An Analysis on Challenges Faced by cyber Security on the latest Technologies

Aarjav Jain*

Class 11th, Student, Sanskriti The Gurukul

Abstract- Cybersecurity is crucial to the information technology industry. One of the largest problems of the modern world is information security. The first thing that springs to mind when considering cyber security is "cybercrimes," which are escalating at an alarming rate. Numerous governmental bodies and corporations are implementing numerous strategies to deter cybercrimes (Hakeem et al., 2020). Despite these precautions, many people continue to have serious concerns about cyber security. the challenges that cybersecurity encounters when coping with the most recent technologies are investigated in this paper. This research investigates the ways in which digital systems might be protected from emerging dangers like as attacks driven by artificial intelligence, weaknesses in quantum computing, and problems with Internet of Things security. The report highlights the challenges that cybersecurity professionals face and highlights the necessity of developing new tactics and working together in order to ensure that our data and computer systems remain secure in a world where technology is always evolving.

Keywords- cyber security, cybercrime, cyber ethics, artificial intelligence, quantum computing, Internet of Things security.

- X -

INTRODUCTION

With just a few button clicks, man may send and receive any type of data these days, including audio and video files and emails. However, has he ever considered how securely his data is being conveyed to the other person without any information leaking? Cybersecurity has the answer (Bhosle et al., 2021). The Internet is currently the infrastructure in daily life that is increasing the fastest. Many of the newest technologies in today's technological environment are transforming humanity. However, because of these new technology, we are unable to protect our personal information very effectively, which is why cybercrimes are growing daily. Since online transactions now account for more than 60% of all business transactions, this industry needs excellent security to provide the most transparent and effective transactions. Thus, one of the newest issues is cyber security. Cybersecurity has applications in many other domains, such as cyberspace, and is not just restricted to protecting data in the IT business. High security is necessary even for the newest technologies, such as cloud computing, mobile computing, e-commerce, net banking, etc. These technologies' security has become essential as they include some very valuable information about an individual (Anand R. et al., 2018) For the sake of both national security and economic prosperity, important information infrastructures must be safeguarded and cyber security must be improved. Developing innovative services and shaping public policy now depend heavily on making the Internet safer (and safeguarding its users). A more thorough and secure strategy is required in the battle against cybercrime. It is crucial that law enforcement agencies are permitted to properly investigate and punish cybercrime, since technological solutions by themselves are unable to prevent any crime. In order to stop the loss of some crucial data, several governments and countries nowadays are enforcing stringent rules on cyber security. To protect themselves from the growing number of cybercrimes, everyone needs to receive cybersecurity training (Reddy et al., 2014).

CYBER CRIME

Cybercrime is the term for any illegal behaviour where the primary means of committing a felony is a computer. The US Department of Justice has expanded the definition of cybercrime to include any unlawful behaviour that uses a computer to store evidence. Cybercrimes include crimes like network invasions and computer virus dissemination that can be carried out using computers. Additionally, they might be computer-based incarnations of crimes that already exist but have grown to be major hazards to both persons and nations, like coercion, identity theft, stalking, and bullying. Any illegal conduct involving the use of a computer and the internet to sell illicit items, steal identities, harass victims, or cause intentional disruption is generally referred to as cybercrime. Cybercrime is defined as illegal behaviour that targets or utilises a laptop, an electronic network, or a networked device. Hackers and cybercriminals looking to profit from their crimes make up the majority of criminal activity, though not all of it. People or organisations are tasked with breaching the law. Certain cybercriminals are very skilled in technology, have advanced tactics, and are well-organized. A few are novice cybercriminals. Cybercrime rarely targets computer systems for purposes other than monetary gain. These might be political or personal. Cybercrime that prevents users from accessing a computer or network or prevents a company from providing a particular service to its clients is known as a denial-of-service (DoS) attack. Using networks or computers to disseminate malware, unlawful data, or illicit photos is one example of cybercrime that uses computers to carry out other illegal actions. Sometimes, cybercriminals act rapidly to perpetrate any kind of crime. Initially, they will go after compromised computers. Use them to propagate malware to further machines or the network as a whole after that. Hackers can also use Distributed-Denial-of-Service (DDOS) attacks as a technique (Singh S.,2016) While this could seem similar to a denial-of-service assault, hackers use a range of hacked devices to stall it. Any time a laptop is used in combination with criminal action, it falls under the third category of lawbreaking recognised by the Department of Justice in North America. Using a laptop to store knowledge that you have acquired is one approach to accomplish this.

Cyber Security

Cyber Security involves safeguarding computers, servers, mobile devices, electronic systems, networks, and data against malicious intrusions, and it goes by various names like information technology security and electronic information security. This concept is applicable in diverse settings, spanning from corporate environments to mobile computing, and can be categorised in several ways. ensuring cybersecurity is crucial to safeguarding our digital assets, such as sensitive personal and financial data, intellectual property, and critical infrastructure. Cyberattacks can result in severe consequences, including financial harm, damage to one's reputation, and even physical danger (Kaur et al., 2021).

Cybersecurity is of paramount importance in every organisation, regardless of its size, as technology continues to proliferate and various sectors, including government, education, and healthcare, increasingly rely on digital data through wireless communication networks. the significance of cybersecurity lies in protecting the information of various organisations, such as email providers like Yahoo, which contain highly sensitive data that could harm both individuals and their reputations. Attackers target businesses, both small and large, to gain access to their critical documents and information (Shrivastava S. 2017).

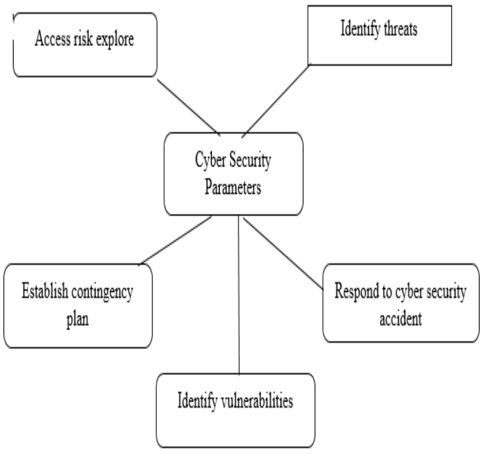
Access risk explore
Identify threats
Cyber Security Parameters
Establish contingency plan
Respond to cyber security accident
Identify vulnerabilities

Figure 1. Cyber security parameters

LITERATURE REVIEW

Reddy Nikita et al. (2014) Computer security is increasingly important due to the interconnected world and the increasing threat of cybercrime. The latest technologies and threats challenge organizations in securing their infrastructure and requiring new platforms and intelligence. While there is no perfect solution for cybercrimes, minimizing them is crucial for a safe future in cyberspace.

K. M Rajasekharaiah et al (2020) Modern life has led to increased technology use for shopping and financial transactions, making safeguarding knowledge increasingly difficult. The growth of social media has increased online crime and cybercrime. Data security plays a significant role in information technology, and cybercrime continues to expand. Governments and businesses take various steps to prevent cybercrime, and many people are concerned about it. This paper focuses on cyber security concerns related to new technology, ethics, and developments impacting cyber security.

Hakeem et al. (2020) This paper explores the challenges of integrating Information and Communication Technology (ICT) and cybercrime in mobile money transaction services in Tanzania. It highlights the increasing prevalence of cybercrimes in these services, highlighting the need for improved cybersecurity measures.

R. Chivukula, et al. (2021) The study provides an overview of cyber security, focusing on the concept of cyber space and its impact on organizations. It discusses the costs and impact of cyber security, the causes of security vulnerabilities, and the challenges of protecting against cybercrimes. It also discusses common cyber-attacks and their prevention methods, and presents a case study of Mirai's attack on high-profile victims, highlighting the importance of proper security measures.

Cybercrime can occur at any time and can have severe consequences.

Bhosle et al. (2021) Computer security is becoming increasingly important due to the interconnected nature of the world and the increasing threat of cybercrime. With the rise of new technologies and threats, organizations must adapt their infrastructure and use new platforms and intelligence to protect themselves. While no perfect solution exists, minimizing cybercrimes is crucial for a secure future in the cyber world.

Kaur, Jagpreet et al. (2021) Cybersecurity is the practice of preventing cyberattacks, data breaches, and security threats. It involves analyzing the challenges faced by organizations, mitigating attacks, and reducing risks. This article reviews existing security standards for encryption and decryption, discussing recent trends and challenges. Recent advancements include RSA, DES, and quantum cryptography, which use XOR and Qubits for security. Quantum computing and quantum mechanics are also being explored. The paper provides a comprehensive survey of cybersecurity, highlighting the challenges and advancements in the field, and suggests the development of polynomial-based encryption for future applications.

OBJECTIVES

The research aims to study on challenges faced by cyber security on the latest technologies as attacks driven by artificial intelligence, weaknesses in quantum computing, and problems with Internet of Things security.

Research questions

- What are the challenges faced by cyber security?
- How cybersecurity dealing with the latest technologies.

Challenges faced by Cyber Security while dealing with the latest technologies

1. Evolving Threat Landscape: Cyber threats are constantly changing and becoming more sophisticated. Attackers use new techniques, such as advanced malware, social engineering, and zero-day exploits, making it challenging for cybersecurity experts to anticipate and defend against these evolving threats.

2. Artificial Intelligence and Machine Learning: Cyber attackers increasingly use AI and ML to automate attacks and evade traditional security measures. Defending against AI-driven threats requires advanced AI and ML tools to detect and mitigate such attacks effectively.

3. Cloud Security: The shift to the cloud introduces new security challenges, including data breaches, misconfigured cloud settings, and insider threats. Organisations must ensure that their data and applications are properly secured within a multi-tenant environment.

4. Quantum Computing: While quantum computing holds the promise of more secure encryption, it also poses a threat to existing systems. Cybersecurity professionals must develop and implement quantum-resistant encryption methods to safeguard sensitive data.

5. Mobile Device Security: The proliferation of mobile devices and the use of mobile apps provide more opportunities for cybercriminals to exploit vulnerabilities. Mobile security involves protecting against malware, data breaches, and unauthorised access.

6. Internet of Things (IoT) Vulnerabilities: IoT devices often lack robust security features and are easy targets for attackers. Their sheer number and diverse range of use cases make it difficult to secure and monitor them effectively.

7. Insider Threats: Malicious insiders and negligent employees can pose significant security risks. Organisations need to implement strategies and technologies to detect and prevent insider threats and unauthorised access.

8. Supply Chain Attacks: Cybercriminals are increasingly targeting the supply chain to compromise software and hardware components. Ensuring the security and integrity of products and services throughout the supply chain is a complex task.

9. Regulatory Compliance: The constantly changing landscape of data protection and privacy regulations means that organisations must continuously adapt to ensure compliance. Violating these regulations can lead to significant financial penalties.

10. Security Skills Gap: The shortage of skilled cybersecurity professionals is an ongoing issue. Hiring and retaining talented individuals capable of addressing the latest threats is a constant challenge for organisations.

11. Zero-Day Vulnerabilities: Zero-day vulnerabilities are unknown to security experts until they are exploited in an attack. This makes it difficult to detect and mitigate these vulnerabilities before they are used to compromise systems.

12. Blockchain Security: While blockchain can enhance security in various applications, it is not immune to vulnerabilities. Issues like smart contract flaws and insecure wallets can lead to security breaches if not properly addressed.

13. Artificial Intelligence for Security: AI is used both by security professionals and attackers. Cyber adversaries can leverage AI to create more advanced and evasive attacks, necessitating the development of equally sophisticated AI-driven security solutions to defend against these threats.

Cyber Ethics

Cyber ethics are nothing more than the internet's code. When we implement these cyber ethics, there are intelligent opportunities for people to use the internet in a safe and appropriate manner. A few of them are shown in the area below:

- DO communicate and interact with others online. It's easy to stay in touch with friends and family, connect with co-workers at work, and share ideas and information with people across town or the other side of the globe thanks to email and instant messaging.
- Avoid being an online bully. Don't insult them, sully them, email them embarrassing pictures, or take any other action that could cause them harm.
- Since the internet is thought of as the world's largest library, it is imperative that you always obtain this material through appropriate and lawful channels.
- Avoid using other people's credentials to access their accounts.
- Never attempt to infect other people's systems with malware in order to corrupt them.
- Never give out your personal information to anyone because there's a good chance someone else will misuse it and you'll end up in a lot of trouble.
- When you're on the internet, never pretend to be someone else or attempt to create a false account on someone else because you could get into trouble for it as well.
- Always respect proprietary data and send games or videos as long as they're allowed. The above are a few cyber-ethics that one ought to adhere to when using the internet. We tend to apply the right rules in our lives from very young on, and the same is true in the online house.

CONCLUSION

The globe is being increasingly interconnected, and networks are being used to conduct vital activities, making cyber security a huge problem that is getting more important. The problem of security in today's information technology is crucial and extremely complex. Each person has a unique perspective on danger levels and security regulations. Establishing the security needs of the moment and use is crucial to designing a safe network. Every action involving the network can then be assessed in light of that policy once it has been established. Accordingly, information security depends heavily on security. With every new year that goes by, cybercrime and information security continue to take divergent turns. Organisations are facing challenges related to infrastructure security, including the need for new platforms and intelligence to keep up with the latest and most concerning technology, as well as the constantly emerging cyber tools and threats. The best way to reduce cybercrime in cyberspace is to employ modern tactics, but there is no perfect solution.

REFERANCES

1. Abraham, S. and Hickok, E. (2012), ―Government access to private-sector data in India‖, International Data Privacy Law, 2 (4): 302-315.
2. Acharya, B. (2013), “The National Cyber Security Policy: Not a Real Policy‖, ORF Cyber Monitor, 1 (1): 1-17.
3. Ahmad, et al. (2012), ―Perception on Cyber Terrorism: A Focus Group Discussion Approach‖, Journal of Information Security, 2012 (3): 231-237.
4. Anand, R et al. (2018), ―Transforming Information Security Governance in India (A SAP-LAP based case study of security, IT policy and egovernance)‖, Information & Computer Security, (26) 1: 58-90.
5. Bhosale, Karuna & Ambre, Siddhi & Valkova-Jarvis, Zlatka & Singh, Anamika & Nenova, Maria. (2023). Quantum Technology: Unleashing the Power and Shaping the Future of Cybersecurity. 1-4. 10.1109/Lighting59819.2023.10299447.
6. Gade, Nikhita Reddy & Reddy, Ugander. (2014). A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies.

7. International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012 1ISSN 2229-5518.

8. J. Li. The research and application of multi-firewall technology in enterprise network security. Int'l J. of Security and Its Applications, 9(5):153–162, 2015

9. Kaur, Jagpreet & Ramachandran, Ramkumar. (2021). The Recent Trends in CyberSecurity: A Review. Journal of King Saud University - Computer and Information Sciences. 34. 10.1016/j.jksuci.2021.01.018.

10. Kutub Thakur1, Meikang Qiu2∗, Keke Gai3, MdLiakat Ali4 An Investigation on Cyber Security Threats and Security Models 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing 978-1-4673-9300-3/15

11. Lee, H.; Lee, Y.; Lee, K.; Yim, K. Security Assessment on the Mouse Data using Mouse Loggers. In Proceedings of the International Conference on Broadband and Wireless Computing, Communication and Applications, Asan, Korea, 5–7 November 2016

12. Mellado, D.; Mouratidis, H.; Fernández-Medina, E. Secure Tropos Framework for Software Product Lines Requirements Engineering. Comput. Stand. Interfaces 2014, 36, 711–722

13. Mohsin, M.; Anwar, Z.; Zaman, F.; Al-Shaer, E. IoTChecker: A data-driven framework for security analytics of Internet of Things configurations. Comput.Secur. 2017, 70, 199–223

14. MdLiakat Ali Kutub Thakur Beatrice Atobatele Challenges of Cyber Security and the Emerging Trends BSCI'19, July 8, 2019, Auckland, New Zealand

15. Nikita TresaCyriacLipsaSadath Is Cyber Security Enough- A study on Big Data Security Breaches in Financial Institutions 2019 4th International Conference on Information Systems and Computer Networks (ISCON) GLA University, Mathura, UP, India. Nov 21-22, 2019

16. Pallangyo, Hakeem. (2020). Cyber Security Challenges, its Emerging Trends on Latest Information and Communication Technology and Cyber Crime in Mobile Money Transaction Services. Tanzania Journal of Engineering and Technology. 41. 10.52339/tjet.v41i2.792.

17. R. Chivukula, T. Jaya Lakshmi, L. Ranganadha Reddy Kandula and K. Alla, "A Study of Cyber Security Issues and Challenges," 2021 IEEE Bombay Section Signature Conference (IBSSC), Gwalior, India, 2021, pp. 1-5, doi: 10.1109/IBSSC53889.2021.9673270.

18. Rajasekharaiah, K. & Dule, Chhaya & Sudarshan, Dr. (2020). Cyber Security Challenges and its Emerging Trends on Latest Technologies. IOP Conference Series: Materials Science and Engineering. 981. 022062. 10.1088/1757-899X/981/2/022062.

19. Ravi Sharma Study of Latest Emerging Trends on Cyber Security and its challenges to Society .

20. Singh, P. (2011), ―Battle-Ready for the Fifth Dimension: Assessing India‗s CyberDefence Preparedness‖, Jindal Journal of International Affairs, 1 (1): 339-351.

21. Singh, S. (2016), ―Digital India –A Roadmap for Future India‖, International Journal in Commerce, IT & Social Sciences, 03 (06): 35-40.

22. Siwach, J. and Kumar, A (2015), Vision of Digital India: Dreams comes True, Journal of Economics and Finance (IOSR-JEF), 6 (4): 66-71.

23. Sliwinski, K. F. (2014), ―Moving beyond the European Union‗s weakness as a cybersecurity agent‖, Contemporary Security Policy, 35 (3): 468-486. Sreejith, S. (2012), ―Varying Faces of Cyber Terrorism in India‖, Global Research Analysis, 1 (5): 112-113.

24. Srivastava, S. (2017), ―Digital India-Major Initiatives and their Impact: A Critical Analysis‖, ELK Asia Pacific Journal of Marketing and Retail Management, 8 (3): 1- 11.

25. VeenooUpadhyay, SuryakantYadav Study of Cyber Security Challenges Its Emerging Trends: Current Technologies International Journal of Engineering Research and Management (IJERM) ISSN: 2349- 2058, Volume-05, Issue-07, July 2018

26. Yim, K. A new noise mingling approach to protect the authentication password. In Proceedings of the 2010 International Conference on Complex, Intelligent and Software Intensive Systems, Seoul, Korea, 30 June–2 July 2012

Corresponding Author

Aarjav Jain*

Class 11th, Student, Sanskriti The Gurukul