A Review of Artificial Intelligence's Impact on Cybersecurity in the Big Data Era

Esra Çakir and A Çağrı Tolga(✉)

Galatasaray University, Çırağan Cad. No .36, 34357 Istanbul, Turkey
{ecakir,ctolga}@gsu.edu.tr

Abstract. This study explores the imperative role of artificial intelligence (AI) for enhancing cybersecurity in the big data environment. With the limitations of traditional cybersecurity approaches in keeping up with the increasing volume, sophistication, and complexity of cyber-attacks, AI and big data analytics (BDA) present viable options for real-time detection, adaptive response, and proactive defense mechanisms. The study discusses the usage of AI technologies like machine learning and deep learning in the most significant cybersecurity tasks such as threat detection, risk analysis, incident response, and protection of critical infrastructure. While the utilization of AI enhances the effectiveness and efficiency of cybersecurity operations, it also poses serious challenges. Some of these challenges include data privacy risks, ethical problems, and vulnerabilities to adversarial AI attacks with the ability to exploit or manipulate intelligent systems. This paper comprehensively discusses these challenges and proposes viable strategies to mitigate the associated risks. With an in-depth analysis of the strengths and weaknesses of AI-powered cybersecurity, the manuscript provides important insights for researchers, policymakers, and practitioners. It concludes by outlining potential research directions and practical implications for the use of AI and big data analytics in designing more advanced and intelligent cybersecurity systems. The findings underscore the capability of AI to transform cybersecurity frameworks in a digitized and data-driven world.

Keywords: Artificial Intelligence (AI) · Big Data Analytics (BDA) · Cybersecurity · Review · Threat Detection · Transformative Impact

1 Introduction

The advent of the age of the digital era has ushered in unparalleled advancements that have transformed communication, business, and access to information. Along with this era came increasingly complex cybersecurity threats. The requirement for the security of data online has increased manifold as people and organizations are threatened by different types of threats, from basic viruses and worms to complex hacking and distributed denial-of-service (DDoS) attacks [4]. Early on, cybersecurity was mainly reliant on rule-based systems and signature identification, which were effective against known threats. However, the traditional cybersecurity methods often prove to be insufficient

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2026
O. Gervasi et al. (Eds.): ICCSA 2025 Workshops, LNCS 15886, pp. 182–192, 2026.
https://doi.org/10.1007/978-3-031-97576-9_12

when faced with rapidly evolving threats, polymorphic malware, and zero-day exploits [2]. These emerging attack techniques are specifically designed to evade signature-based systems, rendering the traditional solutions ineffective in today′s dynamic and increasingly adversarial cyber landscape.

In addition, the exponential increase in data—so-called “big data"—has added complexity to the cybersecurity environment. This constantly increasing flow of structured and unstructured data provides rich information on user activity and possible threats but also inundates conventional systems that were not built for this volume [7]. Amidst this, artificial intelligence (AI) has become a game-changing force in combating cybercrime. AI enables real-time threat detection, predictive analysis, and rapid, automated responses to incidents—capabilities that are critical when dealing with the speed and complexity of modern cyberattacks [2, 8]. AI-driven big data analytics (BDA), leveraging techniques such as machine learning (ML), deep learning (DL), and natural language processing (NLP), allows cybersecurity systems to identify unusual patterns and respond to potential threats with unprecedented accuracy and speed [2, 4, 7].

This paradigm has particular significance to the security of critical infrastructure systems, including energy networks, financial systems, health care systems, and transportation systems, which are becoming more networked and susceptible to cyber-attacks [2, 3]. With those critical infrastructures being digitalized, the danger of weaknesses to cybersecurity issues increases, thereby rendering AI-boosted defensive mechanisms not only useful but essential. BDA and AI enable a more resilient, self-upgrading, and adaptive security solution that enhances the overall capacity of organizations to sense, detect, and neutralize threats in real time. Moreover, increasing reliance on AI in industries like marketing, customer care, and logistics necessitates a similar emphasis on safeguarding sensitive data [1]. Security of such information not only includes aspects of cybersecurity but also involves the public trust, adherence to regulatory requirements, and fulfillment of ethical responsibilities. Hence, the use of AI-driven big data analytics is transforming the cybersecurity paradigm. By transitioning from a purely reactive posture to the adoption of intelligent, predictive, and automated responses, organizations have enhanced abilities to deal with the dangers of an ever-changing digital ecosystem. The modern security paradigm acknowledges the limitations of traditional tools and integrates cutting-edge technologies to protect the future of digital infrastructures in different industries. The combination of artificial intelligence, big data analytics, and cybersecurity represents a turning point—one that enables the creation of a more secure and robust digital age.

This study discusses the deep influence of artificial intelligence on cybersecurity in the era of big data. It discusses the application of AI in a wide range of areas in cybersecurity, such as threat detection, risk analysis, incident handling, and critical infrastructure protection. Further, the challenges associated with artificial intelligence-driven cybersecurity solutions—such as data privacy concerns and ethical considerations, the threat of adversarial AI, and the impact of cyberattacks on data integrity—are discussed, along with possible mitigation strategies [1, 5, 6].

The rest of this paper is structured as follows: Sect. 2 outlines the role of AI and big data analytics in cybersecurity, thus highlighting their pivotal role in modern defense strategies. Section 3 deals with particular applications of AI and BDA, including threat detection, risk analysis, and infrastructure protection. Section 4 discusses concerns

such as data privacy, ethical issues, and adversarial AI, suggesting proposed solutions. Section 5 discusses future directions for research and implementation of AI in cybersecurity. Finally, Sect. 6 concludes by summarizing major findings and outlining the trans-formative potential of AI and BDA for enhancing cybersecurity.

2 Artificial Intelligence and Big Data Analytics in Cybersecurity

Artificial intelligence (AI) has become a transformative force in the domain of cybersecurity with the potential to improve security solutions and bring in new defense mechanisms against cyber-attacks [2, 7, 8]. The area of AI encompasses creating computational systems with the ability to execute tasks traditionally needing human intellectual capabilities, including learning, problem-solving, and decision-making. Artificial intelligence (AI) is used in the area of cybersecurity to scrutinize large data sets, detect recurring patterns and enable the automation of security actions [2, 6]. Major AI approaches that are of special relevance to cybersecurity include machine learning (ML), deep learning (DL), and natural language processing (NLP) [4, 7, 8].

Machine Learning (ML) algorithms enable systems to learn from experience without explicit programming. Supervised learning, unsupervised learning, and reinforcement learning are forms of ML applied in cybersecurity. Logistic Regression and Gaussian Naive Bayes are a few of the models applied in addressing classification problems where the result of a categorical dependent variable is to be estimated [4, 7].

Deep Learning (DL), as a subset of Machine Learning (ML), employs artificial neural networks with many layers to process intricate data. This emerging technology has been a primary driving force in revolutionizing the domain of cybersecurity and has been employed to bolster security controls, detect threats, and minimize risks in various industries [4, 8].

Natural Language Processing (NLP) enables computers to comprehend, analyze, and process human language [8]. NLP, in the domain of cybersecurity, can be applied to the analysis of text-based information, i.e., security reports and threat intelligence, in a bid to glean pertinent information and detect possible threats [4].

AI enhances traditional cybersecurity measures by increasing threat detection, automating incident response, and enabling predictive analysis [2, 8]. The era of digital information has witnessed an exponential proliferation of data, commonly referred to as "big data" [2, 6]. Big data, as characterized by its volume, velocity, and variety, presents both risks and opportunities to cybersecurity. Big data analytics involves the process of collecting, storing, and analyzing these huge volumes of data to gain insightful knowledge [6].

In cybersecurity, the application of big data analytics is at the heart of enhancing artificial intelligence (AI) systems [8]. Through large datasets analysis, AI algorithms are able to detect anomalies, uncover advanced cyber threats, and enhance the quality of risk analysis [2, 6]. The application of AI-driven big data analytics (BDA) presents a cutting-edge method for enhancing cybersecurity architectures through real-time threat detection, predictive analytics, and automated response actions [2].

AI-powered cybersecurity solutions integrate AI techniques and big data analytics to provide efficient security solutions. These solutions typically consist of modules such

as threat intelligence platforms, security information and event management (SIEM) systems, and response systems [2, 6]. Data flow and decision-making in these solutions include data collection and preprocessing, AI-powered analysis, threat detection and alerting, and automated or human-based response [8].

3 Application Areas of Artificial Intelligence and Big Data in Cybersecurity

In cybersecurity, big data analytics (BDA) and artificial intelligence (AI) are key technologies in most application domains. These technologies are most prominent in applications like threat detection and mitigation, risk assessment and management, incident response, and protection of critical infrastructures.

Threat Detection and Prevention: Another critical use of artificial intelligence in the realm of cybersecurity involves the detection and prevention of threats. AI has the ability to scan vast amounts of data in real-time, thus detecting unusual patterns or anomalies that could indicate potential cyber threats. By identifying anomalies in usual patterns of behavior, artificial intelligence is able to identify intrusions, like unauthorized access attempts or malicious behavior, in advance before they can inflict serious damage [9]. This enables earlier response and mitigation of eventual threats. AI-driven tools also better detect malware by monitoring its behavior, as opposed to purely signature-based detection techniques, which may lag behind in identifying new variants [12]. Confronted with advanced persistent threats (APTs), the capacity of artificial intelligence (AI) to manage large amounts of data and to ingest data from emerging attack vectors continuously enables it to identify even highly elaborate cyber threats. In addition, AI is employed to create sophisticated defense mechanisms, like automated firewalls, intrusion detection systems, as well as response mechanisms, that can successfully thwart threats in real-time. AI′s capacity to constantly evolve with new attack strategies also ensures that security controls are efficient in the face of emerging threats.

Risk Management and Analysis: AI and BDA are revolutionizing risk management and analysis with the ability of automatic risk discovery and prioritization of potential cybersecurity threats. Traditional risk analysis is time-consuming and typically fails to account for the scale and complexity of modern cyber space. Computer algorithms, however, can consider massive amounts of information and can provide a more accurate analysis of cybersecurity vulnerabilities and threats that might otherwise have gone undetected. This enables companies to make more informed decisions about which threats need to be overcome right away and others that can be managed over time [11, 15, 19]. AI is also capable of discovering vulnerabilities in system protocols and architectures, pointing out the areas that should be patched or reinforced to prevent future attacks [10, 16]. AI can predict the likelihood of specific types of attacks occurring through machine learning and data-driven analysis, giving organizations the chance to implement proactive security measures. The transition from reactive to proactive security measures allows for improved planning and resource distribution, thereby lessening the impact of cyber events. Additionally, artificial intelligence can strengthen national cybersecurity systems by allowing for a greater understanding of emerging threats and vulnerabilities on a larger scale [9].

Incident Response: During the occurrence of a cyberattack or security incident, artificial intelligence has the potential to significantly enhance incident response time and the efficacy of remedial measures. AI-enabled systems can automatically detect and react to security incidents, thereby decreasing the time interval between threat detection and mitigation. This aspect is particularly crucial for circumstances where cyber threats are ephemeral in nature and demand real-time intervention. In addition, AI accelerates post-incident analysis by quickly examining large volumes of data to determine the cause and scope of the breach, allowing valuable intelligence to guide future defense strategies. By automating some aspects of incident management, AI reduces the workload for cybersecurity teams, allowing them to focus on high-priority tasks and strategic decision-making. Additionally, artificial intelligence facilitates the sharing and collective use of threat intelligence across different organizations and industries, thus enhancing overall security measures. Leveraging AI-powered tools makes it possible to share threat intelligence instantly, which speeds up response times to large-scale cyberattacks and helps identify patterns or tactics that attackers may use on several networks.

Protection of Critical Infrastructures: Protection of critical infrastructures—e.g., those in the energy, transportation, and healthcare sectors—is one domain where AI and BDA are especially vital. These sectors are increasingly reliant on digital systems, making them attractive targets for cyberattacks that can have catastrophic consequences for public safety and national security. Artificial intelligence may be employed to improve the security of such systems by observing their activities round the clock, identifying possible vulnerabilities, and taking action against threats in real time [10, 18, 23]. Artificial intelligence is especially crucial for securing smart cities and the Internet of Things (IoT), which are being progressively incorporated into cities and everyday life. IoT device expansion has widened the attack surface for hackers, yet AI can provide real-time monitoring and automatic defense systems to secure these devices. With the ability to process enormous amounts of data from connected devices, AI has the capability to detect anomalies that could indicate a breach or attack on critical infrastructure [13]. Additionally, artificial intelligence can enhance the national security systems' defense strategies by identifying and eliminating potential threats to essential sectors such as energy infrastructures or transportation systems, which are often targeted by sophisticated adversaries [14, 22].

4 Challenges and Solution Alternatives

Artificial Intelligence (AI) and Big Data Analytics (BDA) hold immense potential in revolutionizing cybersecurity. However, the deployment of these technologies is accompanied by numerous challenges that need to be addressed to ensure their effective and ethical application. This section outlines the primary challenges and presents solution proposals, supported by recent literature.

Data Privacy and Security Issues: The integration of AI and BDA into cybersecurity requires access to and processing of extensive volumes of sensitive data. This data aggregation increases vulnerability to breaches, unauthorized access, and misuse [24–26]. Compliance with privacy laws such as the General Data Protection Regulation

(GDPR) further complicates these processes, demanding stringent controls over data handling [27–29]. Recent works highlight how data security frameworks, encryption protocols, and secure federated learning can mitigate these concerns [30, 31].

Algorithmic Bias and Ethical Concerns: AI systems trained on biased datasets risk perpetuating discrimination and unfair practices [32, 33]. In cybersecurity, this can result in disproportionate surveillance or misclassification of threat actors based on flawed data inputs [34, 35]. Furthermore, the opacity of certain AI models—often termed the "black box" problem—limits interpretability and accountability [36, 37]. Addressing these issues demands transparent AI design, bias auditing, and inclusive datasets [38].

Potential for Attackers to Misuse AI (AI vs. AI): While AI enhances defensive capabilities, it also empowers adversaries. Malicious actors are leveraging AI to develop polymorphic malware, automate phishing, and craft advanced social engineering attacks [39–41]. This escalating "AI arms race" necessitates the development of proactive AI systems capable of countering AI-driven threats in real-time [42, 43].

AI and BDA offer powerful tools for cybersecurity, but their implementation comes with various challenges that need to be addressed to ensure their effective and ethical use. Proposed solutions to these challenges are supported by recent literature. Federated learning enhances privacy by allowing decentralized model training without the need to share raw data [30, 33]. Similarly, blockchain technology is being employed to ensure data immutability, traceability, and secure transactions within cybersecurity contexts [27, 38, 42]. To manage the ethical and legal aspects of AI usage in cybersecurity, robust data governance policies are essential. These policies should include clear standards for data collection, processing, and consent, as well as frameworks for organizational accountability [24, 31]. Adhering to international standards such as the GDPR and establishing independent oversight bodies can help ensure compliance and ethical integrity [28, 29]. Given the evolving nature of cyber threats, AI models must undergo continuous learning. This involves regular retraining with up-to-date threat intelligence and feedback loops to improve performance [40, 41]. Dynamic threat modeling and adaptive security architectures are crucial for resilience. AI should augment, not replace, human expertise. Integrating human-in-the-loop mechanisms ensures critical oversight and fosters trust [32, 34]. Collaborative ecosystems that combine machine efficiency with human judgment are key to comprehensive cybersecurity defense. In conclusion, while AI and BDA offer powerful tools for cybersecurity, their benefits must be balanced with ethical and technical safeguards. Implementing the proposed solutions can help mitigate challenges and enhance the security posture of digital infrastructures.

5 Future Perspectives

The future cybersecurity environment will be significantly influenced by the ongoing development of Artificial Intelligence (AI) and Big Data Analytics (BDA). With the growing sophistication of cyber threats, next-generation AI technologies and novel computational paradigms will assume an ever more vital function in the protection of digital infrastructures. This section explores the future trajectory of AI and BDA in cybersecurity, namely the emergence of generative AI, the potential impact of quantum computing, and the importance of international collaboration and standards.

AI and BDA have transformed the landscape of cybersecurity already by improving threat detection, risk management, and incident response. However, the speed with which the technology is evolving guarantees even greater development in the years to come. The future of AI for the domain of cybersecurity is the continued development of more and more advanced machine learning algorithms as well as neural networks that are capable of processing massive and com-plex data sets. These technologies will enable more accurate threat predictions, faster responses to cyber-attacks, and enhanced system resilience [9, 10, 12]. BDA will play a pivotal role in collecting and analyzing data from varied sources, facilitating real-time monitoring and better-informed decision-making. As artificial intelligence models continue to advance to learn from various types of data, not only will they enhance current cybersecurity frameworks, but they also will allow for the creation of new, proactive defense systems that can foresee and fend off cyber-attacks before they materialize [11, 19].

A significant advancement in the field of artificial intelligence is the creation of generative AI, which has the ability to transform the domain of cybersecurity. Such AI, comprising models like GPT (Generative Pre-trained Transformer) and other deep learning techniques, can generate original content or replicate intricate scenarios founded on existing knowledge. Within cybersecurity, the technology can be utilized to create synthetic data to train artificial intelligence models, facilitate the creation of simulated cyberattack scenarios to test defensive measures, and even develop sophisticated countermeasures to new threats. The application of generative AI has the potential to improve the capacity of cybersecurity systems to evolve with new and unfamiliar attack vectors, thereby rendering them more resilient to unexpected threats [12, 13]. Still, this circumstance also rings alarm bells since generative AI can also be utilized by adversaries to synthesize more complex and misleading attacks, for example, deepfakes or malware. Consequently, while the immense potential that generative AI embodies is greatly significant, its dual nature must be controlled and monitored rigorously to avert its misuse [9, 14].

Quantum computing is another emerging technology that is set to transform the cybersecurity landscape. Quantum computers use concepts of quantum mechanics to solve problems that are currently unsolvable by conventional computers. Quantum computing in cybersecurity can potentially enhance security, as well as pose significant challenges. On the positive side, quantum cryptography has the potential to enable very secure communications methods through quantum key distribution (QKD), which is theoretically immune to unauthorized eavesdropping. This development can signal a revolutionizing era for secure communications, particularly with regard to transmitting sensitive data [13]. However, the threat posed by quantum computing towards existing encryption methods is significant. Quantum algorithms, such as Shor′s algorithm, can potentially weaken widely used cryptographic protocols like RSA and ECC (Elliptic Curve Cryptography) by efficiently factoring large numbers. This capability poses a significant risk to current encryption systems and could force a wholesale change of worldwide cybersecurity protocols [18, 19]. Hence, the development of quantum-resistant encryption methods is increasingly becoming a top agenda item for cybersecurity experts and organizations worldwide.

The growing sophistication and scope of cyber threats demand more international collaboration and the formulation of international cybersecurity standards. Cyberattacks are borderless, and their impact can be experienced in various nations and sectors, thus necessitating international collaboration in fighting cybercrime and securing digital infrastructures. It is important to have international forums for information sharing, threat intelligence, and joint response mechanisms in order to create a more secure cyber ecosystem [18]. The role played by organizations such as the European Union Agency for Cybersecurity (ENISA) and the Global Forum on Cyber Expertise (GFCE) in bringing people together and standardizing is critical. In addition, bringing countries together and aligning cybersecurity law and regulations, including respecting standards like the General Data Protection Regulation (GDPR), is critical in building a single global cybersecurity framework [22, 23]. In the years ahead, international co-operation and agreements on issues such as cybercrime, critical infrastructure protection, and digital sovereignty will become ever more important as digital transformation continues to accelerate.

6 Conclusion

In conclusion, the convergence of Artificial Intelligence (AI) and Big Data Analytics (BDA) within the realm of cybersecurity has been a significant change in how organizations identify, respond to, and neutralize cyber threats. As the frequency and complexity of cyberattacks continue to rise, conventional methods of cybersecurity have found it challenging to keep up. Nonetheless, AI and BDA present enhanced analysis and prediction capabilities that have transformed the effectiveness of contemporary cybersecurity systems. These technologies allow organizations to transition from reactive to proactive defense mechanisms, enabling the anticipation and prevention of threats before they inflict damage. Real-time monitoring, anomaly detection, intelligent threat classification, and automated response mechanisms are some of the innovations that AI and BDA drive, giving rise to a stronger and more effective cybersecurity posture.

The strategic significance of AI and BDA for securing critical infrastructure and digital assets has become increasingly evident. Sectors such as healthcare, finance, energy, transportation, and government infrastructures now rely on data-driven insights for operational security and continuity. AI-powered cybersecurity solutions, with the ability to handle vast amounts of structured and unstructured data at speed, are able to identify subtle patterns of threats that could evade detection by human analysts. In addition, such systems allow for adaptive learning, which makes them evolve according to the new threat vectors. With the digital landscape becoming more and more interconnected and complex, the need for scalable and smart cybersecurity solutions is likely to increase, making AI and Big Data Analytics key components of any successful cyber defense strategy.

For all their potential to revolutionize, the use of AI and BDA in cyberse-curity also introduces new issues that need to be carefully managed. Among the most important of these is the interpretability of AI models. In order for cybersecurity practitioners to make sound decisions, AI systems need to provide transparency and explainability in their reporting. Without good visibility into how models reach their conclusions, trust

and accountability can be undermined. XAI research is thus crucial in filling this gap and improving the performance of AI-based cybersecurity solutions.

Furthermore, the regulatory and ethical aspects of the use of AI and BDA cannot be ignored. Compliance with data protection and privacy laws, as well as adherence to ethical requirements, is imperative for the responsible deployment of these technologies. With AI systems accessing sensitive information and making decisions with high implications, it is imperative that their conformity to human rights and societal values is guaranteed through stringent governance and supervision. Moreover, concern is increasing around adversarial artificial intelligence, whereby malicious actors cause AI models to deceive or breach cybersecurity. To make AI systems more resilient to these attacks involves ongoing innovation and the incorporation of adversarial training and strong validation procedures.

Looking ahead, future research should emphasize the development of transparency in artificial intelligence models, the integration of ethical frameworks, and the exploration of the convergence of artificial intelligence with other emerging technologies, such as quantum computing, blockchain, and generative artificial intelligence. These synergies have the potential to radically change the face of cybersecurity, bringing new paradigms to encryption, authentication, and threat detection. In addition, interdisciplinary efforts among computer scientists, cybersecurity experts, ethicists, and policymakers will be important in guiding the development of secure and ethically sound AI-based systems.

Ultimately, as cybersecurity threats evolve, so too will the technologies and strategies that counter them. AI and BDA will be at the forefront of this evolution, offering powerful tools to secure digital environments from an ever-more varied array of threats. Through investments in innovation, regulation, and education, stakeholders can ensure the future of cybersecurity is both effective and ethical.

Acknowledgements. "This work has been supported by the Scientific Research Projects Commission of Galatasaray University."

References

1. Alhitmi, H.K., Mardiah, A., Al-Sulaiti, K.I., Abbas, J.: Data security and privacy concerns of AI-driven marketing in the context of economics and business field: an exploration into possible solutions. Cogent Bus. Manage. **11**(1), 2393743 (2024)
2. Maharjan, P.: The role of artificial intelligence-driven big data analytics in strengthening cybersecurity frameworks for critical infrastructure. Glob. Res. Perspect. Cybersecurity Gov. Policy Manage. **7**(11), 12–25 (2023)
3. Salako, A.O., Fabuyi, J.A., Aideyan, N.T., Selesi-Aina, O., Dapo-Oyewole, D.L., Olaniyi, O.O.: Advancing information governance in AI-driven cloud ecosystem: Strategies for enhancing data security and meeting regulatory compliance. Asian J. Res. Comput. Sci. **17**(12), 66–88 (2024)
4. Salem, A.H., Azzam, S.M., Emam, O.E., Abohany, A.A.: Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. J. Big Data **11**(1), 105 (2024)
5. Vadisetty, R.: The effects of cyber security attacks on data integrity in AI. In: 2024 International Conference on Intelligent Computing and Emerging Communication Technologies (ICEC), pp. 1–6 (2024)

6. Wickramasinghe, A.: An evaluation of big data-driven artificial intelligence algorithms for automated cybersecurity risk assessment and mitigation. Int. J. Cybersecurity Risk Manage. Forensics Compliance **7**(12), 1–15 (2023)
7. Weng, Y., Wu, J.: Leveraging artificial intelligence to enhance data security and combat cyber attacks. J. Artif. Intell. Gen. Sci. (JAIGS) ISSN: 3006–4023, **5**(1), 392–399 (2024)
8. Al Siam, A., Alazab, M., Awajan, A., Faruqui, N.: A comprehensive review of AI's current impact and future prospects in cybersecurity. IEEE Access (2025)
9. Tatar, Ü., Çalik, O., Çelik, M., Karabacak, B.: A comparative analysis of the national cyber security strategies of leading nations. In: International Conference on Cyber Warfare and Security. Academic Conferences International Limited, p. 211 (2014)
10. Yang, J., Huang, L., Ma, H., Xu, Z., Yang, M., Guo, S.: A 2D-graph model-based heuristic approach to visual backtracking security vulnerabilities in physical protection systems. Int. J. Crit. Infrastruct. Prot. **38**, 100554 (2022)
11. Khan, R.S., Sirazy, M.R.M., Das, R., Rahman, S.: An AI and ml-enabled framework for proactive risk mitigation and resilience optimization in global supply chains during national emergencies. Sage Sci. Rev. Appl. Mach. Learn. **5**(2), 127–144 (2022)
12. Liu, Z., Zheng, J., Wang, S., Muhammad, A.: A novel deep learning based security assessment framework for enhanced security in swarm network environment. Int. J. Crit. Infrastruct. Prot. **38**, 100540 (2022)
13. Nadir, I., Mahmood, H., Asadullah, G.: A taxonomy of IoT firmware security and principal firmware analysis techniques. Int. J. Crit. Infrastruct. Prot. **38**, 100552 (2022)
14. Boyko, S.M.: Political and legal framework of the international information security system: Russian approaches and initiatives. Russ. J. World Politics Law Nations **1**(1–2), 4–22 (2023)
15. Seumo Ntsiepdjap, B.: Ph.D. in cyber security administration: dynamic risk assessment for critical infrastructures under attack. Int. J. Adv. Res. (Indore) **10**(09), 868–908 (2022)
16. Kaul, D., Khurana, R.: AI to detect and mitigate security vulnerabilities in APIs: encryption, authentication, and anomaly detection in enterprise-level distributed systems. Eigenpub Rev. Sci. Technol. **5**(1), 34–62 (2021)
17. Donnelly, P., Abuhmida, M., Tubb, C.: The drift of industrial control systems to pseudo security. Int. J. Crit. Infrastruct. Prot. **38**, 100535 (2022)
18. Khurana, R.: Fraud detection in ecommerce payment systems: The role of predictive AI in real-time transaction security and risk management. Int. J. Appl. Mach. Learn. Comput. Intell. **10**(6), 1–32 (2020)
19. Kure, H.I., Islam, S., Mouratidis, H.: An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. Neural Comput. Appl. **34**(18), 15241–15271 (2022)
20. Di Feo, M., Martino, L.: Public–private partnership (PPP) in the context of European union policy initiatives on critical infrastructure protection (CIP) from cyber attacks. In: Governing Complexity in Times of Turbulence. Edward Elgar Publishing, pp. 54–79 (2022)
21. Gasztold, A., Akrap, G.: Introduction to the special issue: critical infrastructure protection—the challenge of resilience. Secur. Defence Q. **39** (2022)
22. Heino, O.: Intelligent terrorism as a security threat to critical infrastructure. Secur. Defence Q. **39**(3), 33–44 (2022)
23. Putro, P.A.W., Sensuse, D.I.: Review of security principles and security functions in critical information infrastructure protection. Int. J. Saf. Secur. Eng. **12**(4), 459–465 (2022)
24. Manea, O.A., Zbuchea, A.: The convergence of artificial intelligence and cybersecurity: innovations, challenges, and future directions. In: Economic and Political Consequences of AI: Managing Creative Destruction, pp. 321–350. IGI Global Scientific Publishing (2025)
25. Chen, N.: Data security issues and countermeasure suggestions for financial big data: a literature review. Adv. Econ. Manage. Political Sci. **41**, 55–60 (2023)

26. Akpabio, E., Narad, S.: Artificial intelligence and cybersecurity: challenges, opportunities, and defensive. ICT Syst. Sustain. Proc. ICT4SD 2024 **6**, 291 (2024)
27. Yanamala, A.K.Y., Suryadevara, S.: Navigating data protection challenges in the era of artificial intelligence: a comprehensive review. Rev. Inteligencia Artif. Med. **15**(1), 113–146 (2024)
28. Folorunso, A., Adewumi, T., Adewa, A., Okonkwo, R., Olawumi, T.N.: Impact of AI on cybersecurity and security compliance. Glob. J. Eng. Technol. Adv. **21**(01), 167–184 (2024)
29. Chukwunweike, J.N., Yussuf, M., Okusi, O., Oluwatobi, T.: The role of deep learning in ensuring privacy integrity and security: applications in AI-driven cybersecurity solutions. World J. Adv. Res. Rev. **23**(2), 2550 (2024)
30. Ghimire, B., Rawat, D.B.: Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for internet of things. IEEE Internet Things J. **9**(11), 8229–8249 (2022)
31. Ferrag, M.A., Friha, O., Maglaras, L., Janicke, H., Shu, L.: Federated deep learning for cyber security in the internet of things: concepts, applications, and experimental analysis. IEEE Access **9**, 138509–138542 (2021)
32. Chitimoju, S.: Ethical challenges of AI in cybersecurity: bias, privacy, and autonomous decision-making. J. Comput. Innovation **3**(1) (2023)
33. Mmaduekwe, U.: Bias and fairness issues in artificial intelligence-driven cybersecurity. Curr. J. Appl. Sci. Technol. **43**(6), 109–119 (2024)
34. Sarfraz, M., Sumra, I.A., Khalid, B., Fatima, E.: AI-driven predictive threat detection and cyber risk mitigation: a survey. J. Comput. Biomed. Inf. **8**(02) (2025)
35. Radanliev, P., Santos, O.: Adversarial attacks can deceive AI systems, leading to misclassification or incorrect decisions. ACM Comput. Surv. (2023)
36. Kuppa, A., Le-Khac, N.A.: Black box attacks on explainable artificial intelligence (XAI) methods in cyber security. In: 2020 International Joint Conference on Neural Networks (IJCNN), pp. 1–8 (2020)
37. Zhang, Z., Al Hamadi, H., Damiani, E., Yeun, C.Y., Taher, F.: Explainable artificial intelligence applications in cyber security: State-of-the-art in research. IEEe Access **10**, 93104–93139 (2022)
38. Usman, Q., Jackson, M.: Ethical AI in cybersecurity: addressing bias and fairness in automated threat detection systems (2022)
39. Olutimehin, A.T., Ajayi, A.J., Metibemu, O.C., Balogun, A.Y., Oladoyinbo, T.O., Olaniyi, O.O.: Adversarial threats to AI-driven systems: exploring the attack surface of machine learning models and countermeasures. SSRN 5137026 (2025)
40. Begou, N., Vinoy, J., Duda, A., Korczyński, M.: Exploring the dark side of ai: Advanced phishing attack design and deployment using chatgpt. In: 2023 IEEE Conference on Communications and Network Security (CNS), pp. 1–6 (2023)
41. Kolluri, V.: Revolutionary research on the AI sentry: an approach to overcome social engineering attacks using machine intelligence. Int. J. Adv. Res. Interdiscip. Sci. Endeavours **1**(1), 53–60 (2024)
42. Waizel, G.: Bridging the AI divide: the evolving arms race between AI-driven cyber attacks and AI-powered cybersecurity defenses. In: International Conference on Machine Intelligence & Security for Smart Cities (TRUST) Proceedings, vol. 1, pp. 141–156 (2024)
43. Syed, S.A.: Adversarial AI and cybersecurity: defending against AI-powered cyber threats. Iconic Res. Eng. J. **8**(9), 1030–1041 (2025)