I. J. Education and Management Engineering, **2025, 1, 44-51**
Published Online on February 8, 2025 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijeme.2025.01.04

Artificial Intelligence in Security and Privacy: A Study on AI's Role in Cybersecurity and Data Protection

Mahmoud Mohamed*
Electrical and Computer Engineering, King Abdul Aziz University, Saudi Arabia
E-mail: mhassan0073@stu.kau.edu.sa
ORCID iD: https://orcid.org/0009-0003-5213-4019
*Corresponding Author

Khaled Alosman
Electrical and Computer Engineering, King Abdul Aziz University, Saudi Arabia
E-mail: kalosman@stu.kau.edu.sa
ORCID iD: https://orcid.org/0009-0004-1007-6516

Received: 27 May, 2024; Revised: 27 July, 2024; Accepted: 01 November, 2024; Published: 08 February, 2025

Abstract: The increase in value of security and privacy is compounded by the rapid advancements in the digital landscape sprouting new problems in information security. This research explores the use of artificial intelligence (AI) to enhance cybersecurity and to strengthen data protection. This research aims to first assess and critically evaluate the potential of applying AI methods to improve predicting, mitigating, and resolving cyber threats while addressing important ethical issues. Specifically, it wants to determine AI's advantages compared to traditional cybersecurity ways and the plausible technological risks and ethical implications associated with its use. We show that AI tools, especially machine learning and deep learning, can greatly aid the threat detection and response automation. The rise of AI, however, brings forth new vulnerabilities and necessitates stronger ethical frameworks to preclude their misuse. This study offers a balanced view of potential with AI and hazards. The results emphasize the importance of AI in securing both the cybersecurity and data protection portfolio, and urge strongly for ethical standards to be met and the research to be continued in order to mitigate risks and promote responsible AI integration.

Index Terms: Artificial Intelligence, Cybersecurity, Data Protection, Machine Learning

1. Introduction

In the era of technology, where information has gained as much value as petroleum. The topmost priority now is to guarantee its security and privacy. Historically, ensuring cybersecurity has relied on human effort, demanding unwavering attention and significant efforts to oversee and counteract the continuously changing range of risks. The current trend is towards automated systems that utilize the latest technological advancements and artificial intelligence to detect and counter potential threats in real-time. The emergence of Artificial Intelligence (AI) is causing a transformation in the way cybersecurity and data protection is approached. Our systems are now more secure than ever before due to the real-time detection and response capabilities enabled by advancements in AI technology for cyber threat mitigation. The field of cybersecurity is being significantly revolutionized by artificial intelligence, which is distinguished by its ability to acquire knowledge from information and make informed judgments. Advanced systems with unparalleled accuracy and speed to detect and mitigate threats are being developed as a result of this. AI is proving to be crucial in strengthening strategies for safeguarding data. Data security is guaranteed both during transmission and while being stored. Not only are our defensive capabilities being enhanced by these advancements. The cybersecurity domain's strategies and techniques are undergoing redefinition by them. [1] Although AI presents potential solutions for cybersecurity and data protection, it also generates fresh inquiries regarding confidentiality. The mechanisms that render AI a potent security tool are also considered as probable menaces to privacy. The ethical implications of AI in cybersecurity have been extensively debated due to concerns over the intentional or unintentional misuse of vast amounts of data required for the effective functioning of AI systems. Nonetheless, the discussions underscore the

This work is open access and licensed under the Creative Commons CC BY 4.0 License.

necessity of implementing strong measures and precautions to ensure the privacy of users is upheld and to avert possible instances of power exploitation. [2]

In the contemporary digital era, data has become as valuable as petroleum, making its security and privacy a top priority. Traditional cybersecurity approaches, which rely heavily on human oversight and manual intervention, are becoming increasingly inadequate in the face of rapidly evolving threats. The shift towards automated systems, driven by advances in AI, represents a paradigm shift in how we approach cybersecurity and data protection. AI's capacity to process vast amounts of data in real-time, predict potential threats, and respond automatically is revolutionizing the field. However, the adoption of AI in cybersecurity raises important questions about its ethical use and the potential risks to privacy. This study aims to fill the gap in understanding AI's dual role as both a tool for enhancing security and a potential threat to privacy. The objective of this research is to critically evaluate the application of AI in cybersecurity, focusing on its ability to predict, mitigate, and address cyber threats more efficiently than traditional methods. Additionally, the study assesses the technological and ethical risks associated with AI's deployment in this domain, offering a comprehensive analysis of the balance between security enhancement and privacy protection. [3]

The significance of safeguarding cybersecurity and securing data in the present digital scenario cannot be emphasized enough. The rise in security breaches, cyber threats, and data misuse has brought about significant financial and reputational harm to individuals, organizations, and countries. The increasing requirement for strong cybersecurity measures is imperative to safeguard confidential data and obstruct illegal entry. The emergence of AI, with its vast capabilities, has introduced novel opportunities for addressing these issues. The utilization of AI in the fields of security and privacy raises various implications and apprehensions. A comprehensive analysis and comprehension of these issues and potential consequences are imperative. [4] The extensive research on AI applications in various domains contrasts with its limited investigation in cybersecurity and data protection, highlighting the need for further exploration in this specific area. The significance of AI lies in its potential to perform predictive analytics, detect threats and respond to them automatically within the domain of cybersecurity. The system shows the same level of potential in guaranteeing both the confidentiality and integrity of data. The utilization of AI in these domains presents intricate ethical considerations, privacy issues, and regulatory obstacles that demand resolution of significant queries. [5]

The rationale behind this research is the necessity to comprehend and maneuver the complex equilibrium between utilizing AI for improved security purposes. The consideration of privacy is an imperative factor that must not be overlooked. The goal is to offer a thorough summary of the ways in which artificial intelligence is altering the cybersecurity domain. The matter of privacy risks and challenges is closely monitored. The results obtained from this research may provide direction for the advancement of artificial intelligence implementations in the fields of cybersecurity and safeguarding data. The implementation of this measure will guarantee that their performance is both proficient, productive, and adherent to ethical standards. It is imperative to conduct research that keeps up with the advancements and increasing usage of AI. This study adds to the important discussion on responsible and ethical AI practices in cybersecurity and data protection. The upcoming sections will cover the distinct functions performed by AI in ensuring cybersecurity. In addition, an examination of its potential uses for safeguarding data and the associated privacy implications will be conducted. Case studies illustrating the practical ramifications of these concerns will also be demonstrated. In order to provide comprehensive closure, we shall furnish a compendium of our discoveries along with suggestions for prospective investigations. [6]

2. Literature Review

There is also much of a growing body of research on the application of AI in cybersecurity, but there are still critical gaps in this immediate research. Several studies in effect demonstrate the potential of AI, but relatively few present detailed comparisons to traditional CIS methods, or tackle the ethical and technical challenges raised by AI. A good example of this is Buczak and Guven's (2016) study on machine learning for intrusion detection, where they show how AI can detect new threats but fail to offer discussion of AI's computational burdens and data dependency. Following similar vein, Meidan et al. (2018) [8] demonstrate the use of AI to detect malicious behavior in IoT networks, but remain silent on the limitations related to its deployment in resource constrained environments. Recent advancements in AI have brought hope for new solutions to real time threat detection and response using deep learning and reinforcement learning. With all these technologies we still have the technical requirement of very high computational power and large, high quality datasets which might not exist across all sectors. This points to a critical gap in the literature: AI certainly has potential, but there is little discussion of the feasibility of implementing AI in all different industries and the ethical implications of it being used in a broad way. Additionally, studies like Wang et al. (2019) [9] only consider in what way AI can aid data protection without evaluating substantively AI's technical limits including the vulnerability of AI algorithm to bias or the propensity of AI in surveillance systems. [10] In this review, the importance for a more nuanced understanding of AI's role in cyber security, especially in comparison to traditional techniques, technical challenges, and ethical considerations are discussed. [11,12]

In their investigation, Shiravi et al. [13] employed machine learning techniques for identifying and categorizing intrusions on industrial control systems (ICS). In their demonstration, it was proven that the utilization of AI was proficient in safeguarding crucial infrastructure from cyber security menaces. Ahmadian and colleagues [14] proposed an AI-driven technique for safeguarding privacy on social networks in a separate investigation. A proposed AI model is

capable of assessing the degree of privacy risk for varying forms of information disclosed on social media. The utilization of this model would enable individuals to exercise greater authority over the confidentiality of their data. Zeng and colleagues [15] utilized artificial intelligence algorithms to identify and avert data leakage prevention (DLP) in cloud-based settings. To identify possible data leaks, they analyzed patterns and behaviors in data usage.

Shen et al. [16] presented a case study demonstrating the application of AI in financial institutions for fraud detection and safeguarding customer data privacy and security. The results showcased how AI can enhance the risk management procedures of such establishments. The study demonstrated the capability of AI to leverage past records of fraudulent behaviors and make precise forecasts regarding forthcoming fraud trends. The utilization of AI for privacy-preserving distributed deep learning in the medical field was examined by Zhou et al.'s case study [17]. The researchers demonstrated the feasibility of employing AI for training algorithms on datasets distributed across multiple locations without compromising the confidentiality of patients. The literature available emphasizes the possible utilization of AI to improve security and privacy. Nevertheless, it emphasizes the necessity of thoroughly contemplating the ethical repercussions and possible obstacles linked to the application of AI in these domains.

3. Methodology

To achieve a comprehensive understanding of Artificial Intelligence's role in cybersecurity and data protection, the study's methodology was carefully crafted. A mixed-methods approach, comprising of both qualitative and quantitative research techniques, was utilized by the researchers to collect and scrutinize data. The methodology employed in this research comprised of collecting, analyzing, and validating both quantitative and qualitative data, as elaborated later. [18,19]

To collect and analyze prior research on the involvement of AI in cybersecurity and data protection, a methodical literature review was performed. The present analysis offers significant perspectives on the ongoing research in this area. The review included scholarly articles, conference papers, policy documents, and reports from AI and cybersecurity focused organizations. The identification of different AI techniques employed in cybersecurity was facilitated by this review. The article delved into various aspects of AI including the adoption rate in different industries, challenges faced during implementation, and its effects on cybersecurity incident management and data protection techniques. A group of professionals working in diverse sectors, such as finance, healthcare, retail, manufacturing, and education were surveyed in a cross-sectional study. The objective of the survey was to acquire primary data regarding the actual implementation, advantages, and difficulties encountered in utilizing AI for cybersecurity and safeguarding data. [20]

The study employs a mixed-methods approach, combining qualitative and quantitative research techniques to examine AI's role in cybersecurity and data protection. A comprehensive literature review was conducted to identify key AI techniques and their applications in cybersecurity. This review included peer-reviewed journals, conference proceedings, and industry reports focusing on AI and cybersecurity. [21] In addition to the literature review, a cross-sectional survey was conducted targeting professionals across various industries, including finance, healthcare, retail, manufacturing, and education. The selection process was designed to ensure representativeness, with participants chosen through random sampling from industry-specific databases. The survey included questions on AI adoption, challenges in implementation, and the perceived benefits of AI in cybersecurity. A total of 500 respondents participated, with a balanced representation across sectors.[22] For the analysis, thematic coding was applied to the qualitative data from the literature review, focusing on recurring themes such as AI implementation challenges and ethical concerns. The quantitative data from the survey was analyzed using descriptive statistics, including frequency distributions and cross-tabulations. Statistical analysis was conducted using SPSS to ensure accuracy and reproducibility. Additionally, the study employed triangulation, comparing survey results with findings from the literature review to validate the data and ensure comprehensive insights.[23]

The meaningful insights were obtained by analyzing the collected data. A thematic analysis was carried out for the literature review data. The categorization of the data was performed by considering the implementation challenges, adoption rates across different sectors, AI techniques employed and the effect of AI on cybersecurity and safeguarding of data. Descriptive statistics were employed for quantitative analysis of the survey data. The study involved quantifying and organizing various aspects of AI implementation, including the utilization frequency of diverse techniques, the adoption pace across industries, the reported challenges frequency, and progress rates concerning cybersecurity and data protection in distinct domains. [24] In order to guarantee the credibility and authenticity of the outcomes, a triangulation approach was implemented. A comparison and contrast was performed between the results obtained from the literature review and survey to determine similarities and differences. [25] To forecast upcoming patterns, a blend of proficient viewpoints, exploration on developing technologies, and extension of current trends was employed. A thorough examination of the latest developments and research trends in AI, cybersecurity, and data protection was conducted. [26] The approach utilized in this investigation guaranteed the acquisition of strong and exhaustive information. An extensive examination of the involvement of artificial intelligence in safeguarding against cybersecurity threats and preserving data was made possible. This rigorous methodology is accurately represented in the results and discussions sections.

4. Results and Discussion

This segment presents our results regarding how Artificial Intelligence (AI) affects the domains of cybersecurity and data protection. The study's various components are analyzed in six distinct tables. Table 1 displays the different cybersecurity AI techniques implemented, their usage frequency, and the advantages they offer. The technique most commonly employed for minimizing false alarms in threat detection is Machine Learning.

Table 1. Types of AI Techniques Utilized in Cybersecurity

AI Technique	Frequency of Use	Benefit
Machine Learning	180	Reducing false alarms
Deep Learning	160	Detecting unknown threats
Natural Language Processing	120	Identifying phishing attempts
Neural Networks	140	Predicting future attacks
Reinforcement Learning	100	Optimizing security policies

The AI adoption rate for data protection is demonstrated across different sectors in Table 2. According to the data, the finance industry has demonstrated the most significant rate of AI implementation, reaching 70%. The aforementioned suggests a notable dependence on artificial intelligence for safeguarding data within this particular industry.

Table 2. AI Adoption across Sectors for Data Protection

Sector	AI Adoption Rate
Finance	70%
Healthcare	55%
Retail	50%
Manufacturing	45%
Education	30%

The difficulties faced while integrating AI into cybersecurity are illustrated in Table 3. The scarcity of proficient workforce remains the most commonly cited obstacle. The aforementioned emphasizes the necessity for additional instruction and knowledge acquisition within this domain.

Table 3. Challenges in Implementing AI in Cybersecurity

Challenge	Frequency
Insufficient skilled personnel	170
High implementation cost	150
Data privacy concerns	130
Complex AI systems	110
Unclear ROI	100

The rates of enhancement in various domains of incident management in cybersecurity attributed to AI are presented in Table 4. According to the data, incident detection time has shown the most notable enhancement with a rate of 65%.

Table 4. Impact of AI on Cybersecurity Incident Management

Impact Area	Improvement Rate
Incident Detection Time	65%
Incident Response Time	60%
Reduction in False Positives	55%
Predictive Capabilities	50%
User Behavior Analysis	45%

The effects of artificial intelligence on different data protection methods are emphasized in Table 5. Anomaly detection has experienced a noteworthy enhancement with the incorporation of AI, exhibiting an improvement rate of 70%.

Table 5. Impact of AI on Data Protection Techniques

Data Protection Technique	Improvement Rate
Anomaly detection	70%
Data encryption	60%
Identity and access management	55%
Risk assessment	50%
Data loss prevention	45%

The anticipated progress rates for forthcoming advancements in AI used for cybersecurity and safeguarding data are presented in Table 6. It is anticipated that the utilization of AI in IoT security will experience the most rapid expansion. The significance of safeguarding connected devices is illustrated by this.

Table 6. Future Trends in AI for Cybersecurity and Data Protection

Future Trend	Expected Growth
AI for IoT Security	20%
AI-powered Risk Assessment	18%
AI-driven Adaptive Security	15%
Quantum Cryptography	12%
AI for Privacy-Preserving Computation	10%

Our research findings offer significant knowledge on the function of Artificial Intelligence concerning security and privacy. Especially when considering matters of cybersecurity and safeguarding data. The frequency and advantages of different AI techniques in cybersecurity were presented in detail in Table 1. The findings indicated that the technique most commonly employed was machine learning. The reason for the prevalence of machine learning tools in cybersecurity applications is their capacity to learn from data and enhance themselves gradually. The aforementioned characteristic renders them especially valuable in identifying irregularities and minimizing erroneous alerts. Despite being utilized less frequently, deep learning demonstrated considerable promise in identifying unfamiliar dangers. It is probable that this is a consequence of its capacity to acquire intricate patterns and generate forecasts grounded on vast datasets.

This study's results demonstrate compelling benefits of leverage AI to aid in cybersecurity, with a particular focus on threat detection and incident response. The frequent use of the AI technique machine learning as a way to reduce false positives is shown in Table 1. Although, deeper analysis shows (Table 2) that sectors, such as finance and healthcare, which process sensitive data, have higher AI adoption rates. That's probably down to the huge financial and reputation risks involved in suffering a data breach in these sectors. The results also reveal considerable challenge that comes with AI applications, although the capacity of AI to reduce incident detection time (Table 4) is a positive. As is true for other machine learning and artificial intelligence applications, a shortage of skilled personnel continues to be a critical barrier to AI adoption (Table 3), indicating the need for educational programs to provide more emphasis on training in AI and cybersecurity. In addition, high implementation costs and blockages of data privacy were the main obstacles, especially for small and medium firm (SMEs). That implies future AI solutions must be both cost effective and scalable in order to gain wider acceptance.

Table 2 presents the discussion of how much AI is adopted sector by sector, in which industries with very stringent regulatory requirements such as finance and healthcare are more likely to accept AI. But although the adoption lies in part to regulatory pressure, it's not just because AI can deal with huge quantities of sensitive data and detect the most sophisticated threats. For example, sectors such as education happen to have lower adoption rates, perhaps because there are fewer immediate financial risks and less sensitive data. That is a strong signal for the need for context specific AI solutions tailored for each specific industry. Additionally, while AI can also better cybersecurity, technical limitation must be tackled. AI systems are computationally more intensive and need large high-quality dataset to achieve accurate results. Measures that safeguard against AI driven cybersecurity problems pose a significant challenge for many organizations by not being able to meet these technical requirements, potentially making it unfeasible for AI driven solutions to your cybersecurity problems. Therefore, this study also emphasizes that data is key in AI whereas the same mechanism use to check threat can also be misused for a surveillance of data or exploitation of data. AI should be used in cybersecurity and can only be pronounced to be ethical if ethical frameworks are established to govern its use, guaranteeing the security of cybersecurity and at the same time giving respect to user privacy.

Table 1 demonstrates the widespread utilization of Machine Learning in various cybersecurity applications. Supervised Machine Learning algorithms demonstrate exceptional proficiency in data classification and correlation. These algorithms have the ability to analyze enormous quantities of network traffic or system event data within the realm of cybersecurity. The identification of peculiar conduct or doubtful arrangements that could indicate a security breach is carried out by them. The utilization of neural networks with multiple layers (thus the name "deep") in order to comprehend data characterizes Deep Learning, which is a subset of Machine Learning. The analysis of patterns in data sets and predictions have exhibited significant potential in detecting unidentified threats. Traditional security tools may

fail to identify newly emerged malware variants and zero-day exploits, whereas Deep Learning demonstrates high efficacy in detecting them. Considering its capability to acquire knowledge from disorganized information.

The table 2 emphasizes that the finance industry had the highest utilization of AI for safeguarding data. Subsequently, healthcare, retail, manufacturing and education ensued. The finance sector's sensitive data is considered the reason behind the rapid implementation of AI technology. The requirement for advanced technologies such as AI in this sector is reinforced by the significant expenses associated with data breaches. The results indicate that industries dealing with confidential information are inclined towards implementing AI to safeguard their data. Table 2 underscores the considerable disparity in the implementation of AI for safeguarding data across diverse industries. There is a leadership role played by the finance sector. The potential for substantial financial losses and harm to a company's reputation makes a data breach in this industry highly consequential. The incorporation of AI tools in banking and finance is crucial as it enables institutions to identify fraudulent transactions instantly. AI-supported systems are currently applied in the healthcare industry to safeguard confidential patient information and guarantee adherence to regulatory requirements. The implementation of AI is being utilized by both the retail and manufacturing industries aimed at safeguarding their digital infrastructure and ensuring protection of sensitive customer information. The education industry is gradually acknowledging the necessity of AI, despite its lower rate of implementation. Particularly considering the rise of online educational settings.

The difficulties in integrating AI into cybersecurity were detailed in Table 3. The shortage of proficient workforce was the primary hurdle frequently remarked. The presence of an AI-skilled workforce shortage in the cybersecurity industry is suggested by this observation. The aforementioned underscores the pressing necessity to improve the instruction and learning in both artificial intelligence and cybersecurity. The key challenges in incorporating AI into cybersecurity were emphasized in Table 3. The lack of proficient workforce remains a notable obstacle. One potential solution would be to modify educational programs by incorporating dedicated coursework on AI and cybersecurity. Encouraging ongoing education within the work environment could provide further advantages. Another obstacle is posed by the expenses incurred during the implementation process. Investing in advanced AI security tools may pose a challenge for SMEs. Possible rephrased sentence: Government incentives or the creation of affordable AI tools customized for small and medium-sized enterprises may be viable options to tackle this issue.

The positive effect of AI on managing cybersecurity incidents was highlighted by Table 4. The incident detection time showed the most considerable enhancement. This discovery implies that the expeditiousness and aptitude of AI in scrutinizing enormous volumes of data make it probable for AI to considerably improve the efficiency of cybersecurity operations. According to Table 4, the employment of AI significantly diminishes the times for detecting and responding to incidents. The ability of AI to swiftly process and examine massive amounts of data in real-time allows for unparalleled threat detection. AI's potential to aid organizations in promptly and efficiently addressing imminent risks can enhance their overall security measures. As a result, organizations are able to swiftly address risks, thereby minimizing the potential harm. The significance of AI's contribution in minimizing false positives cannot be overlooked. The prevalence of false positives in conventional cybersecurity instruments can burden security personnel and impede their response time. The implementation of AI in threat detection enhances precision by minimizing the occurrence of false positives.

The results presented in Table 5 demonstrate that AI has a noteworthy influence on enhancing diverse data protection methods. The enhancement that demonstrated the most significance was observed in detecting anomalies. The reason behind this is probably the capability of AI to acquire knowledge from patterns and identify variations. This feature enhances its utility in the detection of security risks. The employment of AI has resulted in a remarkable enhancement of data protection methods as demonstrated by the findings in Table 5. AI's proficiency in recognizing patterns and deviations from them is highlighted as anomaly detection emerges as the most prominent task. The capability of identifying insider threats or compromised user accounts is especially advantageous. It is worth noting the contribution of AI in the areas of data encryption, identity, and access management. Data protection comprises crucial domains.

Table 6 delineated the forthcoming directions of AI in cybersecurity and safeguarding data. The rapid growth projected for AI in IoT security highlights the increasing significance of safeguarding interconnected devices. The trend implies that as IoT devices become more widespread, the protection of these devices from possible cyber threats will heavily rely on the implementation of AI. Table 6 offers a valuable prediction regarding the prospective developments in AI concerning safeguarding data and cybersecurity. The swiftest emerging trend is anticipated to be the contribution of AI in guaranteeing security in IoT. The existence of numerous IoT devices and their distinctive security difficulties make this outcome unsurprising. The incorporation of AI-powered risk assessments and adaptive security implies a trajectory in which AI surpasses its role as a mere tool and becomes an essential element of cybersecurity tactics.

Our findings demonstrate the significant role of AI in enhancing cybersecurity and data protection across various sectors. However, challenges such as a lack of skilled personnel and high implementation costs need to be addressed for more widespread adoption. Looking forward, the continued development and integration of AI in cybersecurity and data protection practices appear promising. AI's role in cybersecurity and data protection is transformative and expanding. However, the journey is not without challenges. Addressing these challenges and harnessing the power of AI could lead to a paradigm shift in how we approach cybersecurity and data protection.

5. Conclusion

This research shows the potential for AI to transform cybersecurity and data protection by predicting, detecting and responding to threats more efficiently than what can be done with traditional analytical solutions. Yet, adoption of AI usually means overcoming large technical hurdles, moral concerns, and need of skilled individuals. This research emphasizes the need to notice the balance on the venue of the AI benefits and the hard it brings been data privateness and misuse. These challenges should be addressed by future research in the form of developing cost effective, scalable AI solutions, as well as developing robust ethical frameworks. Furthermore, further detailed study is needed to examine the technical verity of AI within resource constrained environments and to discover industry specific applications for AI. AI has the potential to significantly change the cybersecurity game but only with great care given to both the technical and ethical brings it brings. While this study provides relevant understanding, it is not flawless. With AI and cybersecurity moving at such a fast pace, the current findings may already be out of date. In addition, the use of survey data in the study may introduce bias in that respondents' perceptions may not accurately represent the complexities of AI implementation. Longitudinal studies and real world case analyses will be required for future research on AI's contribution towards cybersecurity and data protection.

References

[1] Alazab, M., Venkatraman, S., & Watters, P. (2018). Cybersecurity threats classification: A machine learning approach. Journal of Network and Computer Applications, 107, 71-80.

[2] Arshad, H., & Tariq, M. (2020). Artificial intelligence for cybersecurity: A review of trends, challenges, and opportunities. Journal of Network and Computer Applications, 152, 102495.

[3] Asghar, H., Imran, M., Zia, T., & Mahmood, K. (2017). Cyber security threats and vulnerabilities: An overview. Journal of Cyber Security Technology, 1(1), 1-12.

[4] Bacivarov, I., & Cotorobai, A. (2020). An overview of artificial intelligence for cybersecurity. Journal of Cybersecurity, 6(1), tyaa003.

[5] Besharati, A., & Haddadi, H. (2019). A novel deep learning approach for intrusion detection in wireless sensor networks. Journal of Network and Computer Applications, 128, 1-12.

[6] Bhatia, S., & Sharma, A. (2018). A survey on artificial intelligence and its application in cyber security. International Journal of Computer Sciences and Engineering, 6(10), 256-260.

[7] Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153-1176.

[8] Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Shabtai, A., Breitenbacher, D., & Elovici, Y. (2018). Detection of unauthorized IoT devices using machine learning techniques. arXiv preprint arXiv:1803.00742.

[9] Wang, Y., Cui, Q., Sun, J., Shen, J., Shen, X., & Zheng, X. (2019). A privacy-preserving deep learning approach for face recognition with cloud support. Journal of Parallel and Distributed Computing, 130, 33-43.

[10] Mittelstadt, B., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. Big Data & Society, 3(2).

[11] Garcia, D. (2020). Bias and fairness in AI decision-making: A review. IEEE Access, 8, 200380-200399.

[12] Garcia, M. (2020). Challenges in machine learning for cybersecurity: A review. Journal of Cybersecurity and Privacy, 4(1).

[13] Shiravi, A., Shiravi, H., Tavallaee, M., & Ghorbani, A. A. (2012). Toward developing a systematic approach to generate benchmark datasets for intrusion detection. Computers & Security, 31(3), 357-374.

[14] Ahmadian, A., He, Y., Kauppinen, I., & Pournaras, E. (2020). Privacy-aware big data analytics as a service for public health policies in smart cities. Sustainable Cities and Society, 54, 102003.

[15] Zeng, Y., Tang, D., & Seneviratne, O. (2019). Cloud-based data leakage detection for trustworthy lifecycle management of personal data. Journal of Cloud Computing, 8(1), 1-17.

[16] Shen, C., Cai, Z., Guan, X., & Du, Y. (2017). Detecting credit card frauds by learning from imbalanced data. In 2017 IEEE Symposium Series on Computational Intelligence (SSCI) (pp. 1-7). IEEE.

[17] Zhou, Q., Du, J., Liu, Y., Chen, Y., & Zhao, J. (2020). Privacy-preserving distributed deep learning and its applications. Journal of Parallel and Distributed Computing, 143, 58-69.

[18] Jha, S., & Kumar, V. (2019). An overview of artificial intelligence for cyber security. International Journal of Advanced Research in Computer Science and Software Engineering, 9(8), 58-66.

[19] Jose, J., & Dhanapal, R. (2019). A survey on artificial intelligence for cyber security. International Journal of Advanced Science and Technology, 28(10), 771-781.

[20] Kaur, A., & Singh, A. (2020). Artificial intelligence techniques for cyber security: A review. International Journal of Humanistic Computing, 3(2), 1-9.

[21] Kumar, A., & Gupta, S. (2020). Artificial intelligence-based cyber security: A systematic review. Journal of Ambient Intelligence and Humanized Computing, 11(11), 4885-4905.

[22] Kumar, A., & Singh, S. (2021). Artificial intelligence in cyber security: A review and future directions. Journal of Ambient Intelligence and Humanized Computing, 12(7), 7709-7726.

[23] Kumar, S., & Singh, A. (2020). A survey on artificial intelligence in cyber security. Journal of Information Security, 11(1), 1-20.

[24] Liao, Y., Huang, Z., & Zhang, H. (2019). A survey on artificial intelligence for cyber security. Journal of Cyber Security Technology, 3(2), 67-85.

[25] Liu, Y., & Li, X. (2019). Artificial intelligence and cyber security: A survey. International Journal of Information Management, 47, 146-157.

[26] Mahajan, A., & Gupta, A. (2020). Artificial intelligence techniques for cyber security: A review. International Journal of Advanced Science and Technology, 29(1), 1843-1852.

Authors' Profiles

Mahmoud Mohamed is a PhD student in the faculty of Computer and Electrical Engineering at King Abdul Aziz University. He received his Bachelor's degree in Computer and Electrical Engineering from King Abdul Aziz University in 2020. His research interests include artificial intelligence, machine learning, and computer vision. He has published several papers in peer-reviewed journals and conferences.

Khaled Alosman is a Master's student in the Computer and Electrical Engineering at King Abdul Aziz University. He obtained his Bachelor's degree in Computer and Electrical Engineering from King Saud University. His research focuses on embedded systems, IoT, and wireless sensor networks. He has participated in various research projects and published several papers in peer-reviewed journals and conferences.

How to cite this paper: Mahmoud Mohamed, Khaled Alosman, "Artificial Intelligence in Security and Privacy: A Study on AI's Role in Cybersecurity and Data Protection", International Journal of Education and Management Engineering (IJEME), Vol.15, No.1, pp. 44-51, 2025. DOI:10.5815/ijeme.2025.01.04