Jurnal Nuansa: Publikasi Ilmu Manajemen dan Ekonomi Syariah
Volume 3, Nomor 1, Tahun 2025
e-ISSN: 3021-8691; p-ISSN: 3024-8388, Hal. 202-217
DOI: https://doi.org/10.61132/nuansa.v3i1.1593
Available Online at: https://journal.arimbi.or.id/index.php/Nuansa

Integration Between Artificial Intelligence and Cyber Security Technologies and Its Impact on Administrative Decisions

Sadeq Dhahir Farhan Alzaidi
Imam AL Kadhum College, Wasit, Iraq

Address: ثانوية خولة بنت الازور, Baghdad, Baghdad Governorate, Iraq
Email correspondence: sadeq.dhahir@iku.edu.iq

Abstract. *This research aims to understand the impact of the integration between artificial intelligence (AI) technologies and cyber security on administrative decisions in three aspects: (1) decision-making speed, (2) decision accuracy, and (3) decision effectiveness. A sample of 150 employees was drawn, and a survey was used to gather the required information. Data analysis was conducted using the statistical program SPSS 25, employing various statistical methods such as mean, standard deviation, correlation coefficient, and simple linear regression. The research concluded with several findings, the most important being: The integration of AI technologies and cyber security leads to improved speed, accuracy, and effectiveness of administrative decisions, The researcher recommended that institutions adopt AI technologies to enhance their cyber security systems, particularly in areas like machine learning and big data analysis.*

Keywords: *AI, Cybersecurity, Decisions, Integration*

1. INTRODUCTION

The latest rapid advances in artificial intelligence technologies (AI) and cyber security are revolutionizing the way organizations operate and make managerial decisions. The integration of AI and cyber security has become a vital aspect of modern enterprise management, enabling the detection and prevention of cyber threats, improving incident response, and enhancing the overall security posture (Alazab et al., 2020). According to recent studies, the use of AI-powered security systems can reduce the risk of cyberattacks by up to 50% (Sarker et al., 2019). Moreover, the integration of AI and cyber security can also improve managerial decision-making by providing real-time threat intelligence, predictive analytics, and automated incident response (Chakrabarti et al., 2019) Gupta et al also pointed out that the use of AI-powered cyber security systems can enhance organizational resilience and reduce the financial impact of cyber-attacks. However, the integration of (AI) and cyber security also raises several challenges, including issues related to data privacy, algorithmic biases, and the need for skilled Cyber security professionals (Singh et al., 2020) Despite these challenges, the benefits of integrating (AI) and cyber security are undeniable, and the risks faced by organizations that fail to adopt these technologies are increasing in a complex and increasingly threatening cyber environment.

Accordingly, this research aims to study the relationship between the integration of artificial intelligence and cyber security technologies and their impact on administrative

Received: Desember 23, 2024; Revised: Januari 07, 2025; Accepted: Januari 29, 2025;
Online Available: Januari 30, 2025

decisions. With the aim of exploring this relationship and the extent of this impact to reach effective recommendations for institutions.

2. RESEARCH DESIGN

Statement of Research

With the rapid development of artificial intelligence technologies(AI) and its increasing reliance in various fields, the need to enhance cyber security has become more urgent than ever. However, the integration of artificial intelligence and cyber security still faces major challenges, which negatively affects the effectiveness of administrative decisions in institutions.

The main problem is that many organizations struggle to achieve optimal integration between (AI) technologies and cyber security systems, leading to security gaps and weak management decision-making capabilities. Effective these gaps may increase the risk of cyber-attacks, data leakage, and loss of confidence in technical systems, which negatively affects the stability of organizations and their ability to achieve their strategic goals.

In addition, the lack of a clear framework that defines how AI can be used to enhance cyber security, and the absence of unified standards for managing the risks associated with this integration, further complicates the problem. This requires in-depth study to understand how the integration between (AI) and cyber security affects the administrative decision-making process, and how organizations can benefit from these technologies to enhance their cyber security and improve the efficiency of their administrative decisions. Hence it emerged problematic we searched this which says:

a. What is it impact Integration of AI and Cyber security Technologies on Decisions Administrative?

The following sub-questions fall under this problem:

a. What is it impact Integration of AI and Cyber security Technologies on speed of taking Decisions Administrative?
b. What is it impact Integration of AI and Cyber security Technologies on effectiveness Decisions Administrative?

Research Hypotheses

The main hypothesis of the research: There is a statistically significant effect of the integration of artificial intelligence and Cyber security technologies on administrative decisions. The following sub-hypotheses branch off from this hypothesis:

a. There is a statistically significant effect of the integration of artificial intelligence and Cyber security technologies on speed of taking Administrative decisions.
b. There is a statistically significant effect of the integration of artificial intelligence and Cyber security technologies on accuracy Administrative decisions.
c. There is a statistically significant effect of the integration of artificial intelligence and Cyber security technologies on the effectiveness of administrative decisions.

Significance

This study is important in that it

The integration of AI and Cyber security technologies is important in the world of business and modern technology. AI can help improve the efficiency of management decisions, analyze data, and improve Cyber security. While Cyber security plays a crucial role in protecting information and data from security threats. Therefore, the integration of these technologies can contribute to improving the efficiency of management decisions, improving Cyber security, and reducing security risks.

Objectives

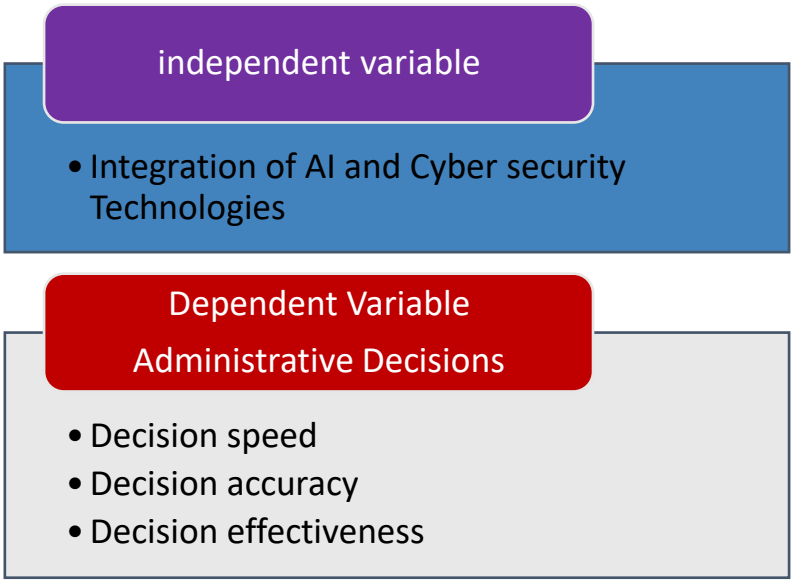
This paper is set to achieve the following:

a. Analyze how using Integrating AI with cyber security technologies to improve the efficiency of management decisions.
b. Understand how using artificial intelligence to improve cyber security, analyze security data, and identify security threats.
c. Identify the security challenges and risks that organizations may face when using AI and cyber security technologies.
d. Evaluating the impact of the integration of artificial intelligence and cyber security technologies on administrative decisions, and improving the efficiency of these decisions.

Hypothetical research plan

Clear Figure No. (1) The hypothetical research plan, which contains the two main variables, which are:

a. Independent variable (X) Integration of AI and Cyber security technologies
b. Dependent variable (Y) Administrative decisions (speed of decision-making – accuracy of decision – effectiveness of decision)



Source: Prepared by the researcher

Figure 1. Planner Hypothetical research

Research Limits

a. Spatial boundaries: Central Bank of Iraq
b. Human boundaries: It includes a sample of employees at the Central Bank of Iraq at various levels.
c. Time limits: The research period extends between the years 2025 - 2024 AD

Research sample

The researcher relied on the random sample. And Simple sampling according to the following law:

$$n' = \frac{n}{1 + \frac{z^2 \times p(1-p)}{\varepsilon^2 N}}$$

$$n = \frac{z^2 \times p(1-p)}{\varepsilon^2}$$

The sample size reached 150 employees from all specializations (employee - accountant - financial manager - manager)

3. THEORETICAL FRAMEWORK

Definition of Artificial Intelligence:

Artificial intelligence (AI)It is a branch of computing concerned with creating systems capable of performing tasks that require a high level of human intelligence, such as learning, reasoning, and pattern recognition. (Poole, 2019) Artificial intelligence is a major field in computer science, focusing on developing technologies that can perform complex tasks like humans. According to DARPA in its report on artificial intelligence, AI is defined as “the

ability to perform tasks thought to require human intelligence" (DARPA, 2020) This definition shows the breadth of AI and its impact on various aspects of life. AI is used in many fields, including computer vision, machine learning, speech recognition, and robotics. AI is also being applied in fields such as health, finance, transportation, Education, currently Artificial intelligence has seen major advances in areas such as deep learning and human learning. New techniques such as artificial neural networks, collaborative learning, and human learning have also been developed. (Sutton & Barto, 2018).

The Importance of Artificial Intelligence:

Artificial intelligence One of the most prominent technologies that is causing radical changes in various aspects of life, starting from industry and healthcare to education and entertainment. The importance of artificial intelligence is represented in the following points: Next (Brynjolfsson, McAfee, 2023)

a. **Improve efficiency and productivity**: It helps MAI automates routine and complex tasks, reducing human error and increasing the speed and accuracy of operations. For example, in the manufacturing sector, AI-powered robots are used to perform dangerous or delicate tasks that require high levels of precision.
b. **Applications Medical**: It is used MAI can diagnose diseases faster and more accurately, and help develop personalized treatments based on patients' genetic data. For example, AI systems are able to analyze medical images such as X-rays and MRIs to detect diseases such as cancer in their early stages.
c. **Enhance your experience user**: Used M Artificial intelligence techniques in analyzing user behavior and providing personalized recommendations, as is the case with platforms such as Netflix and Spotify, where AI algorithms are used to analyze users' preferences and deliver content that suits their tastes.
d. **Innovation in Industry**: It helps M Artificial intelligence in developing new industries and improving existing ones. For example, in the transportation sector, AI technologies are being used in the development of self-driving cars, which could reduce traffic accidents and improve fuel efficiency.
e. **Data analysis Huge**: He is D Artificial intelligence is a powerful tool for analyzing massive amounts of data. (Big Data) and extracting valuable insights that help in making strategic decisions in business and science. For example, machine learning algorithms are used in analyzing market data to predict consumer behavior.

Definition of Cyber Security and Its Importance:

Cyber security is a term that describes the procedures and technology used to protect networks, computers, and data from unauthorized cyber-attacks and intrusions.

Cyber security is vital in the modern age, where so much of our daily activities rely on digital technology. And the Internet (Kizza,2020). Its importance stems from The following points:(Kshetri,2019)

a. **Data Protection:** Cyber security helps protect sensitive data from unauthorized access or theft.
b. **Preventing cyber-attacks:** Cyber security is the prevention of cyber-attacks such as viruses, malware, and phishing attacks.
c. **Ensuring business continuity:** Cyber security helps ensure business continuity by protecting technology infrastructure from damage or disruption.
d. **Identity protection:** Cyber security helps protect the identity of individuals and businesses from theft or fraud.

According to a study published in the journal of Cyber security, Cyber security is one of the most important priorities for companies and organizations in the modern era. The study also showed that investing in Cyber security can reduce the risks associated with cyber-attacks and improve confidence in systems Technology. (Denning, 2018).

Administrative Decisions:

Administrative decisions are an essential part of the management process, as they represent the framework that determines the direction of businesses and organizations. Administrative decisions are decisions taken by management to achieve the organization's goals, and affect the organization's performance and the development of human and material resources. (Barnard, 2019)

Administrative decisions include several aspects, including: (Fayol, 2017).

a. **Planning** Determine the goals and objectives that the organization seeks to achieve.
b. **To organize**: Determine the organizational structure, functions and responsibilities.
c. **Directing** Directing human and material resources to achieve goals.
d. **Censorship** Monitor and evaluate performance to ensure that objectives are achieved.

The importance of administrative decisions: (Barnard, 2019).

a. **Achieving goals** Administrative decisions contribute to achieving the organization's goals and increasing its efficiency.
b. **resource allocation**: Helps in directing human and material resources effectively to achieve goals.

c. **Organization development** Contribute to developing the organization and improving its performance by making the right decisions.
d. **Boost confidence**: It enhances trust among employees, customers and partners, which leads to enhancing the organization's reputation.
e. **Reduce risk**: Helps reduce risks and identify solutions to potential problems.

4. THE PRACTICAL ASPECT

Search Tool:

The questionnaire was adopted as the main tool for data collection. Field, After the researcher has reviewed on Theoretical literature related to the research topic designed by Questionnaire in line with the objectives Search, it included 30 questions, 5 of which were related to information. Character,10 questions about the independent variable (integration) Artificial Intelligence and Cyber security Technologies) and 15 questions for the dependent variable (administrative decisions). At a rate of 5 questions for each dimension.

A total of (190) questionnaires were distributed to achieve the required sample size with a distribution rate of 100%. Of these questionnaires, (16) questionnaires were not retrieved, representing a rate of (8.4%). It was also found that (24) questionnaires were not valid for analysis due to missing data or similar answers, representing a rate of (12.6%). As for the valid questionnaires for analysis, their number was (150) questionnaires, representing a rate of (78.9%). The following is an explanatory table showing these numbers:

Table 1. Distribution of the form

Data	number	%
Total distributed forms	190	100
Unreturned questionnaires	16	8.4
Invalid questionnaires for analysis	24	12.6
Questionnaires suitable for analysis	150	78.9

Source: Prepared by researcher

The general rule is that the percentage of missing data should not exceed 10% of the total data. If the percentage is less than that, the average method can be used to deal with it. If the percentage is higher, it may be better to delete the data.

To ensure that missing data does not affect the results of the analysis, a test can be used. Little's MCAR. This test evaluates the chi-square value, degrees of freedom, and level of significance of the data. Where If the significance level is less than 0.05, it indicates that missing data has an effect on the results.

In the current study, the value of (Chi-Square= 95.722), and degrees of freedom (DF= 84), and the significance level (Sig= 0.063). Since the significance level is greater than 0.05, this indicates that the missing data does not affect the final results of the analysis.

The internal validity and reliability of the instrument:

a. **Internal construction honesty:** Refers to the degree to which the items and scales within a questionnaire accurately measure the concepts or theoretical constructs they are intended to assess. In other words, it is the extent to which a questionnaire measures what it claims to measure.

To assess the internal construct validity of a sample questionnaire, one can use different measurement techniques such as factor analysis, reliability analysis, and correlation analysis. These techniques help determine whether the items in the questionnaire consistently measure the same underlying concept, whether the scale has good internal consistency (i.e., the items correlate well with each other), and whether the scale is adequately related to other variables that it should be related to according to the theory.

The scale should have high internal consistency, meaning that responses to the different items measuring job satisfaction should be highly correlated with each other. Furthermore, scores on the job satisfaction scale should be positively correlated with other variables known to be associated with job satisfaction, such as positive affect or organizational support.

Therefore, establishing internal construct validity requires careful consideration of how items and scales were developed, how they relate to each other and to external criteria, and how consistent they are across time and contexts. A questionnaire with strong internal construct validity provides confidence that the measures obtained from it reflect the true state of the construct being measured. As the analysis shows:

Table 2. Internal construct validity

M	The field	strength of association	SIG	Phrases	Sample 150
				30	
1	Integration of AI and Cyber security Technologies	.902**0	.0000		
2	Administrative decisions	.885**0	.0000		

Source: Prepared by the researcher

Reached First link0.902 at a significance level of 0.00 and The second link is hand 0.885 at a significance level of 0.00. Where it is clear That this Relationships Reliable

b. Thaba T Study tool: Using M Several ways, the most important of which are:

1) Cronbach's Alpha Scale:

Used to assess the internal consistency or reliability of a set of items or questions in a survey or questionnaire. It is typically used to estimate reliability,

Cronbach's alpha calculates the average cross-correlation between all possible splits of items in a scale. Specifically, it estimates the proportion of variance in the overall score that is due to true variance in the construct being measured rather than error variance. This coefficient ranges from zero to one, with higher values indicating greater internal consistency.

A Cronbach's alpha value greater than 0.7 is generally considered acceptable for research purposes, while values between 0.6 and 0.7 may be acceptable depending on the nature of the study and the specific items being measured. Values less than 0.6 indicate poor internal consistency and raise concerns about the reliability of the scale. However, it is important to note that very high alpha coefficients may indicate redundancy in items and may indicate that some items may be removed to improve the effectiveness of the scale.

The process of calculating Cronbach's alpha involves taking the mean of the elements of the diagonal of the covariance matrix divided by the sum of the squared standard deviation of each element multiplied by the number of elements minus one. For Formula:

$$\alpha = (n / (n - 1)) * ((I\ am\_x^2) / (Is\_xy))$$

In short, Cronbach's alpha is a basic measure for assessing internal consistency, providing information about the reliability of a scale and its ability to effectively capture the intended construct.

Table 3. Reliability and Validity

Axes	Stability	Sincerity	Phrases
Integration of AI and Cyber security Technologies	.950**	.915**	10
Administrative decisions	.910**	.895**	15
Average	**.930****	**.905****	

Source: Prepared by the researcher

2) It is clear that the questionnaire achieves a good level of reliability and validity for all axes, as: Average Axial stability0.930 and middle Believe it 0.905 The questionnaire can be said to be reliable and valid for use in sampling and data collection.

3) Method of stability by repetition:

Test-retest reliability, also called retest reliability, is a type of reliability assessment that examines the stability or consistency of a measurement over repeated administrations of the same instrument. This approach assumes that there will be no significant changes in the construct being measured during the time interval between administrations. Test.

Includes N The process usually involves presenting the research form to a group of participants for the first time and again. Other after a period specific, range usually from days to Weeks or months, in The Time Second. Calculates Researchers Factor Link between Results that It was completed get On it in both the Two time points to determine the level of agreement between them. Higher correlation coefficients indicate stronger reliability. Test-retest reliability is particularly useful when researchers aim to demonstrate temporal stability or repeatability of measurement, especially if the construct being measured is assumed to remain relatively stable over time.

4) However, several factors can affect test-retest reliability, including memory effects, practice effects, maturation effects, and situational differences. Memory effects refer to participants remembering their previous answers, leading to artificially inflated associations. Practice effects occur when participants become familiar with the task and perform better on subsequent attempts. Maturation refers to the natural developmental changes that occur between testing occasions, affecting the construct being measured. Situational differences include differences in environmental conditions, instructions, or participant motivations that can lead to inconsistent results.

Researchers should carefully consider these potential sources of bias and monitor for any extraneous variables that might influence the results. They can use strategies such as counterbalancing, randomizing, changing the intervals between tests, or using alternate forms of the same test to reduce the influence of confounding factors. Despite its limitations, test-retest reliability remains a valuable tool for assessing the consistency of a measurement over time. The questionnaire was tested twice on 14 bank employees over a period of two weeks.

Table 4. Reliability

sequence	The field	Scale	%
1	Integration of AI and Cyber security Technologies	.905	.013
2	Administrative decisions	.885	.012
Average		.995	.012

Source: Prepared by the researcher Based on the results of the field study 2024 AD

The coefficients are found to be high, meaning that these questions are suitable for study.

Statistical Methods Used

It was approved. The programGStatisticianspss.25 for calculation (M proportions Oh Yes, Averages, deviation Standard, Analysis Link, regression coefficient Simple.)

Analysis of The Study's Axes and Dimensions:

To evaluate participants' opinions about Questionnaire fields, the arithmetic mean and the verification degree were used as shown below:

Table 5. Average and degree of verification of respondents' responses

The number	Questionnaire	M	Verification
1	Integration of AI and Cyber security Technologies	2.04	High
2	Administrative decisions	2.2	High
Overall average		2.1	High

Source: Prepared by the researcher

The results show that the sample members highly evaluated the study topics. Therefore, the participants believe in the importance of integrating artificial intelligence and Cyber security technologies in administrative decisions.

Hypothesis testing

Testing scientific hypotheses is a fundamental component of the scientific method and involves using evidence-based data to support or refute a proposed explanation for a natural phenomenon. This process helps scientists evaluate the validity of their theories, improve our understanding of the world around us, and make informed decisions. Correct Based on empirical evidence,

This research is based on the following main hypothesis:

Main hypothesis of the research There is a statistically significant effect of the integration of artificial intelligence and Cyber security technologies on administrative decisions. To test this hypothesis, three sub-hypotheses were relied upon.

We will use simple linear regression to model the relationship between the variables using: to prediction equation.

$$y = c + \beta x + \varepsilon$$

The assumption Yes Sub and Number 1 There is a statistically significant effect of the integration of artificial intelligence and Cyber security technologies on speed of taking Administrative decisions. It was used. Program SPSS.25 We get the following results:

Table 6. Hypothesis test Yes Sub and the first I

Speed Administrative decisions	Model indicators						Levels		
	R	R2	**Adjusted**R 2	**F**	**Sig.**	**Durbin-Watson**	**B**	**t**	**Sig.**
(Constant)	**0.770**	**0.484**	**0.471**	**13.24**	**0.00**	**2.4**	**3.001**	**4.106**	**0.00**
Integration of AI and Cyber security Technologies							**0.326**	**3.692**	**0.00**

Source: From Before the researcher

It is clear from the following table:

R=0.770, That is, the relationship between the variables is strong.

R2=0.484, meaning that 48.4% of the variance in administrative decisions is Explain by integrating AI and Cyber security technologies.

F=13.24at a significant level Sig.: 0.00, indicates that the model is statistically significant.

Durbin-Watson=2.4, indicates no autocorrelation problem.

T=3.692at a significant level **, any The impact of the integration of artificial intelligence and Cyber security technologies on management decisions is statistically significant.

a. **prediction equation:**

Y = 3.001+ 0.326X

The equation indicates that Each unit increase in the integration of AI and Cyber security technologies(X) leads to an increase in the speed of making managerial decisions (Y) by 0.326 units.

b. **The assumption Yes Sub and Number 2** There is a statistically significant effect of the integration of artificial intelligence and Cyber security technologies on the accuracy of administrative decisions. We get the following results:

Table 7. Testing the second sub-hypothesis

Accuracy of administrative decisions	Model indicators						Levels		
	R	R2	**Adjusted**R2	**F**	**Sg**	**Durin-Waton**	**B**	**t**	**Sg**
(Constant)	**0.85**	**0.631**	**0.622**	**14.06**	**0.00**	**2.52**	**3.902**	**7.701**	**0.00**
Integration of AI and Cyber security Technologies							**0.866**	**5.122**	**0.00**

Source: From Before the researcher

The table shows the following results:

R=0.85, and Indicates a strong relationship between variables.

R2=0.631, which means that 63.1% of the variance in the accuracy of administrative decisions Explain by integrating AI and Cyber security technologies.

F=14.06, and significance level Sig.: 0.00, indicates that the model is statistically significant.

Durbin-Watson=2.52, indicates that there is no problem with self-correlation.

T=7,701, Sig.: 0.00, any The impact of the integration of artificial intelligence and Cyber security technologies on the accuracy of administrative decisions is statistically significant.

c. Prediction equation:

Y = 3.902 + 0.866X

3.902: Initial value of accuracy of administrative decisions (determinant)

0.266: Impact factor of integration of AI and Cyber security technologies on the accuracy of administrative decisions

It indicates that Each unit increase in the integration of AI and Cyber security technologies Leads to increased accuracy of administrative decisions by 0.866 units.

d. The assumption Yes Sub and Number 3There is a statistically significant effect of the integration of artificial intelligence and Cyber security technologies on Effectiveness of administrative decisions.

Table 8: Test of the third sub-hypothesis

Effectiveness of administrative decisions	Model indicators						Levels		
	R	R2	**Adjusted**R2	**F**	**Sig.**	**Durbin-Watson**	**B**	**t**	**Sig.**

(Constant)	**0.831**	**0.630**	**0.601**	**18.774**	**0.00**	**2.30**	**2.104**	**4.966**	**0.00**
Integration of AI and Cyber security Technologies							**0.799**	**4.595**	**0.00**

Source: From Before the researcher

The following results are shown from the previous table:

R=0.831There is Strong relationship between variables.

R2=0.630, which means that 63% of the variance in the effectiveness of administrative decisions Explains by integrating AI and Cyber security technologies.

F=18,774at a significant level Sig.: 0.00, That is to say The model is statistically significant.

Durbin-Watson=2.30, indicates no autocorrelation problem.

T=4.966At a moral level Sig: 0.00, any The impact of the integration of artificial intelligence and Cyber security technologies on the effectiveness of administrative decisions is statistically significant.

d. prediction equation:

$$Y = 2.104 + 0.799X$$

2.104: The initial value of the effectiveness of administrative decisions

0.799: without to The impact of the integration of artificial intelligence and Cyber security technologies on the effectiveness of administrative decisions.

That is to sayEach unit increase in the integration of AI and security technologies Cyber Leads to increased decision effectivenessAdministrativeBy 0.799 units.

As a result of testing the sub-hypotheses, we prove the validity of the main hypothesis and conclude the existence of an effect. To integrate artificial intelligence and Cyber security technologies on Administrative decisions.

Conclusions and Recommendations

First: Conclusions

a. The research results showed that the respondents agreed to a high degree on to Paragraphs of each of the variables (Integration of AI and Cyber security Technologies-Administrative decisions).

b. The results of the research revealed the presence of an effect of integration. Artificial Intelligence and Cyber Security Technologies On the administrative decisions of the Central Bank of Iraq. From this main result:

1) There is a trace for integration Artificial Intelligence and Cyber Security Technologies on the speed of administrative decisions in the Central Bank of Iraq
2) There is a trace for integration Artificial Intelligence and Cyber Security Technologies On the accuracy of administrative decisions in the Central Bank of Iraq.
3) There is a trace for integration Artificial Intelligence and Cyber Security Technologies On the effectiveness of administrative decisions in the Central Bank of Iraq

c. After accuracy came first, followed by effectiveness and finally speed of administrative decisions.

Second: Recommendations

a. Using AI algorithms to analyze data and Cyber security measures to protect data integrity
b. Provide training to employees on how to effectively use AI and Cyber security tools to improve decision-making accuracy, while ensuring they understand the benefits and limitations of these technologies.
c. Develop a strategic plan for deploying AI and Cyber security technologies to increase the effectiveness of management decisions. This could include identifying areas where AI can automate routine tasks, freeing up resources for more strategic decision-making.
d. Establish clear performance metrics to measure the effectiveness of post-merger management decisions, allowing for continuous evaluation and improvement.
e. Given the rapidly evolving nature of AI and Cyber security technologies, it is essential to regularly review and update existing systems. This ensures that the CBI stays at the forefront of technological advancements, maximizing the benefits of integrating AI and Cyber security.

REFERENCES

Alazab, M., Khraisat, A., & Gondal, I. (2020). Artificial intelligence and cybersecurity: A review of the current state and future directions. *Journal of Intelligent Information Systems*, *57*(2), 23–37. https://doi.org/10.1007/s10844-020-00615-5

Barnard, C. (2019). *The functions of the executive* (10th ed.). Harper Collins.

Chakrabarti, A., Gupta, B., & Kar, A. K. (2019). A framework for integrating artificial intelligence and cybersecurity in organizations. *Journal of Management Information Systems*, *36*(4), 931–954. https://doi.org/10.1080/07421222.2019.1660984

Defense Advanced Research Projects Agency (DARPA). (2020). *Artificial intelligence (AI)*. Retrieved from https://www.darpa.mil/about-us/darpa

Denning, D. E. (2018). *The future of cybersecurity*. Journal of Cybersecurity, 4(1), 1–13.

Fayol, H. (2017). *General and industrial management* (11th ed.). Dunod.

Gupta, S., Kumar, N., & Singh, M. (2020). Artificial intelligence and cybersecurity: A systematic review and future directions. *Journal of Intelligent Information Systems, 57*(1), 39–55. https://doi.org/10.1007/s10844-020-00612-8

Kizza, J. M. (2020). *Guide to computer network security*. Springer.

Kshetri, N. (2019). *Cybersecurity in the digital economy*. Routledge.

Kumar, P., Singh, M., & Kumar, N. (2020). Integration of artificial intelligence and cybersecurity: A review of the current state and future directions. *Journal of Cybersecurity and Privacy, 1*(1), 1–15. https://doi.org/10.1007/s42979-020-00001-5

Poole, D. L. (2010). *Artificial intelligence: Foundations of computational agents*. Cambridge University Press.

Sarker, I. H., Kayes, A. S. M., & Badsha, S. (2019). Cybersecurity data science: An overview from artificial intelligence perspective. *Journal of Intelligent Information Systems, 56*(1), 1–17. https://doi.org/10.1007/s10844-018-0527-5

Singh, M., Kumar, N., & Gupta, S. (2020). Artificial intelligence and cybersecurity: Challenges and future directions. *Journal of Cybersecurity and Privacy, 1*(2), 45–60. https://doi.org/10.1007/s42979-020-00005-1

Sutton, R. S., & Barto, A. G. (2018). *Reinforcement learning: An introduction*. MIT Press.