IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940



International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 10, October 2026

DOI: 10.17148/IJARCCE.2026.1510116

Evolving Cyber Threats, Cyber Frauds, and Attacks: Strategies for Mitigation

Raju B. Amle

Assistant Professor, School of Computer Sciences, Kavayitri Bahinabai Chaudhari North Maharashtra University, Jalgaon, (M.S) India

Abstract: Rapid digitalization has increased reliance on interconnected systems, exposing sectors to cyber threats and fraud involving software vulnerabilities, credential theft, social engineering, ransomware, cloud misconfigurations, third-party risks, and AI-generated deception. This narrative review examines emerging threats, their impacts, and a layered defense framework integrating identity security, patching, monitoring, data protection, user awareness, incident response, and recovery. It also considers responsible AI-based threat detection and associated adversarial and privacy risks. Drawing on public guidance and threat reports. This paper presents overview of cybersecurity, cybersecurity threats/attacks cyber frauds, the presents the related work, then describes the Evolution of Cybersecurity, Cyber Threats and Cybercrimes: From 1960 to the Present, Current Cyber Threats and Cyber Frauds, Impact of Cyber Incidents, and along with Strategies for Mitigation.

Keywords: Cyber Threats, Vulnerabilities, Social Engineering, ransomware, cloud misconfigurations, patching.

1. INTRODUCTION

Cybersecurity has emerged as a critical priority in the digital era, driven by the rapid expansion of the internet, cloud computing, online banking, artificial intelligence (AI), the Internet of Things (IoT), and digital payment systems. While these technologies enhance communication, productivity, and accessibility, they also expose individuals, businesses, educational institutions, and government agencies to diverse cyber threats and fraudulent activities [1-4].

Major cybersecurity threats include ransomware, phishing, malware, identity theft, Distributed Denial-of-Service (DDoS) attacks, data breaches, cloud security vulnerabilities, supply-chain attacks, and AI-powered attacks. Cybercriminals increasingly exploit social engineering, counterfeit websites, deceptive messages, deepfakes, and impersonation to manipulate users and obtain unauthorized access to sensitive information, financial accounts, and organizational networks [1-6].

Cyber fraud represents a significant cybersecurity challenge, encompassing deceptive online activities designed to steal money, personal information, login credentials, and other valuable assets. Common forms include online banking fraud, UPI and QR-code scams, phishing, identity theft, investment scams, Business Email Compromise (BEC), and technical-support fraud. Such incidents can cause financial losses, compromise privacy, damage reputations, and disrupt essential services [1-6].

Effective mitigation requires a multilayered approach that integrates technical safeguards, organizational policies, and user awareness. Key measures include strong passwords, multi-factor authentication (MFA), timely software updates, encryption, firewalls, endpoint protection, secure backups, continuous network monitoring, and access controls guided by the principle of least privilege. AI-based threat detection can support the identification of suspicious activity, while cybersecurity awareness training helps users recognize fraudulent communications and social engineering attempts. Independently verifying payment requests and recipient details is also essential for securing digital payments and financial transactions [1-6].

Digital services are now integral to banking, education, healthcare, government, commerce, and personal communication. While this dependence enhances efficiency, it also exposes systems and users to malicious activity. Cyber incidents can disrupt services, expose sensitive information, cause financial losses, erode trust, and pose safety risks when critical services are affected [1-6].

 This work is licensed under a Creative Commons Attribution 4.0 International License

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940



International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 10, October 2026

DOI: 10.17148/IJARCCE.2026.1510116

2. RELATED WORK

Abdullah, M. et. al [6] A cybercrime trends, drawing on the Council on Foreign Relations' state-sponsored cyber operations database. It explores evolving threats, victim demographics, geographical patterns, complaints, and financial losses to inform cybersecurity strategies, policymaking, public awareness.

Kang Leng Chiew et.al [7] review examines evolving phishing techniques, their platforms, attack vectors, and combinations to support comprehensive prevention. It promotes awareness, identifies research gaps, and informs anti-phishing development and policymaking.

Anuradha Chakraborty et.al [8] focus on the gaps in India's cybersecurity framework, including outdated policies, fragmented institutions, and reliance on foreign technologies, and advocates comprehensive reforms to strengthen resilience against evolving cyber threats.

Sukhdev Singh [9] has reviews evolving cybersecurity threats and advocates layered defenses, software updates, user awareness, AI/ML-based detection, international cooperation, and regulatory policies to strengthen cyber resilience.

Ashraful Goni et.al [10] focus on vulnerability analysis, integrated with incident response, continuous assessment, awareness, and collaboration, as essential to identifying risks, mitigating attacks, and strengthening cybersecurity defenses.

Frank Cremer et.al [11] review identifies 79 datasets from 5,219 studies, highlighting limited cyber-risk data availability and the need for standardized open databases and mandatory reporting to support research, insurance, and risk management.

Abdulbasit A et.al [12] classifies cyber threats based on severity and technical complexity, examines their impacts, and explores technical, organizational, legal, and regulatory countermeasures. It also focuses on the emerging cyber threats and the challenges of maintaining effective cybersecurity in a rapidly evolving digital environment.

Ahsan, M et.al [13] Using machine learning enhances cybersecurity by enabling scalable and automated malware detection. Author focused on the survey reviews techniques such as deep learning, SVM, and Bayesian classification for detecting cyber threats, analyzing evolving attack patterns, and identifying limitations in existing models to improve security systems.

R. B. Amle [14] Cybersecurity is essential in today's digital world as the growth of cloud computing, IoT, and online services increases cyber risks. It protects systems, networks, applications, and data from unauthorized access and attacks. Focused on reviews cybersecurity types, major cyberattacks, their impacts, challenges, solutions, and related literature.

Kamran Razzaq et.al [15] reviews machine learning-based cyber-attack prevention in online retailing using a systematic literature review of 54 articles published between 2018 and 2023. It also focused on the supervised and unsupervised techniques, particularly SVM and Naive Bayes, identifies research gaps, and suggests future directions for improving cybersecurity in e-commerce.

Kang Leng Chiew et. al [16] reviews evolving phishing techniques, their delivery platforms, and attack vectors. It mainly focused on the combined phishing strategies, prevention methods, research gaps, and future directions to support effective anti-phishing systems and cybersecurity awareness.

Akashdeep Bhardwaj et. al [17] proposed a privacy-aware framework and a novel phishing taxonomy to detect and mitigate evolving phishing attacks targeting unsuspecting users and IoT devices. The results demonstrate the framework's effectiveness in identifying multiple phishing attacks.

Rafał Leszczyna [18] reviews 32 cybersecurity assessment methods, evaluating their practical applicability, limitations, and challenges. It identifies research gaps and future directions to help researchers and practitioners select effective assessment methods and improve cyber asset protection.

Akash Jain et. al [19] proposed a machine learning-based framework for real-time cyber threat detection and prevention using Random Forest, Gradient Boosting, and Logistic Regression. Evaluated on 4,506 network traffic samples, it

DOI: 10.17148/IJARCCE.2026.1510116

achieves 100% binary classification accuracy and 90.91% multiclass accuracy, enabling automated threat detection, adaptive firewall protection, and incident response.

3. EVOLUTION OF CYBERSECURITY, CYBER THREATS AND CYBERCRIMES: FROM 1960 TO THE PRESENT

3.1 1960 to 1969

The early 1960s saw initial technological advancements that enabled connectivity. As computers were costly, bulky, and shared by multiple users, time-sharing created a need to prevent unauthorized access to systems and files, giving rise to data and hardware security. Security measures during this period mainly involved physical access controls, locked facilities, and segregation of duties to prevent insider misuse [5,6,20].

3.2 1970 to 1979

In the 1970s, ARPANET—the precursor to the Internet—emerged, creating new opportunities for hackers. Early programs such as Creeper and Reaper appeared, though they were mainly academic experiments rather than malicious software. The 1975 publication of The Protection of Information in Computer Systems established principles foundational to modern cybersecurity, while basic authentication, access control lists, and network isolation were introduced to protect sensitive systems [5,6,21,22].

3.3 1980 to 1989

The 1980s were marked by rapid Internet adoption following the introduction of the Internet Protocol Suite in 1983, which expanded both potential targets and threats. This decade saw the first dictionary attacks, a KGB-linked hacking incident involving sensitive U.S. military documents, and the Morris Worm—the first major Internet malware outbreak. In response, early antivirus tools, regular backups, and user training were adopted to mitigate malware spread and human error [5,6,23].

3.4 1990-1999

In this decade known as the “virus era,” the 1990s saw widespread personal computing, enabling script kiddies to download and deploy ready-made malicious code for vandalism. These attacks drove the adoption of antivirus software, firewalls, patch management, email filtering, and incident response teams, prompting major technology firms to prioritize cybersecurity [5,6,24].

3.5 2000 -2009

The 2000s saw rapid digitalization of banking and financial transactions, increasing credit card breaches, online fraud, and ransomware attacks. In response, organizations adopted two-factor authentication, SSL/TLS encryption, firewalls, fraud detection systems, and the PCI DSS standard to secure payment data [5,6].

3.6 2010-2019

The 2010s saw a peak in sophisticated state-sponsored cyberattacks and cyber-weapon development, with global incidents such as WannaCry and NotPetya causing widespread damage. Organizations responded by adopting advanced IDS/IPS, threat intelligence sharing, zero-trust architectures, red/blue team exercises, and targeted incident-response playbooks [5,6,25,26].

3.7 2020s

Cybercrime in the 2020s has grown in scale and sophistication, driven by AI-augmented attacks, supply-chain breaches, and large-scale financial scams. Generative AI enables more convincing and scalable social engineering, while also supporting defensive applications. In the financial sector, fraud, extortion, and malware-driven theft continue to undermine trust and operational stability. Addressing these evolving threats requires a multidisciplinary strategy combining AI-based detection, regulation, public awareness, and international cooperation [5,6,27,28].

3.8 Present

As global interconnectivity grows, cybersecurity risks continue to rise. Technologies such as 5G, quantum computing, IoT, and cloud services expand the attack surface, requiring proactive and robust mitigation strategies. Recently, side-channel attacks have emerged as a major evolving threat. Rather than exploiting software vulnerabilities directly, they infer sensitive information from physical, electromagnetic, or sensor-based signals, often bypassing conventional network defenses [5,6, 29].

 This work is licensed under a Creative Commons Attribution 4.0 International License

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940



International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 10, October 2026

DOI: 10.17148/IJARCCE.2026.1510116

4. CURRENT CYBER THREATS AND CYBER FRAUDS

4.1 Phishing and Social Engineering

Phishing messages impersonate trusted organizations or colleagues to trick victims into revealing credentials, opening malicious files, approving fraudulent payments, or disclosing one-time passwords. Common variants include spear phishing, smishing (SMS phishing), vishing (voice phishing), QR-code phishing, and business email compromise. AI-generated text, voice cloning, and realistic fake profiles can make impersonation more convincing. Warning signs include unexpected urgency, requests to bypass procedures, unfamiliar payment details, and links or domains that do not match the legitimate service [1-7,10,13,14].

4.2 Ransomware and Data Extortion

Ransomware encrypts data or disrupts access to systems. Many criminal groups also exfiltrate sensitive information and threaten to publish it, creating a double-extortion risk. Common entry points include compromised credentials, exposed remote-access services, phishing, and unpatched systems.

Paying a ransom does not ensure data recovery or prevent disclosure. Therefore, tested backups and a well-defined incident-response plan are essential [1-6,10,14].

4.3 Identity Theft and Account Takeover

Stolen passwords, session tokens, personal information, and authentication codes can enable attackers to compromise email, banking, social media, and enterprise accounts. Password reuse and weak account-recovery procedures further amplify the impact. Compromised email accounts may also be exploited to reset access to other accounts or impersonate employees [1-6].

4.4 Exploitation of Vulnerabilities and Malware

Attackers exploit vulnerabilities in internet-facing applications, operating systems, VPNs, routers, and other software. Malware can steal credentials, monitor user activity, establish remote access, or move laterally within a network. Delayed patching, unsupported devices, excessive privileges, and insecure default configurations increase exposure to such attacks [1-6].

4.5 Digital Payment and Investment Fraud

Fraud schemes include fake payment links, QR-code scams, fraudulent customer-support numbers, UPI or payment-app impersonation, card-not-present fraud, fake investment platforms, romance scams, and requests to transfer funds to a “safe” account. These schemes typically rely on social manipulation rather than a direct technical breach. Independent verification through a trusted channel is therefore a key defense [1-6].

4.6 Business Email Compromise and Invoice Fraud

Criminals exploit or spoof business email accounts to manipulate supplier bank details, invoices, payroll instructions, and executive payment requests. These attacks exploit routine business processes and often bypass traditional malware detection. Out-of-band verification and dual authorization for sensitive transactions are essential preventive measures [1-6].

4.7 DDoS, Web Attacks, and API Abuse

Distributed denial-of-service (DDoS) attacks disrupt online services by flooding them with excessive traffic, while application-layer attacks exploit vulnerabilities in websites and APIs. Weak access controls may expose customer data or enable unauthorized activities. Rate limiting, secure software development, web application protection, and resilient system architecture help mitigate these risks [1-6,10,14].

4.8 Cloud, Supply-Chain, and Third-Party Risks

Cloud data exposure, excessive privileges, leaked credentials, vulnerable software dependencies, and compromised service providers can create indirect security risks for multiple organizations. Effective cybersecurity must extend beyond internal networks to include suppliers, managed service providers, software components, and cloud identities [1-6].

4.9 AI-Enabled and Emerging Threats

Artificial intelligence enables attackers to create convincing messages, translate scams, automate reconnaissance, and generate fake audio or video. AI systems are also vulnerable to prompt injection, data leakage, and training or retrieval data manipulation. Therefore, conventional security measures remain essential, supported by stronger data provenance, access controls, continuous monitoring, and human verification [1-6].

 This work is licensed under a Creative Commons Attribution 4.0 International License

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940



International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 10, October 2026

DOI: 10.17148/IJARCCE.2026.1510116

5. IMPACT OF CYBER INCIDENTS

Cyber incidents cause more than financial losses, including data and intellectual property theft, operational disruption, regulatory penalties, reputational damage, and reduced customer trust. Individuals may face identity theft, financial debt, account loss, and emotional distress. For institutions, compromised accounts can expose wider systems when access privileges and network segmentation are inadequate [1-6].

6. STRATEGIES FOR MITIGATION

Cyber threats are growing and evolving, making traditional security approaches increasingly inadequate. Organizations and governments must therefore adopt proactive measures and adaptive mitigation strategies. In this section discusses mitigation techniques, policy frameworks, and innovative technologies that enhance resilience, reduce vulnerabilities, and limit the impact of cyber threats [5,6].

6.1. Training and Cybersecurity awareness are essential for reducing security threats. Scenario-based employee training helps prevent social engineering and phishing attacks, which often succeed because users lack awareness of modern technologies and attack techniques. Older adults aged 60+ are particularly vulnerable due to limited familiarity with these exploitation methods [5,6].

6.2. Ethical hackers identify and address security vulnerabilities before malicious actors exploit them by simulating controlled real-world cyberattacks. They strengthen cybersecurity, support compliance, and reduce breach risks. AI-enabled penetration testing is increasingly important, as 83% of ethical hackers have encountered AI-enabled attacks. However, its widespread adoption is limited by a shortage of certified professionals and inconsistent regulations across jurisdictions [5,6,30].

6.3. AI-based methods can detect and counter espionage, ransomware, zero-day exploits, and advanced persistent threats by identifying anomalous behaviour and enabling timely response. Advanced approaches, such as Attention-GAN and hybrid federated learning for 5G-enabled smart cities, improve detection accuracy, privacy, and scalability. However, these methods are computationally intensive and require continuous retraining to counter adaptive attackers [5,6,31,32].

6.4. Cloud-based protection services help mitigate DDoS, malware, and phishing attacks through continuous monitoring and blocking of malicious activity. This reduces the attack surface, improves incident response, centralizes policy enforcement, and enables faster recovery after a breach [5,6,33].

6.5. Securing 5G networks requires comprehensive strategies, including robust authentication and authorization, monitoring of abnormal behaviour, and coordination among telecommunications providers. Protocols such as Transport Layer Security should be used to protect communications, while user training and awareness programs can reduce social engineering threats [5,6,34].

6.6. Machine learning and AI can strengthen cyber defense by training models on large datasets to analyze attack behavior and respond when threats are detected. For example, SentinelOne uses machine learning for endpoint security, helping prevent ransomware and other malware attacks [5,6,13,35].

6.7. Cyber defense must evolve with adversary tactics. The MITRE Center for Threat-Informed Defense promotes a continuous feedback loop that uses live threat intelligence to update defense strategies. Frameworks such as MITRE ATT&CK make this an ongoing, improving process, though it requires sustained organizational investment in threat intelligence integration [5,6,36].

6.8. An agile, multi-layered defense should combine proactive penetration testing, AI-enabled monitoring, dynamic threat updates, and post-quantum cryptography preparedness. Together, these measures create a resilient security posture capable of addressing current threats and anticipating future ones. Cross-sector collaboration, consistent regulation, and continuous employee training are essential to its success [5,6].

7. CONCLUSION

Modern cyber threats combine technical attacks with social engineering and the exploitation of business processes. Ransomware, phishing, identity theft, payment fraud, vulnerability exploitation, DDoS attacks, cloud misconfigurations, supply-chain compromises, and AI-driven impersonation pose significant risks. Effective mitigation requires layered

 This work is licensed under a Creative Commons Attribution 4.0 International License

DOI: 10.17148/IJARCCE.2026.1510116

security measures, including strong authentication, regular patching, least-privilege access, continuous monitoring, secure data management, resilient backups, payment verification, user awareness, and tested incident-response plans. Continuous evaluation and adaptation are essential to address evolving threats. Although no single control ensures complete protection, coordinated prevention, detection, response, and recovery can significantly reduce cybersecurity risks.

REFERENCES

[1]. Data Security Council of India (DSCI) and Seqrite, "India Cyber Threat Report 2025", https://www.dsci.in/files/content/knowledge-centre/2024/India-Cyber-Threat-Report-2025.pdf. (Accessed on 20 September 2026).

[2]. Global Cybersecurity Outlook 2026. January 2026 Report © 2026 World Economic Forum. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf. (Accessed on 21 September 2026).

[3]. "Types Of Cyber Attacks: Top 20 Cyber Threats & Prevention Strategies", https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks, (Accessed on 22 September 2026).

[4]. "Top Cybersecurity Threats to Watch in 2026". https://onlinedegrees.sandiego.edu/top-cyber-security-threats/, (Accessed on 25 September 2026).

[5]. Cotrina, L.; León, P.; Reyes, C.; Arbulú Ballesteros, M.; Guzmán, M.; Castillo, J.; Acosta, R.; Morales, A. Cyber Crimes: A Systematic Review of Evolution, Trends, and Research Approaches. J. Educ. Soc. Res. 2024, 14, 96. [CrossRef].

[6]. Abdullah, M.; Nawaz, M.M.; Saleem, B.; Zahra, M.; Ashfaq, E.b.; Muhammad, Z. Evolution Cybercrime—Key Trends, Cybersecurity Threats, and MitigationStrategies from Historical Data. Analytics 2025, 4, 25. https://doi.org/10.3390/analytics4030025.

[7]. Kang Leng Chiew, Kelvin Sheng Chek Yong∗, Choon Lin Tan. " A survey of phishing attacks: Their types, vectors and technical approaches". 0957-4174/© 2018 Elsevier Ltd. http://www.elsevier.com/locate/esw, https://doi.org/10.1016/j.eswa.2018.03.050.

[8]. Anuradha Chakraborty and Sanyogita Tiwari. " International Journal of Criminal, Common and Statutory Law 2025; 5(1): 04-07 E-ISSN: 2789-9500 P-ISSN: 2789-9497 DOI: https://doi.org/10.22271/27899497.2025.v5.i1a.110.

[9]. Sukhdev Singh. " Cyber Security Threats and Mitigation Strategies in the Digital Era". Jagannath University Journal of Research and Review (JUJRR), Volume No. 01, Issue No. 02 (July, 2025) ISSN: 3049-1290.

[10]. Ashraful Goni,Md. Umor Faruk Jahangir, Rajarshi Roy Chowdhury. " A Study on Cyber security: Analyzing Current Threats, Navigating Complexities, and Implementing Prevention Strategies" International Journal Of Research And Scientific Innovation (IJRSI) ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume X Issue XII December 2023.

[11]. Frank Cremer , Barry Sheehan, Michael Fortmann, Arash N. Kia,Martin Mullins,Finbarr Murphy. Stefan Materne. "Cyber risk and cybersecurity: a systematic review of data availability". The Geneva Papers on Risk and Insurance - Issues and Practice (2022) 47:698–736, https://doi.org/10.1057/s41288-022-00266-6.

[12]. Abdulbasit A. Darem , Asma A. Alhashmi , Tareq M. Alkhaldi Abdullah M. Alashjaee , Sultan M. Alanazi , And Shouki A. Ebad. Cyber Threats Classifications and Countermeasures in Banking and Financial Sector. VOLUME 11, 2023 IEEE Access, Digital Object Identifier 10.1109/ACCESS.2023.3327016

[13]. Ahsan, M.; Nygard, K.E.;Gomes, R.; Chowdhury, M.M.; Rifat,N.; Connolly, J.F. Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning—A Review. J. Cybersecur. Priv. 2022, 2, 527–555. https://doi.org/10.3390/jcp2030027

[14]. R. B. Amle. "Overview of Cyber Security, Attacks, Challenges and Solutions: A Review", Journal of Systems Engineering and Electronics (ISSN NO: 1671-1793) Volume 32 ISSUE 12 2022, https://doi.org/10.5281/zenodo.20741197.

[15]. Kamran Razzaq , Mahmood Shah, Mohammad Fattahi & Jing Tang. "Empowering machine learning for robust cyber-attack prevention in online retail: an integrative analysis". Humanities And Social Sciences Communications | (2025)12:733 | https://doi.org/10.1057/s41599-025-04636-y.

[16]. Kang Leng Chiew, Kelvin Sheng Chek Yong∗, Choon Lin Tan. A survey of phishing attacks: Their types, vectors and technical approaches". ww.elsevier.com/locate/eswa, https://doi.org/10.1016/j.eswa.2018.03.050.

[17]. Akashdeep Bhardwaj , Fadi Al-Turjman , Varun Sapra , Manoj Kumar , Thompson Stephan. "Privacy-aware detection framework to mitigate new-age phishing attacks" Computers and Electrical Engineering 96 (2021) 107546, www.elsevier.com/locate/compeleceng https://doi.org/10.1016/j.compeleceng.2021.107546

[18]. Rafał Leszczyna. "Review of cybersecurity assessment methods:Applicability perspective", computer & security 108 (2021) 102376, www.elsevier.com/locate/cose. https://doi.org/10.1016/j.cose.2021.102376.



International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 10, October 2026
DOI: 10.17148/IJARCCE.2026.1510116

[19]. Akash Jain, Dr. Pradeep Yadav. "A Machine Learning-Based Framework for Intelligent Cybersecurity Threat Detection and Prevention ", Vol. 15, Issue 9, September 2026 © International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE) ISSN (O) 2278-1021, ISSN (P) 2319-5940.
[20]. Wisnioski, M.H. Engineers for Change: Competing Visions of Technology in 1960s America; MIT Press: Cambridge, MA, USA, 2012.
[21]. Hauben, M. History of ARPANET. Site l'Inst. Super. Eng. Porto 2007, 17, 1–20.
[22]. Saltzer, J.H.; Schroeder, M.D. The Protection of Information in Computer Systems. Proc. IEEE 1975, 63, 1278–1308. [CrossRef]
[23]. de Jong, B. The KGB in Eastern Europe during the Cold War: On agents and confidential contacts. J. Intell. Hist. 2005, 5, 85–103.
[24]. Kephart, J.O.; Sorkin, G.B.; Chess, D.M.; White, S.R. Fighting computer viruses. Sci. Am. 1997, 277, 88–93. [CrossRef].
[25]. Chen, Q.; Bridges, R.A. Automated behavioral analysis of malware: A case study of wannacry ransomware. In Proceedings of the 2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA), Cancun, Mexico, 18–21 December 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 454–460.
[26]. Fayi, S.Y.A. What Petya/NotPetya ransomware is and what its remidiations are. In Information Technology-New Generations: Proceedings of the 15th International Conference on Information Technology, Las Vegas, NV, USA, 16–18 April 2018; Springer: Berlin/Heidelberg, Germany, 2018; pp. 93–100.
[27]. Schoop, M.; Vogl, R.; Lins, S. Generative AI in Cybersecurity: Risks, Challenges, and Opportunities. arXiv 2025, arXiv:2505.23733.
[28]. Akinbowale, O.E.; Adegboyega, O.; Okere, W. The impact of cybercrime on the banking sector: A balanced scorecard analysis. J. Financ. Crime 2020, 27, 867–884. [CrossRef].
[29]. Ni, T.; Lan, G.; Wang, J.; Zhao, Q.; Xu, W. Eavesdropping mobile app activity via {Radio-Frequency} energy harvesting. In Proceedings of the 32nd USENIX Security Symposium (USENIX Security 23), Anaheim, CA, USA, 9–11 August 2023; pp. 3511–3528.
[30]. EC-Council. Global Ethical Hacking Report: 83% of Ethical Hackers Experience AI-Driven Attacks. 2024. GlobeNewswire. Available online: https://www.globenewswire.com/news-release/2024/01/24/2815519/0/en/Global-Ethical-Hacking-Report-83-of-Ethical-Hackers-Experience-AI-Driven-Attacks.html (Accessed on 20 September 2026).
[31]. Sen, M.A. Attention-GAN for anomaly detection: A cutting-edge approach to cybersecurity threat management. arXiv 2024,arXiv:2402.15945.
[32]. Reis, M.J. AI-Driven Anomaly Detection for Securing IoT Devices in 5G-Enabled Smart Cities. Electronics 2025, 14, 2492. [CrossRef].
[33]. Kumar, S.; Dwivedi, M.; Kumar, M.; Gill, S.S. A comprehensive review of vulnerabilities and AI-enabled defense against DDoS attacks for securing cloud services. Comput. Sci. Rev. 2024, 53, 100661. [CrossRef].
[34]. Shobowale, K.; Mukhtar, Z.; Yahaya, B.; Ibrahim, Y.; Momoh, M. Latest advances on security architecture for 5G technology and services. Int. J. Softw. Eng. Comput. Syst. 2023, 9, 27–38. [CrossRef].
[35]. Licitra, S. Leveraging AI Techniques for Automated Security Incident Response. Ph.D. Thesis, Politecnico di Torino, Torino, Italy, 2024.
[36]. MITRE Center for Threat-Informed Defense. More Threat-Informed in More Ways with More Defenders. 2024. MITRE. Available online: https://ctid.mitre.org/blog/2024/05/02/more-threat-informed-in-more-ways-with-more-defenders/ (Accessed on 10 September 2026).

 This work is licensed under a Creative Commons Attribution 4.0 International License