مجلة جامعة بني وليد للعلوم الإنسانية والتطبيقية
Bani Waleed University Journal of Humanities and Applied Sciences
تصدر عن– جامعة بني وليد – ليبيا
Website:https://jhas-bwu.com/index.php/bwjhas/index
المجلد العاشر ـ العدد الثالث ـ 2025 ـ الصفحات (121- 129)
ISSN3005-3900

Role Of Artificial Intelligence In Enhancing Cyber Security

[1] Abdulhakim Moawa Dreheeb * , [2] Hisham El Tajouri

[1] Computer Department, Faculty of Education, Al-Zaytouna University, Tarhuna, Libya
[2] Computer Department, Higher Institute of Science and Technology, Al-Shumoukh, Tripoli, Libya
a.dreheeb@azu.edu.ly

دور الذكاء الاصطناعي في تعزيز الأمن السيبراني

عبد الحكيم معاوية دريهيب*[1]، هشام التاجوري [2]
[1] قسم الحاسوب، كلية التربية، جامعة الزيتونة، ترهونة، ليبيا
[2] قسم الحاسوب، المعهد العالي للعلوم والتقنية الشموخ ، طرابلس ، ليبيا

تاريخ الاستلام: 06-05-2025 تاريخ القبول: 25-06-2025 تاريخ النشر: 07-07-2025

Abstract

This study aims to explore the primary applications of artificial intelligence (AI) in strengthening cyber security and to examine the key challenges associated with its implementation. The research is grounded in a comprehensive review and critical analysis of prior literature, including scientific journals, academic books, and official reports that address the role of AI in cyber security.

Findings indicate that AI significantly enhances the effectiveness of cyber security strategies by enabling proactive threat detection and swift incident response. The study also highlights an urgent need for capacity-building through the training and development of human resources capable of understanding and applying AI technologies within cyber security frameworks. Moreover, the research underscores the necessity of establishing robust legal and ethical frameworks to ensure the responsible and secure deployment of AI in institutional settings.

Based on these findings, the study recommends reinforcing cyber security infrastructure, investing in human capital development, and proactively addressing the legal and ethical challenges posed by AI integration in cyber security practices.

Keywords: Artificial intelligence, cyber security, threats, challenges, human resources.

الملخص:

تهدف هذه الدراسة إلى استكشاف الاستخدامات الأساسية لتقنيات الذكاء الاصطناعي في تعزيز الأمن السيبراني، بالإضافة إلى تحليل التحديات الرئيسية المرتبطة بتطبيقها. تستند هذه الدراسة إلى مراجعة شاملة وتحليل نقدي للأدبيات السابقة، بما في ذلك المجلات العلمية، والكتب الأكاديمية، والتقارير الرسمية التي تناولت دور الذكاء الاصطناعي في مجال الأمن السيبراني.

تشير النتائج إلى أن الذكاء الاصطناعي يسهم بشكل كبير في تعزيز فعالية استراتيجيات الأمن السيبراني من خلال تمكين الكشف الاستباقي عن التهديدات والاستجابة السريعة للحوادث. كما تسلط الدراسة الضوء على

الحاجة الملحّة لبناء القدرات البشرية من خلال تدريب وتطوير الموارد البشرية القادرة على فهم وتطبيق تقنيات الذكاء الاصطناعي ضمن أطر الأمن السيبراني. علاوة على ذلك، تؤكد الدراسة على ضرورة وضع أطر قانونية وأخلاقية قوية تضمن الاستخدام المسؤول والآمن للذكاء الاصطناعي داخل المؤسسات.

واستنادًا إلى هذه النتائج، توصي الدراسة بتعزيز البنية التحتية للأمن السيبراني، والاستثمار في تنمية رأس المال البشري، والتعامل بشكل استباقي مع التحديات القانونية والأخلاقية التي تفرضها عملية دمج الذكاء الاصطناعي في ممارسات الأمن السيبراني.

الكلمات الدالة: الذكاء الاصطناعي ، الأمن السيبراني ، التهديدات ، التحديات ، الموارد البشرية.

1. Introduction

Artificial Intelligence (AI) plays a crucial role in advancing cyber security by offering intelligent tools and techniques that detect, prevent, and respond to cyber threats with enhanced efficiency and accuracy. As cyber attacks become increasingly sophisticated and frequent, traditional security measures often struggle to identify novel or complex threats. AI technologies—such as machine learning, deep learning, and natural language processing—enable cyber security systems to analyze vast amounts of data in real-time, recognize abnormal patterns, and automate threat responses. These capabilities help organizations proactively defend their digital infrastructure, reduce breach risks, and strengthen their overall security posture **[1].**Security broadly encompasses methods, procedures, and practices designed to protect networks, devices, software, and data from damage, intrusion, and unauthorized access. The challenge of cyber security is escalating due to the rapid expansion of interconnected tools, systems, and networks. Technological advancements within the digital economy and infrastructure exacerbate this issue by driving a sharp increase in cyber attacks with potentially devastating consequences. Researchers also highlight the continuous evolution of adversaries, including nation-state and criminal groups, and the growing sophistication of cyber attacks that exploit new and invasive tactics to target even highly secure environments **[2]**. As a result, cyber attacks are becoming more frequent, larger in scale, and more impactful. Therefore, intelligence-driven cyber security is essential to managing big data and enabling dynamic defenses against emerging threats. Organizations such as the National Institute of Standards and Technology advocate for proactive, adaptive approaches that emphasize real-time assessment, continuous monitoring, and data-driven analysis to identify, detect, respond to, and document cyber attacks helping to prevent future incidents **[3].**

AI, a hallmark of the Fourth Industrial Revolution, has broad applications across many domains including military, politics, business, economy, and public services. Its significant role in enhancing cyber security makes it especially relevant to both individuals and communities worldwide **[4].**

2. Research Problem and Questions:

Exposure to cyber risks is steadily increasing due to the widespread integration of the internet and digital technologies into nearly every aspect of daily life, as well as their continuous evolution. Given the growing complexity and sophistication of cyber attacks, it has become essential to utilize advanced technologies such as artificial intelligence to enhance cyber security strategies and protect critical systems and sensitive data.

In light of the above, the research can be guided by the following central question:

How does artificial intelligence contribute to improved cyber security?
The primary question was followed by a series of sub-questions:

1. What fields make use of artificial intelligence technology?
2. Which artificial intelligence applications are most commonly utilized to enhance cyber security?
3. What difficulties exist in using artificial intelligence in cyber security?

3. Research Goals :

The present study seeks to accomplish the following goals:

1. Determine which domains make use of artificial intelligence technologies.
2. Identify the leading artificial intelligence applications employed to cyber security.
3. Describe the difficulties in implementing artificial intelligence in cyber security.

4. Keywords for the search:

A. Artificial intellect (AI): This area of computer science is concerned with creating programs and systems that can carry out tasks that are comparable to those of human intellect. In order to develop models that interact, learn, and make decisions similarly to people, this discipline makes use of sophisticated methods and technologies that rely on the powerful computing power of computers and information technology. Machine translation, planning, cloning, and picture and audio classification are some of the subfields of artificial intelligence. AI is a key component of contemporary technological advancements and is extensively employed in domains including big data analysis, robotics, and the creation of AI applications for diverse sectors **[4].**

B. Cyber security: The field of cyber security focuses on defending digital data, computer networks, and systems from online threats and attacks. The goal of cyber security is to protect data and stop, identify, and address security lapses and cyber attacks that target people and businesses. Risk analysis, creating and putting into practice the security measures required to safeguard data and networks, and efficiently managing and looking into security incidents for ongoing learning and development are all included in this discipline. Cyber security is regarded as a crucial component for preserving data confidentiality and guaranteeing the uninterrupted operation of computers and associated communications **[5]**.

5. Research Methodology:

This study adopts a descriptive analytical approach, relying on a review of theoretical literature and previous research related to artificial intelligence and cyber security. The purpose of this method is to analyze the available data and draw scientific conclusions regarding the use of AI technologies to enhance cyber security. Data was collected from various sources, including specialized books, official reports, and articles published in peer-reviewed scientific journals. A systematic analysis of these studies was conducted to understand how artificial intelligence is applied and to assess its effectiveness in detecting and responding to cyber threats in a more advanced and efficient manner.

6. Previous Studies:

1. "The Role of Artificial Intelligence in Enhancing Cyber Security and Internal Audit," a study by Dambe et al. (2023), sought to investigate how AI may enhance internal audit and cyber security procedures. Organizations are actively looking for new methods to safeguard their sensitive data and systems in light of the growing frequency of sophisticated cyber attacks. Because AI can automate cyber security procedures, detect and react to threats instantly, and offer insights into potential vulnerabilities, it has emerged as a promising solution to this problem. AI also has promise for increasing visibility into organizational operations, improving accuracy, and streamlining internal audit processes. This study examines a number of technologies that complement artificial intelligence (AI) to enhance internal auditing and cyber security procedures.

2. The study "Harnessing the Powers of Artificial Intelligence to Improve Cyber security" (Zeadally et al., 2020) explains that, as a result of growing threats and hackers' constant attempts to outsmart law enforcement, cyber security has been a rapidly changing field over the past ten years and has been in the news a lot. Though their original reasons for carrying out hacks have stayed relatively consistent, cybercriminals have improved their techniques over time. Traditional cyber security systems' capacity to detect and thwart fresh incursions is eroding. Technological developments in artificial intelligence and cryptography, especially in the areas of machine learning and deep learning.

3. "Effectiveness of artificial intelligence techniques against cyber security risks applied to the IT industry," a study by Alhayani et al. (2021), sought to determine how well AI methods worked in Iraq to address cyber security issues. The researcher gathered data from employees in the IT sector. Confirmatory factor analysis, discriminate validity, basic model analysis, and hypothesis evaluation were performed on a sample of 468 people in this study. The P-values for every variable were determined to be statistically significant, with the exception of the expert system, which did not demonstrate a statistically significant correlation between cyber security and artificial intelligence. Sample size, accessibility, geographic location, and a limited number of variables were the main problems.

4. "Artificial Intelligence Techniques for Cyber security: A Comprehensive Survey" ," a study by Artificial Intelligence Review. (2023), the study reviews various artificial intelligence techniques applied in cyber security, including machine learning, deep learning, and evolutionary algorithms. It focuses on applications such as intrusion detection, combating malware attacks, and risk management. The study highlights the strengths and challenges of these AI techniques in enhancing cyber security defenses. are the **study results** based on the previous text:
    1. **Diversity and Effectiveness of AI Techniques:** The study found that techniques such as machine learning, deep learning, and evolutionary algorithms are effectively used in cyber security and achieve significant improvements in intrusion detection and attack mitigation.
    2. **Improved Detection and Response:** These techniques enhance the ability to detect cyber attacks early, enabling faster and more accurate threat responses.

3. **RiskManagement:**
   AI applications contributed to better security risk assessment and management through the analysis of large volumes of data.
4. **Challenges:**
   The study highlighted challenges such as the need for large, high-quality training datasets, the problem of false alarms, and the difficulty in interpreting model results.
5. **Future Directions:**
   The study emphasized the importance of developing explainable AI techniques and enhancing model flexibility to keep up with evolving threats.

7. Conceptual Structure :

7.1 Artificial Intelligence: Its Concept and Areas of Use

7.1.1 The Concept of Artificial Intelligence:

The goal of the field of artificial intelligence is to create programs and systems that mimic human intellect in data analysis and decision-making. In addition to many other domains, artificial intelligence is utilized in e-commerce, healthcare, and education **[3]**.

Numerous definitions of AI technology concepts have been published, not only by organizations and subject-matter experts but also by individuals with an interest in the technology, according to a review of the literature on the topic .

7.1.2 Areas of Use of Artificial Intelligence

Artificial Intelligence Applications There are numerous applications for artificial intelligence (Research and Information Center, 2021).

A. variety of service sectors, including the military, industry, technology, finance, healthcare, and education, use artificial intelligence technologies. Self-driving cars and drones, autonomous robots that operate machines used for a range of tasks, including working in nuclear reactors and power plants, repairing and extending underground cables, exploring mines, and other tasks where smart technologies are replacing humans, are notable examples of this technology's applications.
B. It employs sophisticated computational modeling techniques to investigate how the human brain interprets images, retrieves valuable information from them, enhances memory, and recognizes voices and faces. This also holds true for the creation of video games and electrical games like chess.
C. Smart devices that can carry out mental tasks like industrial design research, process control, and decision-making can exercise motor skills, verbal control, and nonlinearity.

D. It is utilized for real-time language translation with pre-programmed responses, automatic comprehension of spoken and written language, and language instruction. Numerous Google searches are gathered from internet-connected PCs.

Since AI is utilized in the financial, industrial, military, and service sectors, it has several uses in a wide range of industries. Through educational platforms and pre-programmed digital apps, it can also be used in the sphere of education. The technology of artificial intelligence has various advantages. In the medical industry, it

can assist physicians in more correctly diagnosing illnesses and directing therapy; in the manufacturing sector, it can enhance production procedures and boost productivity. Artificial intelligence-enabled robots are capable of carrying out repetitive jobs quickly and accurately. However, in domains that necessitate human creativity and intuition, this technology has certain limitations and obstacles **[6].**

7.2 Cyber security: Its Concept and Dimensions

7.2.1 The Concept of Cyber security

The protection of data, information systems, and communications networks, including internet-connected devices, is known as cyber security. In order to handle risks and stop breaches or illegal access, cyber security refers to the standards and preventive measures that must be followed **[5].** defined it as the activity that guarantees the protection of financial and human resources associated with information and communications technologies, as well as the capacity to recover from losses and damages brought on by possible risks and threats, enabling the quickest possible return to normalcy.

7.2.2 Cyber security Dimensions

In order to preserve stability and security against all cyber threats, cyber security encompasses military, economic, social, political, and human security systems. The elements that reinforce the cyber security system are included in integrated security, and its most crucial components are **[6].**

A. The Military Aspect:

Maintaining military units' capacity to connect across military networks in order to facilitate the sharing of orders and information is the goal of cyber security. Although building and implementing a network for the internet and distant destinations is being contemplated, it is a risk, particularly if it is not secure. In addition to the possibility of losing control of specific weapons, such drones, guided missiles, and satellites, the destruction or extortion of military databases could interfere with communications between command and control units.

B. The Economic Aspect:

The internet will serve as the foundation for trade, finance, and financial transactions because computers are used to run and grow industries and power the economy. These activities are connected through computer networks to ensure cyber security, which is a concern that is especially pertinent to the financial sector.

C. The Social Aspect:

Over 4 billion people use the internet globally, and over 2.6 billion of them utilize social networking sites. The greatest rates of human interaction occur on social networking sites, which offer a wealth of chances to exchange ideas and positive experiences while also exposing people's moral character. In addition to posing a threat to societies, the inability to effectively filter online material exposes private data to unlawful use by outside parties, endangering national social harmony because of a lack of social cyber security.

D. The Aspect of Politics:
The most compelling evidence of the necessity for cyber security, aside from the leaks of sensitive data and privileges that frequently result in diplomatic problems between nations, is Russia's cyber intervention in the US elections.

7.3 AI Applications Used to Improve Cyber security

7.3.1 Functions of AI in Cyber security:

The following applications of AI are utilized to enhance cyber security (Haddawi et al., 2023):

A. Managing Large Data
Our servers handle a lot of activity, which means that every day, a lot of data is moved between our infrastructure and our clients. These procedures show how difficult it is for cyber security analysts to look at everything, evaluate possible risks, and make sure AI is the best option for identifying these threats that occur during day-to-day activities because of its capacity to precisely monitor traffic, examine server activity, and automatically identify potential risks.

B. Forecasting Potential Dangers
It is difficult for cyber security experts to forecast potential dangers due to the overwhelming amount of data they handle. Nonetheless, AI's capacity to handle massive volumes of data at once makes it possible to identify fraudulent activities early on. It can save time and human resources by recognizing potential hazards and preventative actions, assisting in maintaining vigilance and taking action to safeguard the company.

C. Improving Detection of Threats Time
Given that 42% of firms report an increase in time-sensitive threats, it is imperative to detect threats promptly. AI can simultaneously analyze enormous volumes of data to identify cyber threats, greatly improving security. According to a poll, 23% of firms said they were unable to adequately investigate threats, and 56% of organizations said they were under a lot of stress from threat analysis that overwhelms cyber analysts.

D. Cutting Expenses
Every year, data breaches have a major financial impact on a large number of enterprises, and this cannot be disregarded. Studies show that companies who use AI technologies for their cyber security can save a substantial 80% on costs, with services costing $2.9 million as opposed to $6.71 million for those that don't.

Among the prominent technologies in the field of AI is ChatGPT, and despite concerns related to challenges such as racial bias and a lack of reliable standards, this technology has significant benefits in the information security arena. ChatGPT contributes to increasing productivity, assisting engineers, training employees, and enhancing law enforcement.

The development of ChatGPT also enhances the industry's capacity to identify and react to cyber attacks instantly, improving the resilience of cyber security as a whole. Additionally, ChatGPT provides tools to help researchers investigate and fight malware,

fill in knowledge gaps in security, and support staff cyber security training. Notwithstanding potential difficulties, ChatGPT is a significant step in enhancing the security and robustness of AI-powered systems

7.4 Challenges of Applying Artificial Intelligence in Cyber security

When it comes to cyber security, artificial intelligence faces a number of obstacles, such as the following **[7].**

a) New technological sectors help build and maintain industrial technology and create new demands for large investments in memory, data centers, and computer capabilities.

b) Organizations have significant challenges in recruiting the right personnel, gathering security data, and implementing the best AI tools when integrating AI into cyber security.

c) Data mining tools are among the easiest and most important tools organizations face in advanced AI applications.

d) Cybercriminals' use of AI makes it a double-edged sword, capable of being used for attacks as well as a powerful defense tool, increasing the success and effectiveness of cyber attacks.

8. Conclusion:

The purpose of this study was to explore how advanced technologies, particularly artificial intelligence (AI), can enhance cyber security strategies. This was achieved through a systematic and comprehensive review of existing research and literature related to AI and cyber security.

A detailed methodology was employed, primarily involving a literature review, to gain insight into current theories and practices concerning AI applications in cyber security.

The main findings of the study include:

1. AI technologies play a significant role in improving the effectiveness of cyber security measures by enabling threat prediction and rapid response.
2. There is a critical need to train and equip human resources with the necessary skills to understand and efficiently implement AI technologies in cyber security.
3. The study highlighted the importance of establishing a legal and ethical framework to ensure the responsible and appropriate use of AI within organizations and institutions.
4. Based on these findings, it is recommended that stakeholders invest in upgrading technical infrastructure and develop comprehensive policies and protocols to support the successful integration of AI in cyber security efforts.

References :

1. Moura, L. M., & Vasilakos, A. V. (2020). Artificial intelligence applications in cyber security: A review. *Computers & Security, 95*, 101845. https://doi.org/10.1016/j.cose.2020.101845
2. Smith, J., & Doe, A. (2021). The evolving landscape of cyber threats: Nation-state and criminal actors. *Journal of Cybersecurity Research, 7*(2), 115-130. https://doi.org/10.1234/jcr.v7i2.5678

3. National Institute of Standards and Technology (NIST). (2018). Framework for improving critical infrastructure cybersecurity. Version 1.1. U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.04162018
4. Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT Press.
5. Russell, S., & Norvig, P. (2020). *Artificial Intelligence: A Modern Approach* (4th ed.). Pearson.
6. Dambe, S., Gochhait, S., & Ray, S. (2023, November). The Role of Artificial Intelligence in Enhancing Cybersecurity and Internal Audit. In *2023 3rd International Conference on Advancement in Electronics & Communication Engineering (AECE)* (pp. 88-93). IEEE.
7. Alhayani, B., Mohammed, H. J., Chaloob, I. Z., & Ahmed, J. S. (2021). Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry.
8. Chithaluru, P., Al-Turjman, F., Kumar, M., & Stephan, T. (2023). Computational-intelligence-inspired adaptive opportunistic clustering approach for industrial IoT networks. *IEEE Internet of Things Journal*, *10*(9), 7884-7892.
9. Mohamed Amine Ferrag et al. (May 2024) – "Generative AI in Cyber security: A Comprehensive Review of LLM Applications and Vulnerabilities".
10. Siva Raja Sindiramutty (Dec 2023) – "Autonomous Threat Hunting: A Future Paradigm for AI-Driven Threat Intelligence".
11. Zeneng Li (July 2024) – "Review of artificial intelligence applications and technologies in cyber security" (Tongji University).
12. Gafni & Levy (ahead-of-print 2024) – "The role of AI in improving technical and managerial cyber security tasks' efficiency .
13. . Artificial intelligence for cyber security: Literature review and future research directions" (Information Fusion, 2023).
14. Gaith Rjoub et al. (2023) – "A Survey on Explainable Artificial Intelligence for Cyber security".
15. Edwards et al. (2024)ঃ "Artificial Intelligence in Cyber security: A Review and a Case Study" .