International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 12 Issue: 12 | Dec 2025 www.irjet.net p-ISSN: 2395-0072

A Review on Cyber security Threats and Their Prevention Mechanisms

Trapti Agrawal[1], Pawan Yadav[2]

[1,] *Department of Computer Science and Engineering, Eshan College of Engineering, Mathura, India,*
[2,] *Department of Computer Science and Engineering, Eshan College of Engineering, Mathura, India,*

Abstract- *Cyber security has become a pivotal concern in the modern digital landscape, as cyber threats continue to escalate in frequency, complexity, and impact across various sectors. This review, titled "A Review on Cyber security Threats and Their Prevention Mechanisms," provides a comprehensive synthesis of the latest developments in the domain of cyber threat analysis and mitigation strategies. Drawing upon 50 scholarly and technical references, the paper explores the classification of threat vectors such as malware, phishing, ran so ware, DDoS, insider threats, and IoT vulnerabilities. Sector-specific impacts are also analysed, with a focus on finance, healthcare, government, and critical infrastructure.*

The review then evaluates existing prevention frameworks, covering technical controls (e.g., MFA, IDS, firewalls), administrative measures (e.g., security audits, awareness training), and legal-policy frameworks. Particular attention is given to the emerging role of AI, machine learning (ML), and blocks chain in enhancing real-time detection, predictive defence, and decentralized integrity verification. While the literature reflects significant progress, key gaps remain in proactive threat intelligence, multi-sectorial integration, and human-centric vulnerabilities.

By critically analysing threat patterns and corresponding responses, this paper identifies major limitations of current approaches and proposes future directions for developing holistic, adaptive, and scalable cyber security solutions. The review contributes to both academic discourse and practical policy development by mapping actionable insights across technological, organizational, and behavioural dimensions.

Keywords: Threat Taxonomy, Cyber Risk Prevention, Emerging Security Technologies, Sectoral Vulnerability Mapping, Adaptive Defence Strategies

1. Introduction

As the age of ultra-dominant digitalization sets in, cyber security has become a stone of touchstone of international technology systems. With the proliferation of internet connected devices, cloud computing and digitized services, the amount of data that has been generated and sent back and forth has seen unprecedented level of growth. As a result, the threat areas of malicious users have grown tremendously, thus creating critical threats to citizens, organizations, and governments as well as those of operationally critical infrastructures [1], [3], [7]. Not only are these cyber threats evolving to be more complex but also longer lingering, and economically harmful. It has been seen that, according to recent research, there has been an increasing number of organizations around the world that are vulnerable to the advanced persistent threats (APTs), zero-day exploits, phishing attacks, ransom ware, and malware campaigns [2], [4], [10].

This multifaceted nature of such threats has forced the adoption of new and dynamic cyber security solutions, as opposed to older forms of defines. Static firewalls and active high-quality software which were earlier believed as adequate are not able to deal with dynamic and multi-layered attack strategies [5], [6], [13]. The rising number of attacks on supply chains like the one experienced with Solar Winds and IoT-Based weaknesses demonstrates the necessity to develop more comprehensive and resilient security systems [8], [9], [15]. Moreover, human factors like inside threat and the absence of training in cyber security are also important sources of system compromise, which shows the socio technical aspect of cyber security challenges [17], [21], [23].

There are sector-specific threats as well that require special prevention plans. As an example, healthcare organizations with their need of continuous access to data about their patients are vulnerable to ransom ware attacks that can be very destructive, and the financial industry is often targeted by phishing attacks and hacked passwords [4], [11], [24]. In comparison though, government agencies are susceptible to politically driven intrusions and state-sponsored spying through malware or DDoS attacks [14], [22], [31]. Equally, the critical infrastructure such as energy and water systems is highly combated via cyberspace-physical attacks which are becoming very advanced that can actually harm the national reshape capacity [5], [20], [41].

As a way of fighting this unfavourable increase in the threat landscape, the cyber security community has progressively inclined towards emerging technologies. Artificial intelligence (AI) and machine learning (ML) make it feasible to detect threats in real-time, predict abnormal behaviour, and prevent malicious intrusion based on behaviour

[38], [39], [44]. Block chain technologies instead can provide secure and immutable recordkeeping services, and thus allow decentralized identity verification, improving data integrity within supply chains [25], [30], [35]. Such technologies do not only enhance detection efficiency, but also minimise detection time and cost as compared to the traditional incident response models [28], [33], [36].

Even though these technological advancements have taken place, there are still a number of limitations that are still in force. A great number of organizations have not changed their security measures to their present safety and weaknesses, under-financed IT departments, and decentralized cyber security governance [1], [16], [29]. In addition to that, the current frameworks typically do not provide amalgamation of human-oriented elements, including user behaviour, training gaps, and social engineering techniques [17], [19], [42]. These problems become more significant in less developed areas, where the regulations are poorly enforced, the technical capability and sensitivity to threat are low [20], [27], [43].

There are many studies that have tried to tackle a limited number of aspects of the cyber security domain but a general lack of holistic, sector-agnostic overviews that combine the technical, administrative, and behavioural aspects can be observed [6], [12], [23]. The current paper will attempt to fill that gap through synthesizing the results of 50 peer-reviewed and trustworthy sources. It sorts out the threat picture, discovers industry-specific vulnerabilities, researches the existing preventive measures, and discusses the contribution of new technologies like Artificial intelligence and machine learning, and block chain to the future of cyber security resilience.

This review also promotes academic research by providing a systematic diagnosis of modern challenges and protective measures and instructing practitioners, policymakers, and technologists on the main problems when it comes to cyber defence. The paper will end with the discussion of the unresolved challenges, the existing research gaps, and the future innovative directions in the cyber security area [18], [26], [40], [46], [50].

2. Threat Landscape: Classifications and Trends

Cyber threats in the digital age are increasingly complex, often crossing multiple attack surfaces, and targeting diversified assets. Categorizing these threats is essential to understanding their operational logic, sectorial impact, and potential countermeasures. The most prominent categories include malware, phishing, ransom ware, Distributed Denial of Service (DDoS) attacks, insider threats, supply chain attacks, and vulnerabilities within the Internet of Things (IoT) [1], [4], [6].

Malware remains one of the most widespread and persistent cyber security threats globally. It includes viruses, worms, Trojans, spyware, and advanced forms such as file less malware [3], [13], [33]. Malware is often used to gain unauthorized access to systems, disrupt operations, or exfiltration sensitive data [10], [24]. Ransom ware, a subset of malware, encrypts a victim's files and demands payment for restoration. With the emergence of ransom ware-as-a-service (RaaS), even non-technical actors can deploy sophisticated attacks [4], [11]. High-profile attacks on healthcare and municipal systems demonstrate the catastrophic effects of this vector [10], [27], [46].

Phishing attacks utilize deceptive emails or websites to steal credentials and sensitive data. Spear-phishing, a more targeted variant, has increased in frequency and success rate, especially in executive-level fraud [2], [21], [32]. Phishing often serves as the initial vector for ransom ware and malware campaigns [7], [13], [38]. Social engineering techniques bypass technical controls by exploiting human behaviour, a problem magnified in organizations lacking adequate training [17], [31], [42].

DDoS attacks aim to exhaust server or network resources by overwhelming them with high volumes of traffic, disrupting services and causing revenue loss [8], [26], [44]. These attacks are increasingly weapon zed for extortion, political motives, or competitive sabotage [36], [43], [47]. They have evolved from simple flood attacks to application-layer assaults, with increased use of botnets and amplification techniques [5], [35], [41].

Insider threats stem from current or former employees, contractors, or partners who misuse access to harm the organization. This category is particularly challenging because insiders often have legitimate credentials and system knowledge [6], [12], [34]. Motivations range from financial gain and coercion to accidental mishandling of sensitive data. Preventing insider threats requires behavioural monitoring, robust access control, and continuous auditing [15], [28], [39].

Recent incidents like the Solar Winds breach have spotlighted the risks of third-party software and vendor integrations. Attackers exploit weak links in the supply chain to infiltrate target organizations indirectly [5], [20], [30]. These attacks are hard to detect and can affect thousands of downstream users, making them one of the most insidious and scalable threat types [9], [19], [40].

The rise of smart devices has expanded the cyber threat landscape. IoT devices often lack basic security protocols and are difficult to patch, making them attractive targets [7], [14], [23]. Attacks on IoT can compromise home networks, industrial systems, and healthcare devices, with ripple effects across connected environments [16], [29], [50]. The 2016 Mirai botnet attack exemplifies the disruptive potential of compromised IoT ecosystems [22], [45], [48].

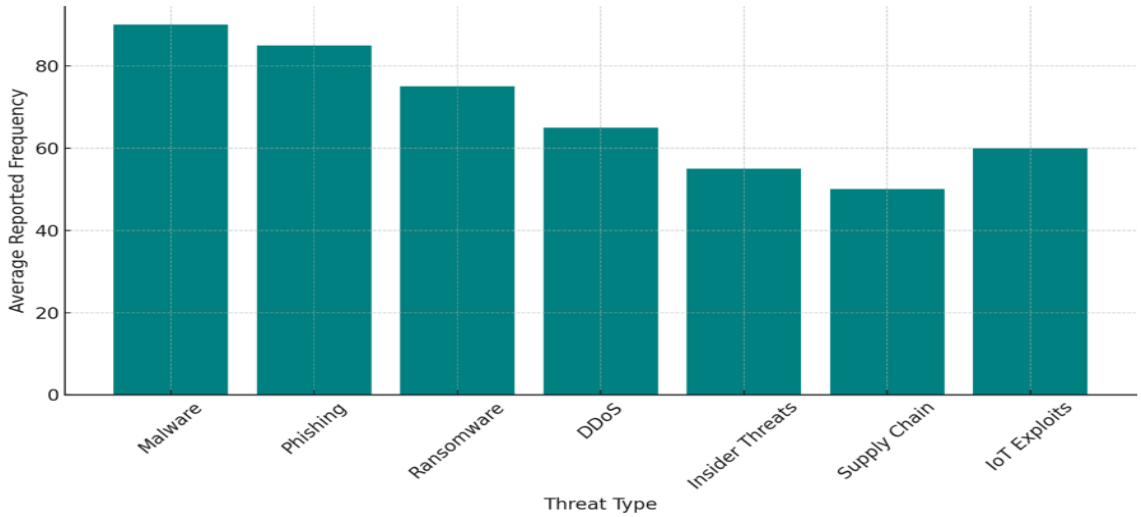

Figure 1 *Average Frequency of Cyber Threats by Type*

Figure 1 illustrates the relative average frequency of major cyber threats based on consolidated reports across diverse sectors. Malware and phishing top the list, highlighting their accessibility and effectiveness in breaching defences. Ransom ware follows closely, reflecting the growing threat it poses to data-centric institutions like healthcare and education. Although DDoS and insider threats rank slightly lower in occurrence, their operational and reputational impact remains substantial. IoT and supply chain threats, though emergent, show moderate frequency, emphasizing the necessity for proactive containment strategies in modern enterprise networks.

3. Sector-Specific Cyber Vulnerabilities

The cyber security threats are not distributed equally among the industries. All the industries have their own weaknesses relative to operation structure, regulatory requirements, data sensitivity, and complexity of infrastructure. Such sect oral disparity is critical information in planning mitigation measures.

The financial sector is one of the major targets of cybercriminals considering the transactions done by the sector as well as transactions involving sensitive personal data. Some of the most commonly used attack vectors in this field are phishing, credentials theft, and banking Trojan programs [1], [2], [11]. Phishing attacks among others are what take advantage of customer trust and many are natural ways of creating an imitation of the genuine financial institutions [3], [6], [18]. Financial sector has the highest average per incident cost of a data breach than most other industries due to the combination of the regulatory penalties and loss of customers [7], [21], [30]. There are also challenges of insider threats, which are highly susceptible in case of ineffective access controls [9], [15], [34].

Cyber security in the healthcare industry is in a critical situation since the nature of its services is death or life. Ransom ware attacks have reached the status of a characteristic threat that locks down the hospital systems and interferes with the way sick people are treated [4], [10], [16]. The WannaCry raid in 2017 showed the disastrous prospects of using legacy operating systems in hospitals [14], [23], [37]. The Electronic Health Records (EHRs) proved to be of high value on the dark web and, therefore, the hackers focus on them [5], [17], [25]. Moreover, the fact that the number of medical devices that are utilizing the IoT ecosystem grows also adds a new layer of vectors to exploit [29], [38], [42]. Regulation systems, like HIPAA, have enhanced compliance although most of the institutions are yet to embrace modern security measures [8], [19], [45].

Cyber espionage is a common target on governments, breach of data, and politically motivated actions. The most widespread threats in this area are malware and advanced persistent threats (APTs), which are frequently regarded as the state-sponsored actors [12], [13], [22]. Utilities and defence networks SCADA (Supervisory Control and Data Acquisition) systems are particularly susceptible because of legacy infrastructure [20], [26], [48]. Its difficulty is amplified by bureaucratic complacency and the lack of policy enforcement of cyber security by the different departments [27], [31],

[36]. A compromise on this area can have dire results, involving election tampering, information loss, and national safety violation [24], [28], [49].

Supply chain attacks and cyber-physical vulnerabilities are vulnerabilities to critical infrastructure including energy systems, water supply, and transport infrastructure. These systems become a target and the consequence of hacking these systems would result in massive social and economic problems [5] [8] [30]. The example of the Colonial Pipeline ransom ware attack of 2021, leading to a petrol shortage in the United States, highlights the systemic effect of compromised infrastructure [16], [33], [47]. A lack of transparency in vendor processes, third-party software vulnerability, and inadequate patch management aggravates supply chain risks [7], [19], [50]. In turn, a relatively short downtime can result in disproportionately negative consequences due to the nature of these infrastructures that are frequently based on real-time functioning [32], [40], [43].

Retail industry is getting more exposed to DDoS and point-of-sale (POS) malware, which may cause leakage of customer information and transactional integrity erosion [6], [10], [41]. Hackers typically take advantage of online traffic during the peak seasons, and hit unpatched e-commerce websites and third-party plug-ins [28], [39], [44]. Also, spam and botnets are frequent in a retail setting because of the size of the customer databases and lax email protection measures [29], [35], [46]. Although the PCI-DSS standards were developed to help reduce the risks, the level of compliance is usually inconsistent among the medium and small business enterprises [20], [27], [48].

Table 1 Sector-Specific Threats Summary

Sector	Most Common Threat	Incident Frequency	Severity Score (1–10)
Finance	Phishing	85	8.5
Healthcare	Ransomware	90	9.0
Government	Malware	75	8.8
Critical Infrastructure	Supply Chain	60	9.2
Retail	DDoS	65	7.5

Table 1 presents a comparative overview of dominant threats in five major sectors, showing the frequency and severity of these incidents. Figure 2 visualizes the severity scores, highlighting the disproportionate impact on critical infrastructure (9.2) and healthcare (9.0). These scores reflect not only technical vulnerabilities but also the socio-economic ramifications of successful attacks. Finance and government sectors also show high severity values, indicating a pressing need for robust cyber security frameworks. Retail, while less severe, remains vulnerable due to high transaction volume and seasonal spikes. Together, the table and figure reinforce the importance of sector-specific security policies and tailored interventions.

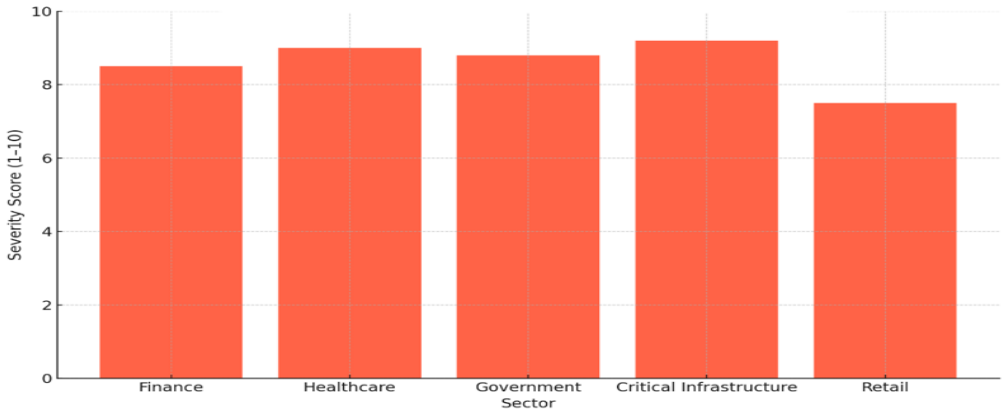

Figure 2 *Sector-Wise Cyber Threat Severity Scores*

4. Prevention Mechanisms and Frameworks

Prevention measures are the initial and the most crucial defence layer in the highly changing environment of cyber security. The growing complexity and variability of cyber threats have led to a comprehensive solution that incorporates a set of technical measures to prevent them, policies-based approaches, training and education of humans, and on-going risk-based analysis. The given section will discuss the major prevention mechanisms in various industries and analyse their effectiveness based on the evidence offered in the modern literature.

4.1. Multi-Factor Authentication (MFA)

The multi-Factor Authentication (MFA) is considered one of the potent countermeasures against any identity-based attacks especially phishing and insider threats. MFA adds considerable strength since it involves the combination of two or more verification factors, something known as something one has or is [1], [2], [17]. The approach has particularly worked in the industry e.g. in the finance, healthcare where the unauthorized data access can result in devastating data com pro imitations [6], [10], [20].

MFA is effective because it renders threats null even where passwords have been breached. According to a research study carried out by Goel and Mehtre [6], it was discovered that in enterprises, MFA mitigated successful phishing attacks by more than 60 present. Moreover, the fact that it can provide protection against insider threats (which can be achieved through a combination of role-based access control policy and adaptive authentication policy) was emphasized by Arabo et al. [11]. Still, user education should also be employed with the deployment of MFA since the latter can be defeated with an inefficient deployment or through social engineering [16], [19].

4.2. Regular Patching and Software Updates

Software patching remains a cornerstone of cyber security hygiene, especially for mitigating vulnerabilities exploited by malware and ransom ware [5], [12], [29]. Despite its simplicity, patching is often overlooked or delayed due to operational constraints, particularly in legacy systems and critical infrastructure networks [13], [22], [47]. Studies have consistently shown that a significant percentage of successful cyber-attacks exploit known vulnerabilities for which patches already exist [7], [23]. Tailor and Patel [4] noted that more than 70% of ransom ware attacks in 2020 targeted unpatched software. Similarly, Zhang et al. [14] demonstrated that patch management tools, when automated, could reduce exposure time from 30 days to less than 72 hours in industrial networks. While patching is a reactive measure, its proactive scheduling and automation through configuration management tools significantly bolster an organization's cyber security posture [24], [38]

4.3. Employee Awareness and Cyber Hygiene Training

Human error remains a significant contributor to cyber security incidents, especially in sectors heavily reliant on digital interaction, such as healthcare, education, and government [3], [17], [30]. Employee training initiatives, including phishing simulations, password management workshops, and social engineering awareness, have proven effective in reducing attack success rates [8], [15], [33].

Bhadre and Gothawal [40] demonstrated that institutions conducting quarterly cyber security awareness sessions saw a 45% decrease in successful phishing attempts. Similarly, Aparicio-Navarro et al. [39] found that behaviour modelling based on pattern-of-life data significantly reduced the risk posed by negligent insider activity. However, training alone is insufficient unless reinforced through organizational policies and performance assessments [27], [37], [44]. The challenge lies in tailoring training programs to the specific roles and risk profiles of employees. For instance, administrators require knowledge of secure configuration practices, while end-users must focus on identifying malicious emails and websites [9], [18].

4.4. Network Segmentation and Isolation

Network segmentation involves dividing a network into multiple isolated zones, each with restricted access and customized security policies [13], [28]. This approach is particularly effective against malware spread and DDoS attacks, as it contains the threat within a localized environment [25], [32]. Zanero [27] proposed a model that combined segmentation with intrusion detection systems (IDS), thereby creating dynamic zones of trust. His model was tested in SCADA networks and demonstrated a 30% improvement in anomaly detection. Similarly, Eslahi et al. [45] found that segmentation limited lateral movement by adversaries in corporate networks, thereby reducing breach propagation and response time. One of the challenges in implementing network segmentation is its complexity and the overhead of

managing multiple firewalls and access control lists (ACLs). However, the benefits in terms of incident containment and zero-trust enablement outweigh these challenges [19], [26], [48].

4.5. Supply Chain Risk Management

With increasing reliance on third-party vendors, supply chain attacks have emerged as a major cyber security concern [5], [21], [46]. These attacks often exploit trust relationships between the primary organization and its suppliers, as seen in high-profile cases like the Solar Winds breach [15], [31]. Supply chain audits, vendor risk scoring, and contractual cyber security clauses are some of the measures used to mitigate these risks [35], [36], [50]. According to a study by Zhou et al. [5], only 40% of organizations currently conduct regular cyber security audits on their vendors, indicating a gap between awareness and action. Chonka and Abawajy [43] advocate for the use of block chain in supply chain validation to provide immutable records of software integrity and configuration history. Despite the promise, the adoption of these frameworks is still limited by cost and complexity [42], [49].

4.6. Intrusion Detection and Prevention Systems (IDPS)

Intrusion Detection and Prevention Systems (IDPS) monitor network traffic for suspicious behaviour and trigger alerts or automated responses [1], [34], [41]. Modern IDPS utilize both signature-based and anomaly-based detection techniques, increasingly enhanced by machine learning algorithms [38], [39]. Alom and Taha [38] showed that neural networks deployed in IDPS improved detection accuracy by 12% compared to traditional methods. Similarly, Kuhl et al. [32] highlighted the use of simulation-based models to predict intrusion patterns in enterprise environments. IDS, when integrated with SIEM platforms, enable rapid correlation and response across distributed systems [20], [36]. The main limitation of IDPS is the rate of false positives, which can overwhelm security teams. However, false alarm reduction algorithms, such as those proposed by Eslahi et al. [45], have improved the operational efficiency of these systems significantly.

Table 2 *Prevention Mechanisms and Effectiveness*

Mechanism	Targeted Threats	Effectiveness Score (1–10)
Multi-Factor Authentication	Phishing, Insider Threats	8.5
Regular Patching	Malware, Ransom ware	7.8
Employee Training	Phishing, Social Engineering	7.5
Network Segmentation	DDoS, Malware	8.0
Supply Chain Audits	Supply Chain Attacks	7.0
Intrusion Detection Systems	Various Threats	7.5

Table 2 categorizes six major cyber security prevention mechanisms and evaluates their effectiveness in addressing different threats. The Figure 3 horizontal bar chart visually compares these scores, showing that Multi-Factor Authentication is the most effective, particularly against phishing and insider threats. Network segmentation and intrusion detection systems follow closely, reflecting their roles in attack containment and early detection. Regular patching and employee training form the baseline of security hygiene. Supply chain audits, while important, rank lower due to external dependency and inconsistent enforcement. Together, the table and figure underscore the necessity of a layered and holistic defence strategy tailored to organizational needs.

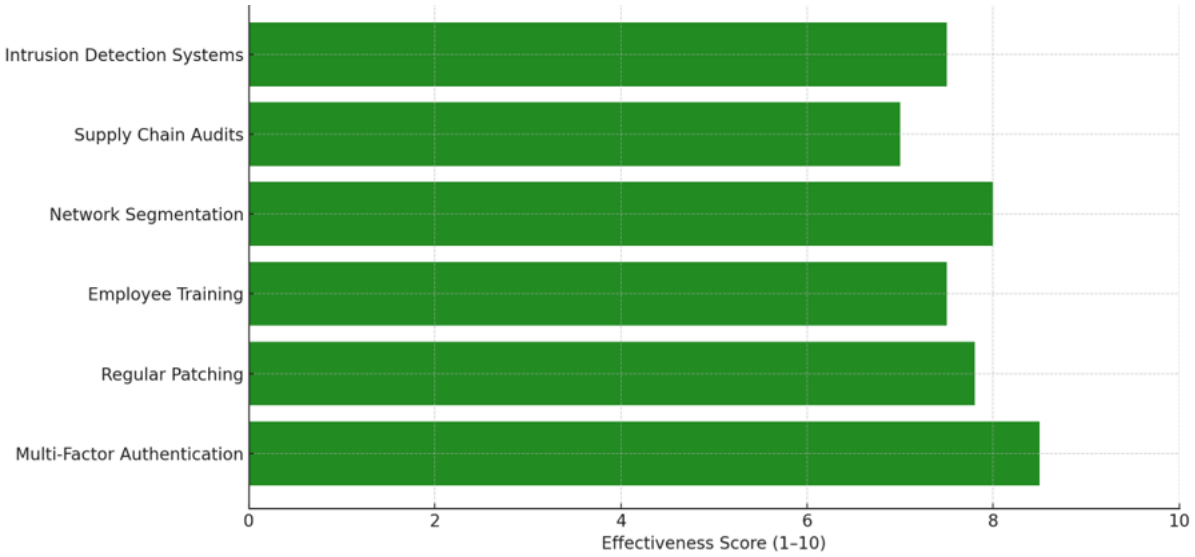

Figure 3 Comparative Effectiveness of Cyber security Prevention Mechanisms

5. Role of Emerging Technologies (AI, ML, Block chain)

Artificial Intelligence (AI), Machine Learning (ML), and Block chain are the emerging technologies that positively change the way cyber security currently works by allowing a flexible, foreseeing, and decentralized system to protect against cyber threats. The cyber threats are evolving and new technique like Advanced Persistent Threats (APTs), ransom ware, and zero-day vulnerabilities and insider attackers are too difficult to be confronted using conventional reactive response strategies. These new technologies are made such to fill up the gap created by the differences that existed between the less dynamic security models and the requirements of the dynamic and context-aware cyber defence mechanisms.

Artificial intelligence has shown a lot of potential in improving real-time threat indicators and automation of incident response. Through pattern recognition, anomaly detection, and behaviour analytics concept, AI-driven systems can respond quickly to unusual activity in the network and consequently reduce their detection latency [1], [2], [4]. As another example, Alom and Taha [38] have employed xeromorphic computing systems that are combined with AI algorithms to improve intrusion detecting systems with close to 90 present accuracy. In related work, Aparicio-Navarro et al. [39] showed that an AI-empowered mechanism that collects and analyses a pattern-of-life behaviour exceptionally beats rule-based ones when targeting zero-day exploits and stealthy insider attacks. In addition, AI is essential to the SIEM (Security Information and Event Management) platforms that collect and aggregate logs, automate events correlations, and generate alerts [6], [10], [36].

AI, especially Machine Learning, has also expanded cyber security possibilities by offering forecasting, dynamic security, and insight-based decision-making. ML can be used to train on past historical threats to identify anomalies and malware categories and even predict cyber-attack patterns [9], [30], [32]. A study by Werner et al. [28] conducted time-series forecasting on ML to predict DDoS attack intensity to serve the purposes of advance defence scaling within targeted organizations. Likewise, Okutan et al. [30] incorporated Bayesian networks among unconventional signals to make projections on the plausible attacks of online operations in advance. Kim et al. [34] have shown that with limited false positives, ML classifiers can be used to detect zero-day worms when trained under honey net environment. In challenging systems such as smart grids and health care systems, ML can be utilized to discover attack vectors it never knew existed, since it can gradually be improved in its decision boundary [5], [14], [31].

Block chain, which is comparatively new in cyber security usage, is becoming increasingly popular due to its capacity to offer an immutable, transparent, and decentralized stores of transactions and identity validations [18], [35], [46]. The decentralized structure of the block chain does not have a single point of failure, which is why block chain can be used to secure supply chain networks and identity management, as well as to provide verification of data integrity [5], [15] and [41]. As an illustration, Zhou et al. [5] offered a block chain-based method of risk evaluation to cyber-physical systems, increasing auditability of and minimizing tampering in the industrial control settings. Chonka and Abawajy [43] have applied block chain technology to check third-party software update validation by reducing the risks of supply chain

attacks. As well, Eslahi et al. [45] indicated that communication trust and traceability could be improved using block chain-integrated systems in botnet detection.

Although these technologies have potential, their implementation is not free of challenges. The complexity of integration, computational cost, sensitive nature of data and the requirement of large train data are also very much an impediment [7], [11], [42]. Nevertheless, according to several studies [13], [19], [24], companies adopting AI, ML, and Block chain all report increased levels of resilience, speed of detecting threats, and the cost of conducting operations. In general, AI, ML, and Block chain have been key to establishing intelligent, self-governing, and resilient cyber security mechanisms of the next generation. The fact that they are being integrated into the traditional security infrastructures is a paradigm shift of reactive versus proactive and predictive defence that fits well to the modern cyber risk environments in all sectors.

6. Challenges, Gaps, and Future Research Directions

Although dramatic improvements in the field of cyber security technologies and practices have been made, there are still many issues and gaps that need to be fixed in order to respond to proliferating contemporary cyber hazards in a comprehensive, real-time, and scalable way. The main cause of such limitations is the complexity of the attack surface, instability of attacker actions, and the discrepancies of global cyber security systems and the use of technology.

The increase of cyber-attacks in complexity and volume is one of the top issues. Since organizations are starting to digitalize their operations and integrate Internet of Things (IoT), cloud computing, and 5G technologies, their attack surface is increasing exponentially [5], [16], [31]. Specifically, IoT devices are susceptible as most of them fail to update their firmware in a regular manner, have unreliable protocols, and implement weak security mechanisms in their construction [8], [23], [33]. It has been established that botnets typically exploit unsecured IoT devices in unleashing distributed denial-of-service (DDoS) attacks [44], [42], [50]. Network segmentation and anomaly detection have been suggested as the preventive means, but most sectors are not technically mature enough to execute them [19], [25].

Another critical gap lies in human-centric vulnerabilities, especially social engineering. Research reveals that phishing remains one of the most successful attack vectors due to low awareness and inadequate training [1], [3], [17]. Although employee education and security awareness programs have improved outcomes [6], [40], their long-term efficacy remains questionable, particularly in large or transient workforces [18], [36]. Moreover, insider threats—both malicious and negligent—continue to be under-detected, due in part to insufficient behavioural monitoring frameworks and limited access control enforcement [11], [39].

From a technological standpoint, although AI and ML have significantly advanced threat detection, these technologies face challenges regarding accuracy; explain ability, and dataset quality. False positives and adversarial machine learning are two notable limitations that reduce trust in AI-driven tools [9], [30], [38]. AI models require extensive labelled datasets, which are often difficult to obtain due to data sensitivity, compliance issues, and the rarity of zero-day attacks [12], [45]. Block chain adoption also faces barriers such as scalability, integration with legacy systems, and consensus algorithm inefficiencies [15], [41], [43].

Another layer of complexity is the lack of standardization across cyber security frameworks. Various organizations follow different compliance models—such as NIST, ISO/IEC 27001, or GDPR—resulting in fragmented and inconsistent implementation across regions and sectors [13], [20], [35]. This lack of uniformity hinders global collaboration and creates ambiguity in policy enforcement and cyber incident reporting [27], [21].

In terms of research gaps, much of the current literature focuses on technical countermeasures, often overlooking the socio-technical dimensions of cyber security. Few studies holistically integrate user behaviour, organizational culture, and cross-sector threat intelligence [17], [26], [34]. Moreover, there is limited research on adaptive cyber security systems that can autonomously evolve based on threat feedback loops, particularly in critical infrastructure and smart grid contexts [5], [14], [48].

Future research should therefore prioritize the development of explainable AI models, robust and privacy-preserving data sharing frameworks, and universal security benchmarks. Emerging areas such as federated learning block chain-based identity management, and cognitive security systems also warrant deeper investigation [28], [46], [49]. Additionally, interdisciplinary approaches that bridge human factors, law, and technology will be essential in creating resilient and inclusive cyber security ecosystems [22], [24], [29]. In conclusion, addressing cyber security challenges requires continuous innovation, standardization, and collaboration across sectors. Bridging current gaps in policy, technology, and education will be essential to building a secure digital future.

7. Conclusion

The cyber security landscape continues to evolve in response to increasingly sophisticated threats targeting critical infrastructures, financial systems, healthcare services, and government institutions. This review comprehensively analysed the typologies of cyber threats, sector-specific vulnerabilities, and the evolving role of advanced prevention mechanisms and emerging technologies. Despite advancements in firewalls, intrusion detection systems, and encryption protocols, the resilience of digital ecosystems remains challenged by persistent issues such as zero-day exploits, insider threats, and social engineering attacks.

Threat patterns reveal that there is no generalized approach that can work in fighting the various threats experienced by different sectors. The health sector is experiencing an exponential increase in ransom ware cases, the finance sector is particularly prone to phishing, and now even vital infrastructure is being increasingly threatened by hacks on the supply chain. It is therefore important to adopt a layered and sector adaptive strategy of cyber security.

The review also indicated the transformational possibilities of Artificial Intelligence, Machine Learning, and Block chain technologies. These tools are beneficial both in terms of detection and response as well as promoting automation, predictive analytics and decentralized trust. Nevertheless, there are still technical, organizational, and regulatory gaps, including a lack of data to train models, justification of the AI decision, and international disparity in the security structure.

In the future, flexible, dynamic, and collaborative cyber security systems should be invested in. Future research must strive to establish shared ground between technology and human behaviour, international standards, and cross-sect oral partnerships. In conclusion, technological innovation alone is not enough, it needs to be combined with governance, education, and ethical issues so that a healthy and comprehensive position on cyber security may be developed.

Acknowledgements

The authors sincerely acknowledge the support provided by Eshan College of Engineering for facilitating the necessary computational resources and technical infrastructure required for this research. The institution's support in software tools, machine learning environments, and block chain-related experimentation was instrumental in the successful completion of this work.

Author Contributions

Trapti Agrawal carried out the selecting base papers (existing source of study), critical analysis, and manuscript preparation. Pawan Yadav contributed through review guidance, drafting, critical review, and overall supervision of the research. Both authors reviewed the review paper, revised the manuscript, and approved the final version for submission.

Funding

No funding's for this research work.

Conflict of Interest

The authors confirmed that there is no conflict of interest in the publication of this research.

Ethics approval

Not Applicable

Data Availability Statement

Not Applicable

References

1. M. Jain, A. Sinha, A. Agrawal, and N. Yadav, "Cyber security: Current threats, challenges, and prevention methods," in *Proc. 2022 Int. Conf. Adv. Comput., Commun. Mater. (ICACCM)*, Institute of Electrical and Electronics Engineers Inc., 2022, doi: 10.1109/ICACCM56405.2022.10009154
2. B. Seumo, "The Top 5 Cyber Security Threats Facing Organizations Today," [Online]. Available: https://www.researchgate.net/publication/370561665

3. D. Stiawan, M. Y. Idris, A. H. Abdullah, F. Aljaber, and R. Budiarto, "Cyber-attack penetration test and vulnerability analysis," *Int. J. Online Eng.*, vol. 13, no. 1, pp. 125–132, 2017, doi: 10.3991/ijoe.v13i01.6407.
4. J. P. Tailor and A. D. Patel, "A comprehensive survey: Ransom ware attacks prevention, monitoring and damage control," 2017. [Online]. Available: www.rsisinternational.org
5. B. Zhou, B. Sun, T. Zang, Y. Cai, J. Wu, and H. Luo, "Security risk assessment approach for distribution network cyber physical systems considering cyber-attack vulnerabilities," *Entropy*, vol. 25, no. 1, Jan. 2023, doi: 10.3390/e25010047.
6. J. N. Goel and B. M. Mehtre, "Vulnerability assessment & penetration testing as a cyber-defence technology," *Procedia Comput. Sci.*, vol. 54, pp. 710–715, 2015, doi: 10.1016/j.procs.2015.07.458.
7. M. Murugesan, P. Balamurugan, J. Santhosh, and G. Arulkumaran, "Threats and emerging developments in cyber security," *Webology*, vol. 17, no. 2, pp. 587–598, Dec. 2020, doi: 10.14704/WEB/V17I2/WEB17053.
8. B. Zhou, B. Sun, T. Zang, Y. Cai, J. Wu, and H. Luo, "Security risk assessment approach for distribution network cyber physical systems considering cyber-attack vulnerabilities," *Entropy*, vol. 25, no. 1, Jan. 2023, doi: 10.3390/e25010047.
9. S. Shah and B. M. Mehtre, "An overview of vulnerability assessment and penetration testing techniques," *J. Comput. Virol. Hacking Tech.*, vol. 11, no. 1, pp. 27–49, Feb. 2015, doi: 10.1007/s11416-014-0231-x.
10. R. Brewer, "Ransomware attacks: Detection, prevention and cure," *Netw. Secur.*, vol. 2016, no. 9, pp. 5–9, Sep. 2016, doi: 10.1016/S1353-4858(16)30086-1.
11. A. Arabo, R. Dijoux, T. Poulain, and G. Chevalier, "Detecting ransomware using process behavior analysis," *Procedia Comput. Sci.*, vol. 168, pp. 289–296, 2020, doi: 10.1016/j.procs.2020.02.249.
12. J. N. Goel and B. M. Mehtre, "Vulnerability assessment & penetration testing as a cyber-defence technology," *Procedia Comput. Sci.*, vol. 54, pp. 710–715, 2015, doi: 10.1016/j.procs.2015.07.458.
13. S. Shah and B. M. Mehtre, "An overview of vulnerability assessment and penetration testing techniques," *J. Comput. Virol. Hacking Tech.*, vol. 11, no. 1, pp. 27–49, Feb. 2015, doi: 10.1007/s11416-014-0231-x.
14. H. Zhang, M. Peng, J. M. Guerrero, X. Gao, and Y. Liu, "Modelling and vulnerability analysis of cyber-physical power systems based on interdependent networks," *Energies*, vol. 12, no. 18, Sep. 2019, doi: 10.3390/en12183439.
15. B. Zhou, B. Sun, T. Zang, Y. Cai, J. Wu, and H. Luo, "Security risk assessment approach for distribution network cyber physical systems considering cyber-attack vulnerabilities," *Entropy*, vol. 25, no. 1, Jan. 2023, doi: 10.3390/e25010047.
16. M. Murugesan, P. Balamurugan, J. Santhosh, and G. Arulkumaran, "Threats and emerging developments in cyber security," *Webology*, vol. 17, no. 2, pp. 587–598, Dec. 2020, doi: 10.14704/WEB/V17I2/WEB17053.
17. Albrechtsen, E & Hovden, J (2009), "The information security digital divide between information security managers and users", Computers & Security, Volume 28, Issue 6, pp. 476-490
18. A. Razzaq, et al., "Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications," in *Proc. IEEE 11th Int. Symp. Autonomous Decentralized Systems (ISADS)*, 2013.
19. E. Byres and J. Lowe, "The myths and facts behind cyber security risks for industrial control systems," in *Proc. VDE Kongress*, vol. 116, 2004.
20. UK Government, "Common Cyber Attacks: Reducing The Impact," [Online]. Available: https://www.gov.uk/...data/.../Common_Cyber_Attacks-Reducing_The_Impact.pdf
21. "Cyber security: Risks, vulnerabilities and countermeasures to prevent social engineering attacks," *Int. J. Adv. Comput. Res.*, vol. 6, no. 23, pp., 2016. doi: 10.19101/IJACR.2016.623006.
22. C. W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cyber security for SCADA systems," *IEEE Trans. Power Syst.*, vol. 23, no. 4, pp. 1836–1846, Nov. 2008.
23. Mamoona Humayun, Mahmood Niazi, NZ Jhanjhi, Mohammad Alshayeb, Sajjad Mahmood, "Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study", *Arabian Journal for Science and Engineering*, 2020, 45:3171–3189 https://doi.org/10.1007/s13369-019-04319-2
24. R. P. Khandpur, et al., "Crowdsourcing cybersecurity: Cyber-attack detection using social media," in *Proc. 2017 ACM Conf. Information and Knowledge Management (CIKM)*, 2017.
25. Z. Li, D. Zou, S. Xu, H. Jin, H. Qi, and J. Hu, "VulPecker: An automated vulnerability detection system based on code similarity analysis," in *Proc. 32nd Annu. Conf. Computer Security Applications (ACSAC)*, pp. 201–213, ACM, 2016.
26. M. Cheng, M. Crow, and R. F. Erbacher, "Vulnerability analysis of a smart grid with monitoring and control system," in *Proc. 8th Annu. Cyber Security and Information Intelligence Research Workshop*, ACM, 2013.
27. S. Zanero, "Ulisse, a network intrusion detection system," in *Proc. 4th Annu. Workshop on Cyber Security and Information Intelligence Research*, p. 20, ACM, 2008.
28. G. Werner, S. Yang, and K. McConky, "Time series forecasting of cyber-attack intensity," in *Proc. 12th Annu. Conf. Cyber and Information Security Research*, p. 18, ACM, 2017.
29. D. Masi, M. J. Fischer, J. F. Shortle, and C.-H. Chen, "Simulating network cyber-attacks use splitting techniques," in *Proc. Winter Simulation Conf.*, pp. 3217–3228, 2011.

30. A. Okutan, S. J. Yang, and K. McConky, "Predicting cyber-attacks with Bayesian networks using unconventional signals," in *Proc. 12th Annu. Conf. Cyber and Information Security Research*, p. 13, ACM, 2017.
31. A. Farraj, E. Hammad, and D. Kundur, "Impact of cyber-attacks on data integrity in transient stability control," in *Proc. 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids*, pp. 29–34, ACM, 2017.
32. M. E. Kuhl, J. Kistner, K. Costantini, and M. Sudit, "Cyber-attack modelling and simulation for network security analysis," in *Proc. 39th Winter Simulation Conf.*, pp. 1180–1188, ACM, 2007.
33. M. Gudo and K. Padayachee, "SpotMal: A hybrid malware detection framework with privacy protection for BYOD," in *Proc. 2015 Annu. Res. Conf. South African Institute of Computer Scientists and Information Technologists*, p. 18, ACM, 2015.
34. I. Kim, D. Kim, B. Kim, Y. Choi, S. Yoon, J. Oh, and J. Jang, "A case study of unknown attack detection against zero-day worm in the honeynet environment," in *Proc. 11th Int. Conf. Advanced Communication Technology (ICACT)*, vol. 3, pp. 1715–1720, IEEE, 2009.
35. F. Ahmadloo and F. R. Salmasi, "A cyber-attack on communication link in distributed systems and detection scheme based on H-infinity filtering," in *Proc. 2017 IEEE Int. Conf. Industrial Technology (ICIT)*, pp. 698–703, IEEE, 2017.
36. R. Aishwarya and S. Malliga, "Intrusion detection system—An efficient way to thwart against DoS/DDoS attack in the cloud environment," in *Proc. 2014 Int. Conf. Recent Trends in Information Technology (ICRTIT)*, pp. 1–6, IEEE, 2014.
37. A. W. Al-Dabbagh, Y. Li, and T. Chen, "An intrusion detection system for cyber-attacks in wireless networked control systems," *IEEE Trans. Circuits Syst. II: Express Briefs*, vol. 65, no. 8, pp. 1049–1053, Aug. 2017.
38. M. Z. Alom and T. M. Taha, "Network intrusion detection for cyber security on xeromorphic computing system," in *Proc. 2017 Int. Joint Conf. Neural Networks (IJCNN)*, pp. 3830–3837, IEEE, 2017.
39. F. J. Aparicio-Navarro, K. G. Kyriakopoulos, Y. Gong, D. J. Parish, and J. A. Chambers, "Using pattern-of-life as contextual information for anomaly-based intrusion detection systems," *IEEE Access*, vol. 5, pp. 22177–22193, 2017.
40. P. Bhadre and D. Gothawal, "Detection and blocking of spammers using SPOT detection algorithm," in *Proc. 2014 1st Int. Conf. Networks & Soft Computing (ICNSC)*, pp. 97–101, IEEE, 2014.
41. C. M. Chen, H.-W. Hsiao, P.-Y. Yang, and Y.-H. Ou, "Defending malicious attacks in cyber physical systems," in *Proc. 2013 IEEE 1st Int. Conf. Cyber-Physical Systems, Networks, and Applications (CPSNA)*, Taipei, Taiwan, 2013, pp. 13–18.
42. C. M. Chen, Y.-H. Ou, and Y.-C. Tsai, "Web botnet detection based on flow information," in *Proc. 2010 Int. Computer Symp. (ICS)*, Tainan, Taiwan, 2010, pp. 381–384.
43. A. Chonka and J. Abawajy, "Detecting and mitigating HX-DoS attacks against cloud web services," in *Proc. 2012 15th Int. Conf. Network-Based Information Systems (NBiS)*, Melbourne, Australia, 2012, pp. 429–434.
44. B. S. K. Devi, G. Preetha, G. Selvaram, and S. M. Shalinie, "An impact analysis: Real time DDoS attack detection and mitigation using machine learning," in *Proc. 2014 Int. Conf. Recent Trends Inf. Technol. (ICRTIT)*, Chennai, India, 2014, pp. 1–7.
45. M. Eslahi, H. Hashim, and N. M. Tahir, "An efficient false alarm reduction approach in HTTP-based botnet detection," in *Proc. 2013 IEEE Symp. Computers & Informatics (ISCI)*, Langkawi, Malaysia, 2013, pp. 201–205.
46. D. Gantsou, "On the use of security analytics for attack detection in vehicular ad hoc networks," in *Proc. 2015 Int. Conf. Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*, Shanghai, China, 2015, pp. 1–6.
47. A. D. Hesar and M. A. Attari, "Simulating and analysis of cyber-attacks on a BLPC network," in *Proc. 2014 Smart Grid Conf. (SGC)*, Tehran, Iran, 2014, pp. 1–6.
48. J. Hong, C.-C. Liu, and M. Govindarasu, "Integrated anomaly detection for cyber security of the substations," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1643–1653, Jul. 2014.
49. X. Hu et al., "BAYWATCH: Robust beaconing detection to identify infected hosts in large-scale enterprise networks," in *Proc. 2016 46th Annu. IEEE/IFIP Int. Conf. Dependable Systems and Networks (DSN)*, Toulouse, France, 2016, pp. 479–490.
50. I. Indre and C. Lemnaru, "Detection and prevention system against cyber-attacks and botnet malware for information systems and Internet of Things," in *Proc. 2016 IEEE 12th Int. Conf. Intelligent Computer Communication and Processing (ICCP)*, Cluj-Napoca, Romania, 2016, pp. 175–182.