IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, November 2025
Impact Factor: 7.67

Threats and Problems in Cyber Security- Short Review

Dr. D. Shoba Rani[1], M. Maruthi Rao[2], PC Prakash[2]
Head, Department of Computer Science and Engineering[1]
PG Scholars, Department of CSE[2]
Chadalawada Ramanamma Engineering College (Autonomous), Tirupati.

Abstract: *The practice of protecting computers, networks, systems, and data from online threats is known as cybersecurity. Its objective is to reduce threats by utilizing technologies, procedures, and human behaviour to prevent illegal access, alteration, or destruction of information. Population in our earth is nearly 760 Crores and nearly 360 Crores are using the internet. Of late social media is big communication platform within the short period of time unprecedented profits and at the same time huge losses also. Come across cyber security social media platform is a right place hackers (Cyber Criminals).Sensitive data, business documents, protected characteristics created by original knowledge, private information, and different kinds of files that are protected by unauthorized access or familiarity might contain a significant amount of former documents.*

Keywords: Cyber security, hackers, social media, internet, protection.

I. INTRODUCTION

As cyber dangers and attacks are becoming more frequent, cyber security is the most important issue. Attackers are now targeting the systems with increasingly complex methods. Individuals, small enterprises, and major organizations are all affected. Therefore, all of these businesses—IT or non-IT—have recognized the significance of cyber security and are concentrating on implementing every strategy to counteract cyber threats."Digital security is mainly about people, methods, and technologies working collectively to encompass the full range of threat mitigation, weakness reduction, caution, international engagement, incident resolution, endurance, and rehabilitation policies and activities, including computer network operations, database validation, law supervision, etc."

II. MEANING OF CYBER SECURITY

Protecting digital devices, networks, and sensitive data from online dangers including malware, phishing, and hacking is known as cybersecurity. It includes a variety of tactics, tools, and best practices intended to prevent cyberattacks on computers, networks, and data.The practice of defending computer systems, networks, and data against online threats, harm, or illegal access is known as cyber security. It entails utilizing a variety of technologies, procedures, and best practices to protect data and guarantee the availability, confidentiality, and integrity of digital assets.

III. LITERATURE REVIEW

Maintaining the organization's technological policies and practices is crucial. However, an organization cannot evaluate the efficacy of a security program unless the policies and processes are tested. Threats and cyberattacks force top management to ensure that the network and systems are secure from hackers. The private data of the media's stories of a security breach that catches fire put clients at risk. One of the most important steps in proving the efficacy of an information security plan is infiltrating a business. The most popular models should be reliable representations of threats and should be used frequently to provide consistent results, even though a specific model isn't established at this point in the threat modelling process. The methodology's primary goal is to model threats according to the capabilities of the attacker. In addition to asset value and acquisition cost, an impact model is necessary so that the company can evaluate potential risks in multiple ways. As a result, you should consider the net intrinsic value of

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 4, November 2025 Impact Factor: 7.67

each item as well as the direct and indirect costs associated with your loss.This is an important step in the process that the company and the pen testers should take very seriously. Because it allows the pen tester to prioritize the company's assets, it provides a foundation for process, procedure, and control testing.

IV. COMMON CYBER SECURITY THREATS

- Ransomware (Computer virus)
- Mobile Technologies
- Internet of things
- Bots (Fake followers)
- Terrorist attacks
- Big data.

Normally users can do in one minutes 1 Lakh 49 thousand and 513 emails, 13 lakhs Fb post, 38 Lakhs Google search, 500 hours you tube videos, 2 Crores 90 lakhs What's up messages, 4 lakhs 48 thousands and 800 hundreds tweets can do. So it is very easy to target a person compare with company.

1. Ransomware: Malware that encrypts a victim's files and demands a ransom—typically in cryptocurrency—for the decryption key is known as ransomware. In addition to locking down data and rendering it unreadable, it may also pose a risk of information leakage. These attacks have the potential to seriously harm an organization's reputation, interfere with systems, and result in large financial losses.

2. Mobile Technologies: In cybersecurity, mobile computing refers to safeguarding data and devices in a mobile setting while addressing the particular threats presented by smartphones, tablets, and other portable devices. To stop data breaches, viruses, and other cyberattacks, this entails protecting apps, networks, and the operating system using techniques including encryption, secure coding, and user education.

3. Internet of things: In cybersecurity, IoT refers to the process of defending networks and internet-connected devices (such as wearables, sensors, and smart home appliances) against cyberattacks. In order to avoid data breaches and unauthorized access, it employs techniques including encryption, network segmentation, and secure upgrades in addition to tackling weaknesses like weak passwords and out-of-date software. IoT security is essential for protecting data and averting assaults due to the growing number of connected devices.

4. Bots (Fake followers) : In cybersecurity, "bots" (fake followers) are automated programs that imitate human behaviour on social media platforms for both positive and negative objectives, like disseminating false information, generating phony engagement, or carrying out automated security checks. Malicious bots are used for social engineering assaults, disseminating false information, and boosting a brand's or person's perceived popularity, but some bots are used for ethical hacking to identify weaknesses.

5. Terrorist attacks:"Cyberterrorism" is the use of cyberattacks for politically or ideologically motivated ends, aiming to cause severe disruption, fear, or physical damage. Many high-profile incidents are attributed to nation-states or large criminal groups, with terrorist attribution often a subject of debate. Initially masquerading as ransomware, this destructive malware attack primarily targeted Ukraine's critical infrastructure, including banks, ministries, and electricity firms. It quickly spread globally, causing over $10 billion in damages and impacting major multinational corporations like Maersk and FedEx. Due to its aim of destruction rather than financial gain, many experts classified it as an act of cyber warfare.

6. Big data: In cybersecurity, big data refers to the use of sizable, varied datasets to enhance threat detection, stop breaches, and automate incident response. Organizations may discover small anomalies, anticipate future threats, and react to incidents more swiftly and efficiently than with traditional security technologies by analysing vast amounts of data from several sources, including firewalls, intrusion detection systems, and user activity patterns.

V. METHODS FOR PREVENTING CYBER THREATS

- In social networking platform only limited information we can post.
- Don't make Friend ship in strangers

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, November 2025
Impact Factor: 7.67

- Online information is not trust
- Keep on changing privacy settings (want to change our requirements)
- Use secured network
- Antivirus software used
- In social media network use strong passwords often to change the pass words
- All social accounts have to set different pass words
- If it is possible face recognition, voice identification, finger recognition is better.

In social networking platform only limited information we can post.: In social network platform only limited information we can post that is all details are need not post this is first method to avoid cyber threat.

Don't make Friend ship in strangers: Don't make friend ship in strangers and un known persons (may be in hackers). Hackers may be target your passwords and personal information so necessary to avoid un known persons.

Online information is not trust: Huge volume of data is generated in daily so it is difficult to identify the fake one or original one. Not trusted every information.

Keep on changing privacy settings (want to change our requirements): One of the most important cybersecurity practices is to regularly evaluate and update your privacy settings. It helps prevent identity theft and other privacy violations, provides you control over your personal information, and reduces the possibility of unwanted access.

Use secured network: A key element of cybersecurity is using a secure network, which includes safeguards like firewalls, encryption, and VPNs to keep data and networks safe. This is accomplished by combining technology, regulations, and best practices that regulate access, filter traffic, and protect data availability, confidentiality, and integrity from cyberattacks and illegal access.

Antivirus software used: Used only antivirus and secured software to avoid cyber threat.

In social media network use strong passwords often to change the pass words: Cybersecurity requires the use of strong, one-of-a-kind passwords for social media. Although it was once advised to change passwords frequently, the current emphasis is on long, strong, and unique passwords rather than frequent changes

All social accounts have to set different pass words: If your password is strong, you won't need to change it as often, but you should still do it right once if a breach is discovered or made public.

If it is possible face recognition, voice identification, finger recognition is better:In cybersecurity, biometric techniques including voice recognition, fingerprint recognition, and facial recognition are frequently employed for multifactor authentication.

VI. CONCLUSION

Threats and problems in cyber security everyone is essential centered digital literacy:

- Creation, Innovation and research
- Technical Proficiency
- Teaching learning and self-development
- Communication, collaboration and Participation.

Technical protections and astute human practices—often referred to as "cyber hygiene"—combine to prevent cyberattacks. The best defence for people and organizations is a multi-layered structure.

VII. ACKNOWLEDGMENT

We thanks to, Dr. D. Shoba Rani, Professor, Head of the Department ,Computer Science and Engineering, CREC, Tirupati, for encouragement and support for the short review. The authors also thank to co staff they gave valuable suggestions and information.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, November 2025
Impact Factor: 7.67

REFERENCES

[1]. Taha, A.F.; et al.: Risk mitigation for dynamic state estimation against cyber attacks and unknown inputs. IEEE Trans. Smart Grid 9(2), 886–899 (2018)

[2]. Cyber Security Challenges In India Would Increase". Centre Of Excellence For Cyber Security Research And Development In India (CECSRDI). 18 November 2014

[3]. National Cyber Security Policy-2013". Department Of Electronics & Information Technology, Government Of India. 1 July 2013. Retrieved 21 November 2014.

[4]. Amid spying saga, India unveils cyber security policy". Times of India. INDIA. 3 July 2013

[5]. Puja Gupta and Rakesh Kumar, "Security Risk Management with Networked Information System: A Review"4 (2) IJEE193– 197 (2012).

[6]. VeenooUpadhyay, Dr.SuryakantYadav, "Study of Cyber Security Challenges Its Emerging Trends: Current Technologies"5 IJERM 2349-2058 (2018).

[7].]Sumanjit Das and TapaswiniNayak, "IMPACT OF CYBER CRIME: ISSUES AND CHALLENGES" 6 IJESET 142-153 (2013).

[8]. https://alpinesecurity.com/blog(Visited on 18th April, 2020)

[9]. https://www.cisomag.com/india-cybersecurity-policy/(Visited on 21st April, 2020)

[10]. https://cybercrime.org.za/definition(Visited on 24th April, 2020).

[11]. AtulArunPatil Research Paper on Cyber Security Challenges and Threats Volume 4, Issue 1, January 2024.

[12]. Computer Security Practices in Non Profit Organisations–A NetAction Report by Audrey Krause.