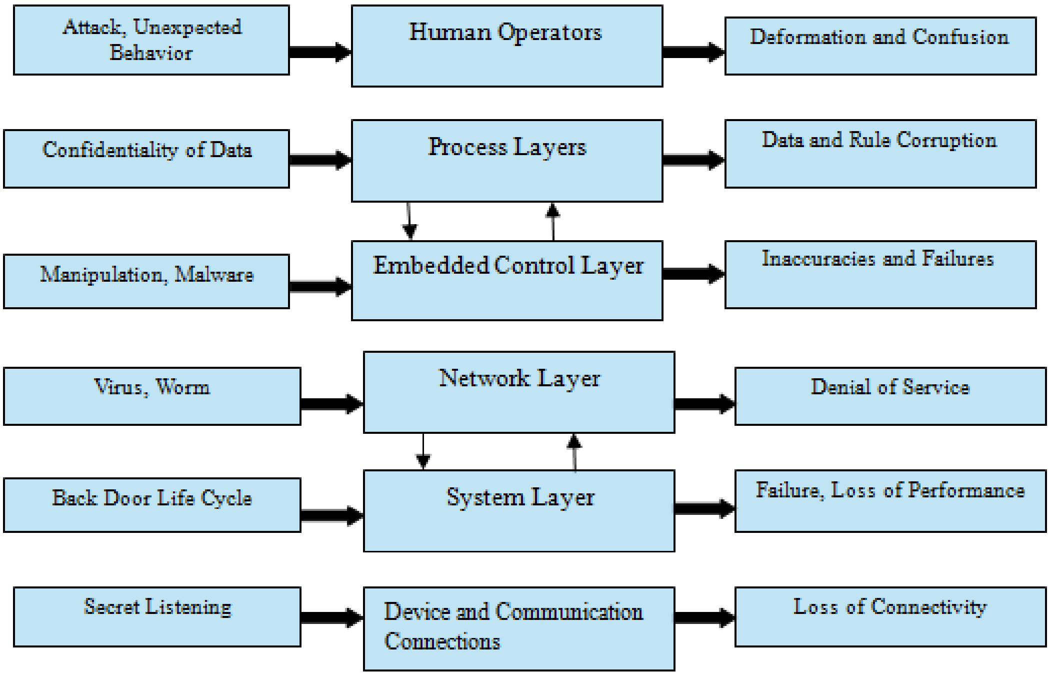

Fig.1 Targets and Effects of Cyber Security in Industry

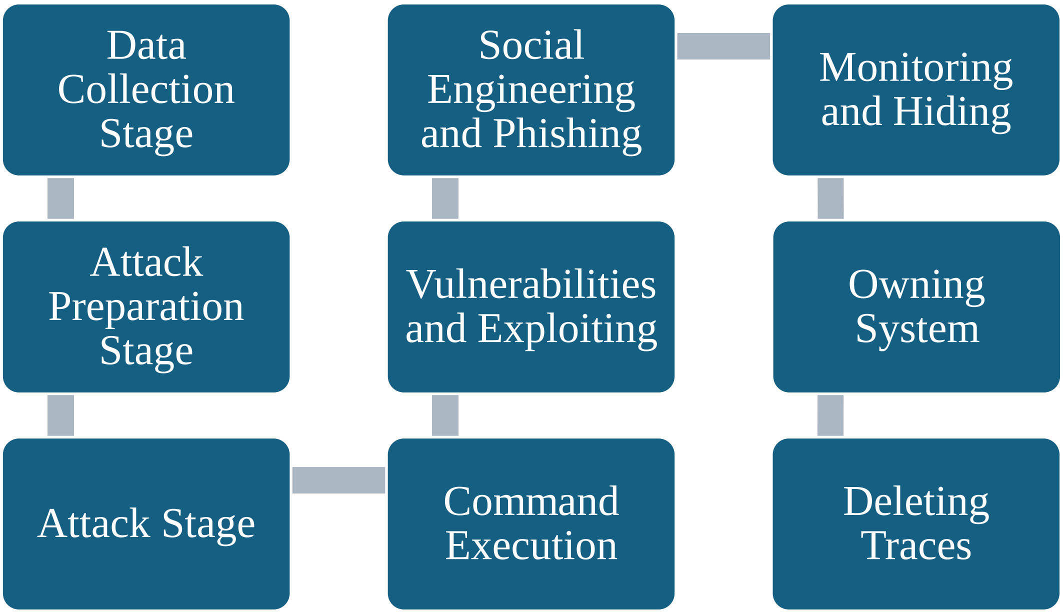

Fig2: Stages of Attacks in Cyber Attack

Three primary issues in ensuring IoT security have been found by the studies. Performance, encryption, and privacy issues are the root causes of these issues. The following methods can be created to guarantee the security of IoT devices [18].

- Apps operating on Internet of Things devices must to be permitted to log in.
- IoT devices require network authentication before data transmission.
- A firewall is necessary on the network to filter data packets since IoT devices have low processing and memory capacities.
- IoT device updates need to be deployed to prevent the usage of extra bandwidth.

The scanning engine attempts to connect to an open port that it finds and logs the connection. Various application users can search via means of these documents [10]. The Information gadgets are utilized in the organization, the Information Security Authority must do IP or domain inquiries on such applications.The query returns access to the IP or domain's open port, location, database, and server status.

IV. IMPACT OF CYBER THREATS

Cybersecurity threats have a big effect on people, businesses, and society at large. The following are a few of the main effects of cyber threats:

a) Financial Loss: Both individuals and companies may suffer significant financial losses as a result of cyberattacks. These losses may result from paying hackers ransom, having sensitive financial information stolen, having businesses disrupted, incurring legal fees, or having to pay for recovery costs following an attack [11].

b) Data breaches: Attackers may obtain illegal access to private information, including financial records, trade secrets, and intellectual property, as a result of cyber threats. Serious repercussions from data breaches could include identity theft, harm to one's reputation, legal ramifications, and fines from regulatory bodies.

c) Services Can Be Disrupted: Cyberattacks have the potential to interfere with vital services, such as transportation networks, healthcare facilities, and communication networks.

d) Privacy Concerns: Personal information is susceptible to misuse and unauthorized access due to cyber dangers. Identity theft, fraud, and targeted advertising are just a few of the ways that compromised personal data may be used against people, robbing them of their privacy and autonomy.

e) Reputational Damage: Cyberattack victims frequently sustain serious harm to their reputations. A security event or data breach may cause stakeholders, partners, and customers to lose faith in you. The process of repairing a tarnished reputation can be difficult and time-consuming.

f) National Security Risks: Cyber risks are a potential hazard to national security. State-sponsored cyberattacks can affect military networks, government systems, and vital infrastructure, perhaps impairing vital services, stealing private data, or even resulting in bodily injury.

V. TECHNOLOGICAL ADVANCEMENTS IN CYBERSECURITY

As our reliance on technology increases, cybersecurity has grown in importance. Recent years have seen the emergence of several technical improvements to stay up with the ever-evolving cyber dangers [12]. The following are some noteworthy developments in cybersecurity:

- Machine learning (ML) and artificial intelligence (AI):

Cybersecurity has been significantly impacted by AI and ML. They make it possible to create sophisticated threat detection and response systems that have the capacity to examine enormous volumes of data, spot trends, and identify abnormalities. These technologies can strengthen threat intelligence, automate security procedures, and strengthen incident response capacities.

- Analytics of Behavior:

The goal of behavioral analytics is to find abnormalities and possible dangers by examining user behavior and system activity. Through the establishment of baseline patterns, this method can identify anomalous or malevolent activity that deviates from the standard [16].

- Threat Intelligence Platform: Platforms that collect, examine, and distribute threat intelligence information from several sources are known as threat intelligence platforms, or TIPs for short. They supply up-to-date intelligence on new threats, weaknesses, and attack avenues to businesses. Security teams can proactively thwart attacks and swiftly address events thanks to TIPs.
- Cloud Security: As cloud computing has gotten more and more popular, protecting cloud settings has become essential. Strong security features like data encryption, access restrictions, identity, and access management (IAM), and cloud workload protection are now possible thanks to advancements in cloud security solutions. Furthermore, visibility and unified administration across different cloud providers are provided by cloud security products.
- Zero Trust Architecture: This strategy questions the established perimeter-based security paradigm.It operates under the premise that no user or device, whether within or outside the network, should be taken for granted. To reduce the possibility of unwanted access, Zero Trust Architecture uses multi-factor authentication (MFA), stringent access rules, and ongoing monitoring [13].
- Blockchain Technology: Blockchain technology, which powers digital currencies like

Bitcoin, may find use in cybersecurity. safe transactions, safe data storage, and identity management are just a few of the areas where its decentralized and unchangeable nature may improve security.20 Blockchain-based solutions are suited for applications such as supply chain security and secure voting systems because they offer transparency, integrity, and resistance to manipulation.

- Internet of Things (IoT) Security: As IoT devices proliferate, it is imperative to ensure their security. The main areas of improvement in IoT security include vulnerability management, secure communication protocols, encryption, and secure device authentication. To further safeguard IoT ecosystems, network segmentation and security monitoring are essential.

These developments in cybersecurity technology show how persistent attempts are being made to counter the always changing threat scenario. It is imperative for security professionals and organizations to consistently use these breakthroughs and adapt to remain ahead of hostile actors, safeguard vital infrastructure, and secure sensitive data [14].

5.1 Cyber Crime Case Studies:

The Indian scenario with internet gambling:

State-by-state regulations governing gaming are allowed to be formulated in India. Casinos are permitted in several jurisdictions, such as Goa. Except for some categories like the lottery and horse racing, common gambling activities like organized betting are prohibited [17].The number of persons placing cash bets on Indian gambling and betting activities that are outlawed has increased in the twenty-first century. Gambling opponents assert that it promotes money laundering, corruption, and criminality. Regulated gambling proponents counter that it may be a significant source of income for the state. In 2013, Goa's casinos brought in Rs. 135 crores for the state.According to recently released data, Maharashtra state provides the popularity of the nation's online casino gamers.

VI. CONCLUSION

The cybersecurity risks that both individuals and companies must deal with are always changing in tandem with technology. It takes a proactive strategy that combines technological controls, user education, and a strong security culture to stay ahead of these new risks. People and organizations may improve their cybersecurity posture and lessen the risks presented by emerging attacks by putting the right countermeasures in place and keeping up to date on the changing threat landscape.ongoing investigation and advancement in fields including reinforcement learning, computer vision, and natural language processing.□ Transparency, accountability, and ethical concerns in AI systems, including guaranteeing fairness and correcting prejudice. investigation of AI's potential uses in customized learning, driverless cars, healthcare, and climate prediction. developments in precision therapy, genomics, and customized medicine.The application of AI and machine learning in drug research, diagnostics, and early illness diagnosis. Integration of remote patient monitoring, telemedicine, and digital health technology to enhance accessibility and healthcare delivery.Security measures are always being improved to fend off new and emerging cyber threats.Improved data privacy standards, authentication procedures, and encryption approaches.Adoption of AI-powered security solutions to identify and respond to threats in real time.

REFERENCES:

[1]. Mitnick, K. D., & Simon, W. L. (2002). The Art of Deception: Controlling the Human Element of Security. Wiley.

[2]. Hadnagy, C. (2010). Social Engineering: The Science of Human Hacking. Wiley.

[3]. Stuttard, D., & Pinto, M. (2011). The Web Application Hacker’s Handbook: Finding and Exploiting Security Flaws. Wiley.

[4]. Erickson, J. (2003). Hacking: The Art of Exploitation. No Starch Press.

[5]. Anderson, R. (2001). Why Information Security is Hard - An Economic Perspective. Proceedings of the 17th Annual Computer Security Applications Conference (ACSAC).

[6]. Lasi, H., Fettke, P., Kemper, H. G., Feld, T., & Hoffmann, M. (2014). Industry 4.0. Business & Information Systems Engineering, 6(4), 239-242

[7]. Lee, J., Bagheri, B., & Kao, H. A. (2015). A CyberPhysical systems architecture for industry 4.0-based manufacturing systems. Manufacturing Letters, 3, 18-23.

[8]. Lu, Y. (2017). Industry 4.0: A survey on technologies, applications and open research issues. Journal of Industrial Information Integration, 6, 1-10.

[9]. Gorecky, D., Schmitt, M., Loskyll, M., &Zühlke, D. (2014, July). Human-machine-interaction in the industry 4.0 era. In Industrial Informatics (INDIN), 2014 12th IEEE International Conference (pp. 289-294). IEEE.

[10]. Almada-Lobo, F. (2016). The Industry 4.0 revolution and the future of manufacturing execution systems (MES). Journal of innovation management, 3(4), 16-21.

[11]. Hsu, D. F., Marinucci, D., &Voas, J. M. (2015). Cybersecurity: Toward a secure and sustainable cyber ecosystem. Computer, (4), 12-14.

[12]. Wells, L. J., Camelio, J. A., Williams, C. B., & White, J. (2014). Cyber-physical security challenges in manufacturing systems. Manufacturing Letters, 2(2), 74- 77.

[13]. Von Solms, R., & Van N., J. (2013). From information security to cyber security. computers& security, 38, 97- 102.

[14]. Arslan, H., Aslan, H., Karkı, H. D., &Yüksel, A. G. (2018, September). Blockchain and Security in the IoT Environments: Literature Review. In 2018 3rd International Conference on Computer Science and Engineering (UBMK) (pp. 254-257). IEEE.

[15]. G.Brindha, P.Ezhilarasi,(2022) Energy Efficient Momento Based Dynamic Scheduling for Lifetime maximization in WSN,Journal of Ambient Intelligence and Humanized Computing (2021) 12:5865–5875 https://doi.org/10.1007/s12652-020-02131-7.

[16]. Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Business Horizons, 58(4), 431-440.

[17]. S., Ramaswamy, R., &Tripathi, S. (2015). Internet of Things (IoT): A literature review. Journal of Computer and Communications, 3(05), 164.

[18]. B., Kelley, P. G., Komanduri, S., Lee, J., Maass, M., Mazurek, M. L, &Christin, N. (2012). How does your password measure up? the effect of strength meters on password creation. In Presented as part of the 21st Security Symposium Security 12) (pp. 65-80).

[19]. Gupta, G. P., &Kulariya, M. (2016). A framework for fast and efficient cyber security network intrusion detection using apache spark. Procedia Computer Science, 93, 824-831.