Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 11, November, 2026
Website: usajournals.org
This work is Licensed under CC BY 4.0 a Creative Commons Attribution 4.0 International License.

THE IMPACT OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES ON ENHANCING CYBERSECURITY: A CASE STUDY OF TELECOMMUNICATIONS COMPANY EMPLOYEES IN MAYSAN GOVERNORATE, IRAQ

Mortdha Abd Ulkadhm Oraibi
College of Administration and Economics,
University of Misan, Amarah, Iraq
Murtazaabd.k@uomisan.edu.iq

Abstract
The research aims to determine the impact of artificial intelligence technologies on enhancing cybersecurity, by applying it to employees of telecommunications companies in Maysan Governorate, Iraq. The researcher relied on a stratified random sample of (125) employees to conduct the analysis. The research was based on the descriptive analytical method, and the results showed the existence of strong significant correlations between artificial intelligence technologies and the dimensions of cybersecurity. The results also showed the existence of a significant impact of artificial intelligence technologies on all dimensions of cybersecurity.

Keywords: Artificial intelligence technologies – Cybersecurity.

Introduction:

Artificial intelligence has become a primary driver of the recent technological revolution in the new millennium, exerting a clear influence on all aspects of life and business. This has led to the integration of artificial intelligence tools and technologies manifested through thousands of applications and algorithms aimed at making life easier, more efficient, and more effective (Moustafa, 2022).
Artificial intelligence technologies such as machine learning, the Internet of Things (IoT), automation, and natural language processing have achieved

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 11, November, 2026
Website: usajournals.org
This work is Licensed under CC BY 4.0 a Creative Commons Attribution 4.0 International License.

tremendous technological progress, impacting nearly every sector and society as a whole (Iansiti & Lakhani, 2020).

Cybersecurity is a global priority, relevant to nations, government organizations, and private enterprises alike. It encompasses a complex array of organizational, technical, and procedural tools, as well as practices designed to protect computers, networks, and the data they contain from breaches, damage, unauthorized alteration, or the disruption of access to information and services (Canelón et al., 2020).

Furthermore, cybersecurity serves as a cornerstone for protecting sensitive information and the digital landscape. It focuses on preventing sophisticated cyberattacks, defending and strengthening security systems, developing advanced defensive strategies, and enhancing training and awareness at both the individual and organizational levels (Kumar et al., 2021).

Artificial intelligence (AI) has emerged as a critical tool in the realm of cybersecurity, offering advanced solutions to address the growing challenges posed by digital threats ranging from detection and prevention to effective response. Traditional, rule-based systems often prove limited in their ability to adapt to modern, constantly evolving attacks (Rjoub et al., 2023).

In light of this, the current research aims to examine the impact of AI technologies on enhancing cybersecurity, with a focus on employees within telecommunications companies in the Maysan Governorate, Iraq. Telecommunications firms are among the most prominent organizations increasingly adopting AI technologies; given their reliance on the exchange of vast amounts of data across digital networks, strengthening cybersecurity is essential to protecting their data and systems from cyber threats.

First: Theoretical Framework: The researcher examines the study variables AI technologies and cybersecurity as follows:

1- The Concept of AI Technologies:

Nikesh Muthukrishnan (2020) defines AI technologies as the capacity of computer systems to accurately interpret data, learn from it, and apply it to achieve specific goals and tasks. This involves the development of algorithms that

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 11, November, 2026
Website: usajournals.org
This work is Licensed under CC BY 4.0 a Creative Commons Attribution 4.0 International License.

enable AI to solve problems and perform human-like tasks with speed and precision.

Torkzadehmahani et al., (2022) defined it as the science and engineering of creating intelligent machines using algorithms or rules that enable these machines to emulate human cognitive functions, such as learning and problem-solving.

Babina et al., (2024) defined it as the development of computer systems capable of performing tasks that typically require human intelligence. Such tasks include learning, reasoning, problem-solving, understanding natural language, perceiving the environment, and interacting with it. Artificial intelligence systems are designed to simulate cognitive functions for instance, learning from data, adapting to new information, and making decisions based on that information.

Meanwhile, Gonzalez & Hernández (2025) defined it as a collection of algorithms and systems that emulate human capabilities such as learning, reasoning, and decision-making based on data analysis. It also contributes to enhancing the performance of systems that rely on prediction and advanced analysis.

2- Artificial Intelligence Technologies:

A number of previous studies addressing artificial intelligence (AI) technologies including those by Dejoux & Léon (2018), de-Lima-Santos & Ceron (2021), Collins et al., (2021), and Sarker (2022) have identified machine learning, expert systems, robotics, natural language processing, and machine vision as the core dimensions of AI. The researcher has adopted these dimensions due to their suitability for the scope of this study, as they offer capabilities that enhance cybersecurity. These include analyzing data, identifying patterns and security threats, predicting potential attacks, detecting anomalous activities, and responding to cyber risks all of which contribute to the protection of information and digital systems. These dimensions are explained as follows:

2/1 Machine Learning:

This refers to a set of methods typically used to solve various real-world problems through computer systems capable of learning how to address a given issue, rather than relying on explicit, pre-programmed instructions (Kühl et al., 2022).

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 11, November, 2026
Website: usajournals.org
This work is Licensed under CC BY 4.0 a Creative Commons Attribution 4.0 International License.

2/2 Expert Systems:

These are knowledge-based systems that rely on specific representations of knowledge. An expert system consists of two subsystems: an inference engine and a knowledge base (Sarker, 2022).

2/3 Robotics:

This refers to an artificial device capable of sensing its environment and interacting with or influencing it in a purposeful manner (Mamak et al., 2025).

2/4 Natural Language Processing:

This is a technology that enables machines to interpret human language. NLP tasks include speech recognition (converting speech into text), word segmentation, lemmatization (reducing words to their root/base form), and natural language generation the process of converting structured data into human language (Sarker, 2022).

2/5 Machine Vision:

This is a branch of artificial intelligence that enables computers and systems to extract useful information from digital images, videos, and other visual inputs, and subsequently take actions or provide recommendations based on that data (Sarker, 2022).

3- The Concept of Cybersecurity:

Galinec & Luić (2020) define cybersecurity as the protection of electronic systems and data against unauthorized access or intrusion, while maintaining the confidentiality and integrity of information. This encompasses securing wired and wireless networks, computers, and smart devices. It also aims to mitigate malicious breaches and risks associated with digital technology, ensuring the continuity of electronic operations without interruption or failure.

Ramirez et al., (2022) define it as a set of actions taken to defend against cyberattacks and their consequences, including the implementation of necessary countermeasures.

Yaacoub et al., (2022) view it as the assessment of digital security for individuals and organizations, the implementation of security policies and procedures, and

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 11, November, 2026
Website: usajournals.org
This work is Licensed under CC BY 4.0 a Creative Commons Attribution 4.0 International License.

effective international cooperation to combat cybercrime including the exchange of information essential for strengthening cybersecurity in the face of continuous technological evolution and innovation.

Meanwhile, Smaili et al., (2023) define it as the secure protection of computer networks and the information they contain against intrusion, damage, or malicious disruption. In this view, cybersecurity encompasses technical solutions, events, strategies, processes, methods, human involvement, and the overarching security framework all of which constitute the core elements of the field.

4- Dimensions of Cybersecurity:

A review of existing literature reveals a relative consensus among researchers regarding the dimensions of cybersecurity. Studies by Li & Liu (2021) and Chang et al., (2023) identify the core dimensions as confidentiality, integrity, and availability. Conversely, other studies such as those by Arpaci & Sevinc (2021) and Takacs & Pogatsnik (2024) adopt a more comprehensive and expansive perspective, incorporating additional dimensions: authenticity, possession/control, and utility. Given this relative alignment in the literature, the researcher has adopted these six dimensions, as they are well-suited to the nature of the field under study. These dimensions are defined as follows:

4/1 Confidentiality:

Confidentiality refers to the principle that only authorized and permitted parties can access sensitive information and functions (Li & Liu, 2021).

4/2 Integrity:

Integrity relates to the accuracy and authenticity of data, ensuring it has not been altered or distorted for malicious purposes. It entails maintaining consistency, precision, and credibility within the cyberspace environment (Arpaci & Sevinc, 2021).

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 11, November, 2026
Website: usajournals.org
This work is Licensed under CC BY 4.0 a Creative Commons Attribution 4.0 International License.

4/3 Availability:
Availability is defined as ensuring that users authorized to access the cyberspace environment are able to do so whenever necessary, and can retrieve the required data and information (Arpaci & Sevinc, 2021).

4/4 Authenticity:
Authenticity refers to the fact that information is correct and genuine, that the information sources are trusted by the user, that they possess a verifiable identity, and that the same requirements apply to other entities as well (Bitzer et al., 2021).

4/5 Possession and Control:
Possession and control refer to the state or quality of owning confidential information (Arpaci & Sevinc, 2021).

4/6 Utility:
Utility refers to usability, relating to the usefulness of information and internet services (Takacs & Pogatsnik, 2024).

Second: Previous Studies:
1- Previous studies addressing artificial intelligence (AI) technologies:
A study by Nazir et al., (2023) aimed to understand how AI technologies influence consumer engagement on social media and conversion rates, with the goal of enhancing consumer satisfaction and repurchase intentions within the hospitality sector. Data were collected from 308 hotel guests across various regions of the Sultanate of Oman who had booked a hotel stay online. The findings revealed that AI technologies have a positive impact on consumer engagement on social media and help improve conversion rates. Furthermore, both consumer engagement on social media and conversion rates contribute to a satisfying consumer experience, which, in turn, increases consumers' intentions to repurchase. Finally, the study found that "consumer habits" play a positive moderating role in the relationship between a satisfying consumer experience and the intention to repurchase.
The study by Nepal et al., (2025) aimed to empirically assess the impact of advancements in artificial intelligence (AI) technologies on energy resilience in

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 11, November, 2026
Website: usajournals.org
This work is Licensed under CC BY 4.0 a Creative Commons Attribution 4.0 International License.

China. It further investigated regional disparities and the underlying mechanisms of this influence. The analysis was based on a balanced panel dataset covering 30 Chinese provinces from 2006 to 2019. The results indicate that innovation in AI technologies can effectively enhance energy resilience—a finding supported by various robustness and validity tests. However, the magnitude of this impact varies by region, peaking in the central region, followed by the eastern and western regions. Furthermore, innovation in AI technologies contributes to the development of green finance, which, in turn, indirectly bolsters energy resilience.

The study by Song et al., (2026) sought to explore the potential synergies arising from the integration of artificial intelligence (AI) technologies and visual communication design (VCD) within the context of e-commerce in the "metaverse." Methodologically, the study employed a literature review to examine existing research on AI applications in environmental design, alongside an analysis of case studies illustrating how visual communication design addresses the requirements of environmental design. By focusing on selected Landscape Environment Design (LED) projects specifically the West Lake Wetland Park in Hangzhou, Zhejiang Province economic data (such as visitor numbers and revenue) were collected both before and after the integration of artificial intelligence (AI) and visual communication design elements. An analysis of this case study revealed a 20% increase in visitor numbers within one year of implementing these AI and visual communication design features, alongside a 30% rise in commercial revenue, driven by enhanced visitor experiences. Furthermore, the integration of AI and visual communication into landscape design not only promotes sustainable development and energy efficiency but also contributes to the growth of the regional Gross Domestic Product (GDP).

2- Previous studies addressing cybersecurity:

A study by Saeed et al., (2023) examined the impact of digital transformation and cybersecurity on achieving business resilience. It highlights the importance of having a comprehensive understanding of cybersecurity risks during the implementation of digital transformation to prevent disruptions caused by

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 11, November, 2026
Website: usajournals.org
This work is Licensed under CC BY 4.0 a Creative Commons Attribution 4.0 International License.

malicious activities or unauthorized access such as attempts by attackers to alter or destroy sensitive information, or to extort users. Through a systematic literature review conducted using the PRISMA methodology, the study concluded that while digital transformation enhances efficiency and productivity, it also introduces new challenges related to cybersecurity risks, including data breaches and cyberattacks.

A study by Maraveas et al., (2024) examined cybersecurity threats within the context of Agriculture 4.0 and Agriculture 5.0, while also exploring potential mitigation strategies. The study employed a secondary research methodology specifically a narrative review through which a wide range of literature on cybersecurity was selected and analyzed. The findings indicate that key factors exacerbating cybersecurity risks for agricultural enterprises include inadequate cybersecurity practices, a lack of governing regulations and policies, and the use of outdated IT software. The study further identified "Denial of Service" (DoS) attacks targeting servers as a primary threat in the Agriculture 4.0 and 5.0 sectors; such attacks disrupt the operation of smart technologies, including equipment used for livestock tracking, climate monitoring, logistics, storage, and crop surveillance. Additionally, the study highlighted the occurrence of malware attacks, in which attackers modify system application code to gain access to sensitive farm data a process that could lead to the alteration of operations within digitized systems.

Meanwhile, a study by Hossain et al., (2025) aimed to clarify the critical cybersecurity challenges faced by local governments within a structured framework, utilizing a systematic literature review methodology based on the PRISMA protocol. The results reveal that the risks associated with cybersecurity in local governments are significant, with primary challenges including limited financial resources, technological vulnerabilities, human factors, and [existing] frameworks. Organizational.

3- Previous studies addressing artificial intelligence (AI) technologies and cybersecurity:

A study by Kaur et al., (2023) provides a systematic literature review and a detailed analysis of AI use cases in the field of cybersecurity. The review

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 11, November, 2026
Website: usajournals.org
This work is Licensed under CC BY 4.0 a Creative Commons Attribution 4.0 International License.

identified 2,395 studies, from which 236 were selected as primary sources. Using a thematic analysis approach, the identified AI use cases were classified based on the Cybersecurity Framework developed by the National Institute of Standards and Technology (NIST). This classification offers readers a comprehensive overview of the potential for AI to enhance cybersecurity across various contexts. Furthermore, the review outlines future research opportunities in emerging cybersecurity-related areas, advanced AI methodologies, data representation mechanisms, and the development of new infrastructures all of which are essential for the successful adoption of AI-driven cybersecurity solutions in an era defined by digital transformation and multifaceted crises.

Commentary on previous studies:

1- There is a consensus among researchers regarding artificial intelligence technologies; the researcher has adopted the following dimensions: machine learning, expert systems, robotics, natural language processing, and machine vision.

2- A review of the existing literature reveals a relative consensus among researchers concerning the dimensions of cybersecurity; the researcher has adopted the following dimensions: confidentiality, integrity, availability, authenticity, possession and control, and utility.

3- To the best of the researcher's knowledge, there is a scarcity of studies addressing the relationship between artificial intelligence technologies and cybersecurity—a clear research gap that the present study seeks to bridge.

Third: Research Problem:

The research problem lies in the increasing number of cyber threats and attacks facing telecommunications companies. This raises questions regarding the extent to which artificial intelligence (AI) technologies can contribute to enhancing cybersecurity and protecting data and networks. Consequently, an applied study is required to analyze this relationship, focusing on employees of telecommunications companies in the Maysan Governorate, Iraq. Therefore, this research seeks to answer the following questions:

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 11, November, 2026
Website: usajournals.org
This work is Licensed under CC BY 4.0 a Creative Commons Attribution 4.0 International License.

1- What is the nature of the relationship between artificial intelligence technologies and cybersecurity?
2- To what extent do artificial intelligence technologies influence the dimensions of cybersecurity?

Fourth: Research Objectives:
1- To determine the nature of the relationship between artificial intelligence technologies and cybersecurity.
2- To determine the extent to which artificial intelligence technologies influence the dimensions of cybersecurity.

Fifth: Research Hypotheses:
H1: There is a significant correlation between artificial intelligence technologies and cybersecurity.
H2: Artificial intelligence technologies have a significant impact on the dimensions of cybersecurity.

From this hypothesis, the following sub-hypotheses are derived:
H2/1 Artificial intelligence technologies have a significant impact on confidentiality.
H2/2 Artificial intelligence technologies have a significant impact on integrity.
H2/3 Artificial intelligence technologies have a significant impact on availability.
H2/4 Artificial intelligence technologies have a significant impact on authenticity.
H2/5 Artificial intelligence technologies have a significant impact on possession and control.
H2/6 Artificial intelligence technologies have a significant impact on utility.

Sixth: Significance of the Research:
1- Scientific Significance:
The scientific significance of this research lies in its contribution to enriching both Arabic and foreign literature concerning artificial intelligence technologies and cybersecurity. It clarifies the nature of the relationship between these two fields

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 11, November, 2026
Website: usajournals.org
This work is Licensed under CC BY 4.0 a Creative Commons Attribution 4.0 International License.

particularly within the telecommunications sector thereby supporting future studies and research in this domain.

2- Practical Significance:

The practical significance of this research lies in providing actionable findings for telecommunications companies in the Maysan Governorate, Iraq. It offers insights into how these companies can leverage artificial intelligence technologies to enhance cybersecurity, detect and counter cyber threats, and protect data and networks ultimately supporting service continuity and elevating the level of information security.

Seventh: Research Methodology:

1- Research Population and Sample:

The research population consists of technical staff and specialists in technological fields working for telecommunications companies in the Maysan Governorate, Iraq, totaling 125 individuals. Their professional roles encompassing computer engineering, telecommunications networks, information technology, systems administration, information security, and cybersecurity are directly related to the research topic and its variables. The job categories included in the research population are outlined in the following table:

Table No. (1) Job categories included in the research population

Computer Engineers	25
Network Engineers	35
Information Technology Staff	30
System Administrators	20
Information Security and Cybersecurity Administrators	15
Total	**125**

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 11, November, 2026
Website: usajournals.org
This work is Licensed under CC BY 4.0 a Creative Commons Attribution 4.0 International License.

2- Research variables and methods for measuring them:

Table No. (2) Research variables and methods for measuring them

Variables	Dimensions	Metrics
Artificial Intelligence Technologies	Machine learning	Collins et al., (2021)
	Expert Systems	
	Robotics	
	Natural Language Processing	
	Machine Vision	
Cybersecurity	Confidentiality	Arpaci & Sevinc (2021)
	Integrity	
	Availability	
	Authenticity	
	Possession and Control	
	Utility	

Source: Prepared by the researcher based on previous studies.

3- Data Collection Tools:

These consist of a questionnaire designed and developed in light of previous studies. It was administered to employees of telecommunications companies in Maysan Governorate, Iraq, and contains a set of statements used to measure the research variables.

4- Statistical Analysis Methods:

1- Descriptive Analysis Methods: Including the arithmetic mean and standard deviation, used to characterize the study variables.

2- Cronbach's Alpha Coefficient: Used to test the reliability of multi-item scales in the current study by assessing the internal consistency of the scale's variables.

3- Pearson Correlation Analysis: Used to measure the strength and direction of the relationship between the study's variables and dimensions.

4- Multiple Regression Analysis: Used to calculate the regression coefficients for the independent variables in relation to the dependent variable.

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 11, November, 2026
Website: usajournals.org
This work is Licensed under CC BY 4.0 a Creative Commons Attribution 4.0 International License.

5- T-test: Used to compare the means of two groups.

6- One-Way ANOVA (Analysis of Variance): Used to compare the means of more than two groups.

Eighth: Field Study:

1- Reliability and Validity Test:

The researcher conducted reliability and validity tests on the survey instrument to examine the extent to which the results of the field study could be relied upon in generalizing the findings. The reliability coefficient was measured using Cronbach's Alpha coefficient for the components of the survey instrument to verify the consistency and reliability of the responses. The validity of the scale was also tested through face validity, which is represented by the square root of the reliability coefficient. Table No. (3) shows the results of the reliability and validity tests for the two research variables.

Table No. (3) Stability and reliability coefficient

No	Research variables	Number of phrases	Cronbach's alpha	Self-honesty coefficient
	Artificial intelligence technologies			
1-	Machine learning	5	.852	.923
2-	Expert Systems	5	.878	.937
3-	Robotics	5	.854	.924
4-	Natural Language Processing	6	.880	.938
5-	Machine Vision	7	.932	.965
	Cybersecurity			
6-	Confidentiality	5	.822	.907
7-	Integrity	5	.807	.898
8-	Availability	5	.861	.928
9-	Authenticity	5	.858	.926
10	Possession and Control	5	.904	.951
11	Utility	5	.885	.941

Source: Statistical analysis results.

Table (3) shows that the Cronbach's alpha coefficient values for artificial intelligence and cybersecurity technologies ranged between (0.807–0.932), indicating that the study instrument enjoys a high degree of reliability and internal

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 11, November, 2026
Website: usajournals.org
This work is Licensed under CC BY 4.0 a Creative Commons Attribution 4.0 International License.

consistency. The self-validity coefficient values also ranged between (0.898–0.965), which reflects the high degree of validity of the instrument and its suitability for application.

2- Descriptive analysis of study variables:

Table No. (4) Arithmetic mean and standard deviation of the study variables and dimensions

variable	Dimension	Arithmetic mean	Standard deviation
Artificial intelligence technologies	Machine learning	4.0677	.73588
	Expert Systems	3.9762	.78874
	Robotics	4.1710	.73091
	Natural Language Processing	4.0068	.76773
	Machine Vision	4.0154	.88683
Sum of arithmetic mean and standard deviation		4.0474	.78202
Cybersecurity	Confidentiality	4.1147	.70661
	Integrity	3.7879	.79969
	Availability	3.9775	.72324
	Authenticity	4.0807	.70764
	Possession and Control	4.0841	.74186
	Utility	4.1931	.67268
Sum of arithmetic mean and standard deviation		4.0396	.72528

Source: Statistical analysis results.

Table (4) shows the high arithmetic means for artificial intelligence technologies, with the overall average reaching (4.0474), and the robotics dimension having the highest average at (4.1710). The overall average for cybersecurity dimensions was (4.0396), with the utility dimension ranking first at an average of (4.1931), reflecting the high level of interest among the sample in artificial intelligence and cybersecurity technologies.

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 11, November, 2026
Website: usajournals.org
This work is Licensed under CC BY 4.0 a Creative Commons Attribution 4.0 International License.

3- Hypothesis Testing and Results Analysis:

1- Testing the First Hypothesis (H1):

There is a significant correlation between artificial intelligence technologies and cybersecurity.

To test this hypothesis, the researcher calculated Pearson's correlation coefficient to determine the type and strength of the relationship. Table (4) shows the statistical analysis of the results related to this relationship:

Table No. (5) Pearson's Correlation Coefficient Test between Artificial Intelligence Technologies and Cybersecurity

Correlations						
	Confidentiality	**Integrity**	**Availability**	**Authenticity**	**Possession and Control**	**Utility**
Machine learning	**.667****	**.634****	**.574****	**.667****	**.634****	**.574****
Expert Systems	.677**	**.661****	**.564****	**.677****	**.661****	**.564****
Robotics	.805**	**.709****	**.678****	**.805****	**.709****	**.678****
Natural Language Processing	.559**	**.601****	**.815****	**.734****	**.819****	**.734****
Machine Vision	.595**	.512**	.729**	.819**	.842**	.842**
****. Correlation is significant at the 0.01 level (2-tailed).**						

Source: Statistical analysis results.

Table (5) shows significant correlations between all artificial intelligence technologies and cybersecurity dimensions at a significance level of (0.01), with correlation coefficients ranging from (0.512–0.842).

Based on the above, the hypothesis that there is a significant correlation between artificial intelligence technologies and all dimensions of cybersecurity is accepted.

2- Testing the second hypothesis (H2):

There is a significant impact of artificial intelligence technologies on the dimensions of cybersecurity.

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 11, November, 2026
Website: usajournals.org
This work is Licensed under CC BY 4.0 a Creative Commons Attribution 4.0 International License.

Testing Sub-Hypothesis H2/1:

There is a significant impact of artificial intelligence technologies on confidentiality.

To test the validity of this hypothesis, the researchers used multiple linear regression analysis, which is used to predict changes in the dependent variable that is affected by a number of independent variables. Table (7) shows the results of the regression analysis as follows:

Table No. (6) Multiple Regression Analysis of the Impact of Artificial Intelligence Technologies on Confidentiality

Dimensions Independent variable	Dependent variable	Non-standard transactions		Standard transactions	Test (T)	
		B	Std . Error	Beta	T	Sig
Constant	**Confidentiality**	.225	.163		1.375	.170
Machine learning		.056	.058	.053	.955	.341
Expert Systems		.221	.049	.229	4.545	.000
Robotics		.642	.058	.612	11.107	.000
Natural Language Processing		.362	.045	.353	7.959	.000
Machine Vision		.401	.040	.444	10.001	.000
				Model Summary		
F		**Sig**		**R**	**R Squares**	**Adjusted R Square**
190.863		.000		.826	.683	.679

Source: Statistical analysis results.

Table (6) shows a significant effect of artificial intelligence (AI) technologies on confidentiality, with an F-value of 190.863. These technologies explained 68.3% of the changes in confidentiality, with robots having the most significant effect. Machine learning, however, did not show a significant effect.

Based on the above, the hypothesis that AI technologies have a significant effect on confidentiality is accepted.

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 11, November, 2026
Website: usajournals.org
This work is Licensed under CC BY 4.0 a Creative Commons Attribution 4.0 International License.

Testing Sub-Hypothesis H2/2:
There is a significant effect of artificial intelligence technologies on integrity.

Table No. (7) Multiple Regression Analysis of the Impact of Artificial Intelligence Technologies on Integrity

Dimensions Independent variable	Dependent variable	Non-standard transactions		Standard transactions	Test (T)	
		B	Std . Error	Beta	T	Sig
Constant	**Integrity**	-.005-	.220		-.023-	.982
Machine learning		.136	.079	.113	1.729	.085
Expert Systems		.335	.065	.300	5.116	.000
Robotics		.513	.078	.423	6.587	.000
Natural Language Processing		.358	.045	.357	8.012	.000
Machine Vision		.386	.039	.436	9.769	.000
				Model Summary		
F		**Sig**		**R**	**R Squares**	**Adjusted R Square**
117.183		.000		.754	.569	.564

Source: Statistical analysis results.

Table (7) shows a significant effect of artificial intelligence (AI) technologies on integrity, with an F-value of 117.183. These technologies explained 56.9% of the changes in integrity, with machine vision showing the most significant effect, while machine learning did not show a significant effect.

Based on the above, the hypothesis that AI technologies have a significant effect on integrity is accepted.

Testing Sub-Hypothesis H2/3:
There is a significant impact of artificial intelligence technologies on availability.

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 11, November, 2026
Website: usajournals.org
This work is Licensed under CC BY 4.0 a Creative Commons Attribution 4.0 International License.

Table No. (8): Multiple Regression Analysis of The Impact of Artificial Intelligence Technologies on Availability

Dimensions Independent variable	Dependent variable	Non-standard transactions		Standard transactions	Test (T)	
		B	Std . Error	Beta	T	Sig
Constant	**Availability**	.299	.242		1.237	.217
Machine learning		.101	.086	.084	1.173	.242
Expert Systems		.188	.072	.168	2.622	.009
Robotics		.611	.085	.502	7.147	.000
Natural Language Processing		.479	.048	.456	9.902	.000
Machine Vision		.280	.043	.302	6.561	.000
				Model Summary		
F		**Sig**		**R**	**R Squares**	**Adjusted R Square**
82.971		.000		.695	.483	.478

Source: Statistical analysis results.

Table (8) shows a significant effect of artificial intelligence (AI) technologies on availability, with an F-value of 82.971. These technologies explained 48.3% of the changes in availability, with natural language processing showing the most significant effect. Machine learning, however, did not show a significant effect. **Based on the above**, the hypothesis that AI technologies have a significant effect on availability is availability.

Testing Sub-Hypothesis H2/4:
There is a significant impact of artificial intelligence technologies on authenticity.

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 11, November, 2026
Website: usajournals.org
This work is Licensed under CC BY 4.0 a Creative Commons Attribution 4.0 International License.

Table No. (9): Multiple Regression Analysis of The Impact of Artificial Intelligence Technologies on Authenticity

Dimensions Independent variable	Dependent variable	Non-standard transactions		Standard transactions	Test (T)	
		B	Std . Error	Beta	T	Sig
Constant	**Authenticity**	.054	.079		.683	.495
Machine learning		.184	.064	.168	2.864	.005
Expert Systems		.046	.065	.044	.703	.483
Robotics		.373	.079	.364	4.702	.000
Natural Language Processing		.328	.074	.330	4.405	.000
Machine Vision		.317	.072	.335	4.215	.000
				Model Summary		
F		**Sig**		**R**	**R Squares**	**Adjusted R Square**
147.844		.000		.842	.709	.704

Source: Statistical analysis results.

Table (9) shows a significant effect of artificial intelligence techniques on originality, with an F-value of (147.844). These techniques explained 70.9% of the variations in originality. The effect of robots was the strongest, while no significant effect was observed for expert systems.

Based on the above, the hypothesis that artificial intelligence techniques have a significant effect on originality is accepted.

Testing Sub-Hypothesis H2/5:

There is a significant impact of artificial intelligence technologies on possession and control.

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 11, November, 2026
Website: usajournals.org
This work is Licensed under CC BY 4.0 a Creative Commons Attribution 4.0 International License.

Table No. (10): Multiple Regression Analysis of The Impact of Artificial Intelligence Technologies on Possession and Control

Dimensions Independent variable	Dependent variable	Non-standard transactions		Standard transactions	Test (T)	
		B	Std . Error	Beta	T	Sig
Constant	**Possession and Control**	.062	.067		.921	.358
Machine learning		.101	.055	.093	1.839	.067
Expert Systems		.046	.055	.044	.823	.411
Robotics		.472	.067	.465	7.007	.000
Natural Language Processing		.334	.063	.339	5.285	.000
Machine Vision		.386	.046	.405	8.359	.000
				Model Summary		
F		**Sig**		**R**	**R Squares**	**Adjusted R Square**
223.097		.000		.887	.786	.782

Source: Statistical analysis results.

Table (10) shows a significant effect of artificial intelligence (AI) technologies on possession and control, with an F-value of (223.097). These technologies explained 78.6% of the changes in possession and control. Robots had the most significant effect, while neither machine learning nor expert systems showed a significant effect.

Based on the above, the hypothesis that AI technologies have a significant effect on possession and control is accepted.

Testing Sub-Hypothesis H2/6:
There is a significant impact of artificial intelligence technologies on utility.

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 11, November, 2026
Website: usajournals.org
This work is Licensed under CC BY 4.0 a Creative Commons Attribution 4.0 International License.

Table No. (11): Multiple Regression Analysis of The Impact of Artificial Intelligence Technologies on Utility

Dimensions Independent variable	Dependent variable	Non-standard transactions		Standard transactions	Test (T)	
		B	Std . Error	Beta	T	Sig
Constant	**Utility**	.088	.045		1.937	.053
Machine learning		.101	.048	.097	2.128	.034
Expert Systems		.015	.054	.015	.273	.785
Robotics		.305	.061	.305	5.025	.000
Natural Language Processing		.528	.053	.527	10.034	.000
Machine Vision		.249	.041	.296	6.113	.000
				Model Summary		
F		**Sig**		**R**	**R Squares**	**Adjusted R Square**
526.217		.000		.915	.837	.835

Source: Statistical analysis results.

Table (11) shows a significant effect of artificial intelligence (AI) technologies on utility, with an F-value of 526.217. These technologies explained 83.7% of the changes in utility, with natural language processing showing the most significant effect, while expert systems did not.

Based on the above, the hypothesis that AI technologies have a significant effect on utility is accepted.

Ninth: Summary of Findings and Research Recommendations:

1- Summary of Results:

1.The results showed that the study instrument possessed a high degree of reliability and validity, confirming its suitability for measuring the study variables.

2.The results revealed a high level of availability of artificial intelligence (AI) and cybersecurity technologies among the study participants.

3.The results showed positive and significant correlations between all dimensions of AI technologies and cybersecurity dimensions.

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 11, November, 2026
Website: usajournals.org
This work is Licensed under CC BY 4.0 a Creative Commons Attribution 4.0 International License.

4.The results demonstrated a significant impact of AI technologies on confidentiality, with robots having the strongest effect.
5.The results showed a significant impact of AI technologies on integrity, with machine vision being the most influential.
6.The results confirmed a significant impact of AI technologies on availability, with natural language processing being the most influential.
7.The results showed a significant impact of AI technologies on authenticity, with robots having the most influential effect.
8.The results showed a significant impact of AI technologies on ownership and control, with robots having the most influential effect. 9. The results confirmed that artificial intelligence techniques have a significant impact on utility, with natural language processing being the most influential.

2- Research Recommendations:

In light of the research findings, the researcher presents a set of recommendations, along with proposed mechanisms deemed appropriate for operationalizing and implementing these recommendations, as follows:

Table No. (12): Study Recommendations

Scope of recommendation	Recommendation	Implementation mechanism	Implementation time	The entity responsible for implementation
Artificial Intelligence Technologies	Expanding the use of artificial intelligence technologies to enhance cybersecurity.	Provision of modern smart software and applications	Within 6 months	Senior Management
Cybersecurity	Focusing on the continuous updating of electronic protection systems.	Performing periodic updates to security systems.	Periodically	IT Department
Employee Training	Increasing employee awareness regarding the risks of cyber threats.	Organizing training courses on cybersecurity.	Every 6 months	Human Resources Department

Source: Prepared by the researcher.

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 11, November, 2026
Website: usajournals.org
This work is Licensed under CC BY 4.0 a Creative Commons Attribution 4.0 International License.

3- Suggestions for future research:

a- A study on the impact of artificial intelligence technologies on cyber risk management, with an application to telecommunications companies.

b- A study on the role of artificial intelligence in the early detection of cyberattacks.

c- A study on the impact of cybersecurity on the protection of data and information within organizations.

d- A study on the role of employee training in strengthening cybersecurity in the context of digital transformation.

References:

1. Arpaci, I., & Sevinc, K. (2022). Development of the cybersecurity scale (CS-S): Evidence of validity and reliability. Information Development, 38(2), 218-226.
2. Babina, T., Fedyk, A., He, A., & Hodson, J. (2024). Artificial Intelligence, Firm Growth, And Product Innovation. Journal of Financial Economics, 151, 103745.
3. Bitzer, M., Brinz, N., & Ollig, P. (2021). Disentangling the concept of information security properties-enabling effective information security governance.
4. Canelón, J., Huerta, E., Leal, N., & Ryan, T. (2020). Unstructured data for cybersecurity and internal control.
5. Chang, V., Golightly, L., Xu, Q. A., Boonmee, T., & Liu, B. S. (2023). Cybersecurity for children: an investigation into the application of social media. Enterprise Information Systems, 17(11), 2188122.
6. Collins, C., Dennehy, D., Conboy, K., & Mikalef, P. (2021). Artificial intelligence in information systems research: A systematic literature review and research agenda. International journal of information management, 60, 102383.
7. de-Lima-Santos, M. F., & Ceron, W. (2021). Artificial intelligence in news media: Current perceptions and future outlook. Journalism and media, 3(1), 13-26.

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 11, November, 2026
Website: usajournals.org
This work is Licensed under CC BY 4.0 a Creative Commons Attribution 4.0 International License.

8. Dejoux, C., & Léon, E. (2018). Métamorphose des managers: à l'ère du numérique et de l'intelligence artificielle. Pearson France.
9. Galinec, D., & Luić, L. (2020). Design of conceptual model for raising awareness of digital threats. WSEAS transactions on environment and development, 16, 493-504.
10. Gonzalez, Juan, & Hernández, Luis. (2025). AI and education: Combination to enhance knowledge. Seminars in Medical Writing and Education, 4(37), 33–56.
11. Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2025). Cybersecurity in local governments: A systematic review and framework of key challenges. Urban Governance, 5(1), 1-19.
12. Kühl, N., Schemmer, M., Goutier, M., & Satzger, G. (2022). Artificial intelligence and machine learning: N. Kühl et al. Electronic Markets, 32(4), 2235-2244.
13. Kumar, V., Ramachandran, D., & Kumar, B. (2021). Influence of new-age technologies on marketing: A research agenda. Journal of Business Research, 125, 864-877.
14. Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion, 97, 101804.
15. Iansiti, M., & Lakhani, K. R. (2020). Competing in the age of AI: Strategy and leadership when algorithms and networks run the world. Harvard Business Press, Brighton.
16. Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, 7, 8176-8186.
17. Mamak, K., Kokkonen, T., Hakli, R., & Mäkelä, P. (2025). Robot Kingdom: On the difficulty of finding the definition of robots. International Journal of Social Robotics, 17(11), 2743-2753.
18. Maraveas, C., Rajarajan, M., Arvanitis, K. G., & Vatsanidou, A. (2024). Cybersecurity threats and mitigation measures in agriculture 4.0 and 5.0. Smart Agricultural Technology, 9, 100616.

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 11, November, 2026
Website: usajournals.org
This work is Licensed under CC BY 4.0 a Creative Commons Attribution 4.0 International License.

19. Moustafa, N. (2022). Digital Forensics in the Era of Artificial Intelligence. CRC Press. book.
20. Nazir, S., Khadim, S., Asadullah, M. A., & Syed, N. (2023). Exploring the influence of artificial intelligence technology on consumer repurchase intention: The mediation and moderation approach. Technology in Society, 72, 102190.
21. Nikesh Muthukrishnan, F. M. (2020). Brief History of Artificial Intelligence. Elsevier Inc, 30(4), 10. Omar Adnan AlShkipi, B. Z. (2024). Implementation of Artificial Intelligence in Interior Design: Systematic Literature Review. Civil Engineering and Architecture, 12(4), 2903.
22. Nepal, R., Zhao, X., Dong, K., Wang, J., & Sharif, A. (2025). Can artificial intelligence technology innovation boost energy resilience? The role of green finance. Energy economics, 142, 108159.
23. Ramírez, M., Rodríguez Ariza, L., Gómez Miranda, M. E., & Vartika. (2022). The disclosures of information on cybersecurity in listed companies in Latin America—proposal for a cybersecurity disclosure index. Sustainability, 14(3), 1390.
24. Rjoub, G., Bentahar, J., Wahab, O. A., Mizouni, R., Song, A., Cohen, R., ... & Mourad, A. (2023). A survey on explainable artificial intelligence for cybersecurity. IEEE Transactions on Network and Service Management, 20(4), 5115-5140.
25. Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. Sensors, 23(15), 6666.
26. Sarker, I. H. (2022). AI-based modeling: techniques, applications and research issues towards automation, intelligent and smart systems. SN computer science, 3(2), 158.
27. Song, F., Xia, T., & Tang, Y. (2026). Integration of artificial intelligence technology and visual communication design in metaverse e-commerce and its potential opportunities. Electronic Commerce Research, 26(3), 3155-3175.
28. Smaili, N., Radu, C., & Khalili, A. (2023). Board effectiveness and cybersecurity disclosure. Journal of Management and Governance, 27(4), 1049-1071.

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 11, November, 2026
Website: usajournals.org
This work is Licensed under CC BY 4.0 a Creative Commons Attribution 4.0 International License.

29. Takács, J. M. & Pogátsnik, M. (2024). A Comprehensive Study on Cybersecurity Awareness: Adaptation and Validation of a Questionnaire in Hungarian Higher Technical Education. Acta Polytechnica Hungarica, 21(10), 533-552.
30. Torkzadehmahani, R., Nasirigerdeh, R., Blumenthal, D. B., Kacprowski, T., List, M., Matschinske, J., ... & Baumbach, J. (2022). Privacy-preserving artificial intelligence techniques in biomedicine. Methods of information in medicine, 61(S 01), e12-e27.
31. Yaacoub, J. P. A., Noura, H. N., Salman, O., & Chehab, A. (2022). Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations. International Journal of Information Security, 21(1), 115-158.