CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES

https://cajmtcs.casjournal.org/index.php/CAJMTCS

Volume: 07 Issue: 01 | January 2026 ISSN: 2660-5309

Article

The Role of CyberSecurity Effectiveness in Iraq for Artificial Intelligence Technology: Exploratory Study

Zahraa Mousa Saad

1. College of administration and Economics, University of Misan, Amarah, Iraq
* Correspondence: Zahraa.m.s@uomisan.edu.iq

Abstract: Balancing between innovation in Artificial Intelligence and Cybersecurity is crucial for ensuring information security and successful modern technological applications in Iraq. As it achieving these objectives will contribute in building a secure cyber environment supporting innovation and achieves sustainable development in Iraq. And the importance of research in enhancing cybersecurity in Iraq and highlights to future challenges and the importance of continuing research in this field. So, previous studies have shown that Iraq faces major challenges in the field of cybersecurity, especially with increasing use of artificial intelligence technologies. And reflect the results the need to develop comprehensive strategies enhance from security effectiveness with a focus on: 1) Cooperation between the public sectors and private sectors: to enhance mutual understanding between government institutions and private companies around the importance of cybersecurity. 2) Training human resources: from through educational programs targeted to ensure the availability of specialists in these fields. 3) Investment in research and development: to ensure that remain proposed solutions for facing cybersecurity threats advanced and effective. 4) Developing appropriate legislation: to ensure data protection and strengthen the legal frameworks necessary for investing in artificial intelligence technologies.

Keywords: CyberSecurity of Effectiveness, Cybersecurity threats, Cybersecurity challenges, Artificial Intelligence Technology, CyberAttacks in Iraq.

Citation: Saad, Z. M. The Role of CyberSecurity Effectiveness in Iraq for Artificial Intelligence Technology: Exploratory Study. Central Asian Journal of Mathematical Theory and Computer Sciences 2026, 7(1), 354-374

Received: 10th Nov 2025
Revised: 21th Dec 2025
Accepted: 14th Jan 2026
Published: 06th Feb 2026

1. Introduction

It has issue of information security and protection from the importance of modern issues, Where the success of any organization depend increasingly on its ability to maintain the integrity and confidentiality of its information and to safeguard the interconnection of its business operations, data, systems and internet network infrastructure Abeyratne [1].

And considered Artificial Intelligence is one of the outcomes of the Fourth Industrial Revolution due to its multiple uses in military fields, industrial, economic, technological, applications medical, educational and service, It is even expected that the next phase will further increase in its ratio depend on AI, especially with the remarkable developments that this field is witnessing and the ongoing interaction between information technology and contemporary brain research Madkour.

And with technological advancements that taking place worldwide in the field of technology and digital transformation, It has become Cybersecurity a fundamental pillar to ensuring information integrity and protecting data at both individual and organizational levels. So, the world faces today increasing threats from CyberAttacks that

targeting digital infrastructure, which leads to losses economic and significant security. In this context, the role of Artificial Intelligence technologies have emerged as advanced modern solutions that can bring about a qualitative transformation in the field of Cybersecurity. As it highlights the importance of the global and local Cybersecurity in Iraq and role of modern technologies and AI in enhancing cybersecurity Abdelrahim [2].

Thus, the tremendous growth of tools and systems and interconnected networks makes cybersecurity more challenging and leads to technological advancements in the digital economy and infrastructure to have exacerbated this issue, which leads to noticeable rise in Cyberattacks which carry severe consequences and considered set of tools and procedures and practices that protect against damage and attacks and unauthorized access to networks, devices, software and data is collectively referred to as security Bhardwaj et al. [3].

And became Cybersecurity and Artificial Intelligence tremendous development in the fields of modern technology as serving an urgent to ensure the protection of digital systems and infrastructure for information. In Iraq, increasing reliance on modern technologies makes it crucial to enhancing Cybersecurity is of utmost importance to ensure safe utilization from Artificial Intelligence technologies Al-Barai.

However, has become CyberAttacks more frequent and larger in scale and more impactful, It is essential to implement intelligence-based Cybersecurity for Big Data Management and provide dynamic defense against emerging cyber threats to the increasing complexity of cyberattacks which detect new methods and intrusive for targeting even the most sophisticated targets. Moreover, the continuous evolution of adversaries with ties to nation-states and criminal organizations Chithaluru et al. [4].

And to achieve methods and techniques Cybersecurity which is considered from through several means, most importantly working to empower employees and involve them in decision-making and granting them greater decision-making authority, self-motivation and continuous training, which leads to an increase knowledge level and expertise in their to confront operations breaches of electronic systems and technologies and confidential organizational information and data Haddawi et al. [5].

It is also considered Artificial Intelligence technology a prominent achievement in the Fourth Industrial Revolution, thanks to its wide-ranging applications in various fields of life. This technology has been used in the economy, industry, services, military sectors and politicaly, In addition to its role is the biggest in enhancing cybersecurity, and This is closely related to the public interest of individuals and communities where it has been used to improve cybersecurity in different countries Dahmani [6].

And considered Artificial intelligence technologies are from the most prominent technological advancements in the twenty-first century where it has significantly impacted various fields in different life fields, including the economy, industry, education and healthcare. With increases depending on these technologies, The cybersecurity threat is increasing. Like other Iraq faces significant challenges in this field, which necessitates adopting effective strategies to strengthen cybersecurity in the face of artificial intelligence risks Zaem.

with various Artificial intelligence its technologies and different applications from the complex and emerging issues and especially in the present era. Amid this technological development, which has encompassed all aspects of life of social, economic and security and given its numerous applications in our daily lives to our world, requiring associated foresight and strategic planning Dahiri.

And The researchers conclude that Iraq is experiencing increasing in digital infrastructure which necessitates effective systems to protecting data and information. And in Amid the rise of cyberattacks and technological challenges, Artificial Intelligence Technologies have become an urgent necessity to enhance Cybersecurity effectiveness. And aims study to explore the current state of cybersecurity implementation and its integration with AI in the Iraqi context, with the aim of identifying gaps and proposing effective developmental insights.

2. Research Problem:

Iraq faces from big challenges in the field of cybersecurity results to weak digital infrastructure and the lack to comprehensive policies protect data and prevent cyber threats. And requires the integration of artificial intelligence technologies by Successfully a secure digital environment, which raises questions about Iraq's readiness to meet these requirements.

Also represented research problem in the absence of a clear and defined framework the effectiveness of cybersecurity in Iraq with regard to artificial intelligence technologies and attention is drawn on the challenges which facing cybersecurity in Iraq, such as weak digital infrastructure, increasing cyberattacks and the lack of knowledge or implementing resources to reflect for AI technologies which is presented in the following questions:

1. What is the role of cybersecurity effectiveness in Iraq for artificial intelligence technologies?
2. What should on governmental and private institutions to protect data and systems from increasing cyber threats?
3. How can cybersecurity to support innovation in the field of artificial intelligence without conflicting with privacy and individual rights?
4. How can AI technologies to improving in enhancing cybersecurity in Iraq? and what challenges which hinder the implementation of these technologies?
5. What is the need to improve cybersecurity systems in Iraq to faced modern challenges?

3. Research Objectives:

This study aims to highlight on the potential which provide artificial intelligence to enhance cybersecurity in Iraq. as these technologies can contribute to improving threat monitoring, predicting cyberattacks and enabling faster and more efficient responses to such challenges. it also relies on technologies such as machine learning, big data analytics and natural language processing, making it an effective tool in confronting evolving threats and which are presented in:

1. Identify on the role of cybersecurity effectiveness in Iraq to artificial intelligence technologies.
2. Clarify the role of governmental and private institutions in it, to protecting data and systems from increasing cyber threats.
3. Determine supports cybersecurity for innovation in the field of AI without conflicting with privacy and individual rights.
4. Examine about AI technologies in enhancing cybersecurity in Iraq and the challenges which hinder their implementation.
5. Identify on improvements cybersecurity systems in Iraq to confronting modern challenges.

4. Research Significance:

That's importance of this research stems from the urgent need to keep pace with global technological developments and to utilize them in protecting digital systems in Iraq. And hope this research to contribute to bridging the knowledge gap about this subject, and to serve as a starting point for developing effective national policies in the field of cybersecurity. The significance of the research is divided into:

4.1. Scientific Significance:

1. Enhancing the role of academic knowledge, both Arab and international around the relationship between cybersecurity and artificial intelligence technologies.
2. Establishing conceptual frameworks and foundational knowledge that open the field for future studies relates at developing more comprehensive cybersecurity policies.
3. Highlighting the addition of new knowledge in the field of cybersecurity and the impact of AI which contributes to the improvement of academic literature and knowledge in this area.

4.2. Practical Significance:

1. Empowering governmental and private institutions to improve cybersecurity strategies.
2. Assisting in the protection of digital infrastructure and reducing the risks associated with artificial intelligence technologies.
3. Contributing in providing practical recommendations for developing cybersecurity strategies that meet the needs of institutions in Iraq.

2. Materials and Methods

5. Theoretical Framework:

5.1. Definition of Cybersecurity:

- It's all procedures and practices related to protecting assets and systems and digital information technologies and the integrity of data and software connected to computer networks and preventing viral intrusions into cyberspace with all mobile applications and social networks as well as financial services and online shopping Al-Samhan [7].

- It's the protection of communication networks and information systems and data including internet-connected devices. Cybersecurity is concerned with preventive measures and standards that must be followed and adhered to in order to confronting threats and reduce violations or unauthorized access Al-Otaibi [8].

- It's a field concerned with protecting computer systems, networks and digital information from electronic threats and cyberattacks. And Cybersecurity aims to secure data, prevent, detect and respond to security breaches and cyberattacks which target individuals and organizations. This field also includes risk analysis, designing and implementing necessary security measures to protect data and networks and effectively handling with investigating security incidents for continuous learning and improvement. And Cybersecurity is considered a fundamental element to maintaining on the confidentiality of information and ensuring the continuity of computing operations and their associated communications Al-Masri [9].

And The researchers conclude that definition of Cybersecurity a set from processes, procedures, practices and technologies designed to protect digital systems and networks from attacks and intrusions and concludes prevention, detection and response to any potential cyber threats to ensure the continuity of computing operations.

5.2. Dimensions of Cybersecurity: The fundamental dimensions of cybersecurity have been identified and the following are their definitions Egelman and Peer [10]:

5.2.1. Device Securement: it uses of passwords to lock devices and enabling automatic locking or manually locking devices before leaving them.

5.2.2. Password Generation: it selects strong passwords and avoiding the reuse of passwords between different accounts.

5.2.3. Proactive Awareness: it's An individual's attention to indicators on websites such as URLs and other from cues in sites or emails and exercising caution when providing information to sites and being proactive in reporting security issues.

5.2.4. Updating: it degrees measure users install security updates continuously and ensure from using software in its latest version.

And there is another opinion about dimensions of cybersecurity which aims to maintaining stability and security from all cyber threats which contributing to the enhancement of the cybersecurity system. And its most important dimensions are identified as follows Mukhtar [11]:

1. Military Dimension: Aims to maintain on the ability of military units to communicate across military networks. thus, facilitating the exchange of information and commands in addition to losing of control risk on some weapons such as drones, guided missiles and satellites.
2. Economic Dimension: it uses computing devices in operate industries and its develop and drive the economy primarily in trade, finance and financial transactions which is particularly relevant to the financial sector.
3. Social Dimension: Social media websites possess are the highest levels of human interaction which provides broad opportunities for sharing ideas and

successful experiences but in the opposite of expose individual ethics and behaviors.

4. Political Dimension: it is the most important evidence of the need for cybersecurity and its importance in the political dimension.
5. Legal Dimension: require the rapid technological development compliance to legislation from through improving legal frameworks to handle with lawful and unlawful activities online, as cybercrimes are considered in generally classified cyber offenses Mukhtar [11].

And The researchers conclude that dimensions of cybersecurity: 1) Technical Dimension: The protecting networks and the systems by using software and equipments. 2) Organizational Dimension: Establishing policies and procedures related to digital security. 3) Human Dimension: Raising awareness and training personnel to minimize human errors. 4) Legal Dimension: Enacting legislation to regulate information security and deter cybercrimes.

5.3. Cyber Threats:

- Cyber threats are any unauthorized attempts to access, damage, or manipulate information systems Al-Ali.
- They include malware, viruses, and attacks targeting sensitive data Mohammed.

The researcher concludes that major cyber threats include:

1. Viruses and malware.
2. Distributed Denial of Service (DDoS) attacks.
3. Phishing attacks.
4. Social engineering.
5. Software vulnerabilities.

5.4. Cybersecurity Challenges:

- The ability to protect information and data from increasing threats Al-Jubouri.
- The technical and human-related challenges faced by organizations in securing their information systems Al-Rifai.

The researcher concludes that the primary cybersecurity challenges are:

1. Weak technological infrastructure.
2. Shortage of specialized human expertise.
3. Outdated security policies.
4. Low societal awareness.
5. Limited cybersecurity budgets.

5.5. Information Security:

- It is a set of policies and procedures aimed at protecting information from unauthorized access Al-Salem.
- It refers to the protection of stored and processed data from loss, manipulation, or unauthorized disclosure Al-Azzawi.

The researcher concludes that definition of Information Security is the protection of data from tampering or theft or unauthorized modification and it focuses on the elements of confidentiality, integrity and availability (CIA Triad).

5.6. Artificial Intelligence (AI):

- It is Computer Programming which engage in tasks that are satisfactorily performed from by humans and so because they require high-level cognitive processes such as perceptual learning, memory organization and critical thinking Mousa & Bilal [12].
- It is systems which behavior exhibit intelligent from through analyzing their environment and taking actions with a certain degree from autonomy to achieve specific goals Boucher [13].
- It is process of developing computer systems so that it's capable of performing tasks that typically requires the use of human intelligence such as human perception, speech recognition, decision-making and translation Abd El-moniem and Ismail [14].
- It is a field focuses on developing systems and software that simulate human intelligence in data analysis and decision-making and artificial intelligence is used in a wide range from the fields such as e-commerce, medicine and education, in addition to many other fields Dahmani [6].

- It is a branch of branches computer science focuses on to performing tasks similar human intelligence and used in this the field techniques and advanced tools depend on the high computational capabilities to computers and information technology to create models interact, learn and make decisions by similar to humans. And include branches of artificial intelligence The image classification, speech and machine translation as well as planning and simulation. It also considered Artificial intelligence is a core component from modern technological innovations and use on a wide range of fields such as robotics, big data analytics and the development of AI applications for various industries Al-Masri [9].

The researcher concludes that definition of Artificial Intelligence is the ability of computer systems to simulate intelligent human behavior such as learning, reasoning, problem-solving and language understanding from through use of advanced algorithms and statistical models to analyze large-scale data with the aim of predicting behavior or supporting decision-making without direct human intervention.

5.7. Types of Artificial Intelligence:

classified Artificial intelligence according to its capabilities to three different types on the following Types of Artificial Intelligence [15]:

5.7.1. Weak or Narrow of Artificial Intelligence: it's a type of artificial intelligence that be able to performing specific tasks and well-defined such as self-driving cars or even recognition programs on speech or image or chess games available on smart devices. And considered this from Artificial Intelligence is the most common types and widely available at the present time.

5.7.2. General of Artificial Intelligence: it's a type that can operate with capabilities similar to ability of human from terms of thinking and focuses on enabling machines to think and plan from autonomously and with a manner comparable to human cognition. However, there aren't any practical examples on this type; All that exists so far is merely research studies needed for a great deal from effort to develop it and turn it to reality and The Artificial Neural Network (ANN) method is considered from study ways general of AI, as they aim to create neural network systems for machines similar which Contained in it the human body.

5.7.3. Super Artificial Intelligence: this a type of surpass the level of human intelligence and it's able to make tasks with better than what can do specialized humans and knowledgeable and this many types of characteristics that encompass; such as the ability to learn, plan, communicate autonomously and make judgments. However, Super AI remains a theoretical concept and does not exist in the present era.

Other scholarly classifications include Al-Barai & Abdelrahim:

a) Based on Power and Capability:

- Weak/Narrow AI: The simplest form of AI.
- Strong/General AI: Represents the development of AI systems to function intellectually and behaviorally equal to humans.
- Super AI: Seeks to replicate and surpass the depth and breadth of human intelligence in machines.

b) Based on Technological and System Structure:

- Algorithm-based AI: Commonly used in computer science.
- Expert System-based AI: Programmed systems that mimic expert-level reasoning in specific fields.
- Machine Learning-based AI: Systems trained to perform tasks by analyzing available data with minimal human guidance.
- Neural Network-based AI: Software programs designed to simulate the human brain in processing information and learning from experience.
- Deep Learning-based AI: Utilizes algorithms modeled after human neural cells to enable self-learning capabilities.

c) Based on Functional Capabilities:

- Reactive Machines: Basic systems that respond to current inputs without storing past data (e.g., Google's AlphaGo).

- Limited Memory: Systems that store and use historical data temporarily, such as autonomous driving systems that monitor nearby cars.
- Theory of Mind: Machines that understand human emotions and interact with people e.g., the robot "Sophia."
- Self-Awareness: A future vision of AI where machines develop self-awareness and personal emotions, aiming to build intelligent systems more capable than humans.

5.8. Characteristics of Artificial Intelligence: The characteristics of Artificial Intelligence (AI) are as follows Athamnia [16]:

- The use of AI to solve presented problems in the absence of complete information.
- The ability to think and perceive.
- The ability to acquire and apply knowledge.
- The ability to learn and understand from past experiences and trials.
- The ability to use past experiences and apply them in new situations.
- The ability to use trial and error to explore different possibilities.
- The ability to respond quickly to new situations and conditions.
- The ability to deal with difficult and complex cases.
- The ability to handle ambiguous situations with a lack of information.
- The ability to differentiate the relative importance of elements in the presented cases.
- The ability to visualize, create, and understand and perceive visual matters.
- The ability to provide information to support management decisions.

In addition to the above, the characteristics of AI can be summarized in a set of applications that make it an effective investment, including Mohammed & Mohammed:

- AI applications on devices and machines enable them to analyze problems.
- AI applications on devices and machines enable them to recognize sounds, speech, and move objects.
- Some AI-enabled devices can understand inputs and analyze them to produce outputs that efficiently meet user needs.
- AI applications enable continuous learning, where the learning process is automated and self-regulated without supervision.
- The ability to process vast amounts of information.
- AI can detect similar patterns in data and analyze them more effectively than human brains.
- AI can find solutions to unfamiliar problems using its cognitive abilities.

The researcher concludes that Characteristics of Artificial Intelligence conclude as follows: 1) Self-learning Ability: Enhancing the capability improve AI systems to its performance over time without direct human intervention. 2) Adaptation with Environment: Changing AI behavior based on the Changes that appear in the surrounding environment. 3) Automated Data for Processing: analyzing large volumes of data for AI Instantly and autonomously. 4) Speed and Accuracy in Decision Making: The ability of AI on make- decisions immediately depend on precise data analysis. 5) Predictive and Pattern Recognition Ability: AI is depend on hidden the patterns in data and predicting future outcomes.

5.9. Challenges of Artificial Intelligence Applications: they're facing artificial intelligence applications the following SDAIA [17]:

5.9.1. Unclear Problem: need to clear objectives to provide useful results and this's depend on defining tasks and specifying it Clearly.

5.9.2. Data Shortage: depend on quality of datas on availability of large amounts from it and so any deficiency in data quantity or quality it will negatively affects in AI results.

5.9.3. Problem Simplicity: no need the problems on AI for relying it and it's depend on rules and clear equations and can be using traditional methods and statistical calculations to solve it.

5.9.4. Unstructured Data: requires many from data collection, organization and systematic storage and accessible retrieval to achieve the desired outcomes.

And the researcher concludes that Challenges of Artificial Intelligence Applications conclude as follows: 1) Limited local data. 2) Weak technical infrastructure. 3) Lack of programming expertise. 4) High costs of intelligent systems. 5) Resistance to organizational change.

5.10. Risks of Artificial Intelligence Applications: it represented in the following SDAIA [17]:

5.10.1. Reliability: Ensuring from to safe AI to use and free from biases intentional or unintentional and this depends on largely transparency and accountability.

5.10.2. Security: Preventing unauthorized manipulation or harmful of AI and especially with the increasing use for open-source code.

5.10.3. Responsibility: Ensuring the absence of AI from errors or legal violations and determining legal accountability in this regard which requires monitoring changes on the legislative requirements and the regulatory.

5.10.4. Control: Sharing roles of the control in task execution between humans and AI according to necessity and nature of the situation and humans' ability in control with critical scenarios.

And the researcher concludes that risks of Artificial Intelligence Applications and which conclude as follows: 1) Possibility bias in algorithms. 2) Losing the human jobs. 3) Weakness transparency in decision-making. 4) possibility of its in exploitation cyberattacks.

5.11. Cyber Attacks:

- it's Any malicious activity aimed to breaching computer systems or networks Hashem.

- it's target data theft or information destruction or service disruption Abbas.

And the researcher concludes that definition of Cyber Attacks it's refers about deliberate attempts to breach or disrupt digital systems or steal information and saving by using various methods such as viruses or Trojan horses or phishing.

5.12. Functions of Artificial Intelligence in Cybersecurity:

It's used to Artificial intelligence in enhance cybersecurity from through the applications following Haddawi et al. [5]:

5.12.1. Handling with Big Data: transferred Large volumes of data between clients and organizational infrastructure daily and appears in the verifying from all things and assessing potential risks and considered Artificial intelligence is an optimal solution for detecting this threats that arise through daily activities, due to its ability on monitor network traffic, accurately analyze server activity and automatically identify potential risks.

5.12.2. Predicting the future threats: it considered the volume of data which handled with it analysts in the predicting by the challenge future threats. However, artificial intelligence can process large amounts of data in the same time, which enables from early detection about malicious activities by identifying potential threats and supporting preventive.

5.12.3. Reducing Time of Threat Detection: threat detection rapidly is critically vital and Artificial intelligence can examine massive from datas in one time to identify cyber threats which significantly enhances security.

5.12.4. Reduction in Costing: Meaning many of organizations from financial effecting severe as a result of data breaches each year and This issue cannot be ignored or stopping about confront cybercriminals.

And the researcher concludes that Functions of Artificial Intelligence in Cybersecurity include in the following: 1) Automatic recognition on anomalous patterns. 2) Prediction with future attacks. 3) Automation response of incident. 4) Enhancement of inspection mechanisms and classification. 5) Support decision-making for security.

5.13. Challenges of Artificial Intelligence application in Cybersecurity: Artificial intelligence has many challenges when applied in cybersecurity including the following Al-Amin:

- Integrating artificial intelligence in cybersecurity systems.
- New technological industries.

- Integrating artificial intelligence in cybersecurity within organizations.
- Data-Mining tools.
- Using cybercriminals to artificial intelligence making it a double-edged sword.
- The Organizations that integrate artificial intelligence in their cybersecurity systems for data.

And the researcher concludes that Challenges of Artificial Intelligence application in Cybersecurity and represented in: 1) Lack of data due to insufficient in training of models. 2) Difficulty in interpreting to intelligent modern. 3) Security threats related to by AI algorithms and machine learning. 4) Weak coordination between technical teams and managerial to modern technologies.

6. Previous Studies:

Li addressed study to the application of artificial intelligence technologies such as deep learning on cybersecurity to build intelligent models for malwar, intrusion detection and smart threat sensing [18]. And faced AI models to a set of various from cyber threats, thereby disrupting the learning process, decision-making and taking sampling. Therefore, Preventing Adversarial Machine Learning, Saving on Machine Learning Privacy and secure federated learning. And What Require AI Models techniques specialized in the defense and the protection in cybersecurity field. And the study concluded to development AI systems are the security with focusing on the aspects of building encrypted Neural Networks and implementing secure federated deep learning.

Al-Khodari et al. aimed study to Identify the extent of availability knowledge to The Saudi universities students with Artificial Cybersecurity in preventing from cyber attacks [19]. And the study concluded to Increasing Interest in Institutional Awareness Saudi universities with information security standards application until it is possible for it face any attacks or unauthorized access it on information systems and organizing training courses for students and faculty of members staff and administrative to train them on cyberscurity appliciactons and organizing training courses for educational leaders develop reliance on artificial intelligence in educational decision-making and working on utilizing artificial intelligence in problems-solving and supporting decision-making.

Al-Zahrani and Al-Shahri aimed study to identify cybersecurity strategies in light of technologies and modern challenges and consisted the study sample from the staff of space research center and the National Center for information security technology at King Abdulaziz City for science and technology and the information security management at the communications and information technology [20]. And the results concluded to necessity of developing and qualification of Specialized human competencies in cybersecurity and which considered from the most challenges.

Zeadally et al. indicated study that cybersecurity has become fastly field for development and appeared in the news repeatedly because increasing the threats and the continuous efforts that hackers exert to overcome on law enforcement and the actions of cybercriminals with improving their methods while their primary motivations to carry out cyber attacks remained fairly stable [21]. Also the ability of traditional cybersecurity systems on detect and stop the new diminishing process gradually decreasing. And Technological advancements in encryption field and artificial intelligence and especially machine learning and deep learning, it has the ability on empower specialists in cybersecurity field from combating dynamic threats which represented the adversaries. And the study concluded to development AI approaches in cybersecurity across a set of the variety of application sectors.

Alhayani et al. aimed study to extend effectiveness artificial intelligence techniques in from cybersecurity concerns in Iraq and data were collected the data by the researchers fom employees in the information technology sector and used this study a sample of 468 participants and conducted confirmatory factor analysis, discriminant validity, baseline model analysis and hypothesis testing and except for the expert system Which did't show any relationship statistically significant between artificial intelligence and cybersecurity [22]. And the study concluded to that the values for all variables statistically significant and the main problems were sample size, accessibility, geographic region and a smaller number of variables.

Tao et al. indicated study to that artificial intelligence is helping in enterprise Cybersecurity Market Diagram for organizing in monitoring Cyberattacks, identifying, detecting it and preventing it for preserve the privacy of its data and enhancing technology and increasing intelligence tools and law enforcement and volume of the information collected from multiple from sources [23]. And the study concluded to supporting these motivating cybercriminals from through extremist non-secular collective interests and transnational information theft and competition between competitors, actions taken to achieve financial gains, damaging the reputation of others and the purpose of the most cyberattacks is profit.

Al-Dagher examined study to elite trends toward utilizing security media for artificial intelligence applications in combating cybercrime and its implications on supporting and enhancing cybersecurity in Egypt [24]. And the study concluded to hiring security media applications in combating cybercrime with different age variable and so for older who perceive the dimensions of modern applications in media content production and which see in it as risks on a security from misuse.

Khalil and Ben Mahdi addressed study importance of artificial intelligence in achieving the cybersecuritd and exposed on data and information vulnerable to compromise as well as reality AI in the context of the new digital environment and recognition on the role of AI in achieving cybersecurity at users social media sites [25]. And the study concluded to the necessity of thinking in employment AI technologies to protection the privacy of individuals and users across various digital platforms and on all fields.

Al-Adwan explored study to highlighting the roles of cybersecurity based on artificial intelligence derived from information security and related to the prevention phase and discovery phase and response Phase [26]. And the study concluded to the presence of nine key roles for the cybersecurity based on AI distributed over the three phases as follows: 1) the prevention phase: it's the automated vulnerability assessment of security and awareness and training and authentication. 2) Detection Phase: it's intrusion and security breach detection and detection of phishing emails and fraudulent phishing emails. 3) Response Phase: it's Private Framework Analysis.

Ahmed et al. addressed study to understand the concept of each of cybersecurity and digital hygiene and understanding the difference between them and identifying on the main attacks that threaten the cybersecurity process as well as the problems which facing digital hygiene [27]. And the study concluded to that the digital hygiene is apart of cybersecurity that there is a relationship between digital hygiene and cybersecurity and artificial intelligence.

Al-Damirdash aimed study to Skills development the cybersecurity depending on supported virtual elements with AI and knowledge management tools and supported virtual elements with AI a brainstorming tool on most of the research variables in particular. And the study concluded to acquiring information and knowledge with differently supported virtual elements with AI and knowledge management tools and but at varying degrees with some having the greatest impact with AI and the learning community tool.

Abdulaziz explored study about development of the cybersecurity field and artificial intelligence technologies which represents waves from use technological advancement in international political issues and the new type from the security threat which is referred to as "hybrid threats" as well as understanding on the nature the new security threats and their impact on the international relations from through two models of those threats, namely the cyber threats and artificial intelligence [28]. And the study concluded to that these models had an impact on the level of interactions and the level of concepts in the field of the international relations in terms of the development of the strongest, the securities, the war, the conflict and their tools.

Bin Barghouth aimed study to revealing the state of cybersecurity and the privacy of digital data present on databases and websites in Algeria and identifying the most important the modern technological which used for breach digital data [29]. And the

study concluded to the important role played by AI in countering cyberattacks and erasing cybercrime.

3. Dambe et al. aimed study to exploring how artificial intelligence can improve cybersecurity and internal audit practices as facing the organizations an increasing number from the advanced cyberattacks and actively seek about new ways to protect their information and their sensitive systems where it is possible to automate artificial intelligence processes, identify threats and respond to in real time and providing insights into potential weaknesses [30] [31] [32] [33] [34] [35] [37] [38] [39] [40]. And the study concluded to that AI has the ability on simplifying internal audit procedures, improve accuracy and increase visibility in the organization processes and different technical that work alongside with AI to enhance cybersecurity and internal audit practices and AI is strong tool can it enhancing the organization's security posture and ensuring compliance with regulatory requirements [41][42][43][44][45][46][47].

And the researcher concludes that from all the previous studies that there an increasing focus on the integration of artificial intelligence with Cybersecurity globally. However, its applications in the Iraqi context are still limited and most studies have indicated that the importance of enhancing awareness, resources and the infrastructure to support effective integration between cybersecurity and artificial intelligence plays an important role in Combating cyberattacks and erasing cybercrime with artificial intelligence.

4. Results and Discussion

7. Research Hypotheses:

H_1: There are statistically significant differences regarding role of cybersecurity effectiveness in Iraq for artificial intelligence technologies.

H_2: There are statistically significant differences regarding role of governmental institutions and private its effect to protect data and systems from increasing cyber threats.

H_3: There are statistically significant differences regarding the support of cybersecurity for innovation in artificial intelligence field without respecting privacy and individual rights.

H_4: There are statistically significant differences regarding artificial intelligence techniques in enhancing of the cybersecurity in Iraq and the challenges that hinder their implementation.

H_5: There are statistically significant differences regarding improvements cybersecurity systems in Iraq to facing the modern challenges.

8. Study Variables:

Represented the variables study in the following shape:

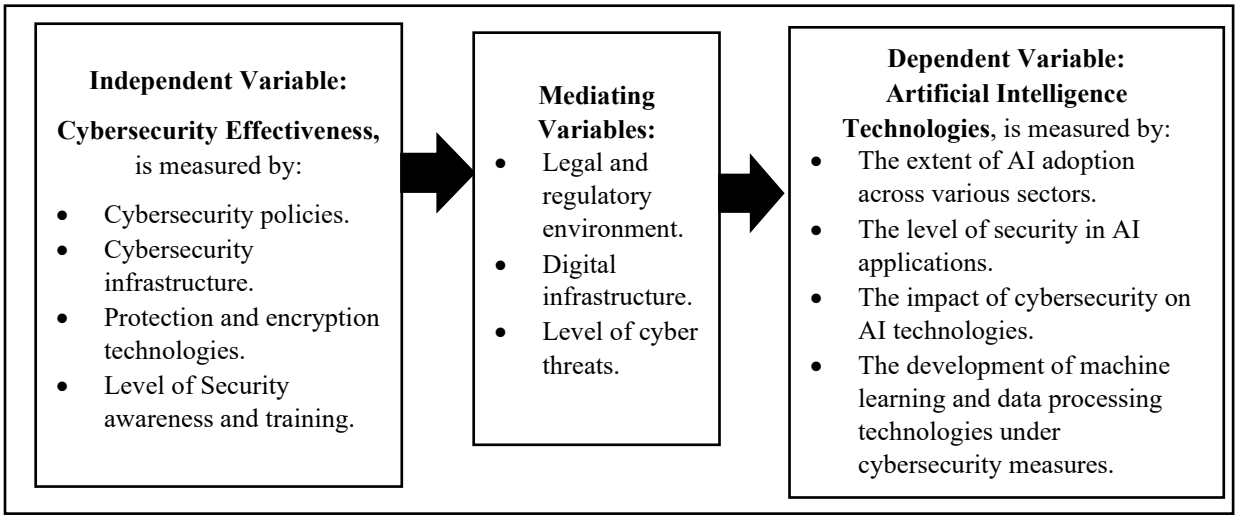

Fig. (1) Conceptual Framework of the Relationship between Cybersecurity Effectiveness and Artificial Intelligence Technologies

9. Objectives of the Exploratory Study:

The exploratory study focused on measuring the perspectives of a sample from assistant lecturers, lecturers, associate professors and professors to identify on their attitudes toward the cybersecurity and artificial intelligence and from through facing a set of questions from through questionnaire and This section aims to present methodology and description variables study as well as presenting results of the statistical analysis and hypothesis testing. And represented methodology of the exploratory study in identifying all from the study population and sample and types of data and their sources as well as identifying the appropriate statistical analysis tools for analytical purposes.

9.1. Study Population: it's representing in assistant lecturers, lecturers, associate professors and professors a total of 200 questionnaires and collected of 148 representing 74% while 52 questionnaires representing 26% could not be retrieved.

9.2. Study Sample: the researchers can define the characteristics of the study sample which depend on it in the analysis of the field study as the following:

Table (1): Total of Study Items according to demographic variables

Variable	Category	Frequency	Percentage
Gender	Male	81	54.7%
	Female	67	42.3%
Age Group	Under 25 years	41	27.8%
	25-34 years	26	17.6%
	35-44 years	11	7.4%
	45-54 years	35	23.6%
	55 years and above	35	23.6%
Academic Qualification	Bachelor's Degree	50	33.8%
	Higher Diploma	15	10.1%
	Master's Degree	43	29.1%
	Doctorate	34	23%
	Others	6	4%
Academic Title	Teaching Assistant	34	23%
	Lecturer	47	31.8%
	Assistant Professor	40	27%
	Professor	27	18.2%
Years of Experience	Less than 3 years	37	25%
	3-5 years	28	18.9%
	6-10 years	18	12.2%
	More than 10 years	65	43.9%
Workplace	Government Sector	42	28.4%
	Private Sector	29	19.6%
	Academic Institution	43	29.1%
	Others	34	22.9%
Do you have sufficient knowledge of cybersecurity?	Yes	98	66.2%
	No	50	33.8%
Does your institution implement cybersecurity policies?	Yes	91	61.5%
	No	57	38.5%
Do you believe cybersecurity is essential for adopting AI technologies in Iraq?	Yes	94	63.5%
	No	54	36.5%
	Yes	88	59.5%

Have you previously participated in training courses on cybersecurity or artificial intelligence?	No	60	40.5%
Total	----	148	100%

Source: results of SPss.

From the previous table, it concluded that the highest percentage by gender is the male category representing 54.7%. The largest age group is those under 25 years and representing 27.8%. and the most qualification is a bachelor's which representing 33.8%. the highest percentage in academic rank is lecturers that representing 31.8%. and the longest experience is in more than 10 years representing 43.9%. and the primary workplace is governmental institutions representing 28.4%. Those are sufficient knowledge of cybersecurity represent 66.2%. the institutions that work on it cybersecurity applications represent 61.5%. Respondents who believe that cybersecurity is necessary for build artificial intelligence technologies in Iraq represent 63.5%, while those who have previously participated in courses around cybersecurity or artificial intelligence represent 59.5%. All of the above indicates on relatively sample in terms of age, academic rank and workplace. There is interest with cybersecurity but practical application and training remain insufficient and represent individuals' awareness of the relationship between cybersecurity and artificial intelligence a good starting point for formulating technological development policies in Iraq.

H_1: There are statistically significant differences regarding role of cybersecurity effectiveness in Iraq for artificial intelligence technologies.

Table (2): results of the Statistical Analysis for Cybersecurity Effectiveness in Iraq and the development uses of Artificial Intelligence

No.	the role of cybersecurity effectiveness in Iraq for artificial intelligence technologies	Mean	Standard Deviation	Rank
X_1	Iraqi institutions have clear cybersecurity policies.	4.297	1.140	1
X_2	Cybersecurity systems are regularly updated to address modern threats.	4.209	1.191	4
X_3	There is sufficient awareness among institutions about cybersecurity risks.	4.162	1.283	6
X_4	Iraqi institutions provide continuous training for their employees on cybersecurity.	4.250	1.272	2
X_5	Information about cyber threats is shared among institutions in Iraq.	4.081	1.363	8
X_6	The cybersecurity infrastructure in Iraq is capable of responding to cyberattacks.	4.243	1.227	3
X_7	Iraqi laws and regulations effectively support and promote cybersecurity.	4.122	1.267	7
X_8	International cybersecurity standards are adhered to in Iraqi institutions.	4.196	1.260	5
X_9	The Iraqi government provides sufficient support to enhance cybersecurity.	4.054	1.329	9
X_{10}	There is coordination between the public and private sectors in the field of cybersecurity.	4.007	1.343	10
Total		4.162	1.268	--

Source: results of SPss.

Evident from the previous table increasing importance for all statements related with effectiveness cybersecurity in Iraq and development uses of artificial intelligence as well as with an overall mean of 4.162 and an overall standard deviation of 1.268. and this indicates an increase effectiveness cybersecurity in Iraq and advancement uses of artificial intelligence.

H_2: There are statistically significant differences regarding role of governmental institutions and private its effect to protect data and systems from increasing cyber threats.

Table (3): results of the Statistical Analysis for the impact of cybersecurity in Iraq on build of artificial intelligence technologies

No.	the role of governmental and private institutions in protecting data and systems from increasing cyber threats	Mean	Standard Deviation	Rank
X_{11}	Cybersecurity directly affects the efficiency of AI applications in Iraq.	4.703	0.742	1
X_{12}	Security challenges hinder the adoption of AI in Iraqi institutions.	4.027	1.261	8
X_{13}	Cybersecurity standards are applied when developing AI systems.	4.291	1.263	3
X_{14}	Cyberattacks pose a direct threat to AI systems in Iraq.	3.953	1.421	10
X_{15}	Cybersecurity tools are integrated with AI technologies to provide protection.	4.311	1.223	2
X_{16}	Iraqi institutions provide a secure environment for testing AI applications.	4.041	1.380	7
X_{17}	Weak cybersecurity leads to institutional hesitation in adopting AI.	4.189	1.316	4
X_{18}	There are plans to address security challenges facing AI applications.	4.020	1.348	9
X_{19}	Institutions rely on advanced security solutions to protect AI data.	4.108	1.294	5
X_{20}	Cybersecurity influences user trust in AI technologies in Iraq.	4.047	1.332	6
Total		4.169	1.258	--

Source: results of SPss.

Evident from the previous table increasing importance for all statements related with the impact of cybersecurity in Iraq on build of artificial intelligence technologies as well as with an overall mean of 4.169 and an overall standard deviation of 1.258. and this indicates an increase the impact of cybersecurity in Iraq on build of artificial intelligence technologies.

H_3: There are statistically significant differences regarding the support of cybersecurity for innovation in artificial intelligence field without respecting privacy and individual rights.

Table (4): results of the Statistical Analysis for challenges and opportunities enhancing cybersecurity to support artificial intelligence in Iraq

No.	the support provided by cybersecurity for innovation in artificial intelligence without conflicting with privacy and individual rights	Mean	Standard Deviation	Rank
X_{21}	Iraqi institutions face a shortage of qualified personnel in the field of cybersecurity.	4.541	0.985	1
X_{22}	There is a need for greater investment in cybersecurity infrastructure.	4.142	1.294	6
X_{23}	Collaboration with global companies helps to enhance cybersecurity in Iraq.	4.169	1.327	4
X_{24}	Artificial intelligence itself is being used to enhance cybersecurity and combat threats.	4.176	1.276	3
X_{25}	Institutions struggle to keep pace with evolving cyber threats.	4.135	1.338	7

X_{26}	Training and awareness programs provide effective solutions to strengthen cybersecurity.	4.081	1.368	8
X_{27}	Blockchain technologies can enhance data security related to artificial intelligence.	4.230	1.190	2
X_{28}	Adequate budgets are allocated to support cybersecurity projects in Iraq.	3.966	1.407	10
X_{29}	Government legislation impacts the development and improvement of cybersecurity in Iraq.	4.155	1.244	5
X_{30}	Partnerships between the public and private sectors can reduce security challenges and promote AI adoption.	4.027	1.424	9
Total		4.162	1.285	--

Source: results of SPss.

Evident from the previous table increasing importance for all statements related with challenges and opportunities enhancing cybersecurity to support artificial intelligence in Iraq as well as with an overall mean of 4.162 and an overall standard deviation of 1.285. and this indicates an increase challenges and opportunities enhancing cybersecurity to support artificial intelligence in Iraq.

H_4: There are statistically significant differences regarding artificial intelligence techniques in enhancing of the cybersecurity in Iraq and the challenges that hinder their implementation.

Table (5): results of the Statistical Analysis for role of cybersecurity effectiveness in Iraq for artificial intelligence technologies

Variable Code	Study Variables	Mean	Standard Deviation
X_1-X_{10}	the role of cybersecurity effectiveness in Iraq for artificial intelligence technologies	4.162	1.268
X_{11}-X_{20}	the role of governmental and private institutions in protecting data and systems from increasing cyber threats	4.169	1.258
X_{21}-X_{30}	the support provided by cybersecurity for innovation in artificial intelligence without conflicting with privacy and individual rights	4.162	1.285

Source: results of SPss.

Evident from the previous table increasing importance for all statements related with impact of cybersecurity in Iraq on build artificial intelligence technologies as well as with an overall mean of 4.169 and an overall standard deviation of 1.258. and this indicates an increase impact of cybersecurity in Iraq on build artificial intelligence technologies while balance all from cybersecurity effectiveness in Iraq and development uses artificial intelligence and challenges and opportunities for enhancing cybersecurity to support artificial intelligence in Iraq and this indicates the existence of a general positive awareness of the effectiveness and impact of cybersecurity in supporting artificial intelligence in Iraq.

H_5: There are statistically significant differences regarding improvements cybersecurity systems in Iraq to facing the modern challenges.

9.3. Reliability and Dependability Test for Variables Study: measures of given on indicate the extent which depend on the questionnaire results and then used the researcher Cronbach's Alpha test and validity coefficient as the most measures reliability on internal consistency between variables study and known in it statistically test shouldn't be about (0.6) with meaning when increase this the measure about (0.6) as a minimum the greater the possibility of the depending on the questionnaire results and explain the previous table results this test as follow:

Table (6): Results of Cronbach's Alpha and Validity Coefficient for the Study Variables

Variable Code	Study Variables	Number of Items	Cronbach's Alpha	Validity Coefficient
X_1-X_{10}	the role of cybersecurity effectiveness in Iraq for artificial intelligence technologies	10	0.936	0.936
X_{11}-X_{20}	the role of governmental and private institutions in protecting data and systems from increasing cyber threats	10	0.940	0.940
X_{21}-X_{30}	the support provided by cybersecurity for innovation in artificial intelligence without conflicting with privacy and individual rights	10	0.960	0.926
		30	0.945	0.934

Source: results of SPss.

And in highlight the previous table evident that the reliability degree ranged between a minimum value and it's 0.936 and a maximum value it's 0.960 at rate of 0.945 for all variables study and Validity Coefficient ranged between a minimum value and it's ranged between a minimum value and it's 0.926 and a maximum value it's 0.936 at rate of 0.934 for all variables study and it's good statisticals degree reflect a strong agreement on the variables study and supporting confidence in variables study and confirm its validity for analysis levels following.

9.4. Test of the Study Dimensions' Dependence on Normal Distribution: this test necessary to determine Validity degree to analyze statistic from through parametric tools and depending on Shapiro-Wilk and Kolmogorov-Smirnov to determination level of dependence of dimensions study to normal distribution and the previous table explain to test of the study dimensions' dependence on normal distribution.

Table (7): Statistical Values for Testing the Normality of Study Dimensions

Variable Code	Study Variables	Shapiro-Wilk			Kolmogorov-Smirnov		
		Test Statistic	Degrees of Freedom	Test Significance	Test Statistic	Degrees of Freedom	Test Significance
X_1-X_{10}	The role of cybersecurity effectiveness in Iraq for artificial intelligence technologies	0.778	148	0.000	0.331	148	0.000
X_{11}-X_{20}	The role of governmental and private institutions in protecting data and systems from increasing cyber threats	0.785	148	0.000	0.326	148	0.000
X_{21}-X_{30}	The support provided by cybersecurity for innovation in artificial intelligence without conflicting	0.776	148	0.000	0.322	148	0.000

	with privacy and individual rights						

Source: Results of Statistical Analysis Spss.

And evident from results of the statistical values to dependence of test the variables for the normal distribution that variables study no follow a normal distribution As it is considered the normal distribution of the variable If the significance level is the test greater than (0.05) and so will be depend on non-parametric test in the next stage from statistical analysis.

9.5. Results of the Correlation Analysis between Variables Study: addressed the researches in this part presents and analyzes the results of the simple correlation coefficient (Pearson) between the study dimensions and so to known on strength, direction and significance of the relationship between variables study the possibility of the nearest the correlation coefficient value from one this implies that strong the correlation between two variables and positive sign indicates on that direct relationship and negative sign indicates on that indirect relationship and explain the following table Correlation Matrix Between Main Dimensions for Variables Study:

Table (8): Correlation Matrix Between Main Study Dimensions

Study dimensions	**The role of cybersecurity effectiveness in iraq for artificial intelligence technologies**	**The role of governmental and private institutions in protecting data and systems from increasing cyber threats**	**The support provided by cybersecurity for innovation in artificial intelligence without conflicting with privacy and individual rights**
The role of cybersecurity effectiveness in Iraq for artificial intelligence technologies.	1	0.925	0.906
The role of governmental and private institutions in protecting data and systems from increasing cyber threats.		1	0.911
The support provided by cybersecurity for innovation in artificial intelligence without conflicting with privacy and individual rights.			1

Source: Results of Statistical Analysis Spss.

And evident from the previous table there is the existence of a significant positive correlation between Main Dimensions for Variables Study and the correlation coefficients ranged between 0.906 and 0.925 and all statistically significant at the 0.05 level and no follow a normal distribution If the significance level is the test greater than (0.05) and the distribution is considered moderate, Otherwise it is considered reached The correlation coefficient value between the effectiveness of cybersecurity in Iraq and development uses the AI and other dimensions 0.925 and 0.906 respectively. Similarly, the correlation

coefficient value between the impact of cybersecurity in Iraq on build AI technologies and respectively reached 0.911. and another side the correlation relationship confirms on validity of the items in measuring the main dimensionsto study and it's really connected and not due to chance.

Results and Recommendations:

Results:

1. Analysis the now Situation: Weaknesses in the law framework and cybersecurity policies in Iraq, the need to update cybersecurity infrastructure and employment specialized personnel.
2. The main challenges which facing the cybersecurity in Iraq and the existing gaps in the new cybersecurity systems.
3. Effectiveness the new initiatives in protecting data from the cybersecurity threats and their successfully in enhancing the trust in AI applications.
4. Analyzing the data and collecting the results of related with artificial intelligence application in cybersecurity and reviewing examples successfully to other countries can be that implementing them the Iraq.

Recommendations:

1. Developing law framework and comprehensive regulatory for cybersecurity, increasing investment in technologies the detecting about cybersecurity threats.
2. Enhancing training programs and building the ability for employees in the cybersecurity field, awareness the society with the importance of cybersecurity in remained digital transformation.
3. Developing strategies of comprehensive cybersecurity included artificial intelligence technologies completely conducting workshops and training for government agencies and companies around the cybersecurity risks and data protection.
4. Encouraging the research and the development in cybersecurity field and artificial intelligence technologies to development innovative solutions, enhancing investment in AI technologies.
5. Building a local abilities in cybersecurity field and the collaborating with international institutions to enhance digital infrastructure.

5. Conclusion

This study finds that cybersecurity effectiveness is among the most important enabling factors for the successful and sustainable adoption of AI technologies in Iraq. The results show a deep and statistically significant connection between cybersecurity policies, infrastructure, awareness, institutional readiness as independent variables and the efficiency, trustiness, and scalability of artificial intelligence applications as depend variables. The study goes on to uncover that though Japanese governmental and private organizations are increasingly aware of the need for cyber resilience, weaknesses remain in digital infrastructure, there are acute human skill shortages, financial allocations are low, the regulatory framework is archaic, and cyberattacks are becoming more sophisticated. Additionally, the study emphasizes that AI technologies themselves are a double-edged sword; they both have the potential to improve cybersecurity capacity—such as threat detection, prediction and automated response—but can also introduce new security threats if they are insufficiently secured. Such findings indicate that for Iraq to ensure a successful digital transformation and innovate, an integrated national strategy that includes cybersecurity governance, legal development, human capacity development, and technological investments is a must. This calls for strengthened collaboration between public and private sectors, expanding training programs, national legislation being aligned to international cybersecurity standards, and the deployment of AI in a safe environment. Longitudinal and sector-specific empirical studies, evaluations of the real-world effectiveness of AI-driven cybersecurity tool mechanisms, and investigations of ethical, legal, and privacy implications associated with the deployment of advanced artificial intelligence systems are crucial for evidence-based policymaking

and sustainable digital development in Iraq; therefore, future research should carry out such studies.

REFERENCES

[1] R. Abeyratne, "Aviation and cybersecurity in the digital world," in Aviation in the Digital Age: Legal and Regulatory Aspects, 2020, pp. 173–211.
[2] M. A. Abdel Rahim, "Artificial intelligence and its impact on liability in Islamic jurisprudence: A comparative jurisprudential study," Journal of Legal Studies, no. 55, pt. I, p. 8, Mar. 2022.
[3] A. Bhardwaj, M. D. Alshehri, K. Kaushik, H. J. Alyamani, and M. Kumar, "Secure framework against cyber attacks on cyber-physical robotic systems (Retracted)," Journal of Electronic Imaging, vol. 31, no. 6, pp. 061802-1–061802-?, 2022.
[4] P. Chithaluru, F. Al-Turjman, M. Kumar, and T. Stephan, "Computational-intelligence-inspired adaptive opportunistic clustering approach for industrial IoT networks," IEEE Internet of Things Journal, vol. 10, no. 9, pp. 7884–7892, 2023.
[5] A. H. Hadawi, D. A. Muslim, and S. T. Mohammed, "Digital leadership and its role in enhancing cybersecurity behavior in organizations: An analytical study of a sample of employees in private banks in Najaf Al-Ashraf," Journal of Human and Natural Sciences, vol. 5, no. 1, 2023.
[6] M. Dahmani, "Artificial intelligence as a mechanism to enhance cybersecurity," Journal of Legal and Political Thought, vol. 7, no. 2, pp. 597–608, 2023.
[7] M. A. Al-Samhan, "Requirements for achieving cybersecurity for management information systems at King Saud University," Journal of the Faculty of Education, Mansoura University, no. 111, pp. 3–29, 2020.
[8] A. B. S. Al-Otaibi, "The role of cybersecurity in achieving Vision 2030," M.S. thesis, Naif Arab University for Security Sciences, 2020.
[9] F. M. Al-Masri, "The role of artificial intelligence in improving cybersecurity," Elite Journal for Studies and Research, vol. 3, no. 2, 2024.
[10] S. Egelman and E. Peer, "Scaling the security wall: Developing a security behavior intentions scale (SeBIS)," in Proc. 33rd Annu. ACM Conf. Human Factors in Computing Systems (CHI), Apr. 2015, p. 2979.
[11] M. Mukhtar, "Cybersecurity: Concepts of the future," Journal of Trends of Events, no. 2, pp. 6–7, 2023.
[12] A. Moussa and A. H. Bilal, Artificial Intelligence: A Revolution in Modern Technology. Cairo, Egypt: Arab Group for Training and Publishing, 2019.
[13] P. Boucher, Artificial Intelligence: How Does It Work, Why Does It Matter, and What Can We Do About It? (STOA). Brussels, Belgium: European Parliamentary Research Service, Jun. 2020.
[14] H. Abdel Moneim and M. Ismail, Economic Implications of the Fourth Industrial Revolution (Artificial Intelligence), Arab Monetary Fund, Economic Studies Series, 2021, p. 7.
[15] "Types of Artificial Intelligence," Javatpoint. [Online]. Available: https://www.javatpoint.com. Accessed: Oct. 7, 2019.
[16] A. Athamnia, Fundamental Concepts of Artificial Intelligence. Berlin, Germany: Arab Democratic Center for Strategic, Political, and Economic Studies, 2019.
[17] Saudi Data and AI Authority (SDAIA), AI for Executives. Riyadh, Saudi Arabia, 2022.
[18] J. H. Li, "Cyber security meets artificial intelligence: A survey," Frontiers of Information Technology & Electronic Engineering, vol. 19, no. 12, pp. 1462–1474, 2018.
[19] J. S. Al-Khudari, H. J. Salami, and N. N. M. Kleibi, "Cybersecurity and artificial intelligence in Saudi universities: A comparative study," Journal for University Performance Development, Mansoura University, vol. 12, no. 1, pp. 217–233, 2020.
[20] A. bin Y. Al-Zahrani and H. bin A. Al-Shahri, "Cybersecurity strategies in light of modern technologies and challenges: A comparative study," M.S. thesis, Naif Arab University for Security Sciences, 2020.
[21] S. Zeadally, E. Adi, Z. Baig, and I. A. Khan, "Harnessing artificial intelligence capabilities to improve cybersecurity," IEEE Access, vol. 8, pp. 23817–23837, 2020.
[22] B. Alhayani, H. J. Mohammed, I. Z. Chaloob, and J. S. Ahmed, "Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry," Materials Today: Proceedings, 2021, doi: 10.1016/… (incomplete in source).
[23] F. Tao, M. S. Akhtar, and J. Z. (Jiayuan), "The future of artificial intelligence in cybersecurity: A comprehensive survey," EAI Endorsed Transactions on Creative Technologies, vol. 8, no. 28, pp. 3–e3, 2021.

[24] M. M. A. J. El-Dagher, "Elite attitudes toward using security media and AI applications to combat cybercrime and enhance cybersecurity in Egypt: A field study," Arab Journal for Media and Communication Research, Ahram Canadian University, no. 33, pp. 4–110, 2021.
[25] K. bin M. M. Saidi, "Artificial intelligence as a necessary trend in cybersecurity protection: Present reality and future challenges," Peace Journal for Humanities and Social Sciences, vol. 6, no. 4, pp. 25–37, 2022.
[26] J. A. A. Karim Al-Adwan, "Roles and challenges of AI-based cybersecurity: A case study," Jordanian Journal of Business Administration, Univ. of Jordan, vol. 18, no. 3, pp. 437–456, 2022.
[27] F. A. I. Ahmed, R. F. A. Youssef, and W. M. El-Sayed, "Cybersecurity and digital hygiene," Egyptian Journal of Information Sciences, vol. 9, no. 2, pp. 3900–422, 2022.
[28] S. M. R. Abdel Aziz, "Hybrid security threats in international relations: Cybersecurity and artificial intelligence as models," Nile Valley Journal for Humanities and Educational Studies, Cairo Univ.–Khartoum Branch, vol. 33, no. 334, pp. 663–700, 2022.
[29] L. Ben Barghouth, "Cybersecurity and digital data privacy protection in Algeria in the age of digital transformation and AI: Threats, technologies, challenges, and countermeasures," International Journal of Social Communication, vol. 10, no. 1, pp. 443–457, 2023.
[30] S. Dambe, S. Gochhait, and S. Ray, "The role of artificial intelligence in enhancing cybersecurity and internal audit," in Proc. 3rd Int. Conf. Advancement in Electronics & Communication Engineering (AECE), Nov. 2023, pp. 88–93.
[31] M. M. Abdel Razek, "AI technologies in media: Current reality and future developments—An applied study on Egyptian and Arab media practitioners," Egyptian Journal of Media Research, no. 81, pp. 1–74, 2022.
[32] D. M. Al-Ameen and B. Jamal Al-Din, "Implications of artificial intelligence on national security," Journal of Private Law, vol. 2, no. 1, pp. 100–122, 2024.
[33] M. J. G. Al-Fatlawi and H. A. M. J. Al-Asam, "The contributions of AI technologies to strategic leadership: A descriptive analytical study at Najaf International Airport," Al-Ghari Journal of Economic and Administrative Sciences, vol. 18, no. 1, pp. 157–179, 2022.
[34] A. Buchmann and G. C. Bowker, "Unsupervised by any other name: Hidden layers of knowledge production in artificial intelligence on social media," Big Data & Society, pp. 1–11, Jan.–Jun. 2019. [Online]. Available: https://journals.sagepub.com/doi/full/10.1177/2053951718819569
[35] A. El-Sayed Mohamed and K. Mahmoud Mohamed, AI Applications and the Future of Educational Technology. Cairo, Egypt: Arab Group for Training and Publishing, 2020.
[36] A. S. A. El-Borai, "Applications of AI and robotics from the perspective of Islamic jurisprudence," Dar Al-Iftaa Journal, vol. 14, no. 48, Jan. 2022. [Online]. Available: https://dftaa.journals.ekb.eg/article_231631.html
[37] N. S. El-Demerdash, "The impact of AI-supported virtual elements and knowledge management tools on developing cybersecurity skills among computer and AI students," Journal of Research in the Fields of Qualitative Education, Minia University, no. 41, pp. 1331–1427, 2022.
[38] A. H. Hadawi, D. M. Ali, and S. T. Mohammed, "Digital leadership and cybersecurity behavior in organizations," Journal of Human and Natural Sciences, vol. 5, no. 1, 2024.
[39] Iraqi Ministry of Communications, Reports on Cybersecurity and Digital Transformation.
[40] International Telecommunication Union (ITU) and other international cybersecurity organizations/agencies, relevant reports and publications.
[41] K. Gammon, "5 ways artificial intelligence will change the world by 2050," USC News, 2019; and "Types of Artificial Intelligence," Javatpoint. [Online]. Available: https://www.javatpoint.com
[42] L. Jin, "Investigation on potential application of artificial intelligence in preschool children's education," Journal of Physics: Conference Series, vol. 1288, no. 1, p. 2, 2019.
[43] P. Grover, A. K. Kar, and Y. K. Dwivedi, "Understanding artificial intelligence adoption in operations management: Insights from the review of academic literature and social media discussions," Annals of Operations Research, Jun. 16, 2020. [Online]. Available: https://link.springer.com/article/10.1007/s10479-020-03683-90
[44] Research and Information Center, "Artificial intelligence in Saudi Arabia," 2021. [Online]. Available: https://www.abhacci.org.sa/
[45] D. F. Salem, "Effectiveness of AI technologies on social media from the perspective of educational media students: Facebook as a model," Egyptian Journal for Public Opinion Research, vol. 1, no. 3, pp. 1–61, 2021.
[46] D. Shi, P. Wang, and K. Abbas, "A survey of deep learning and its applications: A new paradigm to machine learning," Archives of Computational Methods in Engineering, p. 1, 2021. [Online]. Available: https://doi.org/10.1016/j.cosrev.2021.10037

[47] V. Nunavath and M. Goodwin, “The role of artificial intelligence in social media big data analytics for disaster management—Initial results of a systematic literature review,” in Proc. 5th Int. Conf. Information and Communication Technologies for Disaster Management (ICT-DM), 2018.