International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 03 | March - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

Review on: Cyber Security Threats and Protection Methods.

R. Sharuk[1], C. Giri[2], N. Srinivasan[3] ,S. Jai Akash[4] ,Dr. M. Varsha.[5]
[1,2,3,4] *Bsc. IT , Final year, Dept.of Information Technology, Nehru Arts & Science of College, Coimbatore, Tamilnadu, India*
[5]*Associate Professor,*

Dept.of Information Technology, Nehru Arts & Science of College, Coimbatore, Tamilnadu, India

---

Abstract
The extensive growth of computers, mobile devices, cloud platforms, and internet-based services has transformed the way individuals and organizations operate. Services such as online banking, digital education, e-commerce, healthcare systems, and government services heavily rely on secure digital infrastructures. However, this increased dependency has also resulted in a rapid rise in cyber security threats. Cyber-attacks can cause severe consequences, including data breaches, financial losses, privacy violations, system downtime, and loss of organizational reputation. This review paper presents a

comprehensive overview of major cyber security threats and commonly used protection methods. The purpose of this study is to review existing cyber security mechanisms, discuss their effectiveness, and highlight the importance of adopting strong security practices to safeguard digital information systems.

Keywords— Cyber Security, Cyber Threats, Network Security, Malware, Data Protection, Internet Safety

I. Introduction

In the modern digital era, the internet and information technology have become integral parts of daily life. Individuals use digital devices for communication, social networking, online shopping, education, and entertainment, while organizations depend on digital systems for data storage, financial transactions, and business operations. Although technological advancements offer efficiency and convenience, they also introduce new security challenges.

Cyber security focuses on protecting computer systems, networks, and data from unauthorized access, attacks, and damage. Cyber-attacks are increasing rapidly due to factors such as weak passwords, outdated software, lack of security awareness, and system vulnerabilities. Attackers continuously develop new techniques to exploit security loopholes. Therefore, understanding cyber security threats and protection methods is essential. This review paper surveys common cyber threats and reviews existing protection techniques used to reduce cyber risks.

II. Literature Review

Several researchers have studied cyber security threats and protection mechanisms due to the rapid increase in cyber-attacks. Stallings [1] discussed fundamental network security principles and emphasized the importance of encryption and secure communication protocols. Behl and Behl [2] highlighted the growing impact of cyber warfare and the need for strong national and organizational cyber defense strategies.

Garfinkel [3] explained basic computer security concepts and focused on common threats such as malware and phishing, stressing the role of user awareness in preventing attacks. Recent studies published in IJSREM Security & Privacy have reviewed advanced threats including ransomware, distributed denial-of-service attacks, and insider threats, and proposed layered security approaches to mitigate these risks [4].

Several researchers have also emphasized the importance of intrusion detection systems, firewalls, and authentication mechanisms as effective protection techniques. With the emergence of cloud computing and IoT technologies, recent literature suggests adopting advanced security models such as zero-trust architecture and artificial intelligence-based threat detection. Overall, existing literature shows that cyber security requires a combination of technical solutions, policies, and user awareness.

III. Overview of Cyber Security Threats

Cyber security threats refer to malicious actions that aim to compromise the confidentiality, integrity, or availability of information systems. These threats target both individuals and organizations and may result in severe damage. Cyber threats are not limited to technical attacks; many involve social engineering techniques that exploit human behavior.

The growing use of cloud computing, Internet of Things (IoT) devices, and mobile applications has expanded the attack surface. As systems become more interconnected, attackers gain more opportunities to exploit vulnerabilities. Reviewing different types of cyber threats helps in understanding attack patterns and improving defense strategies.

IV. Types of Cyber Security Threats

A. Malware Attacks

Malware is one of the most common and dangerous cyber threats. It refers to malicious software designed to disrupt system operations, steal sensitive data, or gain unauthorized access. Malware includes viruses, worms, Trojans, spyware, adware, and ransomware. These programs can enter systems through infected email attachments, malicious downloads, or compromised websites.

Ransomware attacks encrypt user data and demand payment to restore access. Such attacks have caused major disruptions in healthcare, education, and business sectors. Malware continues to evolve, making detection and prevention more challenging.

B. Phishing and Social Engineering Attacks

Phishing attacks attempt to deceive users into revealing confidential information such as passwords, credit card details, or personal data. Attackers use fake emails, messages, or websites that appear legitimate. Social engineering attacks exploit human trust rather than technical vulnerabilities.

Phishing is highly effective because many users lack awareness of cyber threats. Even well-secured systems can be compromised if users unknowingly provide sensitive information.

C. Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks

DoS and DDoS attacks aim to make systems or services unavailable to legitimate users by overwhelming them with excessive traffic. In DDoS attacks, multiple compromised systems are used to launch the attack simultaneously.

These attacks can cause service outages, financial losses, and customer dissatisfaction. Online services, websites, and cloud platforms are common targets of DDoS attacks.

D. Insider Threats

Insider threats originate from individuals within an organization who have authorized access to systems. These threats may occur intentionally or accidentally. Employees may misuse access privileges or unintentionally expose data due to negligence.

V. Impact of Cyber Attacks

Cyber-attacks can have severe impacts on individuals, organizations, and society. Financial losses are one of the most common consequences, resulting from fraud, ransom payments, and system recovery costs. Data breaches expose sensitive personal and organizational information, leading to privacy violations and legal penalties.

Reputation damage is another major impact, as users may lose trust in organizations that fail to protect their data. In critical sectors such as healthcare, transportation, and government services, cyber-attacks can disrupt essential operations and pose risks to public safety.

VI. Cyber Security Protection Methods

A. Network Security Techniques

Network security plays a vital role in protecting data during transmission. Firewalls act as barriers between trusted and untrusted networks, controlling traffic based on predefined security rules. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) monitor network activities to detect and prevent suspicious behavior.

Regular network monitoring, secure configurations, and timely updates help reduce network-based attacks.

B. Data Protection and Encryption

Encryption is a fundamental technique for protecting sensitive data. It converts readable information into an unreadable format, ensuring confidentiality. Encryption is widely used for securing data storage, email communication, and online transactions.

Data backup and recovery mechanisms are also important for minimizing data loss during cyber incidents.

C. Authentication and Access Control

Authentication mechanisms ensure that only authorized users can access systems. Techniques such as strong passwords, multi-factor authentication (MFA), and biometric verification improve security. Access control policies limit user privileges and reduce the risk of insider threats.

D. Security Software and Updates

Antivirus and anti-malware software detect and remove malicious programs. Regular software updates and patch management help fix security vulnerabilities and prevent exploitation by attackers.

VII. Role of User Awareness and Training

Human errors are one of the leading causes of cyber security incidents. Users often fall victim to phishing attacks due to lack of awareness. Cyber security awareness programs educate users about safe online practices, recognizing suspicious activities, and following security guidelines. Regular training significantly reduces security risks and strengthens organizational security posture.

VIII. Challenges in Cyber Security

Cyber security faces several challenges, including rapidly evolving attack techniques, increasing system complexity, shortage of skilled security professionals, and lack of standard security policies. Emerging technologies such as cloud computing, IoT, and artificial intelligence introduce new vulnerabilities that require advanced security solutions.

IX. Future Trends in Cyber Security

Future cyber security systems are expected to rely on artificial intelligence and machine learning for real-time threat detection and response. Zero-trust security models, automation, and advanced encryption techniques will play a crucial role in strengthening cyber defenses.

X. Conclusion

Cyber security is a continuous and essential process in the digital environment. As cyber threats become more advanced, organizations and individuals must adopt strong security measures and best practices. This review paper discusses major cyber security threats and reviewed commonly used protection methods. A multi-layered security approach combined with user awareness can significantly reduce cyber risks and ensure the protection of digital assets.

References

[1] W. Stallings, Network Security Essentials: Applications and Standards, 6th ed., Pearson Education, 2019.

[2] N. Behl and K. Behl, Cybersecurity and Cyberwar: What Everyone Needs to Know, Oxford University Press, 2017.

[3] S. Garfinkel, Computer Security Basics, 2nd ed., O'Reilly Media, 2020.

[4] S. Abdillah, Z. Shukur, M. Mohd, and T. M. Z. Murah, "Phishing classification techniques: A systematic literature review," IEEE Access, vol. 10, pp. 41574–41591, 2022.

[5] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent developments," Energy Reports, vol. 7, pp. 8176–8186, 2021.

[6] A. I. Tahirkheli et al., "A survey on modern cloud computing security: Threats, vulnerabilities, and countermeasures," Electronics, vol. 10, no. 15, pp. 1–22, 2021.

[7] R. Fathima and S. Arumugam, "A review on cyber security and emerging cyber threats," Advances in Technology Innovation, vol. 6, no. 1, pp. 15–28, 2021.

[8] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," Future Generation Computer Systems, vol. 78, pp. 544–546, 2018.

[9] J. Singh, J. Pasquier, J. Bacon, H. Ko, and D. Eyers, "Twenty security considerations for cloud-supported Internet of Things," IEEE Internet of Things Journal, vol. 3, no. 3, pp. 269–284, 2016.

[10] IEEE Security & Privacy Magazine, "Cyber security threats and defense mechanisms," IEEE Publications, 2023.