ISSN: 2754-6659

Journal of Artificial Intelligence & Cloud Computing

SCIENTIFIC Research and Community

Review Article

Open Access

A Review on the Impact of Artificial Intelligence on Cybersecurity

Vamsy Priya Anne[1]* and Sampath Talluri[2]

[1]Department of Computer Information Systems, Grand Valley State University, 1 Campus Dr, Allendale, MI 49401, USA

[2]Department of Computer Science, Western Michigan University, 1903 W Michigan Ave, Kalamazoo, MI 49008, USA

ABSTRACT

When it comes to protecting against cyber threats, the use of AI is changing everything. Thanks to AI-powered technologies, organizations can now better foresee and handle potential intrusions. These solutions offer unparalleled capabilities in threat detection, real-time monitoring, and predictive analytics. But, with these innovations come significant hazards and difficulties, necessitating thoughtful deliberation and preventative measures. Artificial intelligence's impact on cybersecurity is explored in this article, looking at both the ways AI is improving defense systems and the dangers of cyberattacks powered by AI. Advanced AI threat detection techniques, including behavioral analysis, anomaly detection, and predictive analytics, are discussed. In addition, the article discusses the limitations and difficulties of using machine learning for malware detection. Threats like adversarial assaults, data difficulties, biases, and prejudice are discussed in the article, along with the hazards of AI-powered cyberattacks. To effectively manage these dangers, it stresses the significance of cybersecurity experts, AI researchers, and lawmakers working together in an interdisciplinary manner to create accountable deployment techniques and transparent governance structures. Ethically and responsibly leveraging AI technology to defend digital assets and privacy in an ever-evolving threat landscape requires stakeholders to collaborate and be transparent. This will help them understand the intricacies of AI in cybersecurity.

***Corresponding author**

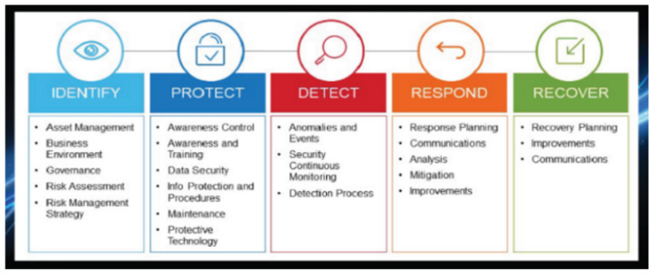
Vamsy Priya Anne, Department of Computer Information Systems, Grand Valley State University, 1 Campus Dr, Allendale, MI 49401, USA.

Received: June 06, 2024; **Accepted:** June 10, 2024; **Published:** June 19, 2024

Keywords: Cybersecurity, Artificial Intelligence, Interface, Limitations, Cyberattacks

Introduction

The incorporation for Artificial Intelligence (AI) into different aspects of our lives has become unavoidable in today's digital era. Out of the various industries experiencing change, cybersecurity is particularly notable for being heavily influenced by AI. Digital security measures and threat management are going through a radical shift as a result of the many opportunities and challenges brought about by the merging of artificial intelligence with cybersecurity. The increasing dependence on digital platforms & the Internet has magnified the significance of strong cybersecurity measures. The increasing complexity and frequency of cyber-attacks require innovative responses that go beyond traditional tactics. Introducing AI, which has the ability to analyze extensive quantities of data, identify trends, and forecast future dangers with unparalleled precision and speed [1]. Artificial intelligence (AI) technologies, such as machine learning, neural networks, or natural language processing, are being used to strengthen cybersecurity defenses. These technologies provide a proactive method for identifying and reducing threats. When it comes to cybersecurity, AI's ability to automate threat detection is a major plus. Conventional cybersecurity solutions frequently depend on pre-established rules & signatures to detect harmful actions. Nevertheless, this strategy may be insufficient when confronted with intricate and perpetually changing dangers. Artificial intelligence, namely through the utilization of machine learning, has the ability to acquire knowledge from past data and adjust to novel, unfamiliar risks by detecting irregularities and patterns that indicate possible cyber assaults.



IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
• Asset Management • Business Environment • Governance • Risk Assessment • Risk Management Strategy	• Awareness Control • Awareness and Training • Data Security • Info Protection and Procedures • Maintenance • Protective Technology	• Anomalies and Events • Security Continuous Monitoring • Detection Process	• Response Planning • Communications • Analysis • Mitigation • Improvements	• Recovery Planning • Improvements • Communications

Figure 1: Cybersecurity Framework

Human analysts are free to focus on more complex and strategic tasks thanks to this ability, which also increases the efficiency and accuracy of detecting possible threats. The predictive capabilities of AI are an additional crucial advantage [2,3]. Through the examination of patterns and trends in data related to cyber threats, artificial intelligence (AI) systems have the ability to predict possible weaknesses and methods of attack before they are taken advantage of. The predictive nature of AI allows organizations to strengthen their defenses in a proactive manner, by identifying and resolving vulnerabilities before they become targets. For example, artificial intelligence has the capability to detect atypical network traffic patterns or abnormal user behavior, indicating them for additional scrutiny. This proactive approach represents a notable departure from the reactive nature of conventional cybersecurity procedures. AI improves the effectiveness of incident response and the process of resolving issues. Swift action is necessary in order to mitigate the impact of a cyber assault. AI-driven systems have the ability to rapidly analyze the characteristics and extent of an attack, offering practical insights and suggestions for containing and recovering from it. The automation for these processes guarantees a prompt reaction, minimizing the timeframe in which attackers might cause harm [4,5]. AI can aid in the post-incident investigation by identifying the underlying reason of the assault and mitigating the likelihood of future incidents. The incorporation of artificial intelligence into cybersecurity is not devoid of obstacles. An important issue to consider is the possibility of cybercriminals using AI as a weapon. AI may be utilized both for cyber defense and for the creation of advanced and precise cyber-attacks. Cyber attackers have the ability to utilize artificial intelligence (AI) to detect weaknesses, automatically generate malicious software, and carry out extensive phishing operations that achieve better rates of success. The fact that AI can be used for multiple purposes requires a constant and adaptable approach to cybersecurity initiatives that are driven by AI. Another obstacle is in the dependence on data for AI training. In order for AI models to be effective, they necessitate enormous quantities of data to acquire knowledge and generate precise forecasts. It is of utmost importance to priorities the quality, diversity, and security of this data. Erroneous or prejudiced data can result in defective models, which may inaccurately identify risks or produce incorrect positive results, resulting in unneeded interruptions and distrust in AI systems [6-9]. The ethical ramifications of artificial intelligence in cybersecurity must not be disregarded. The implementation of AI systems entails substantial authority in decision-making, which gives rise to problems of responsibility, openness, and confidentiality. It is of utmost importance to guarantee that AI functions within ethical parameters and complies with regulatory norms in order to uphold public confidence and protect human liberties. Artificial Intelligence has a significant impact on cybersecurity by providing advanced skills in detecting, predicting, and responding to threats. Although AI offers many advantages, it also brings up novel challenges and threats that need to be tackled. Artificial intelligence (AI) integration into cybersecurity will shape the future of digital security by facilitating the development of robust and adaptable defense systems to address the dynamic nature of cyber attacks. The full use of AI's capabilities in cybersecurity will depend on striking a careful balance between the advantages and risks of the technology [10].

Literature Review

With the progress of digital transformation, organizations are confronted with heightened cybersecurity vulnerabilities, which require the implementation of sophisticated defensive measures [11]. In order to compare and contrast the effects of AI and traditional methods on organizational cybersecurity, this study conducts a systematic literature review (SLR). 73 peer-reviewed articles from 2018 to 2023 were using the PRISMA flow diagram. The results indicate that AI improves cybersecurity by automating processes, providing threat intelligence, and enhancing defense mechanisms. However, it also brings about obstacles such as adversarial attacks and issues related to the quality of data. The findings emphasize the beneficial impact of AI on cybersecurity, improving its effectiveness and resilience and laying the groundwork for additional study and well-informed decisions about the implementation of AI.

Due to the exponential growth in mobile phone usage, Android devices are increasingly vulnerable to malicious threats, particularly in critical applications such as banking [12]. Detecting Android malware is essential for ensuring cybersecurity. This article introduces a method that uses bioinspired artificial intelligence to detect and classify Android malware (BAI-AMDC). The BAI-AMDC integrates swarm intelligence, neural networks, and evolutionary algorithms to select features and use a bidirectional gated recurrent unit (BiGRU) model for detection. The arithmetic optimization algorithm (AOA) improves the accuracy of detection. The system's efficiency in recognizing Android malware is demonstrated through experimental validation on the CICAndMal2017 database, which consists of 10,000 incidents.

Focuses into the possible applications of xAI in the domains of AI and deep learning, with a focus on how it can influence cybersecurity [13]. Beginning with an in-depth analysis of xAI methodologies, the essay goes on to highlight their value and benefits in cybersecurity. The authors then present a systematic mapping analysis that may be used as a tool to systematically find research directions and opportunities for integrating explainable AI (xAI) into deep learning, AI, and cybersecurity. A number of potential avenues are thoroughly investigated in the paper. The report closes by integrating the collected insights and delivering definitive conclusions derived from the thorough analysis.

Having secure and decentralized AI systems to tackle cyber threats is of utmost importance, especially with the increasing use of AI in cybersecurity [14]. By utilizing distributed and immutable data storage, blockchain technology (BT) enhances the confidentiality and integrity of AI systems. The goal of this literature analysis is to improve cybersecurity by methodically exploring the combination of decentralized AI (Artificial Intelligence) with BT (Blockchain Technology). The study analyses the many uses, challenges, and potential benefits of BT in this setting and offers a complete categorization scheme. As an added bonus, the research weighs the pros and cons of using decentralized AI in cybersecurity. When applied to real-world cybersecurity issues, the results show that BT and decentralized AI work well together. The possibility for decentralized AI powered by blockchain to strengthen AI systems' privacy, security, and trustworthiness is a promising area for further study.

Having robust cybersecurity measures is crucial in this day and age [15]. For increased security, it is necessary to use upgraded versions like the cybersecurity mesh. The cybersecurity mesh is a durable, adaptable, and scalable design. It paves the way for coordinated and cooperative intelligence systems to offer security services. There are challenges with scalability, federated systems, and technology integration in designing such a mesh. Technology that works well should make it easier to deal with growing workloads and make it easier for many systems to cooperate without a master controller. Cryptography relies heavily on algorithms and AI models like blockchain, federated learning, and swarm intelligence. This study examines intelligent systems by looking at their latest innovations, connections, pros, and cons. In accordance with PRISMA guidelines, the study used data retrieved from Scopus and the Web of Science databases.

Table 1: Literature Summary

Author/Year	Method/Model	Research Gap	Parameters
Kelly /2023 [16]	Review of cybersecurity challenges and mitigation strategies for radiology AI.	Integrate cybersecurity concepts into radiology AI projects to mitigate risks.	Radiology AI projects face cybersecurity challenges, requiring awareness and mitigation strategies.
Mishra/2023 [17]	AI-based Cyber Security model enhances financial sector's defense efficiency.	Inadequate methods for comprehensive defense against evolving cyber threats.	Unauthorized access, data protection, AI-based security, encryption, risk mitigation.
Marwan/2023 [18]	Mod-QR approach for Stackelberg security games in cloud computing.	Enhanced defense strategies for dynamic cloud computing cybersecurity.	Cybersecurity threats, defense strategy, Stackelberg games, Mod-QR, uncertainty, effectiveness.
Rjoub/2023 [19]	Explainable AI enhances cybersecurity by providing interpretable explanations for decisions.	XAI enhances cybersecurity by providing interpretable AI models.	AI models, Explainable AI, cybersecurity, interpretable explanations, defense effectiveness.
Srinivasan/2023 [10]	Utilizing XAI to enhance comprehension and adoption in cybersecurity.	Application of XAI in cybersecurity for interpretable AI.	AI model interpretability, XAI, cybersecurity, threat understanding, defense effectiveness.

How AI Enhances Threat Detection and Response

By improving attack detection and response capabilities, artificial intelligence (AI) is drastically changing the cybersecurity landscape. Cybersecurity approaches that depend on static rules and signature-based detection are becoming more inadequate when confronted with complex and ever-changing threats. To protect digital environments, AI provides a proactive and dynamic solution with its learning, adapting, and predicting capabilities [20-23].

AI enhances threat detection through several innovative techniques, primarily leveraging machine learning (ML) algorithms and deep learning models. These technologies excel in identifying patterns and anomalies within large datasets, enabling the detection of malicious activities that might elude traditional systems.

Behavioral Analysis: AI systems are instrumental in establishing a comprehensive baseline of normal behavior for users, devices, and applications within a network, a process known as behavioral profiling. This baseline is created by monitoring and analyzing vast amounts of historical and real-time data to understand what constitutes typical activity. For example, an AI system tracks patterns such as login times, frequency of access to specific files, data transfer volumes, and the regularity of interactions between network entities. Once this baseline is established, the AI system continuously monitors ongoing activities, comparing them against the normative patterns it has learned. Any deviation from these patterns is promptly flagged as a potential threat. For instance, if an employee who usually logs in between 9 AM and 6 PM suddenly logs in at 3 AM, this anomalous behavior triggers an alert. Similarly, if a user who typically accesses a specific set of files suddenly starts downloading large volumes of data they have never interacted with before, this irregular data transfer is identified as suspicious. AI can detect subtler anomalies, such as slight deviations in the frequency or sequence of access patterns, which might be overlooked by human analysts or traditional security systems. These capabilities enable AI to identify potential security breaches early, even those involving sophisticated tactics like credential stuffing or lateral movement within the network. By flagging these deviations promptly, AI enhances the ability of security teams to respond swiftly and mitigate potential damage, thereby significantly strengthening the overall security posture of the organization.

Anomaly Detection: Through unsupervised learning techniques, AI systems can identify anomalies without needing prior knowledge of specific threats. These models analyze data to recognize patterns and detect deviations from normal behavior. By understanding what constitutes typical activity, AI can spot unusual behavior indicative of novel threats. This feature shines in the face of polymorphic malware, which alters its code on a regular basis to avoid detection, and zero-day assaults, which take advantage of vulnerabilities that have not been publicly disclosed. By focusing on deviations rather than known signatures, unsupervised learning enables AI to uncover and respond to new and evolving cyber threats swiftly and efficiently.

Predictive Analytics: Predictive models use past data to foretell potential dangers. The probability of certain types of attacks happening again can be determined by AI by examining historical occurrences, trends, and patterns. Through this study, AI is able to foresee possible dangers and proactively set up defenses. For instance, AI can foresee future attempts by a certain kind of malware to exploit a specific vulnerability and notify the security team. Organizations can fortify their defenses and take preventative actions by adopting this proactive strategy so avoiding attacks before they do damage. In order to keep a strong cybersecurity stance, such planning is essential.

Real-Time Monitoring and Anomaly Detection with AI

Continuous and adaptive monitoring of network activities is being provided by AI-powered real-time monitoring and anomaly detection, which is fundamentally altering cybersecurity. These state-of-the-art systems quickly process and analyze massive amounts of data from a variety of sources, such as system logs, user actions, and network traffic, using machine learning algorithms. As they happen, this allows for the quick detection of suspicious activity. Artificial intelligence models undergo extensive training to identify and establish patterns of usual network behavior, including typical user activities, data flows, and access times. By creating these baselines, AI can detect deviations that may indicate potential threats. Moreover, AI systems can automatically correlate data from diverse sources, improving threat detection accuracy. For instance, an unusual login attempt combined with an unexpected data transfer might seem harmless individually but can signify a security breach when analyzed together. Unsupervised learning techniques enable these systems to identify anomalies without requiring labeled training data, making them effective against unknown threats. The behavioral analysis further enhances security by continuously monitoring user and entity behaviors, spotting anomalies like irregular data transfers or atypical access patterns, which is crucial for detecting insider threats and compromised accounts. Additionally, AI systems continuously adapt and learn from new data, ensuring they remain effective against evolving threats, thereby solidifying their role as essential tools in modern cybersecurity defenses [24-26].

The Role of Machine Learning in Identifying Malware

ML plays a pivotal role in fortifying defenses against malware threats. Sophisticated algorithms, machine learning enables the precise identification and classification of malicious software with heightened accuracy. By departing from traditional signature-based methods and instead scrutinizing patterns and behaviors, machine learning models adeptly discern novel and evolving malware strains that frequently elude conventional detection techniques. Supervised learning algorithms may learn to distinguish between safe and malicious files by analyzing complex factors like network traffic, code structures, and file behavior. Unsupervised learning techniques augment detection capabilities by autonomously clustering data and identifying aberrations indicative of previously unknown or zero-day malware. Deep learning architectures, notably CNNs and RNNs, excel in processing intricate data formats like binary files and network packets, unearthing subtle indicators of malware activity. Continuously refined with the infusion of real-time threat intelligence, machine learning frameworks dynamically adapt to emergent threats, thereby furnishing cybersecurity defenses with a potent arsenal for robust malware detection and mitigation, emblematic of the transformative impact of artificial intelligence in safeguarding digital ecosystems [27-29].

Challenges and Limitations of AI in Cyber Defense

The use of AI brings both new possibilities and new threats to the field of cybersecurity. Though AI-driven solutions improve defense mechanisms, they also increase the attack surface, making systems vulnerable to attackers who can trick AI algorithms with adversarial attacks, such as adversarial examples. Deep learning models and other opaque AI algorithms make interpretability difficult, which reduces confidence in AI-driven choices and makes validation more difficult. Significant obstacles to training reliable and resilient AI models are data issues, such as the lack of labeled training data and the requirement for ongoing upgrades to handle changing threats. It is important to carefully assess and continuously monitor AI systems to ensure they do not unintentionally reinforce biases in the training data. This could result in discriminating outcomes or the failure to detect specific threat vectors. To overcome these obstacles, lawmakers, cybersecurity professionals, and AI researchers must work together to create accountable deployment plans and open governance frameworks. Collectively tackling these concerns will allow stakeholders to make use of AI in cybersecurity while reducing risks and strengthening defenses against new attacks [30-36].

Increased Attack Surface: AI-driven solutions, while promising for cyber defense, introduce new vulnerabilities and expand the attack surface. Adversaries can exploit these vulnerabilities through adversarial attacks, such as adversarial examples, to deceive AI algorithms and compromise cyber defense mechanisms. These attacks can manipulate input data in subtle ways, leading AI systems to make incorrect decisions or classifications, posing serious risks to cybersecurity infrastructure and data integrity.

Opacity and Interpretability: The inability to comprehend and trust the decisions made by many AI algorithms—especially deep learning models—is due to their lack of interpretability and transparency. This lack of transparency makes it harder to validate and makes it harder to identify and counteract possible dangers. Without clear insight into how AI algorithms arrive at their conclusions, cybersecurity professionals may struggle to identify and address vulnerabilities or malicious activities in a timely manner.

Data Challenges: Training robust and accurate AI models for cyber defense is made much more difficult by the dearth of labelled training data. Due to the ever-changing nature of cyber threats, training datasets must be regularly updated to keep AI models effective against new attack vectors. However, acquiring and curating large-scale, diverse datasets for training can be resource-intensive and may require substantial infrastructure and expertise.

Biases and Discrimination: AI systems trained on biased or incomplete datasets may inadvertently perpetuate biases and lead to discriminatory outcomes in cyber defense applications. Biases present in training data can result in AI models overlooking certain threat vectors or unfairly targeting specific demographics. Addressing these biases requires careful consideration of dataset composition, algorithmic fairness, and ongoing monitoring to ensure that AI-driven cyber defense mechanisms remain unbiased and equitable.

Interdisciplinary Collaboration: Effectively addressing the challenges of AI in cyber defense requires interdisciplinary collaboration among cybersecurity experts, AI researchers, and policymakers. The development of open governance frameworks and accountable deployment techniques to reduce risks and maximize the advantages of AI-driven cyber defense requires collaborative efforts. Stakeholders may improve their cybersecurity posture and react to new threats by working together and sharing knowledge across disciplines to build AI-powered solutions [37-40].

Conclusion

As a conclusion, the use of AI in cybersecurity is a huge step forward in protecting against cyberattacks that are getting smarter all the time. Companies can now better anticipate and prevent such breaches with the help of AI-driven solutions, which offer unmatched capabilities in threat detection, real-time monitoring, and predictive analytics. Although there are many advantages, there are also significant risks and difficulties that must be carefully considered and addressed. Systems are more vulnerable to exploitation by adversaries who can trick AI algorithms through adversarial attacks, as the attack surface expands as a result of AI-driven solutions. There is a lack of faith in judgements made by AI and validation attempts are impeded because of the difficulties in understanding some AI algorithms, especially deep learning models. Training accurate and resilient AI models is made more difficult by data issues, such as the lack of tagged training data and the requirement for ongoing upgrades to handle changing threats. Concerns about discriminating outcomes and threat vector oversight arise from the potential for AI systems to perpetuate biases existing in training data. To overcome these obstacles, cybersecurity professionals, artificial intelligence (AI) researchers, and lawmakers must work together to create accountable deployment plans and open governance frameworks. Assuring the ethical and responsible use of AI technologies to protect digital assets and privacy can be achieved through the promotion of collaboration and transparency, which will help stakeholders better understand the intricacies of AI in cybersecurity. The potential of AI to strengthen cybersecurity defences is enormous, but we must not ignore the risks and difficulties that come with it. In the dynamic field of cybersecurity, stakeholders may fully utilise AI by working together and taking proactive steps to reduce risks and strengthen defences against new threats.

References

1. Nganga A, Scanlan J, Lützhöft M, Mallam S (2024) Enabling Cyber Resilient Shipping Through Maritime Security Operation Center Adoption: A Human Factors Perspective. Appl. Ergon 119.
2. Shukla D, Chakrabarti S, Sharma A (2024) Blockchain-based cyber-security enhancement of cyber–physical power system through symmetric encryption mechanism. Int. J. Electr. Power Energy Syst 155: 109631.
3. Durst S, Hinteregger C, Zieba M (2023) The effect of environmental turbulence on cyber security risk management and organizational resilience. Comput Secur 137: 103591.
4. Patterson CM, Nurse JRC, Franqueira VNL (2024) I don't think we're there yet: The practices and challenges of organisational learning from cyber security incidents. Comput Secur 139.
5. Sabaliauskaite G, Bryans J, Jadidbonab H, Ahmad F, Shaikh S, et al. (2023) TOMSAC - Methodology for trade-off management between automotive safety and cyber security. Comput Secur 140: 103798.
6. Cartwright A, Cartwright E, Edun ES (2023) Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies. Comput Secur 131.
7. Tonhauser M, Ristvej J (2023) Cybersecurity Automation in Countering Cyberattacks. Transp Res Procedia 74: 1360-1365.
8. Bozorgchenani A, Zarakovitis CC, Chien SF, Ting TO, Ni Q, et al. (2023) Novel modeling and optimization for joint Cybersecurity-vs-QoS Intrusion Detection Mechanisms in 5G networks. Comput. Networks 237: 110051.
9. Rizvi M (2023) Enhancing cybersecurity: The power of artificial intelligence in threat detection and prevention. Int J Adv Eng Res Sci 10: 55-60.
10. Srinivasan R, Kavitha M, Kavitha R, Uma S (2023) Cybersecurity and Artificial Intelligence: A Systematic Literature Review. Recent Trends Comput Intell Its Appl pp. 33-345.
11. Jada I, Mayayise TO (2024) The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. Data Inf Manag 8: 100063.
12. Alotaibi SD, Alabduallah B, Yahia S, Siwar Ben HH, Abdulaziz A Alzubaidi, et al. (2024) Bioinspired artificial intelligence based android malware detection and classification for cybersecurity applications. Alexandria Eng J 100: 142-152.
13. Pawlicki M, Pawlicka A, Kozik R, Choraś M (2024) Advanced insights through systematic analysis: Mapping future research directions and opportunities for xAI in deep learning and artificial intelligence used in cybersecurity. Neurocomputing 590: 127759.
14. Shamsan Saleh AM (2024) Blockchain for secure and decentralized artificial intelligence in cybersecurity: A comprehensive review. Blockchain Res Appl 100193.
15. Ramos-Cruz B, Andreu-Perez J, Martínez L (2024) The cybersecurity mesh: A comprehensive survey of involved artificial intelligence methods, cryptographic protocols and challenges for future research. Neurocomputing 581: 127427.
16. Kelly BS, Quinn C, Belton N, Lawlor A, Killeen RP, et al. (2023) Cybersecurity considerations for radiology departments involved with artificial intelligence. Eur Radiol 33: 8833-8841.
17. Mishra S (2023) Exploring the Impact of AI-Based Cyber Security Financial Sector Management. Appl Sci 13.
18. Ait Temghart A, Marwan M, Baslam M (2023) Stackelberg Security Game for Optimizing Cybersecurity Decisions in Cloud Computing. Secur Commun Networks 2023: 1-13.
19. Gaith R, Jamal B, Omar AW, Rabeb M, Alyssa S, et al. (2023) A Survey on Explainable Artificial Intelligence for Cybersecurity. IEEE Trans Netw Serv Manag 20: 5115-5140.
20. Kaur R, Gabrijelčič D, Klobučar T (2023) Artificial intelligence for cybersecurity: Literature review and future research directions. Inf Fusion 97.
21. Michalec O, Shreeve B, Rashid A (2023) Who will keep the lights on? Expertise and inclusion in cyber security visions of future energy systems. Energy Res Soc Sci 106: 103327.
22. Sharma D, Mittal R, Sekhar R, Shah P, Renz M (2023) A bibliometric analysis of cyber security and cyber forensics research. Results Control Optim 10: 100204.
23. Rawindaran N, Jayal A, Prakash E, Hewage C (2023) Perspective of small and medium enterprise (SME's) and their relationship with government in overcoming cybersecurity challenges and barriers in Wales. Int J Inf Manag Data Insights 3: 100191.
24. Botta A, Rotbei S, Zinno S, Ventre G (2023) Cyber security of robots: A comprehensive survey. Intell Syst with Appl 18: 200237.
25. M, Haleem A, Singh RP, Suman R (2023) Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. Cyber Secur Appl 1.
26. Agrawal J, Kalra SS, Gidwani H (2023) AI in cyber security. Int J Commun Inf Technol 4: 46-53.
27. Bıçakcı AS, Evren AG (2022) Thinking multiculturality in the age of hybrid threats: Converging cyber and physical security in Akkuyu nuclear power plant. Nucl Eng Technol 54: 2467-2474.
28. Bahassi H, Edddermoug N, Mansour A, Mohamed A (2021) Toward an exhaustive review on Machine Learning for Cybersecurity. Procedia Comput Sci 203: 83-587.
29. Srivastava S, Paul B, Gupta D (2022) Study of Word Embeddings for Enhanced Cyber Security Named Entity Recognition. Procedia Comput Sci 218: 449-460.
30. Branley-Bell D, Coventry L, Dixon M, Joinson A, Briggs P (2022) Exploring Age and Gender Differences in ICT Cybersecurity Behaviour. Hum Behav Emerg Technol 2022.
31. Xue X, Tan W (2022) Matching Cybersecurity Ontologies on Internet of Everything through Coevolutionary Multiobjective Evolutionary Algorithm. Secur Commun Networks 2022.
32. Akram B, Jan N, Nasir A, Alabrah A, Alhilal MS, et al. (2022) Cyber-Security and Social Media Risks Assessment by Using the Novel Concepts of Complex Cubic T-Spherical Fuzzy Information. Sci Program 2022.
33. Mahmood S, Chadhar M, Firmin S (2022) Cybersecurity Challenges in Blockchain Technology: A Scoping Review. Hum Behav Emerg Technol 2022: 1-11.
34. Fabien C, Harry CT, Solayman A, François GP, Yufei H, et al. (2022) Explainable artificial intelligence for cybersecurity: a literature survey. Ann des Telecommun 77: 789-812.
35. Jun Y, Craig A, Shafik W, Sharif L (2021) Artificial Intelligence Application in Cybersecurity and Cyberdefense. Wirel Commun Mob Comput 2021.

36. Ramadan RA, Aboshosha BW, Alshudukhi JS, Alzahrani AJ, El-Sayed A, et al. (2021) Cybersecurity and Countermeasures at the Time of Pandemic. J Adv Transp 2021.
37. Xie B, Shen G, Guo C, Cui Y (2021) The Named Entity Recognition of Chinese Cybersecurity Using an Active Learning Strategy. Wirel Commun Mob Comput 2021.
38. Piotr K, Krzysztof K, Paweł K, Andrzej O, Karol B, et al. (2021) Cyber-Security Assessment of Industry 4.0 Enabled Mechatronic System. Complexity 2021.
39. Das R, Sandhane R (2021) Artificial Intelligence in Cyber Security. J Phys Conf Ser 1964.
40. Sarker IH, Furhad MH, Nowrozy R (2021) AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. SN Comput Sci 2.