Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 3, Issue 6, 2025

A COMPREHENSIVE STUDY ON CYBER SECURITY THREATS AND PREVENTION MECHANISMS

Mariam Nayab[*1], Waqar Ahmad[2], Abdullah Jahlil[3], Jawaid Iqbal[4]

[*1,2,3] *Master in Computer Science, Riphah International University, Islamabad*
[4] *Assistant Professor, Department of Cyber Security, Riphah International University Islamabad*

[*1]khanmaryam8584@gmail.com, [2] waqar.ahmad9960@gmail.com , [3]qaziabdullahjalil@gmail.com, [4]jawaid.iqbal@riphah.edu.pk

DOI: https://doi.org/10.5281/zenodo.15607728

Keywords
Cyber-Security, vulnerabilities, Security Threats, Internet Security, Standards Emerging and articles

Article History
Received on 29 April 2025
Accepted on 29 May 2025
Published on 06 June 2025

Corresponding Author: *
Mariam Nayab

Abstract
This article expresses emerging security threats and how we use different techniques to prevent them. As matter-of-fact previous research study shows just how to apply these security methods with different solutions but not provide future solutions as much as we need it in current time situation some of them explain universal security standards. This article contains future directions with emerging universal standards for cloud environment. The aim of writing this paper is to clarify the standards which help to protect from different threats like system data breaches, unauthorized access etc. cyber security is one of the leading process which help provide data and information protection and make sure to refrain from internet threats cyber bullying and online harassments. To control any type of internet security threats and vulnerabilities cyber security widely uses protraction measurements of every individual. Cyber securities reduce risk level based on different type's situations like IOT weaknesses, IAM (Identify and access Management) and lie BYOD (Bring your own Device). In this study we purposing prevention techniques and also giving solution for prevention of common security threats.

INTRODUCTION

Cyber security threats are malicious acts targeting computer systems, networks, and data, aiming to cause damage, steal information, or disrupt operations. This defines that cyber security and its core objectives like protecting data, preventing attacks, and ensuring data integrity. Different challenges measures are undertaken to prevent online threats this study show the phenomenological approach to solve these critical issues [{Amoo, 2024 [1]}. The cyber security threats increasing vulnerabilities in different area of networking and trying to breech in cloud networking as well the increasing reliance on the internet in daily activities e.g. in(E-commerce ,social activities).Its highlights the need of strong security protection against increasing threats to our sensitive data or devices like phishing, deep fakes etc.[{Shabbir, 2025 [2]}.Cyber security threats define that malicious action taken by the evil minds that they try spoofing on personal and confidential data ,upsetting damaging and causing chaos in cyberspace as well. They consistently stay ahead of the curve which makes it harder for the people .Cyber security refers to the proactive measure done to protect the vast domain of cyber space which includes data software and information from all possible threats [{Rajendran, 2023 [3]}.Cyber security as the practice and measures employed to prevent unauthorized

access, attacks or damage to digital systems and data .Now a days it become chaos for the world How to apply different strategies to overcome the emerging cyber security threats. It emphasizes that growing dependence on digital technologies has made it progressively vulnerable to cyber-attacks [{Yadav, 2020 [4]}.This highlight that the significant opportunities and advancements come with the digital age but there are also more cyber security risks for people, business. An overview of the paper underlines the importance of comprehensive cyber threat to develop effective prevention and mitigation strategies [{Sleem, 2022[5]} . The introduction sets the stages by highlighting the increasing reliance of the digital technologies and the corresponding effective preventions and mitigations. It also presents the structure of the paper which includes methodology, result discussion, challenges and treatments. The next study shows that privacy and integrity of reporting system mechanisms are increasingly critical specifically in environment where trust and believing are non - existent due to data breeches{Far, 2024 [8]}.

2: Literarture Review:

It examines the qualitative exploratory for the understanding of emerging threats related challenges. Cyber security threats are now gradually different, sophisticated, and disorderly across all domains ranging from regional to industrial systems. This study shows that the growing reliance of digital infrastructure, cloud services, and IoT devices significantly expanded the attack surface for cybercriminals. Common threats include malware, ransom ware, phishing, SQL injection, DDoS attacks, insider threats, and many more [2]. These threats target both organizational assets and individual data, causing financial losses, service disruption, reputational damage, and even national security implications [3]. one intermittent image is the persistence of old-fashioned legal framework and lose enforcement as emerging technologies for real time threat detection ,behavioural analysis and anomaly recognition despite the availability of advanced technologies ,the literature main pressure that cyber security strategies remain under-implemented due to limited resource data and implied poor integration and disconnected cyber governance[4].All the methods provide deep knowledge and theory related to security protection which are not enough to apply provided techniques which are not fully protected and lack in security that whys multi-level approaches that are recommended to make system adaptable and holistic can combined technical redolence and development through coordination and with international approaches . As we all know about that cyber security has become critical concern that needs the attention of organization to confidentially ensure the protection and security of information system [5]. Following paper mentioned comprehensive overview of cyber security and also describe key element like challenges and opportunities it also intended to connect with occurrence of cyber security in block chain and internet of things (IOT).Cyber security plays a critical role in different virtual system [{Admass, 2024[6]}. This paper provides a robust framework for securing data from social threats but enhance the need for continuous innovations in authentication methods. It defines different exposure and provides related solutions through proposed scheme “BrightPaas” version such of “Randomized and Dynamic Brightness threshold” [{Thotadi, 2024 [7]}.

The next paper defines cloud –computing cyber threats through layered architecture by comprising of “ IAAS,PAAS,and SAAS” that provide unique and understanding security challenges and its protecting result. Collectively theoretical described that threats are countermeasure and framework into layered domains, physical network applications user level examining real-life attack and offering under fire countermeasures, it contributes to the development of more secure cloud computing environments. Cybercrimes that are drastically increased with time which wide spread spectrum of potent criminals in any domains due to lack of protection measures and systematics approaches and resources which adhered security gaps and vulnerabilities{Shombot, 2024 [9]}.

3: Common cyber security attacks:

Following are described sources of attacks that are responsible for system vulnerabilities.

Illegal Breech of Data: It's often engage in cybercrime for financial gain using techniques like phishing, malware and ransom ware.

Unauthorized Person: Individual or groups who my compromise system and data for personal gain or malicious intent.

Hacking Activists: individual or groups who use cyber-attacks to promote political, social or environmental agendas.

Organizational Threats: Employees or individuals with authorized access who may intentionally or UN –intentionally compromise security.

Business related threats: Business rivals who may attempt to steal confidential information or disrupt services.

Nation-wide threats: Governments that may use cyber-attacks for espionage or to disrupt the activities of the other nation.

Illegal Activities: May use cyber-attacks to steal information, disrupt operations or spread fear.
Broken Data: Collect and sell user data without explicit consent, often through underground workplaces.

4: Common Threats:
Malware: This encompasses various malicious software lie viruses, worms, Trojans, spyware and adware. It can be used to gain unauthorized access, steal data or cause damage to systems.

Phishing: This involves attackers using fake emails or websites to trick users into revealing sensitive information like passwords or credit card details.

Ransom ware: This type of malware encrypts a victim's files and demands ransom payment for their release.

Social Engineering: This involves manipulating individuals into revealing confidential information or performing actions that compromise security.

DOS/DDOS (Denial of Service/Distributed Denial of service): These types of attacks flood system traffic, marketing them and unavailable to legitimate user.

Insiders Traffics: These types of threats come from the individual from inside of organization who misuses their privileges to access the damage system and the data.

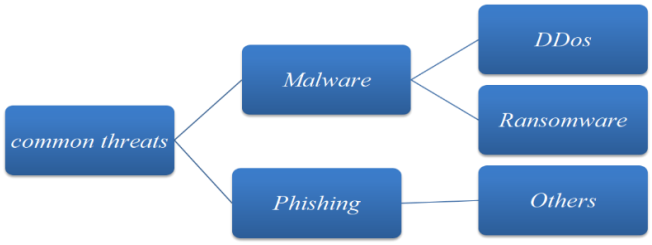
SQL-Injection: These types of attacks exploit vulnerabilities on web applications to gain unauthorized access to the database.

Men in the Middle: This attacks intercept communication between two parties allowing the attacker to eavesdrop on modifies data.

Supply Chain Attacks: In this attacker target an organization's supplier or vendors, potential compromising their systems and organization's data.

Password Attackers: These attacks involve trying to guess or crack password to gain unauthorized access to accounts.

Fgure 1: Conceptual Diagram of Common Threats



5: Different Prevention Techniques Are Suggested As Follows:

5.1: Prevention For Core Security:

The prescribed techniques are fire wall and Intrusion Prevention System (Ips) are mostly widely used because these techniques help to reduce the threats that might occur due network traffic or web application traffic using firewall can help to filter information and data flow as well as like fire wall IPS is also used to protect and monitor the system after threats which mostly occur through network traffic this technique alert system through real time detection.

5.2: Prevention through Advanced Detection and Automation:

By using Advanced Machine learning techniques like real time detection system it helps to detect anomlies and it also used different antivirus for different situations. Ai and behavioral analysis help to in learning process on different criteria to detect performance , behaviour and reactions based on analysis it define what actual need or system to handle any threating situations.

5.3: Prevention Techniques for Authentication & Role Based Access Control:

As name suggested it important to first check the detail related to user who wants an access to system data's it is possible if we use and keep our focus or authorization which help us to decide whom to give access of confidential information and prevent threats. Role Based Access control is basically restrict user to use only resource of the system for necessary of their role that how it used for restriction of system and allowing using the system only authorized and authentic person who have permission. Multi factor authentication is one of the best examples for approval of authority.

5.4: Prevention Techniques for Data security:

Encryption is the best approach to protect our system from fall and prevent malicious errors the new emerging concept of hashing and signature help to protect at high level rate because encryption convert data information into code and hashing process generate unique values in each time process.

5: Prevention of Threats At Network Level Defence:

Segmentation is one of the emerging techniques that help to increase data security from threats in cyber warfare the reason is that it make our personal information small units that helps system to remain safe from attacks if one unit is cracked by attackers it make no such huge impact on whole system just like that Secure DNS and Anti Spoofing also help and make protection walls against illegal acts and threats.

5.6: Prevention Through User Understanding and Process Control:

By teaching Security Protection Ethics to make secure the user information from phishing , social engineering and other online attacks because essential that humans make errors and create more complexities and top level breeches. Patch management concept is also applied in this process to remove vulnerabilities and make system high performance through regular updates.

5.7:Prevention Through Specialized Techniques:

Block chain and Federated Specialized learning process make secure data sharing transferring with temper proof logging and helpful as it is decentralized and audit trail system process and for specialized the modern Ai machines are get trained to all types of domain processes and also provide data privacy to each individual.

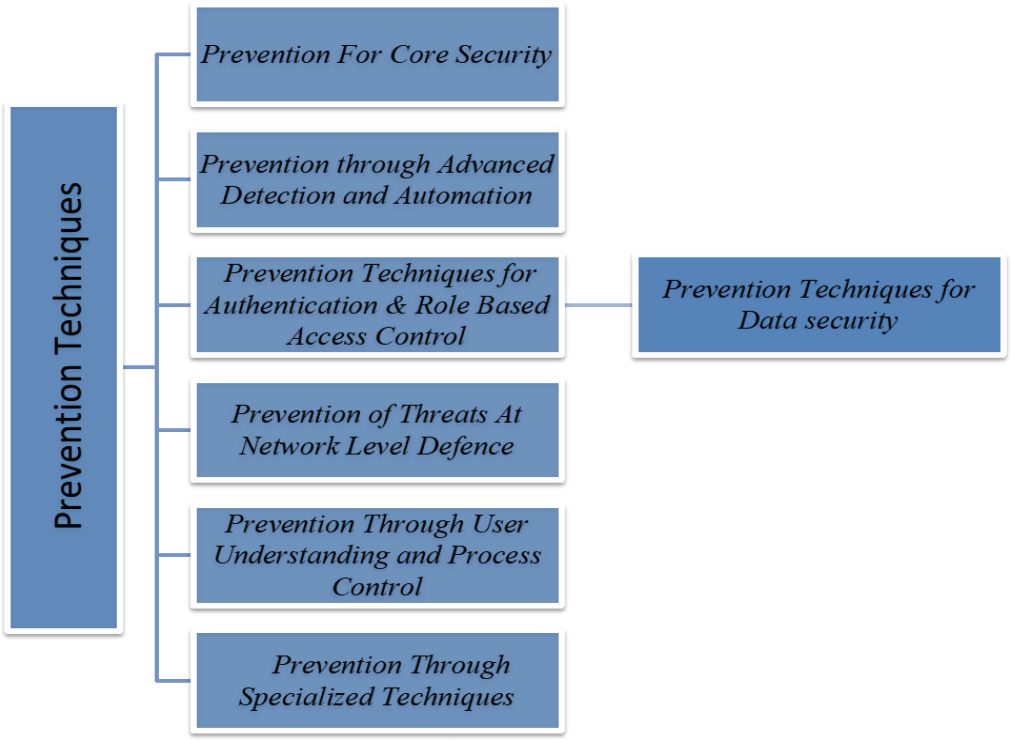


Figure 2: Conceptual Diagram of Prevention Techniques

6: Final Thoughts: These preventions might not be grateful and efficient for all networks and system due to lack of these preventions in latest attacks innovations like evolving threats that are timely being changed .Attackers always try to use new tactics like Ai phishing ,deep fake identity fraud ,zero –day exploits, Advanced Persistent threats. Prevention techniques much lack when the human factor, insider threats misconfigurations and lack of regulation and standardization.

Risk reduces when the layered, evolving and people centred approach make system reliable and efficient. digital or virtual platforms enhance security measures at high level that help to identify security standards that involved in transforming critical tools for organizations that may be risky for them{Taherdoost, 2022 [11]}.

8.Methodology of Cyber Security Threats and its Preventions:

By studying all the existing work we discover that "IDS "also known as Intrusion Detection System" and network monitoring remains embedded and initial to all modern system and recent survey shows that modern IDS blend machine is now learning optimization and feature engineering techniques (e.g. explainable-Ai, Genetic Algorithms)etc. To enhance and raise the detection quality and ratio effectively. As this article provide different solutions for protecting digital twins by applying measures (e.g. Robust system for zero trust architectures to enhance reliability, IDs for removing inconsistencies , blockchain for inflexible logs for digital logs){Alhumam, 2025 [12]} Researchers even explore block-chain and quantum enthused methods to protect and make secure IDS data in decentralized IOT/Cloud infrastructure setting. Key factors involves real time anomly detection, evasion and imbalanced training data, that's why lightweight adaption of IDS framework for dynamic heterogeneous environment. Decentralized data techniques (e.g. block-chain based identity) are emerging to source credential and logs design increasingly follows zero trust and defence In depth principles (Depth –Of-Depth) continuously validating user and devices behaviour. AI enabled platforms privacy and transparency an emphasized

ML and DL (Machine learning and Deep learning) not only to IDS but also malware. It measure Classification, behavioural, user-proofing and automated threats intelligence. As followed theories of existing paper explain in pandemic(Covid-19) that the digital space of the internet breakdown because online crimes increases in timely manner and transferred information from physical to as well to digital rising technologies such as cloud computing, IoT, social media and other wireless communications that are risking in digital space and it might be concerning for future as well as integrated systems.{Aslan, 2023 [10]}

Key Principles: following are given below:

- Light Weight Adaptive Models.
- Multi- level/layers Defence.
- Behavioural and anomly Collaborations
- Standards and Threats Framework

7.EVALUATION AND BENCH-MARK:

To ensure for validation these methods studies applied often on public datasets and somehow these are simulated test-beds. SID (standard intrusion Datasets) are (e.g. NSL - KDD, CIC-IDS2017, UNSW-NB15) are widely used to bench-mark anomly detectors. Researcher combines ml and multi-layer control defence against evolving threats. The proposed scheme are based augmented of AI with Help of NLP for traditional security methods making them more adaptive, anticipated and intelligent based on real time analysis with the help of (SIEM) security event management that generate detections and alerts without people communication.{Naik, 2022 [15]}.

9.Result of Preventing Cyber Security Threats:

The Combined result from all previous studies shows that cyber threats order avoidance activities based on their effectiveness for multiple instances such as Multi –Factor Authentication and Passwords are extremely effective toward its implementations and proximately with minimum price. It defines how generative AI and LLMS moving for cyber security for security concerns by developing responsive threat detectors ,phishing replication and sensor based detections for making system forceful and threat free Awareness and training is reasonably{Ferrag, 2025[13] }, but on other side AI-Driven detection systems and national policy reform often high security but needs more time, planning and resources to deploy furthermore. And lastly the major point is “E bright paas” mode uses different techniques which user-friendly and highly authenticated process by having GUI system for future implementations in mobile applications through balances security measures and prevention with convenience. The increasing chaos in IoT emerge to reduce critical difference that lack and low in standardization process it make major impact on system devices to prevent them researcher provide rapidly expansion between interconnected of IoT. Complex ecosystem and broader attacks to diverse it{Tariq, 2023[14]}.

10.Comperative Analysis of Reviewed Paper On Cyber Security Approaches:

Approaches that are sugguested to prevent threats	IRJET Paper (2023)	Pakistan Cyber-security Study paper (2025)	E-Bright-Pass (2024)
Password Security	Recommend strong, dynamic passwords	Basic awareness emphasized	Graphical + dynamic PINs with decoys
Security Education & Awareness	Advocated for users and staff	Major research focus (cultural weakness)	Usability study suggested to reinforce use
Legislation & Policy	Not central	Strongly advocated; key national priority	Not discussed
Technology Based Defences	Firewalls, IDS, anti-malware	Lacking in public institutions	Custom app-level security model
Automation	Suggested for future research	Suggested but underdeveloped in Pakistan	Not applied yet

(2FA)	Mentioned	Not implemented widely	Enhanced form via graphical password
User-Centric Usability	Less emphasized	Awareness needed, no systems deployed	High emphasis: balance between security and convenience

11.Future Directions: For protecting our systems and digital data from cyber crimes and data breeching it is important to make a relaible system that is based on real time detection to prevent any type of threats. The Proposed Theme is "Human sensory detector approach" that can detect human errors or what type of Information he /she trying to get and in what way it is help ful and usefull without hurting anyone. A trained Model like "NLP" or SIEM with integrated security of "RSA andECC"that are tarined in way where they help for user to protect their data and information and also get protected by cyberbullying because this may help to make our system effective and also increase security level. These Ai models just need to be trained in such a way where they only react on critical situation for cyber secruity without misusing of users sensitive information for (greedy traing) . The Proposed scheme base on the idea of using " HYPER-SELTNITM (HYBRID SECURITY ENCRYPTION LAYERED TECHNIQUE using NLP based INTELLIGENCE TRAING MODEl") where this syetem provide not only highly level security but also protect users sensitive data also prevent threats with reliable solutionss in critical stituations.

12.Conclusion:

As whole discussion of this paper defines that cyber security threats are increasingly, diverse and pervasive in the digital age, affecting individuals, organization and entire nations. From definitive attacks like malware, phishing, and DDoS to modern challenges such as deep fakes Ai generated exploit and insider threats the evolving threat and adaption. The reviewed literature and research paper eventually describe how combating cyber-security threats is not one time effort but an going process of different domain in society cross sector partnership the threat intelligence. To endure defensive events alongside probable security threats, academics and experts mention a mixture of practical, structural, and human-centric methods with multi-layered tactics. An overview of this paper conclude that cyber security emphasize that our systems must be safe and protected from threats and from other effective factors .It is also known as information technology security and E information. It is not one time effort for combating cyber threats.

Refernces:

1. Amoo, O. O., et al. (2024). "Cyber security threats in the age of IoT: A review of protective measures." International Journal of Science and Research Archive 11(1): 1304–1310.
2. Shabbir, N. and M. Adnan (2025). "Cyber Security: A Growing Challenge to Pakistan." Annals of Human and Social Sciences 6(1): 372–384.
3. Rajendran, R. M. and B. Vyas (2023). "Cyber - security threat and its prevention through artificial intelligence technology." International -Journal for Multidisciplinary Research" 5 (6).
4. Yadav, V. (2020). "A Study of Threats, Detection and Prevention in Cybersecurity." International Research Journal of Engineering and Technology (IRJET), May: 1150–1153.
5. Sleem, A. (2022). "A Comprehensive Study of Cybersecurity Threats and Countermeasures: Strategies for Mitigating Risks in the Digital Age." Journal of Cybersecurity & Information Management 10(2).
6. Admass, W. S., et al. (2024). "Cyber security: State of the art, challenges and future directions." Cyber Security and Applications 2: 1000
7. Thotadi, C., et al. (2024). "E-Brightpass: A Secure way to access social networks on smartphones." Cyber Security and Applications 2: 100021.
8. Far, S. B. and M. R. Asaar (2024). "A blockchain-based anonymous reporting system with no central authority: Architecture and protocol." Cyber Security and Applications 2: 100032.

9. Shombot, E. S., et al. (2024). "An application for predicting phishing attacks: A case of implementing a support vector machine learning model." Cyber Security and Applications 2: 100036.
10. Aslan, Ö. et al. (2023). "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions", Electronics 12(6): 1333.
11. Taherdoost, H. (2022). "Understanding cyber-security, frameworks and information security standards—a review and comprehensive overview." Electronics 11(14): 2181.
12. Alhumam, N., et al. (2025). "A Comprehensive Review on Cybersecurity of Digital Twins Issues, Challenges, and Future Research Directions." IEEE Access.
13. Ferrag, M. A., et al. (2025). "Generative AI in Cybersecurity: A Comprehensive Review of LLM Applications and Vulnerabilities." Internet of Things and Cyber-Physical Systems.
14. Tariq, U., et al. (2023). "A critical cyber security analysis and future research directions for the internet of things: A comprehensive review." Sensors 23(8): 4117.
15. Naik, B., et al. (2022). "The impacts of artificial intelligence techniques in augmentation of cyber security: a comprehensive review." Complex & Intelligent Systems 8(2): 1763–1780.