Journal of Engineering and Technology for Industrial Applications

ISSN ONLINE: 2447-0228

ITEGAM-JETIA

Manaus, v.12 n.58, p. 296-303. March/April, 2026.

DOI: https://doi.org/10.5935/jetia.v12i58.3041

RESEARCH ARTICLE OPEN ACCESS

ARTIFICIAL INTELLIGENCE STRATEGIES IN ENHANCING CYBERSECURITY: AN ANALYSIS OF ADVANCED APPLICATIONS AND TECHNIQUES

Nibras Yousif-Algburi[1*], Ali Chasib Alhasnawy[2], Tara Sabah Mehdi[3]

[1,3]College of Medicine, University of AL-Qadisiyah , Iraq.
[2]Ministry of the Interior, Iraq.

[1]https://orcid.org/0009-0007-4307-3022, [2]https://orcid.org/0009-0006-8394-4147, [3]https://orcid.org/0009-0005-8490-2398

Email: * nibras.yousif@qu.edu.iq, tara.sabah@qu.edu.iq, alijasib2018@gmail.com

ARTICLE INFO

Article History
Received: December 2, 2025
Reviewed: January 1, 2026
Accepted: January 13, 2026
Published: March 31, 2026

Keywords:
Artificial Intelligence,
Cybersecurity,
Cyber- attack and defense,
Ethical Considerations;

ABSTRACT

In this research, we aim to detect the important role of Artificial Intelligence (AI) in increasing cyber security measures against rapidly refined cyber threats. Since cyber-attacks develop in complexity and frequency, traditional safety methods are often inadequate, which requires integrating AI-controlled solutions to increase danger, reaction time, and general safety flexibility. The study will be engulfed by various AI applications in the cyber security domain, including detection of nonconformities, automatic danger information analysis, and future analysis. By analyzing existing literature and case studies, research will emphasize how AI technologies such as machine learning and natural language treatment can be utilized to improve the effect of cyber security structure. Besides, there will be challenges and moral ideas related to distributing AI in security contexts, including privacy and concerns related to algorithm bias. Large findings of recent studies indicate that AI can increase cyber safety ability by quickly identifying and more accurate risk assessment of hazards. This research outlines the transformation effect of artificial intelligence on cyber security practices and provides recommendations for organizations to effectively use AI-controlled strategies. By promoting a deep understanding of skills and limitations in the cyber defense structure, the purpose of this study is to contribute valuable insights that can lead to future development in this important field at the present time.

I. INTRODUCTION

With the rapid progress of information and communication technology, digital society depends on refined systems to protect fast data and information. Due to large data, which may contain abnormal patterns that may indicate cyber hazards, increase the risk of loss and reduce the speed of the response. Other than this. With remarkable developments in science and technology and the use of different methods of storage and exchange of information - which is usually known as the transfer of data from one place to another in the network - safety awareness has become very necessary. From this situation, artificial intelligence emerged as a powerful tool that mimics human mental decisions with the aim of improving communications security and preserving information, for example, we see that the study [1]. Has revealed the use of machine learning and deep learning algorithms, such as SVM, LSTM, and CNN-LSTM, to detect malicious software on Android systems, This study confirmed that the SVM algorithm achieved 100% accuracy on the CICAndMal2017 dataset, while the LSTM reached 99.40% accuracy on the Drebin dataset. In addition, AI solutions contribute to more effective vulnerability analysis by combining traditional methods with AI-operated functionality. These solutions automate security scanning processes, identify important threats and learn of historical data, increase scalability, and accuracy, and adapt to new threats.

By combining traditional methods with AI-powered techniques for analyzing complex security vulnerabilities, the study [2] aims to detect critical threats, thwart attacks, and reduce human error. The cyber security sector is facing a significant challenge in explaining the results of the AI system based on the Deep Learning (DL) algorithm, which has led to a clear AI (XAI) to improve transparency and enable operators to make the right assessment. The literature review primarily explores the latest work in AI-powered cybersecurity tools and techniques such as machine learning algorithms, deep learning networks, and natural language processing [3]. And so is the study [4] Challenges facing AI cybersecurity include privacy violations, algorithmic bias, the use of AI in cyber-attacks, accountability, openness, and security issues, So we see many studies that have addressed these challenges, the ethical and legal challenges posed by the use of AI in cybersecurity, particularly in the ethical framework of data protection, where criminal risks such as ambiguity and sophisticated cyber-attacks are increasing, requiring a specific legal framework. Thus, it is clear that artificial intelligence plays an important role in expanding confidence in digital systems and opening new ways to get better security for sensitive information, by opening the danger and providing advanced solutions to the response.

II. RELATED WORK

II.1 CURRENT STATE OF KNOWLEDGE

Recent progress in artificial intelligence (AI) has changed cybersecurity practice much. Artificial intelligence (AI) is a powerful technology that helps cybersecurity teams automate repetitive tasks, accelerate threat detection and response [5].Machines are equipped with many techniques, software, mass databases, and complex algorithms capable of analyzing them, converting them into information-solving problems, and selecting the most appropriate options to solve problems and make appropriate decisions, let's make the term "artificial Intelligence "origin from American computer scientist John Macarthi, when this concept was first introduced during a scientific conference at Dartmouth College in 1956, which is designing a wise machine capable of mimicking the human mind. The opportunity was to detect. For instance, research shows that AI-driven tools can process vast amounts of threat intelligence data more efficiently than human analysts, thus improving situational awareness and decision-making processes [6], [7] . Relying on artificial intelligence technologies in cybersecurity is no longer a luxury but an indispensable tool for detecting threats, automating responses, and reducing the time required to detect attacks [8][9].

The rapid growth in digital governance has led to high levels of profitability, and the impact of regulatory risks associated with cybersecurity has resulted in a broader awareness and deeper understanding of how these risks affect strategic decision-making[10]. Based on the foregoing, we present here a research problem that focuses on the increasing sophistication of cyberattacks , which generates several critical challenges for malicious actors and organizations seeking to protect infrastructure, considering the methods and techniques employed by cybercriminals. The term artificial intelligence is a comprehensive term that provides many innovative solutions and smart devices, and offers new innovations as various fields of life develop [11]. This is what the future of urban cybersecurity requires maximizing the use of systems to repel, resist, and recover from malicious attacks [12]. This research paper offers insights into the potential for new opportunities related to artificial intelligence technologies in this context by examining how AI can be effectively integrated into cybersecurity practices. With the rapid development of AI technologies, its potential to improve communications infrastructure management through sophisticated anomaly detection is increasingly evident.

Furthermore, to fully realize this potential, more research is needed to address practical challenges related to scalability, immediate implementation, and long-term maintenance [13]. Ultimately, research will contribute to a better understanding of how AI can be used to solve modern cyber security challenges, and to ensure responsible and efficient distribution. One of the most prominent recent studies and results that demonstrate the effectiveness of artificial intelligence in detecting threats and analyzing risks is what the study reached [14]which resulted in the fact that they endorse a comfy records school sharing and conditional dissemination scheme with multi-proprietor in cloud computing, in which knowledge proprietor will share private statistics with a group of shoppers through the cloud in a totally cozy process, and knowledge communicator will broadcast the information to a trendy college of customers if the attributes satisfy the get right of entry to rules within the cipher text . Although researchers have found these solutions, a major challenge arises in interpreting the results of learning-based AI, leading to the emergence of the concept of explainable AI (XAI).

II.2 RESEARCH GAPS

Despite the remarkable development and progress in the role of artificial intelligence in supporting cybersecurity, there are some research gaps which must be pointed out, including: Interpreting AI systems' decisions: Deep learning algorithms often remain a mystery, making it difficult for experts to understand the decision-making mechanism, and affecting confidence in the systems. Theoretically, and despite the existing literature including a large number of research papers, we have found a deficiency in considering realistic scenarios in their content. It is important to note that useful scientific contributions should go beyond applying artificial intelligence techniques to cybersecurity datasets, and it is very important to make greater efforts to bridge the gap between the fields of artificial intelligence and cybersecurity [15]. Algorithmic bias: Numerous studies have confirmed the existence of biases in artificial intelligence algorithm techniques, which lead to the production of unfair or inaccurate decisions, especially with unbalanced data. The problem of algorithmic bias is one of the most significant challenges facing AI applications and cybersecurity. Studies emphasize the importance of addressing algorithmic bias, as it raises ethical and legal concerns, including combined dimensions, to ensure trust in artificial intelligence technologies and the rights and privacy of individuals and communities in our increasingly AI-led world [16]. Ethics& Privacy: AI applications in cybersecurity have raised numerous ethical and legal issues related to data privacy, accountability, and decision transparency. Many of the proposed frameworks seek to provide solutions that are just a part of compounding and escalating situations.

The transaction speed and scalability of technologies like BC can create a barrier to data protection rights, targeted cyber-attacks, and the ability to update and track users, however there are advantages in making separate forms that when produced as a whole, can support data verification , transparency and accountability in many industries [17]. Reliability and scalability: More research is required on how to scale the AI system to suit large, sometimes changing business environments, and ensure immediate responsibility and long -lasting efficiency.

III. METHODOLOGIES AND TECHNIQUES

This research used a descriptive and analytical approach to examine the role of artificial intelligence (AI) in increasing cybersecurity against developing threats online. The study begins by establishing a basic understanding of electronic information protection, defines the most important elements, forms, integrity, and accessibility and classifies the widespread threats, from human errors and environmental factors to hacking and sophisticated cybersecurity such as hacking and computer viruses. The methodology offers several key pillars to support a comprehensive understanding of the technical capabilities of artificial intelligence and its implications. The main components of the methodology can be summarized as follows:

- Descriptive Analysis: This pillar provides a comprehensive analysis of recent literature and academic studies to identify key AI applications and emerging trends in cyber threats and their mitigation. This section addresses how AI techniques can be used, such as in malware detection, incident response, and risk assessment.

- Quantitative Data Analysis: This research conducted a comprehensive quantitative analysis of cybercrime statistics between 2015 and 2022[18] Various categories of cyber threats were identified, as shown in Table 1 and Figure 2, to pinpoint the main trends in online criminal activity. Given the complexity of these threats and attacks, the use of artificial intelligence techniques to mitigate their impact has become essential.

- Review of case studies and advanced AI techniques: The research included a review of experimental studies and real-world applications demonstrating the practical effectiveness of advanced artificial intelligence algorithms and models. Focusing on modern techniques such as support vector machines (SVMs), long short-term memory (LSTMs), and hybrid models such as convolutional neural networks and long short-term memory (CNN-LSTMs), which have proven effective in malware hunting, vulnerability analysis, and other cybersecurity tasks.

III.1 ELECTRONIC INFORMATION SECURITY

III.1.1.The concept of electronic information security:

Today's advancements in wireless communications technologies have generated massive amounts of big data. Most of our information is part of a vast network that connects devices around the world [12]. And we can define Information security culture, which guides how things are done in the organization regarding information security, to protect the information assets and influence employees' security behavior[19]. Moreover Information security is defined as a set of measures and procedures adopted by an organization that becomes more sophisticated, especially information and data use, such as tamper unauthorized access, cybercrime, , using advanced technique injuries, illegal [1]. Electronic information protection refers to the protection of ordered data stored or transmitted through electronic systems from the dangers and attacks that can lead to data violations, losses, or unauthorized changes. This includes the implementation of guidelines and a series of technologies to ensure privacy, integrity, and availability of confidentiality, integrity, and information such as encryption and firewalls. In addition, electronic security depends on the access control mechanism that defines who is authorized to view or change the data. In the digital age, electronic information protection is important for individuals and organizations to protect against increasing risks, such as cyber-attacks and harmful software.

Information security is defined by three different approaches: educational, technical, and legal. From an academic point of view, information is a scientific field that studies principles and strategies to protect information from hazards and malicious activities. From a technical point of view, it includes equipment, methods, and procedures required to ensure the protection of information from both internal and external risks. From a legal point of view, information is related to security studies and to combat the confidentiality of information, along with measures to protect the integrity and availability of information, to break or utilize information systems for criminal purposes. Information security is a set of measures taken by an organization to protect its information systems in various ways, physical measures to protect the organization's hardware from damage can be defined as logical measures as protective software designed to prevent theft, hacking, or material manipulation. Information security should exist to be effective. Growth for cyber threats extends far beyond traditional security areas administered by information technology software [20]. To be effective and excellent information protection, three basic and important conditions must be met:

- Disponibility: It refers to access to data so that they can read and find it easily.
- Integrity: This means keeping information during transmission, processing, or storage, unchanged in material or size. Generally, the system ensures the accuracy of the information and prevents it from being replaced by third parties, its accuracy and perfection..
- Confidentiality: This indicates that information can only be read and accessed by people with special access rights.

These items are in line to create a complete concept of information protection, as illustrated in the following data:

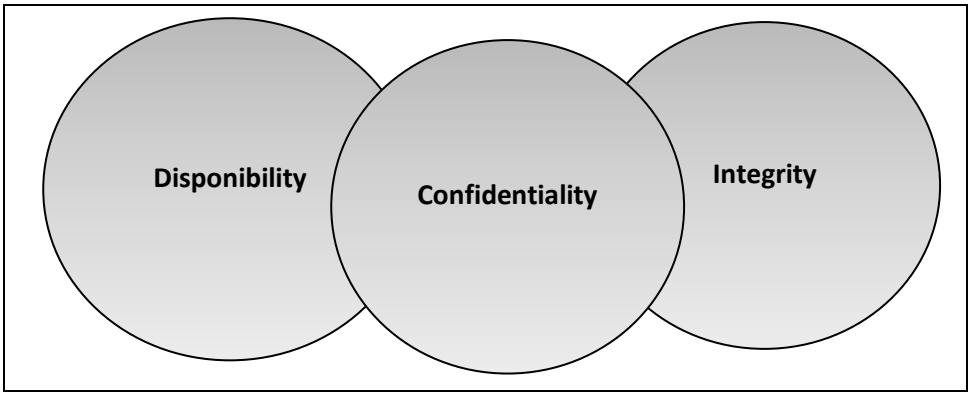

Figure 1: Represents information security elements.
Source: Authors, (2026).

When focused, large amounts of electronically stored data become more vulnerable to new dangers when stored manually. Advanced technologies and software have helped to expand the extent of these risks. We can describe these dangers this way:

- Human Threats-: These occur at some point of the layout of hardware or information systems , and they include activities consisting of programming, testing, facts compilation, and the input of statistics into the machine
- Environmental Threat:- These embody herbal failures together with earthquakes, storms, floods, and hurricanes. They additionally include problems related to electricity failures, fires, and the malfunctioning of conditioning and cooling structures, among different environmental elements which could have an effect on machine availability.
- Cybercrime hacking:- unauthorized access or infiltration in the system through the use of hacking tools or software
- Computer virus: Independent software that is built into computer programs and causes, causing potential damage or dissolution of the system.
- Digital crime: to increase the risk of privacy security from modern technologies, including surveillance technologies (e.g. camcorders), electronic identity cards, and cutting or surveillance methods.
- Hacking is the process of illegal infiltration of systems and equipment using advanced equipment and techniques to reach sensitive information or take control of data. This may include stealing data, destroying the system or even disrupting important operations of companies and organizations.

These categories illustrate the diverse range of threats that can impact electronic data, arising from human actions, environmental factors, or cybercriminal activities. A study [18] has shown an increase in the level of cybercrime in the era of electronics and digitization, as shown in the following table:

Table 1: Changing trends in cybercrime attacks (in millions).

Incidents	2015	2016	2017	2018	2019	2020	2021	2022	%Increase /Source
Fraud	3.439	3.546	3.736	3.879	4.157	4.455	4.746	5.191	50%[21]
Denial of Service	0.368	0.544	0.676	0.755	0.946	1.276	1.383	1.567	327% [21]
Cyber Harassment	0.345	0.454	0.655	0.764	0.845	1.156	1.266	1.478	328% [22]
Vulnerability reports	0.310	0.515	0.614	0.811	0.915	0.990	1.372	1.491	381% [23]
Malicious code	0.410	0.545	0.756	0.967	1.176	1.245	1.444	1.580	285% [23]
Content related	0.203	0.375	0.576	0.848	1.177	1.176	1.277	1.364	578% [21]
Total	5.075	5.979	7.013	8.024	9.216	10.298	11.488	12.671	

Source: Authors, (2026).

The following diagram represents the number of cybersecurity incidents from 2015 to 2022, which is classified by that type of attack.

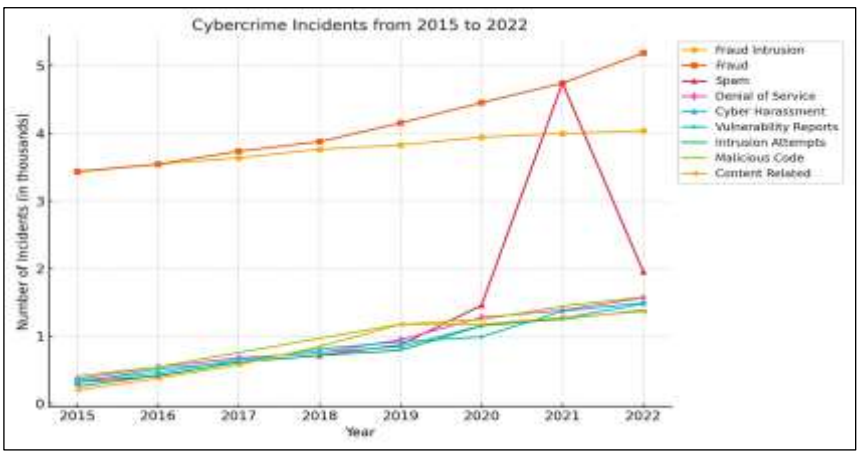

Figure 2: Diagram shows Cyber security incidents (2015-2022).
Source: Authors, (2026).

As a result of the increasing reliance on digital technologies and the internet, cyberattacks increased significantly between 2015 and 2022. The increased vulnerability of systems to attacks by vulnerable individuals has led to a significant increase in breaches. These breaches affect key sectors in countries, including healthcare.

III.1.2 Different forms of cyber- attacks

Cyber -attacks that can target the equipment, software and network of an organization, take different forms and use more methods. They are constantly evolving and used to break or damage all the weaknesses of the system. The Internet is a favorite medium for hackers to commit these crimes. Some of these attacks include the following:

- Malware : This is represented in viruses, worms, and Trojans , aimed at damaging or breaking devices and systems.
- Hacking: Attacker infiltrates the system or network to access sensitive data or information.
- Ransomware: Attackers encrypt the victim's data and information and demand a ransom to decrypt it.
- Phishing Attackers trick users into giving away their personal or financial information through fake messages or scams.
- DDoS (Distributed Denial of Service) Attacks: a large amount of data is sent to the sink and disables it.
- **Man-in-the-Middle Attacks** : Prevent communication between two parties to access the data transferred to the attackers.
- Exploitation of Security Vulnerabilities attackers utilize software or systems to access networks or data.

These attacks are developing to maintain frequent technological advances, making it necessary to update security systems regularly.

III.2 CONCEPT OF ARTIFICIAL INTELLIGENCE

Artificial intelligence (AI) can be defined as the theory and development of computer systems capable of performing tasks that previously required human intelligence, such as voice recognition, decision -making and pattern identity. AI is a comprehensive term that includes many techniques, including AI algorithms and technology, deep nervous networks and deep learning models. AI algorithms analyze and learn from data to extract the pattern and then decide. Deep neural networks are advanced models inspired by the human brain and are used in applications such as Natural Language Processing (NLP) and image recognition. Through deep learning models, AI can improve accuracy over time by learning from large amounts of data. It is also known as science and engineering subjects to create intelligent machines, especially intelligent computer programs. It is associated with overlapping tasks, namely the use of computers and algorithms to understand human intelligence, but artificial intelligence is not limited to methods that can be observed biologically [24]. In addition, some claim that the AI leadership varies from IT management in the past.

AI is not just a technique or set of technologies, but rather a constantly evolving horizon of emerging computing capabilities and innovations [25]. Moreover ,we can point to a very important aspect in dealing with artificial intelligence technologies: AI governance. This is a fundamental aspect, especially when tasks such as prediction and rapid decision-making are delegated to artificial intelligence systems (AIs). Recent policies, particularly in Europe, highlight the importance of this issue and emphasize the need for guarantees that the AI system is transparent Artificial intelligence (AI) is a paradigm to imitate the logic of the people, e.g. Already unpublished computer classification of future events such as stock market trends, sales and consumer behavior predict. The term "artificial intelligence" (AI) has recently gained popularity, legal scholars have provided different definitions. From a technical perspective, a remarkable definition AI describes as a "computer program that depends on algorithms and specific processes to perform special features or features.

This system is designed to receive automatic inputs, which are processed according to the program's instructions. From this we conclude that artificial intelligence depends on the software algorithms that are entered into the computer, the inputs of which depend on codes and rules. A great use of AI can be seen in advanced robotics. AI depends on computers equipped with real knowledge, and the origin of AI is represented through a process -based sequencing method through this knowledge. Despite the meaning, AI responsibility is often defined as the values, exercises and goals of the AI system, which is used inadequately in practical applications [26]. In addition, it should be noted that artificial intelligence cannot be underestimated, especially in relation to large data and its effect on social, political and social structures created by individuals as communication. This is part of the greater digital transformation, and its future potential is difficult to predict given the massive growth in computing power alone and its interaction with the "analog world"[27].

III.3 EVOLUTION OF TRADITIONAL ANOMALY DETECTION

A questioner may ask: What is a traditional anomaly?

The term actually refers to discovering deviations when it comes to abnormal phenomena or patterns from the pattern, distracted by general or expected behavior in the network. The aim of detecting the deviation aims to identify nonconformities that may indicate problems such as previous quality, abuse of service, traditional anomalies, cyber halls or returns. Legislators - rulers use some rules and predetermined criteria to identify unusual patterns. For example, fixed thresholds can be used to monitor network traffic, if the values are more than these thresholds, an alert can be triggered. Although technology has improved our lives a lot by making information and communication easily accessible through devices such as computers and mobile phones. These devices not only help us manage individual and professional features, but also save important data including credit card details and passwords. However, this data can be unsafe for cyber criminals who benefit from weaknesses through various attacks and require unauthorized access. Awareness of different types of cyber threats is required for security [28]. As the volume of data increases, it is necessary to protect this data from theft, tampering or intrusion.

According to a recent review published in Springer (Edozie et al., 2025) [13] there are several limitations to traditional methods. First, rule-based systems lack flexibility and are difficult to handle with new networks. Not to mention the erroneous rates that can result, leading to false alerts or failure to detect critical events . There is a recent study [13] that shows in (Figure 1)a sufficient increase in global data volume from 2010 to 2024. This figure indicates rapid expansion in the amount of data generated in the network and system and the processed data provides an indication. The dependence on digital infrastructure from organizations, companies and officials is increasing. This figure indicates that this significant data text corresponds to technological advances such as 5G networks and Internet of Things (IoT), leading to an increase in the complexity of the network environment. This complexity creates traditional methods, such as the rules system, insufficient to address the increasing security threats .As a result, the integration of advanced technologies such as artificial intelligence (AI) has become necessary to effectively analyze this data and not to detect analogies. The heavy growth in the data volume emphasizes the immediate need for a system that detects noise and is able to process large amounts of information in real time. These systems can learn autonomy and improve the performance of Ti35me, network traffic patterns and new threats. Given the frequent errors and the difficulty of electronic adaptation, the need arose to search for more efficient solutions

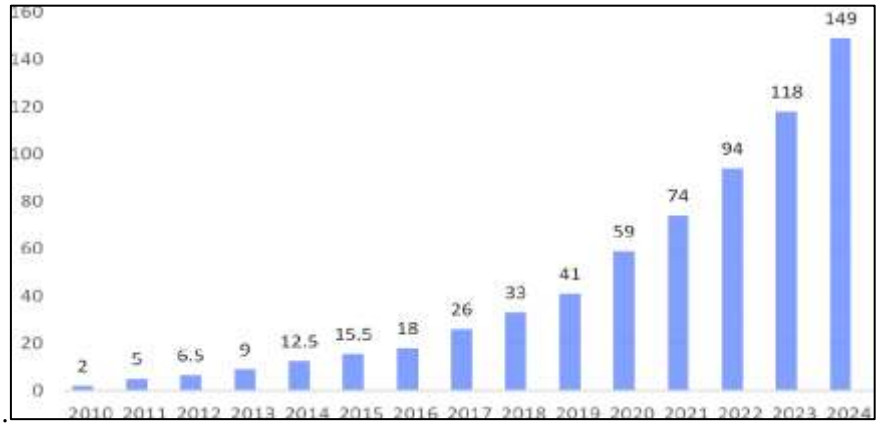

Figure 3: Data Growth Worldwide 2010–2024.
Source: Authors, (2026).

Therefore, it is important to highlight the role of artificial intelligence techniques in improving network anomaly detection. The main objectives of this research can be added as follows:

-AI Efficiency Analysis: Artificial intelligence technologies, especially deep learning algorithms, machine learning, and natural language processing, are used to obtain accurate results for detection systems, leading to increased cybersecurity defenses.
-Identifying current challenges: Highlighting anomalies as ways to detect traditional deviations, such as high false positive frequencies and difficulties in adapting to new computer patterns.
-Explore innovative solutions: Providing an innovative AI-based solution to address cybersecurity challenges, including the use of advanced deep learning models such as Recurrent Neural Networks (RNNs) and Convolutional Neural Networks (CNNs).
-Develop research hypothesis: to prepare hypotheses related to AI's role in strengthening cyber security, such as how it can detect danger and response time.
-Discuss moral ideas: Data to address moral ideas related to privacy and how to use AI affects cyber security practice.
-Provide practical recommendations: To offer practical recommendations for stakeholders in the cyber security sector, how to effectively be integrated into systems to detect deviations to AI technologies.

IV.RESULTS AND DISCUSSION:

This study analyzes the application of artificial intelligence (AI) to increase cyber security towards developing hazards online. The data reveals a significant tendency to integrate AI technologies to detect the danger, event reaction and general security. AI-operated equipment shows increased efficiency in the treatment of the danger intent, which improves status awareness and decision-making. AI reduces timely reaction time automatically by blocking malicious traffic and separating the infected system. Some machine learning algorithms show high accuracy in detection of harmful software, and contribute to an active defense against cyber -attacks. In addition, AI increases vulnerability analysis by automating security scanning and prioritizing dangers. Analysis of online crime data reveals an increase in the frequency and processing of cyber- attacks, and requires integration of AI to improve cyber security. Cybercrime has increased dramatically, highlighting the need for more effective security solutions. AI provides the ability to address the abilities by identifying these developed dangers constantly, and detecting asymmetrical behavior and automatically to the reaction of the event. However, the analysis also highlights moral ideas on the use of AI in cyber security. Ensuring openness and confidence in AI-operated systems presents an important challenge. The deployment of AI in cyber security increases the concerns of privacy violations, algorithm bias and accountability. The moral structure of data security becomes especially important when it comes to AI-operated cyber security solutions. Based on the research results, the researcher recommends the following:

-Develop Advanced Ai-Powered Detection Systems: Analyzing The Discrepancy Pattern and Predicting Cyber Attack Before Occurring, Focusing on the Use of Machine Learning Algorithms to analyze user behavior and detect any suspicion.
- Invest in training employees on how to identify cyber threats: to educate them on the latest phishing and malware techniques, and provide them and their outfits, which provide the equipment and skills required to protect them from cyber- attacks.

-Use strong security measures: for example, multifactor authentication, encryption of sensitive data, and regular software and system updates to reduce the security weaknesses utilized by the attackers.
- Establishment of clear laws and regulations that control the use of AI in cyber security: to ensure the safety of privacy and security, and to define responsibility and responsibility in the event of security incidents.
- Encourage cooperation and information sharing between organizations and public agencies: To raise awareness of cyber threats and exchange best practices in cyber security.

V.CONCLUSION AND FUTURE WORK

V.1 CONCLUSION

This research emphasizes the developed role of artificial intelligence in increasing cyber security against new digital dangers. Since modern society depends on the technical systems that are growing rapidly, the need for AI-controlled solutions to strengthen the traditional security protocol has become clear. While AI plays an important role in the Founding, the event reaction and the vulnerability assessment, it is necessary to address moral concerns related to openness, privacy and potential prejudices in the AI algorithm. In order to use AI, organizations must prefer responsible strategies focused on moral guidelines, collaboration between AI experts and cyber security people and continuous performance monitoring. By understanding the strength and boundaries of AI in Cyber Defense, this research contributes to valuable insights that can lead future development and distribution in this important field, ensuring a safer digital future for individuals, institutions and officials.

V.2 FUTURE WORK

Despite the remarkable progress this study makes in enhancing the AI-managed cyber domain, it is merely the beginning of numerous promising and open-ended avenues for exploring future visions and more clearly defined developments, particularly AI models- so-called Explainable AI (XAI), to increase user confidence and ensure the soundness of decisions made in the field of cybersecurity. Furthermore, there is a need to formulate a strong defense against hostile digital assaults is important that the research also addresses the long-term ethical, legal and societal implications of deploying artificial intelligence in cybersecurity, including protecting confidentiality, algorithmic fairness and avoiding bias Also, multidisciplinary collaboration between AI experts, cybersecurity specialists and legal researchers is needed to develop comprehensive guidelines for the responsible use of AI in digital defense. Finally, it is recommended to conduct thorough and realistic studies to assess the effectiveness, limitations, and unintended consequences of AI-managed cybersecurity systems. This work will ensure that future AI solutions not only enhance technical capabilities but also align with social values and evolving needs, contributing to a more secure and resilient digital ecosystem.

VI. AUTHOR'S CONTRIBUTION

Conceptualization: Nibras Yousif-Algburi, Ali Chasib Alhasnawy, Tara Sabah Mehdi
Methodology: Nibras Yousif-Algburi, Ali Chasib Alhasnawy
Investigation: Nibras Yousif-Algburi, Ali Chasib Alhasnawy
Discussion of results: Nibras Yousif-Algburi, Ali Chasib Alhasnawy, Tara Sabah Mehdi.
Writing – Original Draft: Nibras Yousif-Algburi
Writing – Review and Editing: Nibras Yousif-Algburi, Ali Chasib Alhasnawy.
Resources: Nibras Yousif-Algburi, Ali Chasib Alhasnawy
Supervision: Ali Chasib Alhasnawy.
Approval of the final text: Nibras Yousif-Algburi, Ali Chasib Alhasnawy, Tara Sabah Mehdi

VII. ACKNOWLEDGMENTS:

We extend our sincere thanks to the College of Medicine at Al-Qadisiyah University for their ongoing support and for facilitating official communication with the National Security Directorate. We also express our deep gratitude to the National Security Directorate's Cybercrime Department for their active participation in this study and their invaluable support. Finally, we extend our sincere thanks to the staff of the Cyber Extortion Unit for their insightful feedback and outstanding communication.

VIII. REFERENCES

[1] H. Alkahtani and T. H. H. Aldhyani, "Artificial Intelligence Algorithms for Malware Detection in Android-Operated Mobile Devices," Sensors, vol. 22, no. 6, pp. 1–26, 2022, doi: 10.3390/s22062268.

[2] Ezekiel Onyekachukwu Udeh, Prisca Amajuoyi, Kudirat Bukola Adeusi, and Anwulika Ogechukwu Scott, "The integration of artificial intelligence in cybersecurity measures for sustainable finance platforms: An analysis," Comput. Sci. IT Res. J., vol. 5, no. 6, pp. 1221–1246, 2024, doi: 10.51594/csitrj.v5i6.1195.

[3] N. U. Prince, M. A. Faheem, O. Ullah, K. Hossain, A. Alkhayyat, and A. Hamdache, "AI-Powered Data-Driven Cybersecurity Techniques : Boosting Threat Identification and Reaction," vol. 10, pp. 332–353, 2024.

[4] Z. I. Khisamova, I. R. Begishev, and E. L. Sidorenko, "Artificial intelligence and problems of ensuring cyber security," Int. J. Cyber Criminal., vol. 13, no. 2, pp. 564–577, 2019, doi: 10.5281/zenodo.3709267.

[5] R. Kaur, D. Gabrijelčič, and T. Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions," Inf. Fusion, vol. 97, no. April, 2023, doi: 10.1016/j.inffus.2023.101804.

[6] Adebimpe Bolatito Ige, Eseoghene Kupa, and Oluwatosin Ilori, "Analyzing defense strategies against cyber risks in the energy sector: Enhancing the security of renewable energy sources," Int. J. Sci. Res. Arch., vol. 12, no. 1, pp.

2978–2995, 2024, doi: 10.30574/ijsra.2024.12.1.1186.

[7] Y. Gao, “Cyber Attacks and Defense: AI-Driven Approaches and Techniques,” Acad. J. Comput. Inf. Sci., vol. 7, no. 7, pp. 41–46, 2024, doi: 10.25236/ajcis.2024.070706.

[8] C. Y. Haryanto et al., “Contextualized AI for Cyber Defense: An Automated Survey Using LLMs,” 2024 17th Int. Conf. Secur. Inf. Networks, SIN 2024, 2024, doi: 10.1109/SIN63213.2024.10871242.

[9] C. Science, C. Science, C. Science, C. Science, and C. Science, “Enhancing Network Security : A Framework for Proactive Cyber Defense Using Artificial Intelligence and Big Data Abstract : The Meaning of Computer Network System
Security Maintenance,” 2024, doi: 10.59324/ejtas.2024.2(6).15.

[10] M. Kianpour and S. Raza, “More than malware: unmasking the hidden risk of cybersecurity regulations,” Int. Cybersecurity Law Rev., vol. 5, no. 1, pp. 169–212, 2024, doi: 10.1365/s43439-024-00111-7.

[11] ENISA, Cybersecurity and Privacy in Ai – Forecasting Demand on Electricity Grids, no. June. 2023. doi: 10.2824/92851.

[12] C. Gupta, I. Johri, K. Srinivasan, Y. Hu, and S. M. Qaisar, “A Systematic Review on Machine Learning and Deep Learning,” Prog. Biophys. Mol. Biol., no. June, 2022, [Online]. Available: https://doi.org/10.1016/j.pbiomolbio.2022.07.004

[13] E. Edozie, A. N. Shuaibu, B. O. Sadiq, and U. K. John, “Artificial intelligence advances in anomaly detection for telecom networks,” Artif. Intell. Rev., vol. 58, no. 4, 2025, doi: 10.1007/s10462-025-11108-x.

[14] K. Geyamallika and E. Kesavulu Reddy Asst Professor, “Survey of Emerging Threats in Cyber Security; Survey of Emerging Threats in Cyber Security,” Int. J. Eng. Res. Technol., vol. 8, no. 2, pp. 1–3, 2020, [Online]. Available:
https://ieeexplore.ieee.

[15] F. Charmet et al., “Explainable artificial intelligence for cybersecurity: a literature survey,” Ann. des Telecommun. Telecommun., vol. 77, no. 11–12, pp. 789–812, 2022, doi: 10.1007/s12243-022-00926-7.

[16] “View of Artificial Intelligence and Bias_ Challenges, Implications, and Remedies.pdf.”

[17] V. Wylde et al., “Cybersecurity, Data Privacy and Blockchain: A Review,” SN Comput. Sci., vol. 3, no. 2, pp. 1–12, 2022, doi: 10.1007/s42979-022-01020-4.

[18] D. Dave, G. Sawhney, P. Aggarwal, N. Silswal, and D. Khut, “The New Frontier of Cybersecurity: Emerging Threats and Innovations,” Proc. - ICT 2023 - 29th Int. Conf. Telecommun. Next-Generation Telecommun. Digit. Incl. Univers. Access, pp. 1–6, 2023, doi: 10.1109/ICT60153.2023.10374044.

[19] A. Alhogail and A. Mirza, “Information security culture: A definition and a literature review,” 2014 World Congr. Comput. Appl. Inf. Syst. WCCAIS 2014, 2014, doi: 10.1109/WCCAIS.2014.6916579.

[20] D. DiMase, Z. A. Collier, K. Heffner, and I. Linkov, “Systems engineering framework for cyber physical security and resilience,” Environ. Syst. Decis., vol. 35, no. 2, pp. 291–300, 2015, doi: 10.1007/s10669-015-9540-y.

[21] J. M. Alghazo, Z. Kazmi, and G. Latif, “Cyber security analysis of internet banking in emerging countries: User and bank perspectives,” 4th IEEE Int. Conf. Eng. Technol. Appl. Sci. ICETAS 2017, vol. 2018-Janua, pp. 1–6, 2017, doi: 10.1109/ICETAS.2017.8277910.

[22] L. J. Trautman and P. Ormerod, “Wannacry, Ransomware, and the Emerging Threat to Corporations,” SSRN Electron. J., vol. 86, no. 2, 2018, doi: 10.2139/ssrn.3238293.

[23] J. Jang-Jaccard and S. Nepal, “A survey of emerging threats in cybersecurity,” J. Comput. Syst. Sci., vol. 80, no. 5, pp. 973–993, 2014, doi: 10.1016/j.jcss.2014.02.005.

[24] J. J. Y. Sung, “Artificial intelligence and the future of medicine,” Artif. Intell. Med. From Ethical, Soc. Leg. Perspect., pp. 1–12, 2024, doi: 10.1016/B978-0-323-95068-8.00001-7.

[25] P. R. Krausman, “Managing artificial intelligence,” J. Wildl. Manage., vol. 87, no. 8, pp. 1433–1450, 2023, doi: 10.1002/jwmg.22492.

[26] C. Novelli, M. Taddeo, and L. Floridi, “Accountability in artificial intelligence: what it is and how it works,” AI Soc., vol. 39, no. 4, pp. 1871–1882, 2024, doi: 10.1007/s00146-023-01635-y.

[27] H. Ruschemeier, “AI as a challenge for legal regulation – the scope of application of the artificial intelligence act proposal,” ERA Forum, vol. 23, no. 3, pp. 361–376, 2023, doi: 10.1007/s12027-022-00725-6.

[28] J. M. Biju, N. Gopal, and A. J. Prakash, “Cyber Attacks and Its Different Types,” Int. Res. J. Eng. Technol., vol. 6, no. 3, pp. 4849–4852, 2019, [Online]. Available: www.irjet.net