OPEN ACCESS
World Journal of Arts, Education and Literature
ISSN: 3049-0766 | Vol. 2, No. 10, Oct. 2025
Website: https://wasrpublication.com/wjael/

Artificial Intelligence (AI) Cybersecurity: review paper

Ms. Amna Hassan Ali Al-Shidi*

IT Instructor, University of Buraimi, Oman.

Received: 11/07/2025	Accepted: 20/09/2025	Published: 23/10/2025

Abstract: The rapid advancement of technology has led up to the amalgamation of artificial intelligence into cybersecurity, with a strong focus on its ability to enhance security protocols. AI is distinctive by its capability to mimic human intelligence and plays a big role in performing repetitive tasks and providing responses to potential threats. The AI technologies discussed in previous studies in this paper, such as machine and deep learning, and others, enable systems to identify and predict vulnerabilities and respond to incidents at present. The literature review in this paper includes studies from 2018 to 2025 that investigation the application and use of (AI) in cybersecurity, its challenges, ethical considerations, and benefits. Notably, data privacy challenges, ethical challenges such as algorithmic biases, and the need for explainable AI (XAI) are highlighted. This research paper has reached many of the findings included in previous studies, revealing gaps in research and emphasizing the need to develop proficiency and implement skills in AI applications in the field of cybersecurity. The researcher used systematic literature review methodology, categorizing and dividing studies according to thematic structure, such as the "National Institute of Standards and Technology" (NIST) Cybersecurity Framework. The results demonstrated that AI can significantly assist defense mechanisms in various areas, including intrusion detection and malware identification, and network anomaly detection. In addition, this research paper discussed the challenges of emerging technologies such as blockchain, and clarified the economic, regulatory, and social implications and future direction of AI in the domain of cybersecurity. The main and fundamental challenges identified included the potential for losses, rising costs, and vulnerabilities in AI systems. This study emphasizes the need to explore new AI technologies and integrate them with other technologies to promote and develop cybersecurity mechanisms. This research ultimately emphasizes the transformative possibility of AI in mitigating cyber threats and enhancing and intensifying comprehensive cybersecurity postures.

Keywords: Artificial Intelligence; Cybersecurity; Deep Learning; Machine Learning.

Cite this Article:

Al-Shidi, A. H. A., (2025). Artificial Intelligence (AI) Cybersecurity: review paper. *World Journal of Arts, Education and Literature*, *2*(10), 1-12.

Introduction

The digital age has led to an increase in cyber-attacks, making cybersecurity a critical pillar for organizations worldwide. While traditional security measures are essential, they may be entirely insufficient to effectively address evolving threats (Dambe et al., 2023). Artificial intelligence, known as the ability, to mimic humans' intelligence through machines and technical tools programmed to learn and think, it appeared as a machine to reinforce and develop cybersecurity by performing tasks, identifying anomalies, and discovering highly effective responses to anticipated threats (Burhanuddin et al.,2024).

Cybersecurity is the application of defense networks, systems, organization, and personal data from cyber-attacks, unauthorized access, damage, etc. It is one of the most important fields for organizations and institutions at the present time (Laato et al., 2024).

Artificial intelligence in cybersecurity has a large range of applications, it contains natural language processing, machine and deep learning (Ankalaki, 2025). These modern technologies and advanced systems enable vulnerability prediction, rapid real-time incident response, and capability to identify modality in data (Adewusi et al., 2024).

The development of (AI), machines and deep learning is expanding very rapidly, impacting various fields, including cybersecurity (Geluvaraj et al., 2019). The primary goal of systems design is to configure and configure machines to function as if they possess and contain human intelligence, enabling them to solve problems and complete complex tasks (Balajiet al., 2024). In the scope of cybersecurity, these modern technologies help detect and identify cyber threats and respond to them immediately, which are currently evolving at a rapid pace, eliminating the need for traditional detection methods (Nageab al., 2024).

This paper explores the role of (AI) in cybersecurity, discussing its most important current applications, challenges, prospects, and benefits. By integrating artificial intelligence with traditional security practices, institutions and organizations can enhance and strengthen their defense mechanisms and procedures and ensure better data protection against all cyber threats.

***Corresponding Author**

Ms. Amna Hassan Ali Al-Shidi*

IT Instructor, University of Buraimi, Oman

1. Literature Review: First Section Covers Studies Published Between (2018 to 2021)

1.1 To begin with, the study by Apruzzese et al., (2018) this study focused on the applications and techniques of machine and deep learning around cybersecurity. The researchers used a literature review to assess the benefits of these approaches in developing and improving systems security methods and procedures. They also examined and focused on the moral implications of using artificial intelligence in cybersecurity. This study identified the multiple ways in which machine and deep learning can enhance and improve cybersecurity, especially in the areas of threat identification, detection, and systems security, with a focus on the ethical implications that must be considered when applying and using artificial intelligence in cybersecurity.

1.2 Furthermore, the study by Blancaflor et al., (2020) this study takes a qualitative approach to understanding the ethical integration of (AI) into cybersecurity, focusing on balancing AI's capabilities and effectiveness in cybersecurity while ensuring and protecting ethical standards and human rights. It highlights apprehensiveness such as data confidentiality and algorithmic bias, two critical issues when applying AI technologies to cybersecurity. This integration may require equal protection of human rights as AI advances.

1.3 Additionally, the study by Zhang et al., (2020) this study utilizes a literature review and competitive analysis approach to discuss the role of artificial intelligence (AI) in addressing cybersecurity challenges, strongly emphasizing the lack of AI-specific competencies. It proposes organizing and implementing cybersecurity competitions as an effective tool for developing expertise and competencies in this field. It also focuses on building the human capital necessary to meet the growing demand for AI applications in cybersecurity and ensuring the readiness of specialized experts to confront advanced cyber threats.

1.4 Moreover, Bokhari (2020) this study explores various AI-based security techniques, by using a literature review approach, and it focuses on intrusion detection, malware, and network anomalies. It also discusses the progress role of AI in countering and addressing cybersecurity threats, predominately in 5G networks. Modern AI technologies play a powerful role in enhancing and improving the overall security and protection of modern network infrastructure and malware detection, given the growing number of cyber threats. Figure: (1) Explains the path of the framework suggested by the previous study to know the level of cybersecurity in smart cities, and the moderating importance of stakeholder engagement was systematically tested using structural equation modeling (SEM) in SmartPLS 4.0.

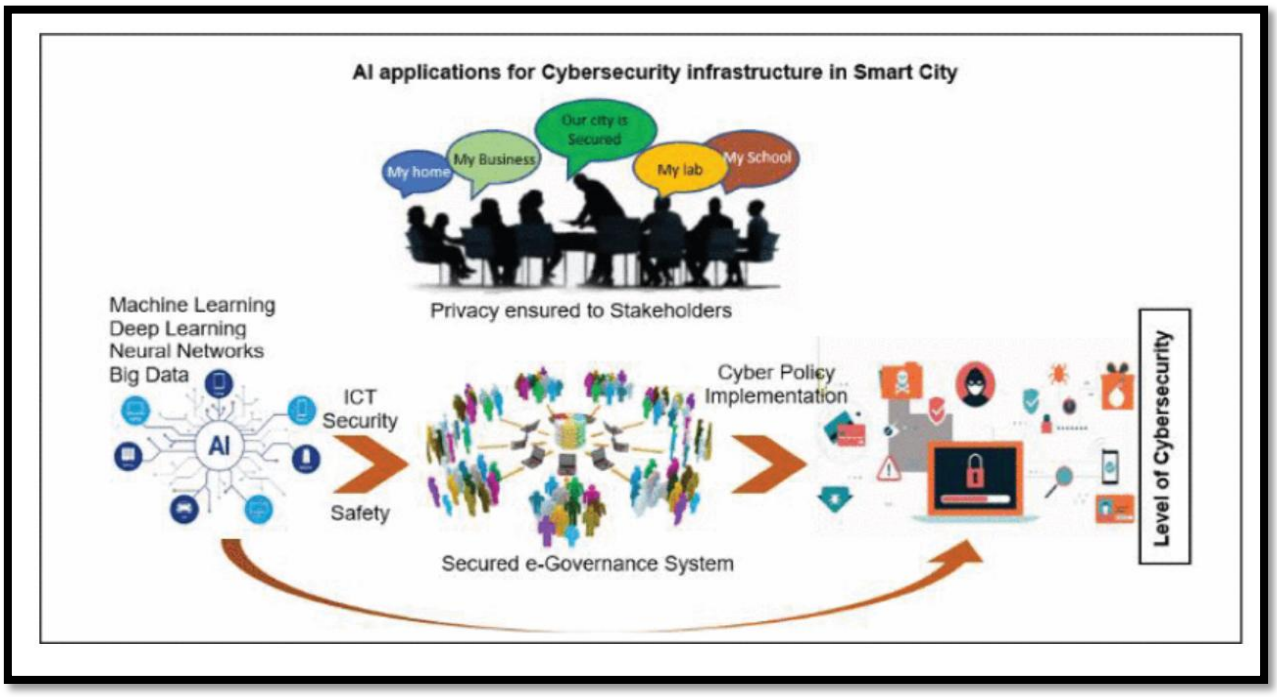


Figure: (1) (Bokhari, 2020)

1.5 In addition, Morovat (2020) this study uses a literature review to explore the evolving impact of artificial intelligence for improving and supporting cybersecurity, with increasing prevalence of cyberattacks, AI technologies are being used to create and design intelligent models that are fully capable of protecting systems from phishing and other threats. This study highlights the rapid developments in AI to address growing security challenges and it has become a key component of modern cybersecurity protection systems.

1.6 Furthermore, this study by Welukar et al., (2021) this study utilizes data analysis to examine how AI processes massive amounts of data efficiently, identifies methods, and provides a response to threats. It highlights various AI applications and techniques, such as fraud detection and botnet detection, while considering challenges such as high costs, privacy concerns, and potential job losses. Despite these challenges, the study demonstrates that AI can respond quickly to threats and can enhance cybersecurity, enabling robust security measures.

1.7 Moreover, the study by Hariharan et al., (2021) this study utilizes a literature review and qualitative analysis to explore the importance of explainable AI in cybersecurity, it discusses the necessity and importance of making AI decisions clear, while balancing this with accuracy in cybersecurity applications. This study also emphasizes the importance of having highly interpretable evidence (AI) models and methods, as transparency in AI-related decision-making is crucial to enhancing the effectiveness of cybersecurity measures.

1.8 Furthermore, the study by Kaur et al., (2021) this study proposes a classification based on a literature review to categorize AI technologies based on their role in cybersecurity. This classification examines important scientific research papers, discusses AI applications in cybersecurity, and highlights research gaps. This classification helps clarify the various applications of AI in cybersecurity and provides a framework for further research in this area.

1.9 The study by Capuano et al. (2022) used a systematic review and literature review methodology to review over 300 research papers on explainable artificial intelligence (XAI) in cybersecurity. It explores the risks associated with declining AI transparency and how AI methods and approaches can address these challenges. This study identifies areas where AI attacks are likely to be vulnerable due to declining explainability and emphasizes the need to enhance transparency to mitigate security risks.

1.10 Finally, the study conducted by Zhang et al., (2022) in this study, the researchers conducted a comprehensive review of (AI) applications in cybersecurity, focusing on particular areas of interest, including network state awareness, monitoring malicious behavior, detecting abnormal network traffic, authentication, and user access. This study also highlights the challenges that may be encountered in AI deployment mechanisms and the opportunities it offers in enhancing and strengthening cybersecurity protocols. It also highlights the effective contribution of AI in improving and developing system security while addressing the challenges of implementing these technologies.

Results and Discussion of the literature Review according to the above studies:

Serial No.	Author & Year	Problem of Study	Directions/Gaps	Method	Findings
1	Apruzzese et al., 2018	Application of ML and DL in cybersecurity.	The ethical impact of (AI) technologies in the fields of cybersecurity.	Literature review	AI technologies are advancing and improving security levels, but ethical problems such as biases and data privacy need to be processed
2	Blancaflor et al., 2020	The Ethical Integration of (AI) into Cybersecurity.	Balancing the power of AI with human rights and ethical standards.	Qualitative analysis	Artificial intelligence has improved cybersecurity but raises concerns about bias and data privacy.
3	Zhang et al., 2020	Shortage in the number of specialists in artificial intelligence for cybersecurity.	The need for educational programs to build experience in artificial intelligence in the ambit of cybersecurity.	Literature review and analysis of competitions	Artificial intelligence can enhance, strengthen, and support cybersecurity, but it requires greater numbers of skilled professionals.
4	Bokhari, 2020	AI-based security mechanisms and technologies in the scope of cybersecurity.	The role of (AI) in securing 5G networks.	Literature review	Artificial intelligence helps detect malware, especially in complex systems such as 5G.
5	Morovat, 2020	The accelerating impacts of artificial intelligence on cybersecurity.	Rapidly evolving AI technologies address defense and protection against modern threats.	Literature review	Rapid developments in artificial intelligence have helped effectively handling cyber threats.
6	Welukar et al., 2021	The role of (AI) in processing large data for cybersecurity purposes.	Rising costs, privacy concerns, and job displacement.	Case studies and data analysis.	AI improves and enhances the efficiency of threat response time, but it raises the issue of data privacy and high cost.
7	Hariharan et al., 2021	Explainable AI (XAI) in cybersecurity.	Achieving a balance between interpretability and accuracy in cybersecurity decision-making.	Literature review and qualitative analysis.	AI is critical to trust but must balance transparency and decision accuracy
8	Kaur et al., 2021	Classification of AI technologies and applications in cybersecurity.	Identify research gaps in AI-based cybersecurity applications.	Literature review and taxonomy.	Proposing a framework for AI in cybersecurity and identifying key research gaps.
9	Capuano et al., 2022	Lack of transparency in AI systems.	The need for better, explainable (XAI) methods for cybersecurity.	Systematic review	XAI can reduce the risks associated with non-transparent AI, particularly in the areas of cybersecurity.
10	Zhang et al., 2022	AI in user access authentication and network awareness.	Identifying challenges in deploying AI in cybersecurity.	Literature review	Artificial Intelligence enhances and strengthens the security of the system.

2. Literature Review: Second Section Covers Studies Published Between 2023 to 2025

2.1 To begin with, Kauret et al., (2023) in this study, researchers used a comprehensive review of 2,395 studies to categorize AI use cases in cybersecurity, based on the "National Institute of Standards and Technology" (NIST) framework. The study confirmed AI's ability to perform tasks and identify threats efficiently. It also pointed to new future research directions, including exploring new AI technologies for cybersecurity applications and systems.

2.2 In addition, Ozkan-Okay et al., (2024) the researchers used algorithmic analysis and focused on the function of machine learning in malware discovery. The study discussed the importance of minimizing human intervention in real-time threat detection and highlighted how appliances learning algorithms can be used to detect malware and enhance security measures with minimal human oversight.

2.3 Moreover, Yadav et al., (2023) this study explored the potential of "open-source intelligence" (OSINT) to strengthen and enhance cybersecurity, by using a data analysis methodology. It also examined how AI can extract valuable information from publicly obtainable data, such as social media and other open sources, to enhance and improve threat detection and rapid response strategies and mechanisms.

2.4 Furthermore, Michael et al., (2023) they used a literature review methodology to discuss the role of (AI) in performing cybersecurity tasks and responsibilities. The study confirmed AI's strength to identify threats quickly and efficiently, leading to improved cybersecurity operations in organizations. Despite these advantages, the research paper also discussed the risks associated with AI in cybersecurity, including system vulnerabilities.

2.5 Also, study by Choithani et al., (2024) In this research paper, the researchers used a cross-sectional review methodology to explore the application of AI techniques, such as "support vector machines" (SVMs), "artificial neural networks" (ANNs), and long short-term memory (LSTMs), cryptocurrency security. The paper discussed how these techniques can detect fraud and predict prices in the rapidly evolving fields of finance and cybersecurity.

2.6 Moving on to another study in 2024, Jada et al., (2024) Researchers evaluated the effectiveness and efficiency of AI-based technologies in cybersecurity using literature review methodology. They analyzed 73 peer-reviewed articles, focusing on the service of (AI) in enhancing threat intelligence and protection mechanisms. They also highlighted numerous defy, such as attacks and the necessity for high-quality data for AI deployment.

2.7 Similarly, Al Siam et al., (2024) the researchers conducted a literature review to explore the role of AI in five aspects of cybersecurity, as illustrated in figure (2): threat detection and awareness, endpoint security, fraud detection, network security, and authentication. The study also discussed developments in anomaly detection algorithms, machine learning, and deep learning, and identified gaps in current research.

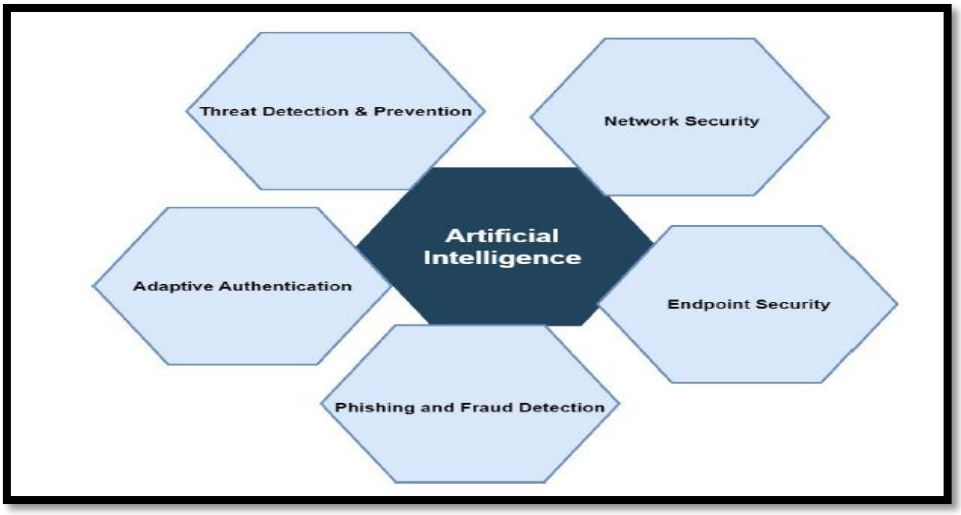


Figure (2) Artificial intelligence solution domains in security

2.8 In addition, Mohammed et al., (2024) the researchers used a literature review methodology to explore AI-powered intrusion detection systems (IDSs) and focused on their advantages over other intrusion detection systems. The study concluded that AI-powered IDSs are more robust in detecting cyber threats, potentially improving and enhancing an organization's overall security framework.

2.9 Furthermore, research conducted by, Ramos et al., (2024) explored how blockchain technologies can enhance and strengthen AI-powered cybersecurity, by using a literature review methodology. They discussed the mechanisms for integrating blockchain with AI to improve data governance and access control, highlighting the potential of blockchain to prevent attacks such as data leakage.

2.10 Moreover, Saleh (2024) The researcher investigated the role of blockchain technologies in providing AI models. This study demonstrated how blockchain can enable stable and transparent data storage, enhancing the integrity and reliability of AI models used in cybersecurity.

2.11 The researcher, Salem et al., (2024) conducted a study that aimed to examine AI-powered cyberattack detection techniques and mechanisms. They analyzed 60 research papers to propose a structure for evaluating the performance of AI in detecting

malware and malicious emails. Also, addressed the importance of leveraging AI to protect against cyber threats.

2.12 A study by Obioha-Val et al., (2025) The researchers used a literature survey method to explore the role of AI in cyber espionage operations. Also, they discussed the offensive applications of artificial intelligence in cyber espionage strategies and plans, emphasizing and clarifying the accuracy of AI-based cyber-attacks and ethical security challenges and concerns.

2.13 As well as studying by Radanliev (2024) the researcher examined the influence of modernistic technologies, such as artificial intelligence, blockchain, and IoT on cybersecurity. The study concluded that these technologies could enhance threat detection and data confidentiality, while introducing new risks, such as AI-driven attacks. The researcher emphasized the need for cooperation among countries to address these challenges.

2.14 Furthermore, Rafy et al., (2025) the study focused on strategies and mechanisms for mitigating risks and vulnerabilities in cybersecurity using artificial intelligence. Researchers used a literature review and risk assessment approach. The study emphasized the negative social and economic consequences and impacts of integrating artificial intelligence into cybersecurity and highlighted the need for effective guidelines and a framework to maximize and enhance the benefits of artificial intelligence while minimizing the potential risks.

2.15 Additionally, Patel et al., (2025) the study explored how to integrate generative AI into cloud security using case studies and algorithm evaluation. It concluded that AI could improve and enhance threat detection and vulnerability management. The study also discussed how AI can enhance operational efficiency, but on the other hand, challenges posed by risks and complex decision-making processes remain.

2.16 Moreover, this study was carried out by a researcher Sontan et al., (2024) they reviewed various papers to examine the effective role of AI in cybersecurity, with a strong focus on machine learning modelsand natural language processing techniques. The study highlighted the potential of artificial intelligence in detecting threats, analyzing vulnerabilities, and responding quickly, while also addressing ethical concerns such as machine learning in cybersecurity.

2.17 In addition, Ajayi et al., (2025) several researchers in this study used machine learning models and data analysis to effectiveness of artificial intelligence. They used machine learning models such as random forest classifiers with a cryptographic transaction dataset. The results showed that security measures using AI helped reduce fraudulent attacks by 76.86%. However, these models had a high false negative rate (89.54%), indicating that many fraudulent actions went undetected due to algorithmic bias. The variance-to-equality ratio was 0.7793. The study proposes improving anomaly detection mechanisms and methods to improve the reliability of AI.

2.18 Jain et al., (2025) they used case studies and forensic analysis to explore the responsibility role of artificial intelligence in cybersecurity forensics and address cyber threat challenges. AI enhances forensic analysis by improving and enhancing the examination of digital evidence and identifying threat actors. The study highlights the impact of AI on privacy and transparency concerns. Real-life cases, such as human trafficking in Thailand and child nudity on Facebook, demonstrate AI's effectiveness in detecting malware and predicting threats. Also, they highlight the need to continue integrating AI in security part to enhance and strengthen forensic analysis capabilities, protect and preserve digital evidence, and improve cybercrime response strategies and mechanisms.

2.19 Moreover, Sharko et al., (2024This study discusses the role of artificial intelligence (AI) algorithms in enhancing and improving the protection and defense of systems. The researchers used a literature review and systems analysis to identify the fundamental strengths of AI in cybersecurity, including its benefits and practical applications at a major global company like Amazon. The study also highlights the advantages of using AI technology to enhance cybersecurity.

2.20 Additionally, Malatji (2024) The researchers in this study used a model development and system analysis methodology to develop a model of human-AI interaction to enhance cybersecurity operations. This model integrates various models of human-machine interaction, such as "interactive systems," to manage AI-based cybersecurity tasks. The model includes five main elements: decision-making matrices, a dynamic model, task allocation, feedback, and interoperability, which together improve efficiency and protect against evolving cyber threats. Further research directions are proposed, including improving the overall understanding of the model through developments in artificial intelligence and machine learning.

2.21 Finally, Nour et al., (2025) Researchers discussed the essential part of artificial intelligence in addressing the challenges faced by traditional cybersecurity methods. They utilized literature reviews and predictive modeling to explore how AI can enhance cybersecurity through various techniques such as automated Learning and data prediction. The paper identifies various AI-based strategies and mechanisms, such as anomaly detection and predictive modeling, to enhance cybersecurity and protection. The paper also addresses the shortcomings of artificial intelligence in cybersecurity, including data privacy concerns and vulnerability to attacks. The paper emphasizes the importance of AI in cybersecurity and provides recommendations for future research and development growth in this field.

Findings and Discussion of the literature Review according to the above studies:

Serial No.	Author & Year	Problem of Study	Directions/Gaps	Method	Findings
1	Kauret et al., 2023	Distinguishing the areas of use and employment of AI in the Sector of cybersecurity.	Review and explore new AI technologies for cybersecurity applications and systems.	Comprehensive review.	AI can perform tasks and improve security, with future trends in developing new AI methods.
2	Ozkan-Okay, 2024	Machine learning in malware detection.	Human intervention has a Essential negative impact on the efficiency of real-time threat detection.	Case study and algorithm analysis.	Machine learning helps reduce human intervention in malware detection and improves timely threat response.
3	Yadav et al., 2023	Open-source intelligence (OSINT) in cybersecurity.	Extracting valuable information from open sources to detect and identify threats.	Data analysis and case studies.	OSINT can enhance and strengthen threat detection and awareness by using publicly available data, such as social media.
4	Michael et al., 2023	Performing cybersecurity tasks using artificial intelligence.	Risk of security vulnerabilities and system failure.	Literature review	AI can detect threats very efficiently, but there are risks related to system vulnerabilities.
5	Choithani et al., 2024	Using artificial intelligence techniques and mechanisms in cryptocurrency security.	Fraud detection and price prediction.	Literature review and case studies.	Artificial intelligence technologies are working to identify fraud and manage cryptocurrency security.
6	Jada et al., 2024	AI-based technologies in cybersecurity.	Challenges posed by attacks and the need for Reliable data.	Literature review	Artificial intelligence is strengthening threat intelligence and protection mechanisms.
7	Al Siam et al., 2024	Artificial intelligence and its role in cybersecurity.	Gaps and loopholes in machine learning and neural Networks for knowledge and anomaly spotting.	Literature survey.	Artificial intelligence has developments in aspects of cybersecurity.
8	Mohammed et al., 2024	AI-based Intrusion Detection Systems (IDSs).	The power of AI compared to other intrusion detection systems.	Literature review, and system evaluation.	AI-powered intrusion detection systems provide flexibility in detecting cyber threats.
9	Ramos et al., 2024	Blockchain technology and its integration with machine learning in cybersecurity.	Blockchain technology can mitigate and reduce the severity of attacks such as data theft.	literature review.	Blockchain technologies can enhance cybersecurity through artificial intelligence, by protecting data.
10	Saleh, 2024	Blockchain technology in securing AI models.	Improving and developing the transparency of AI models.	Literature review, system analysis	Blockchain can enable stable and transparent data storage.
11	Salem et al., 2024	AI-based cyberattack detection mechanisms.	Evaluating the effectiveness and efficiency of artificial intelligence in detecting network intrusions and detecting malware.	Literature review	Artificial intelligence enhances the detection of cyber-attacks by addressing threats and improving response mechanisms.
12	Obioha-Val et al., 2025	Artificial intelligence in cyber espionage.	Precision of AI-driven cyberattacks and attribution challenges.	Literature review	AI plays a role in both offensive and defensive cyber espionage, raising challenges in ethical concerns.
13	Radanliev, 2024	The impact of modern technologies on cybersecurity.	New risks of AI attacks and IoT privacy concerns.	Literature review & policy analysis.	IoT, blockchain, and AI are strengthening cybersecurity, but new risks exist that require international cooperation.
14	Rafy et al., 2025	Mitigating vulnerabilities using artificial intelligence.	Integrating artificial intelligence into cybersecurity and its social and economic impacts.	Literature review & risk assessment	Artificial intelligence can mitigate cybersecurity risks, but strong ethical and economic frameworks are needed.

15	Patel et al., 2025	Integrating AI into cloud security.	Risks and complex decision-making in cloud security.	Case studies & algorithm evaluation	AI improves cloud security but poses challenges due to complex attacks and decisions.
16	Sontan et al., 2024	The contribution of (AI) to Cybersecurity Using machine learning	Ethical Challenges and Machine Learning in Cybersecurity.	Literature review	AI enhances and supports cybersecurity and there are ethical issues, especially regarding learning technologies.
17	Ajayi, 2025	The effectiveness and power of artificial intelligence in detecting fraud using machine learning.	There are high rates of false negatives due to algorithmic bias	Machine learning models & data analysis.	AI reduces fraud by 76.86%, but there are high rates of false negatives due to algorithmic bias.
18	Jain et al., 2025	AI in cybersecurity forensics.	Challenges in cyber threats and incident responses.	Case studies & forensic analysis	Artificial intelligence has enhanced and strengthened forensic analysis and incident responses to cybercrimes, leading to improved digital evidence.
19	Sharko et al., 2024	Artificial intelligence algorithms play a role in improving system protection.	Real-world application in large companies.	Literature review & system analysis	AI enhances system protection and security, especially in large companies
20	Malatji, 2024	Human-AI teamwork model for cybersecurity operations.	Improving understanding processes through artificial intelligence and machine learning.	Model development & system analysis	A model that enhances cybersecurity operations by integrating AI with human decision-making.
21	Nour et al., 2025	The increasing role of (AI) in cybersecurity approaches.	Concerns related to data privacy and attack mitigation.	Literature review & predictive modeling	AI improves cybersecurity by enhancing threat recognition, but data privacy challenges exist.

Research Methodology

In this study, the researcher relied on Comprehensive literature review to evaluate the influence of artificial intelligence in cybersecurity, with a comprehensive focus on automated learning and deep learning. The methodology follows a systematic approach to obtaining comprehensive information on relevant research, enabling the verification of research gaps.

The number of cyber threats has increased significantly, causing significant changes in cybersecurity approaches, and the complexity of attacks is now greater than the capabilities of established strategies, so artificial intelligence technologies must be integrated into cybersecurity (Tariq et al., 2023).

1. Research Design

The researcher relied on qualitative research design and methods, collecting results from conferences, reports, and peer-reviewed scientific articles. The central objectives of this study are:

- Investigating the mechanisms of artificial intelligence in enhancing cybersecurity.
- Addressing ethical issues in the field of AI-based cybersecurity.
- Analyzing challenges and guiding future research.

2. Data Collection

Data collection included relevant studies from academic databases, including:

- IEEE Xplore
- Springer
- Elsevier
- ACM Digital Library
- Academic journal platform
- Google Scholar

3. Inclusion and Exclusion Criteria

To ensure the significance and quality of the selected studies, the researcher applied the following criteria:

Inclusion Criteria:

- The researcher selected articles published in academic journals and conference papers.
- The researcher focused on selecting studies published between 2018 and 2025.
- Research focused on AI technologies in cybersecurity.
- Research papers discuss the challenges of AI in cybersecurity.
- Studies evaluating the impact of AI on cybersecurity operations and risk assessment.

Exclusion Criteria:

- The researcher did not select unreviewed blog posts.
- Research papers using outdated AI methodologies.

4. Data Analysis

The researcher used a thematic analytical approach to categorize the reviewed literature into key areas:

- AI Applications in Cybersecurity.
- Ethical Considerations in AI-Powered Cybersecurity.
- Explainable AI.
- Modern AI Technologies in Cybersecurity.
- Challenges and Future Directions.

5. Ethical Considerations

Ethical considerations were maintained by:

- Avoiding plagiarism.
- The researcher's commitment to presenting the research fairly, without misrepresentation or misinterpretation.
- Allegiance to adhering to the standards and principles of academic integrity.

6. Future Research Directions

Based on previous studies, future research should focus on:

- Analyzing new AI technologies.
- Enhancing AI's ability to counter attacks.
- Integrating AI with other new technologies.

Results and Discussion

Table: (1) Show the number of research areas in this paper:

Subject	Number of Research Studies
AI in Cybersecurity (General)	9 studies
Ethical Considerations in AI and Cybersecurity	2 studies
AI-based Defense Mechanisms	2studies
Explainable AI (XAI) in Cybersecurity	4 studies
AI Taxonomy for Cybersecurity	1 study
Machine Learning for Threat Detection	4 studies
Open-Source Intelligence (OSINT) in Cybersecurity	1 study
AI in Cryptocurrency Security	3 studies
AI and Blockchain Integration	2 studies
AI for Intrusion Detection Systems (IDS)	1 study
AI in Cyber Diplomacy and National Security	2 studies
AI in Cloud Security	1 study
AI-Driven Cyber Forensics	1 study
AI in Cybersecurity Governance and Risk Mitigation	1 study
AI for System Protection in Large Companies	1 study
Human-AI Teaming (HAIT) in Cybersecurity	1 study

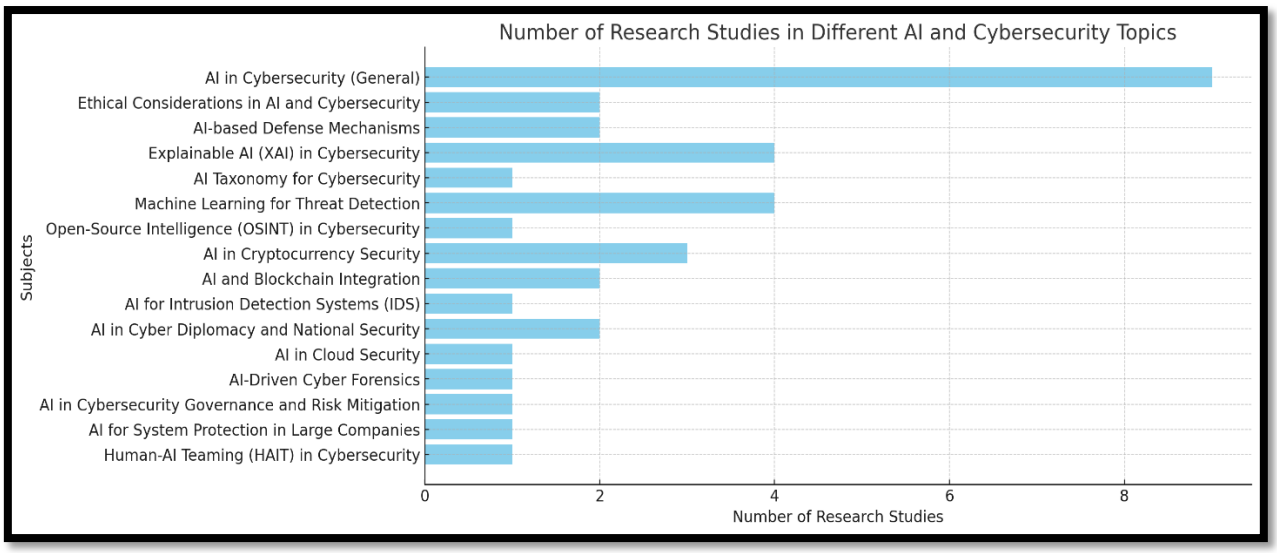


Figure 3

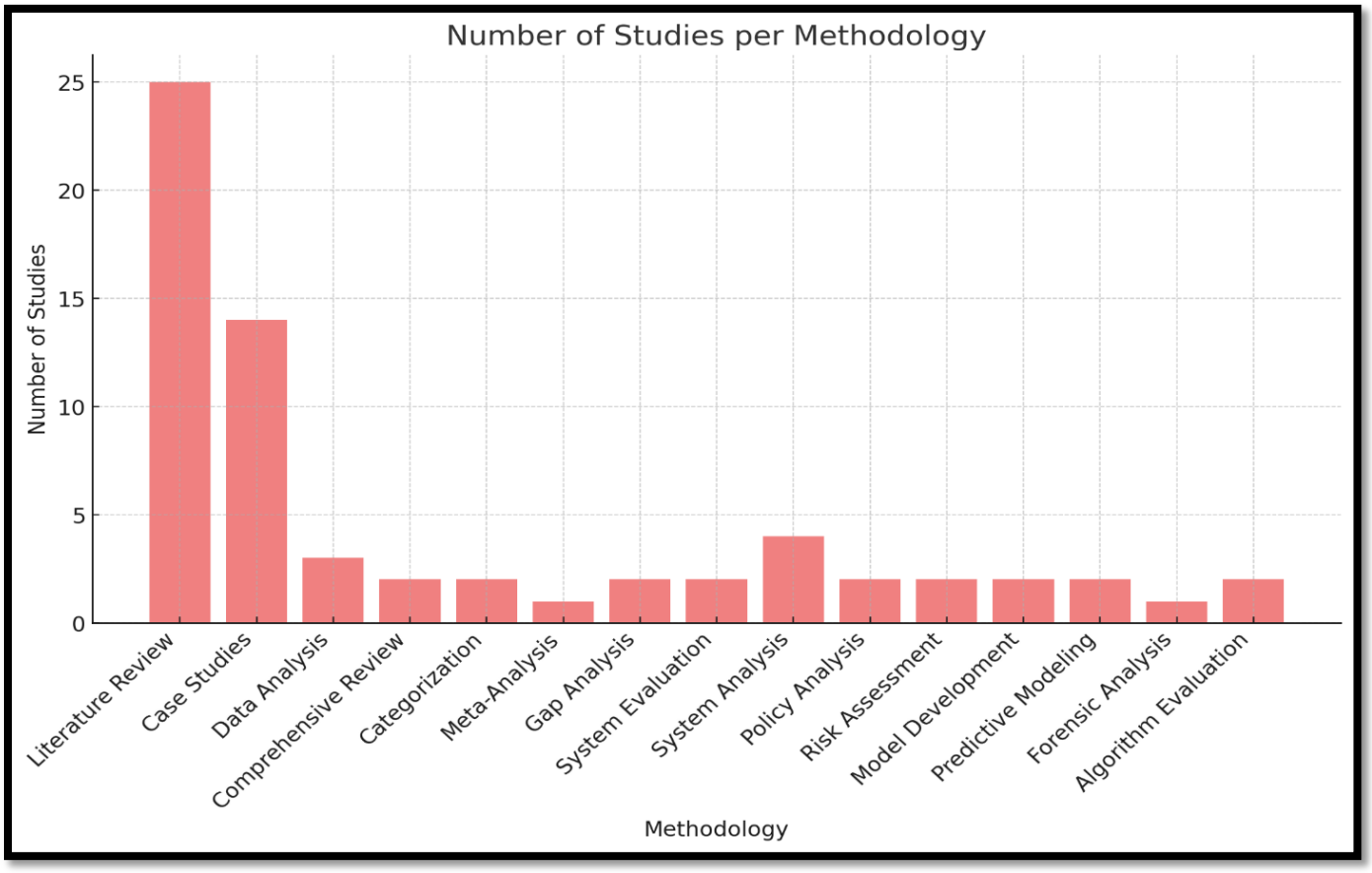
Source: My own preparation.

The graph shows scientific studies on the topics of artificial intelligence and cybersecurity. It also shows that the number of scientific papers in the field of "artificial intelligence in cybersecurity in general" is the largest and of great interest to researchers, while many specialized topics in this field are of less interest to researchers.

Table: (2) Below is a comprehensive summary of the number of studies that used each methodology:

Methodology	Number of Studies
Literature Review	25
Case Studies	14
Data Analysis	3
Comprehensive Review	2
Categorization	2
Meta-Analysis	1
Gap Analysis	2
System Evaluation	2
System Analysis	4
Policy Analysis	2
Risk Assessment	2
Model Development	2
Predictive Modeling	2
Forensic Analysis	1
Algorithm Evaluation	2

The chart shows a representation of the number of studies for each methodology



:

Figure 2

Source: My own preparation.

Conclusion

To summarize: this research paper examines the role of artificial intelligence in enhancing and strengthening cybersecurity, and its potential to enhance digital security and address challenges. With the increasing number of cyber threats, which often fail traditional security methods, this calls for the adoption and use of AI technologies such as machines and deep learning. These technologies have proven effective in detecting threats, handling anomalies, and responding quickly to cyber risks, enabling significant development and increased efficiency in cybersecurity. Previous studies examined by the researcher from 2018 to 2025 have highlighted the applications of AI in cybersecurity, including intrusion detection, malware detection, and fraud prevention. However, the integration of AI has ethical considerations, including algorithmic biases and data privacy. Studies discussing biases and privacy issues have highlighted these issues. Another identified challenge is the decline in the number of AI cybersecurity specialists, underscoring the need for skill-building educational programs that prepare, develop, and qualify the workforce to meet the demand for specialists in this field. Previous studies indicate that explainable AI... In conclusion, while AI offers significant advances in cybersecurity, careful consideration of its challenges and extensive research into its ethical implications is essential. Through a comprehensive understanding of AI capabilities, organizations can design robust cybersecurity systems that can effectively and consistently counter threats.

References

[1] Burhanuddin, L. A. B., Shibghatullah, A. S. B., Ilias, I. S. C., Zainudin, Z. B., & Zamry, N. B. M. (2025). AI-enhanced cybersecurity: A comprehensive review of techniques and challenges. In M. A. Al-Sharafi, M. Al-Emran, M. A. Mahmoud, & I. Arpaci (Eds.), *Current and future trends on AI applications* (Vol. 1178, pp. 107–125). Springer, Cham. https://doi.org/10.1007/978-3-031-75091-5_7

[2] Laato, S., Farooq, A., Tenhunen, H., Pitkämäki, T., Hakkala, A., & Airola, A. (2020). AI in cybersecurity education: A systematic literature review of studies on cybersecurity MOOCs. *In 2020 IEEE 20th International Conference on Advanced Learning Technologies (ICALT)* (pp. 6–10). IEEE. https://doi.org/10.1109/ICALT49669.2020.00009.

[3] Adewusi, A. O., Okoli, U. I., Olorunsogo, T., Adaga, E., Daraojimba, D. O., & Obi, O. C. (2024). Artificial intelligence in cybersecurity: Protecting national infrastructure: A USA review. *World Journal of Advanced Research and Reviews, 21*(1), 2263–2275. https://doi.org/10.30574/wjarr.2024.21.1.0313.

[4] Geluvaraj, B., Satwik, P. M., & Ashok Kumar, T. A. (2019). The future of cybersecurity: Major role of artificial intelligence, machine learning, and deep learning in cyberspace. In S. Smys, R. Bestak, J. Z. Chen, & I. Kotuliak (Eds.), *International Conference on Computer Networks and Communication Technologies* (Vol.

15, pp. 661–668). Springer. https://doi.org/10.1007/978-981-10-8681-6_67.

[5] Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. (2018). On the effectiveness of machine and deep learning for cybersecurity. In 2018 10th International Conference on Cyber Conflict (CyCon) (pp. 371–390). IEEE. https://doi.org/10.23919/CYCON.2018.8405026.

[6] Blancaflor, E. B., Eleccion, F. G., Ferry, F. L., Oplado, J. P., Pajarillo, R. E., & Villaluz, A. (2024). Ethical use of AI for cybersecurity and facing digital threats in the Philippines. *In 2024 IEEE 7th International Conference on Computer and Communication Engineering Technology (CCET)* (pp. 241–245). IEEE. https://doi.org/10.1109/CCET62233.2024.10837790.

[7] Zhang, F., Cui, X., Wang, Z., Chen, S., Liu, Q., & Liu, C. (2020). A systematic study of AI applications in cybersecurity competitions. In 2020 IEEE 14th International Conference on Big Data Science and Engineering (BigDataSE) (pp. 138–146). IEEE. https://doi.org/10.1109/BigDataSE50710.2020.00026.

[8] Bokhari, S. A. A., & Myeong, S. (2023). The influence of artificial intelligence on e-Governance and cybersecurity in smart cities: A stakeholder's perspective. *IEEE Access, 11*, 69783-69797. https://doi.org/10.1109/ACCESS.2023.3293480.

[9] Morovat, K., & Panda, B. (2020). A survey of artificial intelligence in cybersecurity. *In 2020 International Conference on Computational Science and Computational Intelligence (CSCI)* (pp. 109–115). IEEE. https://doi.org/10.1109/CSCI51800.2020.00026.

[10] Welukar, J. N., & Bajoria, G. P. (2021). Artificial intelligence in cybersecurity - A review. *International Journal of Scientific Research in Science and Technology (IJSRST), 8*(6), 488–491. https://doi.org/10.32628/IJSRST218675.

[11] Hariharan, S., Velicheti, A., Anagha, A. S., Thomas, C., & Balakrishnan, N. (2021). Explainable artificial intelligence in cybersecurity: A brief review. *In 2021 4th International Conference on Security and Privacy (ISEA-ISAP)* (pp. 1–12). IEEE. https://doi.org/10.1109/ISEA-ISAP54304.2021.9689765.

[12] Kaur, H., & Tiwari, R. (2021). Endpoint detection and response using machine learning. *Journal of Physics: Conference Series, 2062*(1), 012013. https://doi.org/10.1088/1742-6596/2062/1/012013.

[13] Capuano, N., Fenza, G., Loia, V., & Stanzione, C. (2022). Explainable artificial intelligence in cybersecurity: A survey. IEEE Access, 10, 93575–93600. https://doi.org/10.1109/ACCESS.2022.3204171.

[14] Zhang, Z., Ning, H., Shi, F., et al. (2022). Artificial intelligence in cybersecurity: Research advances, challenges, and opportunities. *Artificial Intelligence Review, 55*, 1029–1053. https://doi.org/10.1007/s10462-021-09976-0.

[15] Kauret, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion, 97*, 101804. https://doi.org/10.1016/j.inffus.2023.101804.

[16] Ozkan-Okay, M., et al. (2024). A comprehensive survey: Evaluating the efficiency of artificial intelligence and machine learning techniques on cybersecurity solutions. *IEEE Access, 12*, 12229–12256. https://doi.org/10.1109/ACCESS.2024.3355547.

[17] Yadav, A., Kumar, A., & Singh, V. (2023). Open-source intelligence: A comprehensive review of the current state, applications, and future perspectives in cybersecurity. *Artificial Intelligence Review, 56*(11), 12407–12438. https://doi.org/10.1007/s10462-023-10454-y.

[18] Michael, K., Abbas, R., & Roussos, G. (2023). AI in cybersecurity: The paradox. *IEEE Transactions on Technology and Society, 4*(2), 104-109. https://doi.org/10.1109/TTS.2023.3280109

[19] Choithani, T., Chowdhury, A., Patel, S., & others. (2024). A comprehensive study of artificial intelligence and cybersecurity on Bitcoin, cryptocurrency, and banking system. *Annals of Data Science, 11*, 103–135. https://doi.org/10.1007/s40745-022-00433-5

[20] Jada, I., & Mayayise, T. O. (2024). The impact of artificial intelligence on organisational cybersecurity: An outcome of a systematic literature review. *Data and Information Management, 8*(2), 100063. https://doi.org/10.1016/j.dim.2023.100063.

[21] Al Siam, A., Alazab, M., Awajan, A., & Faruqui, N. (2024). A comprehensive review of AI's current impact and future prospects in cybersecurity. *IEEE Access, 13*, 14029-14050. https://doi.org/10.1109/ACCESS.2025.3528114

[22] Mohammed, Y. B., Badara, M. S., & Dan'azumi, H. (2024). An intelligence-based cybersecurity approach: A review. *Journal of Intelligent Communication, 3*(2), 32–43. https://doi.org/10.54963/jic.v4i1.232

[23] Ramos, S., & Ellul, J. (2024). Blockchain for artificial intelligence (AI): Enhancing compliance with the EU AI Act through distributed ledger technology. A cybersecurity perspective. *International Cybersecurity Law Review, 5*, 1–20. https://doi.org/10.1365/s43439-023-00107-9

[24] Saleh, A. M. S. (2024). Blockchain for secure and decentralized artificial intelligence in cybersecurity: A comprehensive review. *Blockchain: Research and Applications, 5*, 100193. https://doi.org/10.1016/j.bcra.2024.100193.

[25] Salem, A. H., Azzam, S. M., & Emam, O. E. (2024). Advancing cybersecurity: A comprehensive review of AI-driven detection techniques. *Journal of Big Data, 11*(105). https://doi.org/10.1186/s40537-024-00957-y

[26] Obioha-Val, O. A., et al. (2025). Cyber espionage in the age of artificial intelligence: A comparative study of state-sponsored campaigns. *Asian Journal of Research in Computer Science, 18*(1), 184–204. https://doi.org/10.9734/ajrcos/2025/v18i1557.

[27] Radanliev, P. (2024). Cyber diplomacy: Defining the opportunities for cybersecurity and risks from artificial intelligence, IoT, blockchains, and quantum computing. *Journal of Cyber Security Technology, 9*(1), 28–78. https://doi.org/10.1080/23742917.2024.2312671.

[28] Rafy, M. F. (2024). Artificial intelligence in cybersecurity. *SSRN*. http://dx.doi.org/10.2139/ssrn.4687831

[29] Patel, A., Pandey, P., Ragothaman, H., Molleti, R., & Peddinti, D. R. (2025). Generative AI for automated security operations in cloud computing. *2025 IEEE 4th International Conference on AI in Cybersecurity (ICAIC)*, Houston, TX, USA, 1–7. https://doi.org/10.1109/ICAIC63015.2025.10849302.

[30] Sontan, A. D., & Samuel, S. V. (2024). The intersection of artificial intelligence and cybersecurity: Challenges and opportunities. *World Journal of Advanced Research and Reviews, 21*(2), 1720–1736. https://doi.org/10.30574/wjarr.2024.21.2.0607

[31] Ajayi, A. J., Joseph, S. A., Metibemu, O. C., Olutimehin, A. T., Balogun, A. Y., & Olaniyi, O. O. (2025). The impact of artificial intelligence on cybersecurity in digital currency transactions. *Archives of Current Research International*, *25*(2), 329–351. https://doi.org/10.9734/acri/2025/v25i21090.

[32] Jain, P., Verma, P., Debnath, T., & Balouria, S. (2025). Cybersecurity forensics with AI. In *Quantum computing* (Chap. 10). https://doi.org/10.1201/9781003499459-10

[33] Sharko, A. D., Sharko, G., & Qose, S. (2024). Artificial intelligence in cybersecurity applications. In *Proceedings of the 2024 IEEE 28th International Conference on Intelligent Engineering Systems (INES)* (pp. 175-180). IEEE. https://doi.org/10.1109/INES63318.2024.10629129

[34] Malatji, M., & Tolah, A. (2024). Artificial intelligence (AI) cybersecurity dimensions: A comprehensive framework for understanding adversarial and offensive AI. *AI & Ethics.* https://doi.org/10.1007/s43681-024-00427-4

[35] Nour, S. M., & Said, S. A. (2024). Harnessing the power of AI for effective cybersecurity defense. In *Proceedings of the 2024 6th International Conference on Computing and Informatics (ICCI)* (pp. 98-102). IEEE. https://doi.org/10.1109/ICCI61671.2024.10485059

[36] Dambe, S., Gochhait, S., & Ray, S. (2023). The role of artificial intelligence in enhancing cybersecurity and internal audit. *2023 3rd International Conference on Advancement in Electronics & Communication Engineering (AECE)*, 88–93. https://doi.org/10.1109/AECE59614.2023.10428353

[37] Balaji, T. S., Nadanasabai, R., Ravikumar, R. J., Sharanyaa, S., Meenal, R., & Deepthi, N. P. (2024). Research on the application of artificial intelligence in cybersecurity: Integrating advanced technologies to improve threat detection and response. *Proceedings of the 2024 5th IEEE Global Conference for Advancement in Technology (GCAT)*, 1–6. https://doi.org/10.1109/GCAT62922.2024.10923991

[38] Nageab, W. M., Alrasheed, R., & Khalifa, M. (2024). Cybersecurity in the era of artificial intelligence: Risks and solutions. *2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS)*, 240–245. https://doi.org/10.1109/ICETSIS61505.2024.10459584

[39] Ankalaki, S., Atmakuri, A. R., Pallavi, M., Hukkeri, G. S., Jan, T., & Naik, G. R. (2025). Cyber attack prediction: From traditional machine learning to generative artificial intelligence. *IEEE Access*, *13*, 44662–44706. https://doi.org/10.1109/ACCESS.2025.3547433

[40] Tariq, U., Ahmed, I., Bashir, A. K., & Shaukat, K. (2023). A critical cybersecurity analysis and future research directions for the Internet of Things: A comprehensive review. *Sensors*, *23*(8), 4117. https://doi.org/10.3390/s23084117