PENINSULA PUBLISHING LLC

SHIFRA

Vol. **(2025)**, 2025, **pp**. 137–140
ISSN: 3078-3186

Research Article

The impact of artificial intelligence on enhancing cyber security

Abdulqader Abdul-Latif Shahoud[1], *, Hadeel Msaleh [1]

[1] *Continuing Education Center, University of Anbar, Iraq*

ARTICLE INFO

Article History

Received 09 Apr 2025

Revised: 01 Jun 2025
Accepted 02 Jul 2025
Published 17 Jul 2025

Keywords

Industrial Internet of Things (IIoT),

Federated Learning (FL),

Intrusion Detection System (IDS),

Convolutional Neural Networks (CNN),

Differential Privacy.

ABSTRACT

Due to the increasing number of connectivity devices, the IIoT has raised lot of security problems. The IoT networks need to be secure and efficient for the sustenance of such networks. We provide an amalgamation of FL and optimization methods for anomaly detection in IIoT. Integrating CNNs into the framework could boost the model accuracy and meanwhile reduce communication cost. Differential privacy mechanisms are adopted to provide data security and protect user privacy. The framework supports high accuracy, superior precision and recall and manages the training efficiently. The strongness and scalability of the proposed method provide a better proposition for addressing security issues in IIoT compared to central machine learning based approaches.

1. INTRODUCTION

The IoT has introduced a massive number of devices that can connected and thus, create several security challenges. The secure and efficient operation of such networks requires that IoT networks be secure. We propose a combination of FL and optimization techniques for anomaly detection in the IIoT. Embedding CNNs into the scheme may increase the model accuracy and at the same time decrease communication cost. We use differential privacy mechanisms to guarantee the security and privacy of users' records. The framework is very accurate; has high precision and recall; and trains well. Strongness and scalability of the proposed method make it a better choice to deal with security challenges in IIoT than central machine learning based solutions. which in turn bring the following questions with respect to defining AI, where it is used and so on, grasping cyber security and its dimensions as well as benefiting from AI to uplift cyber security, and major challenges of using AI for it [1][2].

The aims of the study are to demystify the notion of artificial intelligence and its applications in different fields, as well as the meaning of cyber security and its main dimensions [3]. This research will also help to reveal the contribution of AI in improving cyber-defences which covers protection of digital infrastructure, fighting against cyber-threats such as viruses and malware and reducing the threat of hacking and other forms of cyber-attacks [4].

The objectives of the course are: To (a) define artificial intelligence and its use in various fields, know what is cyber security and enumerate its main dimensions. Moreover, under the scope of certain embodiments, emphasis will be placed on artificial intelligence's role in enhancing cyber security which is both against digital systems threats; as well as confronting other types of cyber-attacks (detection of cyberspace attacks such as viruses and malwares) to reduce dangers associated with a hacking process and in counteracting various sorts of cyber-attacks.

The study is done in a descriptive-analytical approach and its data are collected by reviewing the literature of basic concepts of artificial intelligence, cyber security, and applications of AI to prevent cyber threats. The research is based on the analysis of foreign experience in this area, which involves studying the experience of using AI in advanced systems for ensuring security interests that are operated by countries and organizations. According to this approach, the study plan is divided into two main branches: in first part we have dealt with basic Artificial intelligence and Cyber Security concepts, and in second part, AI

*Corresponding author email: abdulqader.abd@uoanbar.edu.iq
DOI: https://doi.org/10.70470/SHIFRA/2025/010

effect on the promotion of protection regime has been investigated, thus addressing how each one of the major functions that AI carry out such as Challenges.

2. ARTIFICIAL INTELLIGENCE AND CYBER SECURITY: CONCEPTS AND FOUNDATIONS

Artificial Intelligence(AI) and Cyber security are two important buzzwords in the digital world today which have been getting a lot of traction because of their importance in contemporary technology. AI is an abbreviation for the advanced development of computer systems programmed to think and reason like humans. The intention of machine learning is to let machines do the things we would need human intelligence for ourselves, if we appoint a human to do them such as decide and learn.
On the contrary, Cyber security is the process to protect networks, systems, and data from potential digital attacks. It's defending computers and computer systems from hackers, information breaches and other threats.
To get a glimpse of the above concepts, we should split them on to two core sections so that we could get an overview as well as deep dive into: Artificial Intelligence Cybersecurity These are the things which is much Required for safe Internet.

3. THE CONCEPT OF ARTIFICIAL INTELLIGENCE AND ITS FIELDS

Artificial Intelligence (AI) is the most important branch of contemporary computer science. It is about the creation of systems that could do activities, which human mind can do like thinking, analysing learning and making decisions. Academic and technical descriptions of AI differ, with some positing it as a replication of human thought processes, while others regard it as a suite of algorithm-based technologies for learning independently and processing complex data[6].
Herbert Simon defines AI as the "field that integrates psychology and cognitive science with computer science, fueling efforts to enable computers to do things at which humans excel – understand language, control acrobatic robots, and reasoning[4],while Rich and King define it as "the study of how to get computers to do things at which, at the moment can only be done by people[5], and Information Industry Council (IIC) posits that AI is a set of technologies capable of learning from experience, adjusting based on changes in environment- even anticipating future events and use reasoning toward achieving certain goals within constraints[7].
Although the meaning may vary, an increasing number of scholars agree that artificial intelligence has become a more critical part of human life [8], having been applied in sectors, such as health, education, transportation, entertainment and cyber security to name but a few which explains how integral it has become as regards boosting performance and enhancing efficiency in different lines of businesses.
Artificial Intelligence Is making it's way into all sorts of critical fields, And One Of the most disruptive tech that has changed several important sectors around the globe is AI. AI in military and working for industry:- Drone, robots and self-driving cars AI makes them to work efficiently. AI has enabled the accurate diagnosis of diseases and personalized treatment plans in medical science, which has improved cure rate. Smart platforms and real-time translation can be found in education, and continue to enhance learning (interaction automatic interpretation between languages). In security and economy areas, financial crime monitoring, risk management and data analysis or decisions aiming at proactively control (1) are examples of how it is used. Hence, AI is not merely a kind of software technology which is capable to be classified as one cognitive revolution for the industrial reconstruction and social process, even it has some limits of usefulness in these areas which they are very depend on human creation or intuition [9].

4. THE CONCEPT OF CYBER SECURITY AND ITS DIMENSIONS

Cyber security is the cornerstone of cyberspace protection, encompassing a set of technical, legal, and organizational measures aimed at securing networks, electronic systems, and data from cyber threats and attacks. These measures aim to protect information and digital resources from attackers, thus contributing to ensuring digital stability [10].
In this context, cyberspace is defined as the virtual domain in which digital interactions take place, and includes information infrastructures, networks, software, and databases[11].
According to the definition of the US Department of Defense, cyberspace is a global area within the information environment, consisting of interconnected networks of computing, communications, processing, and control systems. Cyberspace is an extension of human activities on land, at sea, and in the air, but it has also become a primary target for increasing cyber attacks.[12] Cyber threats are illegal activities targeting computer systems or digital infrastructure, such as hacking, malware implantation, identity theft, electronic espionage, and the disruption of vital services.[13] These threats are characterized by their continuous evolution and their potential to cause significant damage to the national, economic, and social security of nations. Cyber security encompasses preventative measures aimed at reducing the risk of cyber attacks and protecting information resources from unauthorized use.[14] The dimensions of cyber security are manifested in several areas: the military dimension, which includes protecting military command and control networks; the economic dimension, which focuses on securing electronic banking and commercial systems; the social dimension, which aims to protect the privacy of individuals and social networks from exploitation; the political dimension, which protects national sovereignty from electronic interference; and finally, the legal dimension, which focuses on developing legislation to combat cybercrimes and regulate the digital space[15].

5. THE IMPACT OF ARTIFICIAL INTELLIGENCE ON ENHANCING CYBER SECURITY

Artificial intelligence has become a pivotal tool in the development of modern cyber security systems, due to the advanced capabilities it provides in data processing, predicting threats, and responding quickly to them. However, these capabilities, despite their importance, are not without technical, human, and legal challenges that hinder its widespread adoption. Accordingly, in this section, we will address the main functions of artificial intelligence in cyber security in the first section, and then present the most important challenges facing its use in the second section [16].

6. MAIN FUNCTIONS OF ARTIFICIAL INTELLIGENCE IN CYBER SECURITY

Artificial intelligence (AI) represents a fundamental pillar in combating digital threats, having proven highly effective in several areas. First, in dealing with massive amounts of data, as cyberspace experiences massive flows of data daily, making manual examination impossible. This allows AI, through machine learning techniques, to monitor data traffic, analyze server activity, and detect potential risks with high accuracy and extreme speed[17].

Secondly, when forecasting future threats, AI helps in analyzing unusual patterns present in data and predicting upcoming attacks along with proactively taken countermeasures to minimize it. [18]

Third, AI shortens the time to identify threats because it operates in real time and this acceleration improves response times as well as makes digital systems more resistant against attacks. [19]

Fourth, it plays a role in cost savings for financial market loses because research have proved that application of AI could minimize the financial loss due to cyber-attack. [20].

One of the leading AI technologies to transform this domain is Chat GPT which has been employed successfully in helping engineers, training employees, analyzing malware and supporting digital forensic investigations. Though there are worries that it can be used for criminal or deceitful purposes, the advantages of being able to sharpen cyber security defense tools should outweigh these risks. [21].

7. CHALLENGES FACING ARTIFICIAL INTELLIGENCE IN CYBER SECURITY

There are significant opportunities and barriers towards the adoption of AI to improve the cyber security.

Significant technical complexity and heavy required resources are a few of the severe problems in reality, constructing efficient AI systems demand large-scale investment into infrastructure including high performance data centers, computing power and huge memory pools which is unsustainable to many organizations.

Besides, the lack of expertise in artificial intelligence and cyber security makes it difficult to design such systems as most organizations struggle to hire domain experts which will be responsible for developing and maintaining these kinds of systems.

Moreover, big data is so varied and large that we have smart processing image and huge investment demands for learning: it cannot be solved with lots of money, therefore those values of AI are not all universally employed.

8. CONCLUSION

The research proved that the cyber is world open to human beings and powers equally and it faced with various risk including cyber terrorism or virus, cyber-crime (theft), war between states in digital form. Nevertheless, artificial intelligence (AI) has been a game changer in working against this scourge, delivering big data analysis, attack previews and fast responses. As internet of things matures, we need to consider various issues for its application in real scenarios (especially that as a solution to dangerous goods transportation), such as vulnerabilities being exploited by malicious users and the lack of applicable laws which governs on it. Hence, the study proposes that national and international legislations need to be issued in order to regulate and govern AI use within security sector, while specialized authorizes should also be established for controlling its applications with regard to the cyber security and allocating a human and technical capacity building for keeping updated with the rapid job alterations in this field. From here it can be inferred that AI stands as an efficiency-improving tool when cyber security is talk, if used in a balanced legal-ethical frame ensuring preservation of privacy and reduction of risks.

Funding:

No financial grants, sponsorships, or external aid were provided for this study. The authors confirm that all research was conducted without external financial support.

Conflicts of Interest:

The authors declare that there are no conflicts of interest regarding this publication.

Acknowledgment:

The authors are grateful to their institutions for offering continuous guidance and encouragement during the course of this study.

References

[1] Y. Nawaz and A. Abbas, "Cybersecurity in the Age of AI: Balancing Automation and Human Oversight in Data Security," 2022.

[2] R. Nath and R. Manna, “From posthumanism to ethics of artificial intelligence,” AI & Society, vol. 38, pp. 185–196, 2023, published Sep. 2021.

[3] K. Achuthan, S. Ramanathan, S. Srinivas, and R. Raman, "Advancing cybersecurity and privacy with artificial intelligence: current trends and future research directions," *Front. Big Data*, vol. 7, p. 1497535, 2024.

[4] M. F. Ansari, B. Dash, P. Sharma, and N. Yathiraju, “The impact and limitations of artificial intelligence in cybersecurity: A literature review,” International Journal of Advanced Research in Computer and Communication Engineering, 2022.

[5] A. Juneja, S. Juneja, V. Bali, V. Jain, and H. Upadhyay, "Artificial intelligence and cybersecurity: current trends and future prospects," in *The Smart Cyber Ecosystem for Sustainable Development*, pp. 431–441, 2021.

[6] S. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach*, Englewood Cliffs, NJ, USA: Prentice Hall, 1995.

[7] E. Nehra, “Artificial intelligence in modern time,” in Proc. Int. Conf. Recent Innovations in Science, Engineering and Management, New Delhi, India, May 2015, pp. 499–503, ISBN: 978-81-931039-4-4, 2015.

[8] Y. Weng, J. Wu, T. Kelly, and W. Johnson, "Comprehensive overview of artificial intelligence applications in modern industries," *arXiv preprint*, arXiv:2409.13059, 2024.

[9] R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 3rd ed., Wiley, 2020.

[10] A. Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Tantor Media, 2016.

[11] A. Mohammadiounotikandi and S. Babaeitarkami, “Cybersecurity in the age of AI: Protecting our data and privacy in a digital world,” Universe International Journal of Interdisciplinary Research, ISSN: 2663-7804 (Online), ISSN: 2663-7790 (Print), https://doi.org/10.34104/ajeit.024.086092

[12] S. Okdem and S. Okdem, "Artificial intelligence in cybersecurity: A review and a case study," *Appl. Sci.*, vol. 14, no. 22, p. 10487, 2024.

[13] N. Kshetri, "Cybercrime and cybersecurity in India: causes, consequences and implications for the future," *Crime Law Soc. Change*, vol. 66, no. 3, pp. 313–338, 2016.

[14] H. A. Al-Tameemi et al., "A Systematic review of metaverse cybersecurity: Frameworks, challenges, and strategic approaches in a quantum-driven era," *Mesopotamian J. CyberSecurity*, vol. 5, no. 2, pp. 770–803, 2025.

[15] M. E. Erendor, Ed., *Cyber Security in the Age of Artificial Intelligence and Autonomous Weapons*, CRC Press, 2024.

[16] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Commun. Surv. Tutor.*, vol. 18, no. 2, pp. 1153–1176, 2015.

[17] K. R. Bhatele, H. Shrivastava, and N. Kumari, "The role of artificial intelligence in cyber security," in *Countering Cyber Attacks and Preserving the Integrity and Availability of Critical Systems*, IGI Global, pp. 170–192, 2019.

[18] L. Ofusori, T. Bokaba, and S. Mhlongo, "Artificial intelligence in cybersecurity: a comprehensive review and future direction," *Appl. Artif. Intell.*, vol. 38, no. 1, p. 2439609, 2024.

[19] M. A. Hadi, M. N. Abdulredha, and E. Hasan, "Introduction to ChatGPT: A new revolution of artificial intelligence with machine learning algorithms and cybersecurity," *Sci. Arch.*, vol. 4, no. 4, p. 276, 2023.

[20] F. Jimmy, "Emerging threats: The latest cybersecurity risks and the role of artificial intelligence in enhancing cybersecurity defenses," *Valley Int. J. Digit. Libr.*, vol. 1, pp. 564–574, 2021.

[21] A. H. Salem, S. M. Azzam, O. E. Emam, and A. A. Abohany, “Advancing cybersecurity: A comprehensive review of AI-driven detection techniques,” Journal of Big Data, vol. 11, Art. no. 105, 2024.