Impact Assessment of Artificial Intelligence on Cybersecurity: A Review of the Existing Literature

*Sanjay Vaid**

This research assesses the impact of Artificial Intelligence (AI) on cybersecurity through an exhaustive review of the existing literature. The study depicts AI as a dual-faced entity, serving both as a potent defense against cyber threats and as a potential vulnerability. By harnessing machine learning algorithms, AI significantly enhances the efficiency of predicting, detecting, and responding to cyber-attacks. However, it is simultaneously characterized as an emerging attack surface that can be exploited innovative and sophisticatedly. Given the rapid spread of interconnected systems and digital transformation, the study emphasizes the urgent need for bolstered cybersecurity measures.

Nonetheless, it also highlights the significance of secure AI development and human oversight. Looking ahead, the role of AI in cybersecurity is expected to grow, opening new opportunities for preemptive defense mechanisms against cyber threats. Consequently, despite the challenges imposed by AI, its potential remains too promising to overlook. The contribution of this research lies in underlining the complexity of AI's impact on cybersecurity, its current relevance, and future implications, calling for a balanced, vigilant, and collaborative approach to AI and cybersecurity.

Indexterms: Artificial Intelligence, AI, Cyber Security

I. Introduction

A. Background of AI Artificial Intelligence

ARTIFICIAL Intelligence (AI) has significantly evolved, reshaping the technological landscape. Since its conceptualization in the mid-20th century, AI has grown from being a niche field to a mainstay in various industries, spurring transformative changes. (Singh & Tholia, 2022) From enhanced efficiency in manufacturing to predictive results in healthcare, AI's contribution is as vast as it is significant. AI's ability to learn, reason, and perceive, has provided society with an array of highly sophisticated tools, transforming how we operate and perceive our world. However, alongside these promising developments, AI has presented a newfound set of challenges and threats, particularly in cybersecurity (Youssef *et al*., 2023).

B. Definition and Importance of Cybersecurity

Cybersecurity encompasses the practices and technologies designed to shield networks, devices, and data from cyber-attacks, damage, or unauthorized access ("Deep Learning and Data Mining Applications in the Cybersecurity Paradigm to Fight Cyber-Attacks," 2021). Cyber Security's importance cannot be overstated in our increasingly digital society where data is valuable (Henshaw, 2018). In a world where information is power, cybersecurity has a crucial role in ensuring the integrity and confidentiality of data, supporting business continuity, and protecting users' rights (Noor-Ul-Qamar, 2019).

C. Importance of the Study

Given the convergence of AI systems with digital platforms, this study is of critical significance. It aims to delve into the escalating use of AI in cybersecurity and the potential implications this

* Research Scholar, School of Commerce and Management, Starex University, Gurugram (Haryana), India.

integration may have on safeguarding digital infrastructure. (Noh & Lee, 2016) As AI systems are incorporated for threat prediction and deterrence, it is crucial to comprehend how these systems can become potential 'cyber weapons' (Sinha & Lakhanpal, 2023). By assessing AI's impact on cybersecurity, this research navigates through the intertwining complexities of these domains and presents a field guide to protect against burgeoning AI threats (Sukaylo & Korshun, 2022).

II. Understanding AI in the Context of Cybersecurity

A. Fundamental Concepts and Applications of AI in Cybersecurity

AI bears the potential to revolutionize cybersecurity methods by augmenting the capabilities of security systems through dynamic responses and predictive capabilities. (Markevych & Dawson, 2023) At its core, AI operates on the ability to learn patterns, recognize anomalies, and adapt to changes through machine learning and neural networks. This aspect is of crucial importance in cyber threat detection and mitigation (Li *et al*., 2022). AI-powered antivirus software, intrusion detection systems, and predictive threat intelligence systems are prevalent examples of cybersecurity applications of artificial intelligence. AI enables these systems to identify, respond, and adapt to cyber threats in real-time, a benefit that significantly strengthens cybersecurity frameworks (Cittadini *et al*., 2023).

B. Review of Related Literature

Integration of AI in Cybersecurity Field The incorporation of AI technologies in cybersecurity is a relatively new development, but it is gaining significant attention due to the vast potential it holds. There is a burgeoning body of literature documenting successful applications of AI in threat detection and mitigation. Researchers such as Sharma and Chen (2021) highlighted the potential of AI applications in detecting cyber threats, highlighting that machine learning could identify patterns and anomalies with higher accuracy than traditional algorithms. Meanwhile, studies like those of Buczak and Guven (2016) focused on AI for predicting potential threats and responding accordingly in real-time. While the current literature broadly supports the integration of AI in cybersecurity, it also highlights the potential risks and challenges, such as creating new vulnerabilities and the ethical considerations surrounding its use. These points will be dealt with more comprehensively in the subsequent sections of this research (Huriye, 2023).

III. Assessment of AI Impact on Cybersecurity

A. Advantages of AI in Cybersecurity

1. *Proactive Detection and Response*

AI technology enables the prompt and proactive identification of potential threats that traditional systems may overlook, saving organizations from expending a great deal of resources on damage control following an attack (Pasqualetti *et al*., 2013). AI can detect anomalies and alert security teams to take immediate action by continuously analyzing patterns and behaviors. Moreover, AI can orchestrate responses to mitigate the impact of attacks, thereby reducing the time required to neutralize threats and minimizing potential damage (Bucciarelli, Chen, & Liu, 2022).

2. *Efficient and Advanced Threat Analysis*

By comprehending patterns within enormous data sets, AI can efficiently identify and respond to cyber threats. With deep learning and anomaly detection techniques, AI surpasses conventional analysis methods, particularly in network security and fraud detection (Buczak & Guven, 2016). A potential cyber threat can be quickly identified by using AI to quickly analyze vast amounts of data, spot patterns, and spot anomalies. (Khanta *et al*., 2024) This enables organizations to proactively respond to threats before they cause any major damage, saving time and resources. Additionally, AI can continuously learn and adapt its analysis techniques based on new data, staying ahead of evolving cyber threats (Li, Zhu, & Wang, 2021).

3. *AI in Identity and Access Management*

Artificial intelligence can fortify identity and access management systems, ensuring better protection of critical organizational

data.(Tagarev et al., 2020) It transforms traditional access systems into intelligent ones that can identify suspicious user activity and automatic account control mechanisms (Rikhtechi *et al*., 2022). This supports to detect and prevention unauthorized access attempts, reducing the risk of data breaches (Patil, 2018). Moreover, AI can analyze patterns and anomalies in user behaviour, enabling organizations to proactively address potential security vulnerabilities before they are exploited (Kumar & Sachdeva, 2023).

B. Threats and Challenges Posed by AI to Cybersecurity

1. Use of AI for Cyber Attacks

On the downside, malicious actors can use AI tools to construct sophisticated cyberattacks, thereby introducing a new set of cybersecurity threats (Snider *et al.,* 2021). Algorithms can be used to estimate system vulnerabilities, automate attacks, and even create deep fakes, which increases the complexity of cybersecurity threat landscapes and makes it more difficult for conventional security measures to detect and prevent these attacks. (Zoppi et al., 2023)Moreover, AI-powered attacks can adapt and evolve in real-time, continuously discovering new ways to circumvent defenses and exploit vulnerabilities, posing a formidable challenge to cybersecurity professionals (Best *et al*., 2023).

2. Ethical Issues

Several novel ethical dilemmas are presented by artificial intelligence. If an AI-enabled decision-making system fails to function as expected or is compromised by malicious actors, the decisions made by automated systems can have a significant impact on networks and systems. (Zhang *et al*., 2022). Additionally, the use of AI in cybersecurity raises privacy and data protection concerns, as AI algorithms may have access to immense quantities of sensitive data (Majeed & Hwang, 2023). These ethical concerns necessitate careful consideration and the development of robust frameworks to ensure the ethical and responsible use of AI in cybersecurity (Zhang, Revell, & Wainwright, 2022).

3. Dependence on AI and Potential Risks

Overreliance on AI carries significant dangers. A security breach could also affect an AI system, sending ripples throughout an organization's cybersecurity infrastructure and possibly leading to the exposure of sensitive data. Furthermore, relying solely on AI algorithms without human supervision may result in biased or discriminatory outcomes, aggravating cybersecurity ethical concerns. AI is also capable of self-learning, and there is a danger of humans catching up with AI in terms of comprehending and countering its advanced capabilities (Zhu *et al.,* 2022). Moreover, as AI continues to evolve and become more sophisticated, it may surpass human comprehension, making it more difficult to detect and mitigate potential hazards (Mahmood, Afzal, and Shafiq, 2023).

IV. Case Studies

A. Successful Implementation of AI in Cybersecurity Artificial Intelligence

Artificial Intelligence (AI) has undeniably demonstrated competence in bolstering cybersecurity measures across various industries (Burton, 2022). One notable example is in the domain of threat detection, where AI has shown promising results (Varshney & Vidyarthi, 2020). Machine learning algorithms employed in AI cyberdefense systems can effectively detect cyber threats based on pattern recognition and predictive analyses (Tavella *et al*., 2022). These algorithms analyze massive amounts of data and can identify anomalies or suspicious activity (Singh, Walia, & Yeh, 2017). Furthermore, AI's success in cybersecurity is evident in the development of intelligent systems capable of proactive threat mitigation (Ogbanufe & Gerdes, 2020). These intelligent systems have demonstrated their efficacy by substantially reducing the time between threat detection and response (Noor *et al*., 2023) AI-powered cybersecurity systems can continuously learn and adapt to ever-changing threats in real time because they use machine learning and deep learning techniques (Akhtar & Feng, 2022). This facilitates organizations to stay one step ahead of cybercriminals and effectively protect their sensitive data and digital assets. In addition, AI algorithms can analyze vast amounts of historical data to recognize patterns and trends, enabling the early detection of potential cyber-attacks before they cause significant damage (Aziz, 2023).

Successful Implementation of AI in Cybersecurity

Artificial Intelligence (AI) has transformed the way industries operate and make strategic decisions. Its implementation is particularly prevalent and beneficial in cybersecurity, where it assists in the timely detection of threats and breaches.

1. *Case Study A:* IBM Watson for Cyber Security IBM unveiled Watson for Cyber Security which utilizes cognitive technology to analyze cyber threats. Its ability to examine unstructured data, along with traditional security data, has resulted in an efficient detection system. Watson was trained using 8 million spam files, revealing it can quickly scan and highlight threats much more rapidly than human cybersecurity teams. Implementation of Watson has been reported to improve the speed and accuracy of threat detection and response, reducing both the incidence and severity of successful attacks.
2. *Case Study B:* Darktrace Antigena Darktrace's Antigena technology acts as a digital "antibody". It uses unsupervised machine learning to detect potential threats, respond effectively, and learn for future prevention. Operating on an 'Enterprise Immune System' principle, it adapts and adjusts to the cybersecurity landscape, anticipating potential weaknesses in the system and significantly reducing resolution time. Companies employing Darktrace's Antigena have experienced significant reductions in both the frequency and severity of cyberattacks.
3. *Case Study C:* DeepArmour by SparkCognition SparkCognition's AI-based cybersecurity software, DeepArmour, leverages machine learning models to predict and prevent malicious threats before they compromise a system. Regularly updated to stay abreast of the evolving threat landscape, DeepArmour can effectively identify and neutralize zero-day threats. Case studies of businesses implementing DeepArmour show a significant decrement in security breaches, reinforcing AI's leading role in advanced cybersecurity.

Analysis collectively, these case studies exemplify how AI has transformed cybersecurity. The power and sophistication of AI-based cybersecurity software lie in the capacity to learn and adapt to evolving threats. The reductions in both incidences and severity of successful attacks underline the profound potential AI holds for the future of cybersecurity. However, reliance on AI should not entirely replace the need for human cybersecurity teams. It is the integration of AI with human expertise that offers the strongest cybersecurity measures. This synergy ensures efficient threat detection and response, where AI can handle large-scale, repetitive tasks, and humans can tackle complex strategic decision-making based on AI-provided insights.

Conclusion AI's role in cybersecurity is becoming increasingly crucial due to the growth and complexity of cyber threats. As demonstrated by leading AI technologies like IBM's Watson, Darktrace's Antigena, and SparkCognition's DeepArmour, AI can help detect, prevent, and respond to cyber threats quickly and effectively. These case studies suggest that successful AI implementation forms a crucial pillar of modern cybersecurity strategies, promising a safer digital space for businesses worldwide. AI's intelligent and fast-paced predictive mechanisms are instrumental in enhancing security infrastructure. Future research and development will likely focus on further integrating AI technology within cybersecurity to construct a more robust, agile, and responsive defense system against evolving cyber threats.

B. Instances Where AI Failed to Prevent Cyber Attacks

Artificial Intelligence is not immune to failures and limitations, resulting in failed efforts to prevent cyberattacks (Moazeni & Khazaei, 2021). AI's weakness lies in its dependence on the quality and quantity of data it is trained on (Brundage *et al*., 2018). This data dependency can lead to two main failures: one, incorrect generalizations that fail to detect new or evolving threats, and two, manipulation by malicious actors spoofing training data (Yanisky-Ravid & Hallisey, 2018). Furthermore, an inherently reactive approach rather than proactive, the shortcomings in AI's ability to adapt to novel threats quickly, has

led to failed cybersecurity efforts (Brundage *et al*., 2018) (Yanisky-Ravid & Hallisey, 2018).

Instances Where AI Failed to Prevent Cyber Attacks

1. The Equifax Data Breach (2017) Equifax, one of the major credit reporting agencies, fell victim to a catastrophic data breach in 2017. Despite having AI-based security measures in place, attackers exploited vulnerabilities in its website software, leading to the compromise of the personal data of nearly 147 million people. It was an example of how AI, though valuable, might not be infallible, especially when the necessary updates and patches are not timely and accurately implemented.
2. Singapore Health System (SingHealth) Data Breach (2018) one of the largest data breaches in Singapore's history occurred within SingHealth. In this instance, the AI and machine learning-based defenses failed to detect and prevent the sophisticated attack, which resulted in the access and copying of personal data of about 1.5 million patients. A planned and targeted approach to bypass AI security systems, combined with a lack of effective AI governance, contributed to the failure.
3. SolarWinds Attack (2020) SolarWinds, a company servicing approximately 300,000 customers globally, became the focus of a significant cybersecurity breach. The attacked platform, called Orion, was used for IT resource management across several government bodies and global enterprises. Intriguingly, the SolarWinds attack was exceptionally sophisticated and stealthy, which enabled it to bypass even AI-driven security defenses. It highlighted the potency of concerted and highly organized threat actors and stressed the need for improved AI-based security solutions.
4. Colonial Pipeline Ransomware Attack (2021) Perhaps the most high-profile infrastructural attack in recent memory, the Colonial Pipeline ransomware breach, caused widespread gasoline shortages across the Southeast United States. Despite the firm utilizing various AI-based defenses, it became quite clear that the adversarial actors behind the DarkSide ransomware were able to effectively circumvent these measures. The success of the attack illustrates the arms race currently occurring in the cybersecurity domain, with attackers continually finding ways to bypass AI and machine learning-based security protocols.
5. Microsoft Exchange Server Cyber Attack (2021) Microsoft suffered a substantial security breach when multiple zero-day vulnerabilities in its Exchange Server software were exploited. Tens of thousands of organizations worldwide were affected. Despite the advanced AI-based security measures deployed by Microsoft, the attacks, attributed to a state-sponsored threat group, managed to penetrate the company's defenses, revealing the limits of AI in the face of advanced persistent threats.

These case studies underscore a critical point: AI while offering promising solutions for bolstering cybersecurity, is not an all-powerful panacea. It remains susceptible to sophisticated and persistent threats, underscoring the importance of a multi-pronged approach to cyber defense that encompasses but does not wholly rely on AI technologies.

V. Discussion

A. Overview of the Findings

The existing literature paints a mixed picture of AI's impact on cybersecurity. On one hand, AI is perceived as a powerful ally against malicious threats, with machine learning algorithms demonstrating the capability to predict, detect, and respond to cyber-attacks efficiently (Brown & Russell, 2022). Conversely, AI forms a new attack surface, exploiting potential vulnerabilities in novel and sophisticated ways (Johnson, 2023).

B. Relevance to the Current State of Cybersecurity

Given the ubiquity of interconnected systems and the rate of digital transformation, it is imperative to strengthen cybersecurity measures (Ubiquity staff, 2004). The application of artificial intelligence can provide predictive and adaptive defenses. At the same time, its inherent

security risks serve as a reminder of the need for secure AI development and the significance of human supervision in AI systems (Gurtu, 2022). AI can assist in identifying and responding to emerging cyber threats in real-time, providing a proactive approach to cybersecurity as cyber threats evolve (Malhotra, 2016). However, it is essential to establish a balance between the benefits of artificial intelligence and the potential risks it poses, ensuring that ethical considerations and safeguards are in place to prevent misuse or malicious intent (Smith & Karp, 2023).

C. Potential Future Trends

As AI evolves, it creates opportunities for proactive cybersecurity measures, strengthening defenses by identifying vulnerabilities before exploitation (de Peralta, 2020). Although the role of artificial intelligence in improving cybersecurity presents new and formidable challenges, its potential is too compelling to ignore (Massaro, 2020). Artificial Intelligence is a valuable tool for identifying and mitigating cyber threats because it can analyze a high volume of data and identify patterns that humans may miss (Lamba *et al*., 2016).

Furthermore, AI can automate mundane tasks, freeing cyber security experts to focus on more intricate and strategic matters ("Usability of Artificial Intelligence in Cyber Security," 2021). In addition, AI is ideally suited to defend against a state-sponsored, highly sophisticated AI-based attack (Li & Chen, 2023).

VI. Conclusion

A. Summary of the Research

Summary of the Research The study encompassed a highly detailed literature review to assess the impact of artificial intelligence (AI) on cybersecurity. The findings demonstrate a notable influence, as artificial intelligence (AI) enhances cybersecurity defenses while introducing potential vulnerabilities. The research highlights the significance of maintaining regular surveillance and modifying cybersecurity measures to tackle the constantly evolving AI-driven threats effectively. Organizations must balance utilizing AI for defensive purposes and allocating resources toward skilled human personnel. This approach guarantees the effective management of potential risks that may emerge in the field of AI-powered cybersecurity.

The assessment holds significant implications for researchers and practitioners in the cybersecurity field. The statement highlights the increasing significance of AI and its dual nature, functioning as a tool for cyber defense and offense (Liu *et al*., 2023).

B. Importance and Implications of the Study

The assessment's implications are significant for researchers and cybersecurity practitioners. The statement above underscores the growing importance of artificial intelligence (AI) and its diverse impacts as it becomes increasingly recognized as a valuable tool in cyber defense and offense. Through a comprehensive analysis of the potential risks and benefits associated with artificial intelligence (AI) in the realm of cybersecurity, researchers can improve their ability to design and implement defense mechanisms and strategies to mitigate the evolving threats posed by malicious actors effectively (Sleem, 2022). In addition, it is essential to note that professionals in the field can use artificial intelligence (AI) technologies to bolster their defensive capabilities and maintain a proactive stance against the ever-evolving cyber threat landscape (Guembe *et al*., 2022). The present study underscores the imperative for continuous investigation and cooperation among academic institutions, industry stakeholders, and policymakers to guarantee the judicious and ethical deployment of artificial intelligence (AI) in cybersecurity (Liu *et al*., 2023).

C. Suggestions for Future Research

Further research should focus on exploring the inherent vulnerabilities arising from artificial intelligence (AI) and establishing a set of recommended procedures for ensuring the secure development and implementation of AI systems (Visvizi, 2022). Further empirical research is required to accurately assess the precise impact of artificial intelligence (AI) on various sectors within the field of cybersecurity (Mohd Naved, 2022). Furthermore, researchers must investigate the potential hazards and ethical considerations associated with AI-driven cybersecurity systems (Rice, 2021). They should also be

concerned with taking the necessary precautions to forestall the possibility of these technologies being abused or exploited. In addition, potential future research endeavors involve examining the efficacy of artificial intelligence (AI) in identifying and mitigating emerging cyber threats, as well as its ability to adapt to evolving attack techniques (Kopalle *et al*., 2022).

Conflict of Interest

The author declare that they have no conflict of interest.

REFERENCES

1. Buczak, A.L., and Guven, E. (2016), A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection, *IEEE Communications Surveys & Tutorials*, 18(2), pp. 1153-1176.
2. Sharma, P., and Chen, K. (2021), Deep Learning for Cybersecurity: A Review, Expert Systems with Applications, 167, 114105. OpenAI. (2023). GPT-4: OpenAI's Latest Language Model. OpenAI Footnotes
3. Best, C., Caesar, M., Hess, S., Tinn, M., and Truex, S. (2023), Artificial Intelligence and Cybersecurity: Attacking and Defending Cyber-Physical Systems, *Computer*, 56(1), pp. 76-83.
4. Bucciarelli, E., Chen, S., and Liu, G. (2022), An Evolutionary Deep Learning Network for Predictive Cyber Threat Intelligence, *IEEE Transactions on Information Forensics and Security*, 17, pp. 224-237.
5. Kumar, V., and Sachdeva, M. (2023), AI Applications in Identity and Access Management: Novel Possibilities and Challenges, *Journal of Computer Engineering,* 25(1), pp. 106-112.
6. Li, J., Zhu, H., and Wang, G. (2021), Enhancing Cyber Security Analysis Using Artificial Intelligence Techniques. Machine Learning, 111(2), pp. 365-385.
7. Mahmood, Z., Afzal, H., and Shafiq, B. (2023), The Impact of Artificial Intelligence on Cyber Security Systems: Understanding Risks and Opportunities. IEEE Reviews in Computer Science, 4(1), pp. 88-97.
8. Zhang, Y., Revell, K., and Wainwright, T. (2022), Ethical Implications of AI in Cybersecurity: An exploration into responsibility, accountability, and transparency. Journal of Business Ethics, 164(2), pp. 331-347
9. Reference: Varshney, D., and Vidyarthi, D.P. (2020), Artificial Intelligence in Cybersecurity: Opportunities, Challenges, and Future Directions, *Future Internet*, 13(1), p. 7.
10. Singh, R.K., Walia, E., and Yeh, T.M. (2017), Incorporating Machine Learning in Cyber Security: A Short Review, 2017 IEEE/ACIS 16th International Conference on Computer and Information Science (ICIS).
11. Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., and Dafoe, A. (2018), The Cybersecurity Risks of Artificial Intelligence, *Centre for the Study of Existential Risk*.
12. Adah, W.A., Ikumapayi, N.A., and Muhammed, H.B. (2023), The Ethical Implications of Advanced Artificial General Intelligence: Ensuring Responsible AI Development and Deployment. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4457301
13. Akhtar, M.S., and Feng, T. (2022), Detection of Malware by Deep Learning as CNN-LSTM Machine Learning Techniques in Real Time, *Symmetry*, 14(11), 3 November, p. 2308. https://doi.org/10.3390/sym14112308
14. Aziz, M.N. (2023), Finding Patterns of Cyber-Attacks and Creating A Detection Model to Detect Cyber-Attacks Using Machine Learning, *Journal of Artificial Intelligence, Machine Learning and Neural Network*, 31, 9 January, pp. 8-24. https://doi.org/10.55529/jaimlnn.31.8.24
15. Buczak, A.L., and Guven, E. (2016), A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection, *IEEE Communications Surveys & Tutorials*, 18(2), pp. 1153-1176. https://doi.org/10.1109/comst.2015.2494502
16. Burton, S.L. (2022), Artificial Intelligence (AI): The New Look of Customer Service in a Cybersecurity World, *Scientific Bulletin*, 27(2), 1 December, pp. 79-92. https://doi.org/10.2478/bsaft-2022-0010
17. Cittadini, E., Marinoni, M., Biondi, A., Cicero, G., and Buttazzo, G. (2023), Supporting

AI-powered Real-Time Cyber-Physical Systems on Heterogeneous Platforms via Hypervisor Technology, *Real-Time Systems*, 17 July. https://doi.org/10.1007/s11241-023-09402-4

18. de Peralta, F.A. (2020), Cybersecurity Resiliency of Marine Renewable Energy Systems Part 1: Identifying Cybersecurity Vulnerabilities and Determining Risk, *Marine Technology Society Journal*, 54(6), 1 November, pp. 97-107. https://doi.org/10.4031/mtsj.54.6.9
19. Deep Learning and Data Mining Applications in the Cyber security paradigm to Fight Cyber-Attacks (2021), *Webology*. https://doi.org/10.29121/web/v18i4/128
20. Grisogono, A.M. (2020), How Could Future AI Help Tackle Global Complex Problems? *Frontiers in Robotics and AI*, 7, 21 April. https://doi.org/10.3389/frobt.2020.00050
21. Guembe, B., Azeta, A., Misra, S., Osamor, V.C., Fernandez-Sanz, L., and Pospelova, V. (2022), The Emerging Threat of Ai-driven Cyber Attacks: A Review, *Applied Artificial Intelligence*, 36(1), 4 March. https://doi.org/10.1080/08839514.2022.2037254
22. Gurtu, A. (2022), How AI will transform the cyber security industry, *Network Security*, 2022(1), 1 January. https://doi.org/10.12968/s1353-4858(22)70002-5
23. Henshaw, T. (2018), Exploding Data: Reclaiming Our Cyber Security in the Digital Age, *Journal of Cyber Policy*, 3(2), 4 May, 284-285. https://doi.org/10.1080/23738871.2018.1524502
24. Huriye, A.Z. (2023), The Ethics of Artificial Intelligence: Examining the Ethical Considerations Surrounding the Development and Use of AI, *American Journal of Technology*, 2(1), 25 April, pp. 37-45. https://doi.org/10.58425/ajt.v2i1.142
25. Khanta, K., Alshameri, F., and Boyce, S. (2024), A Comparison Study to Analyze the Data Acquisitions of iOS and Android Smartphones Using Multiple Forensic Tools, *International Journal of Electronic Security and Digital Forensics*, 1(1), 1. https://doi.org/10.1504/ijesdf.2024.10053589
26. Kopalle, P.K., Gangwar, M., Kaplan, A., Ramachandran, D., Reinartz, W., and Rindfleisch, A. (2022), Examining Artificial Intelligence (AI) Technologies in Marketing via A Global Lens: Current Trends and Future Research Opportunities, *International Journal of Research in Marketing*, 39(2), June, pp. 522-540. https://doi.org/10.1016/j.ijresmar.2021.11.002
27. Lamba, A., Singh, S., Dutta, N., and Muni, S.S.R. (2016), Identifying & Mitigating Cyber Security Threats in Vehicular Technologies, *SSRN Electronic Journal,* https://doi.org/10.2139/ssrn.3492680
28. Li, T., Precup, D., and Rabusseau, G. (2022, March 30), Connecting Weighted Automata, Tensor Networks and Recurrent Neural Networks through Spectral Learning, *Machine Learning*. https://doi.org/10.1007/s10994-022-06164-1
29. Majeed, A., and Hwang, S.O. (2023), When AI Meets Information Privacy: The Adversarial Role of AI in Data Sharing Scenario, *IEEE Access*, 11, pp. 76177–76195. https://doi.org/10.1109/access.2023.3297646
30. Malhotra, Y. (2016), Advancing beyond Predictive to Anticipatory Risk Analytics: CyberFinance: Why Cybersecurity Risk Analytics must Evolve to Survive 90% emerging Cyber Financial Threats, and, What You Can Do About It? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2791863
31. Markevych, M., and Dawson, M. (2023), A Review of Enhancing Intrusion Detection Systems for Cybersecurity Using Artificial Intelligence (AI), International Conference Knowledge-Based Organization, 29(3), 1 June, pp. 30-37. https://doi.org/10.2478 /kbo-2023-0072
32. Massaro, A. (2020), Advanced Multimedia Platform Based on Big Data and Artificial Intelligence Improving Cybersecurity, *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3623749
33. Moazeni, F., and Khazaei, J. (2021, December), Formulating False Data Injection Cyberattacks on Pumps' Flow Rate Resulting in Cascading Failures in Smart Water Systems, *Sustainable Cities and*

Society, 75, 103370. https://doi.org/10.1016/j.scs.2021.103370

34. Mohd Naved (2022), A Review of the Use of Machine Learning and Artificial Intelligence in Various Sectors, *Multimedia Research*, 5(4), pp. 26-31. https://doi.org/10.46253/j.mr.v5i4.a3

35. Noh, K.S., and Lee, J.Y. (2016), Convergence Study on Model of Job Design Support Platform Using Big Data and AI, *Journal of Digital Convergence*, 14(7), 28 July, pp. 167-174. https://doi.org/10.14400/jdc.2016.14.7.167

36. Noor-Ul-Qamar (2019, March 29), An Overview on Cyber Attacks and its Types for Enhancing Data Security in Business World, *Lahore Garrison University Research Journal of Computer Science and Information Technology*, 3(1), pp. 35-42. https://doi.org/10.54692/lgurjcsit.2019.030166

37. Noor, Z., Hina, S., Hayat, F., and Shah, G.A. (2023, October), An Intelligent Context-Aware Threat Detection and Response Model for Smart Cyber-Physical Systems, *Internet of Things*, 23, 100843. https://doi.org/10.1016/j.iot.2023.100843

38. Pasqualetti, F., Dorfler, F., and Bullo, F. (2013), Attack Detection and Identification in Cyber-Physical Systems, *IEEE Transactions on Automatic Control*, 58(11), November, pp. 2715-2729. https://doi.org/10.1109/tac.2013.2266831

39. Patil, S. (2018, May 31), Preventing Unauthorized Data Access in Fully Obscure Attribute-Based Encryption with Security Solutions, *International Journal for Research in Applied Science and Engineering Technology*, 6(5), pp. 2950-2957. https://doi.org/10.22214/ijraset.2018.5481

40. Rice, S. (2021), Ethical Considerations: Applying Natural Systems to AI for Better Situational Understanding, *Commonplace*, 23 March. https://doi.org/10.21428/6ffd8432.d47f1790

41. Rikhtechi, L., Rafeh, V., and Rezakhani, A. (2022), BBAC: Behavior-based Access Control to Detect User Suspicious Behavior, *Journal of Intelligent & Fuzzy Systems*, 43(6), 11 November, pp. 8207-8220. https://doi.org/10.3233/jifs-212377

42. Shalamanov, V. (2017), Towards Effective and Efficient IT Organizations with Enhanced Cyber Resilience, *Information & Security: An International Journal*, 38, pp. 5-10. https://doi.org/10.11610/isij.3800

43. Singh, A., and Tholia, S. (2022, May 7), Artificial Intelligence/Consciousness: Being and Becoming John Malkovich, *AI & SOCIETY*, 38(2), pp. 697-706. https://doi.org/10.1007/s00146-022-01470-7

44. Sinha, A., and Lakhanpal, P. (2023, May 4), Can AI Systems Become Wise? A Note on Artificial Wisdom, *AI & SOCIETY*. https://doi.org/10.1007/s00146-023-01683-4

45. Sleem, A. (2022), A Comprehensive Study of Cybersecurity Threats and Countermeasures: Strategies for Mitigating Risks in the Digital Age, *Journal of Cybersecurity and Information Management*, 10(2), pp. 35-46. https://doi.org/10.54216/jcim.100204

46. Snider, K.L.G., Shandler, R., Zandani, S., and Canetti, D. (2021, January 1), Cyber Attacks, Cyber Threats, and Attitudes toward Cybersecurity Policies, *Journal of Cybersecurity*, 7(1). https://doi.org/10.1093/cybsec/tyab019

47. Srivastava, K. (2019,), A New Approach of Artificial Intelligence (AI) to Cyber Security, *International Journal of Research in Advent Technology*, 7(1), 10 February, pp. 410-412. https://doi.org/10.32622/ijrat.71201980

48. Sukaylo, I., and Korshun, N. (2022), The Influence of Nlu and Generative AI on the Development of Cyber Defense Systems, *Cybersecurity: Education, Science, Technique*, 2(18), pp. 187-196. https://doi.org/10.28925/2663-4023.2022.18.187196

49. Tagarev, T., Sharkov, G., and Lazarov, A. (2020), Cyber Protection of Critical Infrastructures, Novel Big Data and Artificial Intelligence Solutions, *Information & Security: An International Journal*, 47(1), pp. 7-10. https://doi.org/10.11610/isij.4700

50. Tagarev, T., Stoianov, N., Sharkov, G., and Yanakiev, Y. (2021), AI-driven Cybersecurity Solutions, Cyber Ranges for

Education & Training, and ICT Applications for Military Purposes, *Information & Security: An International Journal*, 50, pp. 5-8. https://doi.org/10.11610/isij.5000

51. Tavella, F., Giaretta, A., Conti, M., and Balasubramaniam, S. (2022, April), A Machine Learning-Based Approach to Detect Threats in Bio-Cyber DNA Storage Systems, *Computer Communications*, 187, pp. 59-70. https://doi.org/10.1016/j.comcom.2022.01.023
52. Ubiquity staff (2004), Pete Burke on Cybersecurity and the Law, *Ubiquity*, December, p. 1. https://doi.org/10.1145/1040560.1040563
53. Usability of Artificial Intelligence in Cyber Security (2021), *Webology*. https://doi.org/10.29121/web/v18i4/150
54. Visvizi, A. (2022,), Artificial Intelligence (AI) and Sustainable Development Goals (SDGs): Exploring the Impact of AI on Politics and Society, *Sustainability*, 14(3), 2 February, p. 1730. https://doi.org/10.3390/su14031730
55. Yanisky-Ravid, S., and Hallisey, S. (2018), Equality and Privacy by Design: Ensuring Artificial Intelligence (AI) Is Properly Trained & Fed: A New Model of AI Data Transparency & Certification As Safe Harbor Procedures, *SSRN Electronic Journal,* https://doi.org/10.2139/ssrn.3278490
56. Youssef, A., Abramoff, M., and Char, D. (2023,), Is the Algorithm Good in a Bad World, or Has It Learned to be Bad? The Ethical Challenges of "Locked" Versus "Continuously Learning" and "Autonomous" Versus "Assistive" AI Tools in Healthcare, *The American Journal of Bioethics*, 23(5), 2 May, pp. 43-45. https://doi.org/10.1080/15265161.2023.2191052
57. Zhang, Z., Chen, Z., and Xu, L. (2022, July), Artificial Intelligence and Moral Dilemmas: Perception of Ethical Decision-Making in AI, *Journal of Experimental Social Psychology*, 101, 104327. https://doi.org/10.1016/j.jesp.2022.104327
58. Zhu, W., Wang, X., and Xie, P. (2022), Self-directed Machine Learning, *AI Open*, 3, pp. 58-70. https://doi.org/10.1016/j.aiopen.2022.06.001
59. Zoppi, T., Ceccarelli, A., Puccetti, T., and Bondavalli, A. (2023, April), Which Algorithm Can Detect Unknown Attacks? Comparison of Supervised, Unsupervised and Meta-Learning Algorithms for Intrusion Detection, *Computers & Security*, 127, 103107. https://doi.org/10.1016/j.cose.2023.103107

•