How to Cite This Article: Oleiwi, A. K. (2025). The Role of Using Artificial Intelligence Technologies in Improving Information Security: An Analytical Study on a Sample of Employees Working in the Banking Sector. *Journal of Social Sciences Review*, 5(3), 252-264. https://doi.org/10.62843/jssr.v5i3.591

Volume 5, **Issue** 3 (Summer 2025)
Pages: 252-264
ISSN (Online): 2789-4428
DOI: 10.62843/jssr.v5i3.591
Corresponding Author: Abeer Kadum Olleiwi (Email: inm.ako@atu.edu.iq)

JOURNAL OF SOCIAL SCIENCES REVIEW (JSSR)

The Role of Using Artificial Intelligence Technologies in Improving Information Security: An Analytical Study on a Sample of Employees Working in the Banking Sector

Abeer Kadhim Oleiwi [a]

Abstract: *This research aims to evaluate the impact of artificial intelligence (AI) technologies on information security in commercial banks. It focuses on understanding how these technologies contribute to enhancing protection and detection capabilities against cyber threats. The research relied on a quantitative approach, selecting a random sample of 152 accountants and technicians working in various commercial banks. Data was collected using a specially designed questionnaire and analyzed using SPSS. The results indicate a strong, positive relationship between the application of AI technologies and improved banking information security, confirming the effectiveness of these technologies in addressing growing security challenges. The research recommends that banks invest in and develop AI technologies, as well as train their staff on how to use them effectively, to ensure the highest levels of protection and security.*

Keywords: Artificial Intelligence Technologies, Information Security, Commercial Banks

Introduction

To manage and maintain the operation of any business, information is an important component. It gives a competitive edge to a business and helps it at all levels. Information safety is thus a significant concern because it is susceptible to many types of attacks. Information safety involves individuals from both within and outside the company who communicates with the system (Dhingra & Jadon, 2016). Artificial Intelligence Technology has progressed in recent years. In particular, deep learning methods have enabled people to use large datasets, achieve better results and use more capacity. This has greatly changed the lives of individuals and redefined traditional AI technologies. The AI has a diverse array of applications, including face recognition, speech recognition, and robotics, although its access image is much more spread beyond these three domains of voice, and behavior. This includes several extraordinary applications in cybercity domains, including malware monitoring and detection of infiltration. During the first stages of AI technology development, machine learning (ML) was important in addressing internet hazards. Despite its considerable capacity, the machine learning feature is very much dependent on the extraction.

This weakness is particularly clear in the field of information security. To enable a machine learning solution for malware identification, it is necessary to manually assemble several factors related to malware, which naturally reduces the effectiveness and accuracy of the danger detection. This happens because the machine learning algorithms are operated on the basis of predetermined special features, which means that predetermined features will be avoided and will remain unseen. Most machine is accidental on the accuracy of the learning algorithm's efficacy feature and the accuracy of extraction (Golovco, 2017). Due to obvious shortcomings in traditional machine learning, researchers began the discovery of Deep Neural Network (DNN), usually called deep learning (DL), which forms a subfield of machine learning. An important conceptual difference between classical machine learning and deep learning is that deep learning can be trained on raw data without direct feature extraction. In recent years, Deep Learning has realized a 20% -30% increase in performance in computer vision, voice recognition and text competition, which mark a significant progress in Artificial Intelligence Research (Deng and Yu, 2014). Dip learning can identify non -linear relationships hidden inside the data, adjust many new file formats, and can identify unseen attacks, presenting a significant edge in information security . In recent years,

[a] Al-Furat Al-Awsat Technical University, Najaf, Iraq.

deep learning information security is quite advanced in reducing weaknesses, especially in thwarting upgraded constant danger attacks. A deep nerve network (DNN) can understand the high-level abstract characteristics of advanced consistent danger (APT) attacks using the most sophisticated theft methods (Yuan, 2017).

"This research aims to analyze and evaluate the impact of artificial intelligence technologies on information security in the Iraqi banking sector". The research will seek to understand how Iraqi banks are leveraging AI tools to enhance their security defenses against growing cyber threats. The research will also analyze the challenges these banks face in adopting and implementing these technologies, in addition to exploring the potential risks of using AI in this vital sector. Although numerous global studies have examined the role of artificial intelligence in information security, there is a clear lack of research focusing on the application of these technologies in local contexts such as the Iraqi banking sector. Iraqi banks face unique challenges, including limited technological infrastructure, reliance on traditional systems, and a regulatory and legal environment that may not be fully prepared to adopt modern technologies. Therefore, the research gap lies in the absence of a comprehensive study that addresses the specific challenges and opportunities of applying artificial intelligence in information security within Iraqi banks, taking into account the specificities of the local environment.

Theoretical Background

The following section provides observation of theoretical foundation of artificial intelligence applications and information security .

Artificial Intelligence

Artificial Intelligence originated in the 1950s, and the current progress in the region has greatly affected the innovation and automation in the industry. Despite the internal benefits of AI technology, its use has ignited the discussion on potential maleist uses (Angelopoulos et al., 2020). Artificial intelligence is a domain within computer science that prepares ideas, functioning, strategies and systems to repeat and increase human feeling in the computer (Li, 2018). The aim of AI is to equip the robot with human intelligence. Machine is a technique for executing artificial intelligence using Learning algorithms that examine and receive insight from data. Deep learning machine is the technique used in learning, which facilitates the comprehensive of artificial intelligence capabilities (Ji et al., 2020). The origin of AI is established on the basis that human intelligence can be expressed properly, which allows its simulation by machines and/or software ,Artificial intelligence includes subjects such as thinking, knowledge, planning, automation, machine learning, natural language processing, robotics, human cognition and cyber security (Trifonov et al., 2018) The AI app offers an interdisciplinary convergence with cyber security challenges. As AI technologies improve and spread, cyber-attacks against cyber-physical systems are increasing, capitalization on interfaces between physical and cyber components (Brundage, 2018) The danger environment incorporates many actors, in which the attackers target diverse weaknesses to carry out their attacks. These attacks include advanced persistent hazards and sophistication, nefarious activities in cyberspace and commercialization of cybercrime (Kaloudi, 2020). The cyber security community should understand the use of AI in cyber-halls and understand its weaknesses to execute defensive measures (Novikov, 2019)

Artificial intelligence techniques

Combating cybercrime requires smart, effective, adaptable tools that offer cost-effective solutions. Therefore, the primary goal of cyber security companies has become developing tools capable of detecting and preventing breaches in real time. Some of the most prominent applications of artificial intelligence are as follows

Artificial Neural Networks: "An artificial nerve network is an information processing system created after the biological brain network. The nerve networks are construction made of several processing units (neurons), executing each basic numerical operations and spreads results for adjacent units through

weighted connections. Most infiltration systems using artificial nerve networks use two types of neural networks: multilayer feed forward neural networks and self-resulting maps of Kohon'' (Veselý, 2009). Alan Bivence et al. Used a system using self-sermon, which has shown efficacy in the automatic grouping and visual organization. Their technique is a modular-based network ID that analyzes TCPDUP data and develops window traffic intensity patterns. The educational method employs an architectural learning phase (Bivens et al., 2002). ''Burman and Khatainar used an intrusion and used an artificial nerve network (ANN) using backpragation as a prevention system (IDP). Ann-Based IDPS KDD99 will use 41 characteristics of an intrusion signature from a dataset'' (Barman et al., 2012) Min and Kang developed a system of detecting an advanced intrusion (IDS) using a deep nerve network (DNN) to increase the safety of the in-vehicle network (IDS). Mehdi and Mohammed are in appearance. A multi-layer perceptron (MLP) is used to detect infiltration using an offline analytical approach. The purpose of their project is to deal with a multi-class issue in which the identified neural network matches the nature of the attack (Moradi& Mohammad, 2004)

Artificial Immune Systems: Artificial immune system (AIS) was inspired by strong, decentralized, error-poisoning and adaptable characteristics of the human immune system (Aziz et al., 2012) ''They include their chemicals, cells and tissue that provide resistance to the human body against infections caused by viruses and other pathogens. AIS can identify and eliminate many infections from self-cells. This serves as an excellent source of inspiration for the protection of computer systems, especially infiltration detection systems (IDS). ''The first researchers of this domain include farmers, pacords and parrelson. Their algorithm depicts a functioning to detect changes predicted on the production of T-cells inside the immune system. In 1994, the Forest and his team at the University of New Mexico began research to develop an intrusion detection system (IDS) using the Artificial immune system (AIS). He presented a negative selection technique to take advantage of his procedure for the process of detecting an advanced discrepancy''(Forrest et al., 1987). Liu et al. (2011) Offer an intrusion approach to IOT that mimics itself and non-self-entertainment. Evolution detectors, mature detectors and memory detectors develop dynamically to thwart infiltration. Their system provides a novel approach to detect infiltration into the IOT environment (Liu et al., 2011).

Machine Learning: Researchers are using machine learning approaches to detect network infiltration due to their generalization capabilities, which facilitate the understanding of infiltration of predetermined pattern (Panda et al., 2011). There are two categories of machine learning techniques: single classifier and hybrid classifier (Zuma et al., 2015) In their study, provide a comprehensive description of machine learning methods. The future of machine learning is still in its newborn stages, which estimates the infiltration and prevention systems, which estimates many scientific progresses.

Fuzzy Logic and Fuzzy Sets: Zadeh proposed a fuzzy set theory to address uncertainty. Fuzzy logic is a rule-based system that takes advantage of the practical expertise of an operator, effectively surrounds the knowledge of experienced physicians. FL functioning simulates human decision making by incorporating all intermediate options that ranges from 0 to 1. Jongsubsuk et al. (2013) suggested a system of detecting a network intrusion using a ''fuzzy genetic algorithm. Fuzzy rules are used to classify network attack data, while a genetic algorithm serves as an adaptation technique that helps identify appropriate fuzzy rules and provide an ideal answer''(Chimfly et al., 2006). Clustering analysis introduced fuzzy Rough C-Mines (FRCM). Conclusions obtained from performance are much better than K-means approaches.

Genetic Algorithms: Genetic algorithms integrate the principles of Darwinian theory. He took inspiration from biological development, natural selection and genetic rebuilding. Genetic algorithms can be used to develop fundamental principles for network traffic. GA prepares a collection of rules that can be used to differentiate between regular and pathological network traffic later. Methods of generating these data sets use a chromosome -like data structure and develop chromosomes using selection, regeneration and mutation operators. Li (2004) presented an intrusion detection system (IDS) with 57 genes inside chromosomes, an eccentric connection characteristic with each gene, such as source IP address, destination IP address, source port, destination port, period, protocols, bights sent by promoter, and

sended by bites, among others. As a result of the efficacy of the assessment ceremony, the latter population is diagonal to the rules that match with aggressive connections.

Goyal and Kumar (2008) proposed a systematic teaching system, called the genetic algorithm (GA), which is to detect fraudulent nodes. The program evaluates several features of network connections including protocol types, network service, network service, and connection state to prepare type-based rules. Ozugo et al. Rules-based infiltrators "have used genetic algorithms to create systems. His research employs a genetic algorithm-based functioning that uses a collection of classification rules obtained from data network audit and uses a support confidence structure as a fitness function to assess the quality of each rule. The software implementation system tries to increase network security to ensure the privacy, integrity and availability of resources" (Ojugo et al., 2012). A GNP-based fuzzy membership presented to identify dangers, attacks or intrusion on the Internet These approaches address both discomfort and continuous features and can be used in a flexible manner for various types of attacks (Emmannavar et al., 2015).

Intelligent Agents: Agents are autonomous, problem-making computational institutions that can work well in dynamic and open contexts (**Luck et al., 2003**). Agents are often assigned to references where they interact and cooperate with other agents, including people and software, which may be entitled to anti - purposes. In 2012, Ganpathy et al. Introducing an approach that integrates an intelligent agent-based Wasted Destance Outlair Detection (IAWDBOD) algorithm with an intelligence agent-based enhanced enhanced multiclass support vector machine (IAEMSVM) algorithm.

Information Security

The concept of information safety is defined as availability, integrity, privacy and conservation of ownership of information, while it is defined unauthorized use, sabotage, deception, deformation, change, misinterpretation, deletion, misuse, misuse, or informally accession, monitoring, duplication, or theft (Al-Ta'I & AlKilani, 2015) In addition, it is characterized by conservation of privacy, integrity and availability of information, while the information safety management system is described as organized tasks aimed at directing and controlling the availability of privacy, integrity and information (Tipton, 2019). Information safety forces illegal access, misuse, disclosure to irrelevant parties, or security and information systems of information and information systems against corruption and change of data (Rossouw, & Niekerk, 2013). This involves distorting and destroying information to maintain the user's confidence and organizational integrity. Additionally, it refers to procedures that protect legitimate organizational information from theft, unauthorized amendments, changes or use (Kritzinger & Smith, 2008). This promotes the ongoing confidence of the beneficiaries in the organization, its integrity and the ability to restore that trust. (Alghizzawi et al., 2023)

Information process has significant importance in information safety management due to their work in increasing the proficiency of experts in information safety management and increasing the proficiency of experts in the protection of data and information (McIlwraith, 2021). The company guarantees information protection by optimizing the ongoing training, information management and recovery and starting with the latest progress. Training workforce improves productivity and equips the personnel for educational programs. It cultivates students' analytical and investigative abilities, in which outsourcing works aimed at identifying a competent organization and replacing leadership.

This includes the preventive protocol implemented by the organization to ensure information privacy and a series of measures implemented by the organization. It involves protection against internal and external threats, including theft, manipulation, unauthorized access, or destruction, confirming the entries, secures them in a safe place, first, or after data entry, in a safe place, and nominate the personnel authorized to manage this data. As a result, the security of data during admission in system and information protection includes transmission within organization, storage and use. In addition, the expected elements of information safety are accidental on the nature of information, its applications and the nature of the related services. All information is not required for the same level of privacy to prevent

unauthorized disclosure, nor is there all information within the same feature of equal importance about access or safety against tampering (Al-Najjar, 2018).

Information Security Dimensions

There are different approaches on information protection, in which legal experts identify three dimensions: integrity, privacy and availability. It was referred to as a CIA triangle. Chapel et al. (2018) has used these three primary dimensions of information security:

i. **Integrity:** The concept of dependence, validity and integrity on data prevents unauthorized changes, ensuring its accuracy, untouched state and security. When safety measures are effectively implemented, they convenience permission amendments, protecting intentionally and harmful activities, such as viruses and spams, as well as errors made by authorized users.

ii. **Confidentiality:** It refers to the protocols used to protect the privacy and safety of data, goods or resources. The purpose of privacy security is to reduce or reduce illegal access to data. The purpose of privacy and security protocol is to guarantee that only the nominated receiver of communication receives it. Privacy enables individuals to reach and attach resources. Nevertheless, it hinders unpublished individuals from doing so. A diverse array of safety measures can protect privacy, in which encryption, access range and information are not limited to hiding.

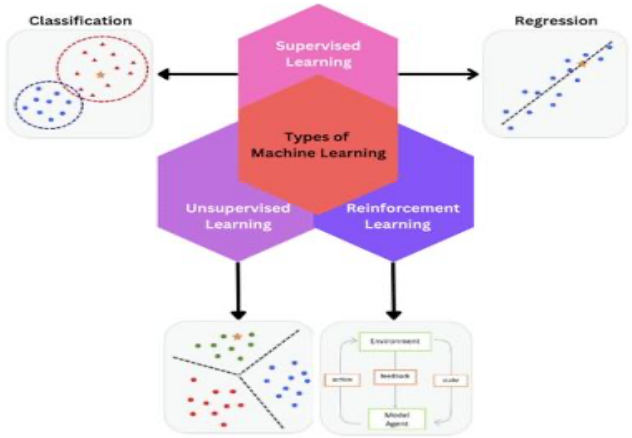
iii. **Availability:** It gives each authorized individual early quick and continuously access to goods. Availability protection rules often provide sufficient bandwidth and rapid processing by the organization or reference. If the security mechanism emphasizes availability, it will provide a high degree of assurance that data, objects, and resources are accessible to authorized users. Availability includes efficient, uninterrupted access to resources and the prevention of denial-of-service (DoS) attacks. Furthermore, this indicates that the foundational infrastructure may get legitimate access to data services, communication, and access control methods for both operational and authorized users.

AI and information security

"Artificial intelligence involves the manufacture of computer systems capable of performing activities that often require human intelligence, such as learning, problem-solving and decision. The concept of artificial intelligence varies in several decades. Artificial intelligence is a concept with flexible borders, which emphasizes the origin of the material above the special vocabulary, highlighting the freedom of the language of its definitions and the progressive formation of its unique meaning (Chowdhary et al. 2020) Artificial intelligence is a branch of science and technology that focuses on creating intelligent machines designed to automate manual jobs, so affects many industries deeply by increasing efficiency and production. Wang et al. (2019) Define AI as a basic course in computer science, widely integrated into many engineering subjects. It incorporates domains such as automation, language interpretation, robotics and other specialist systems, highlighting the adaptability of AI and its widespread prevention in many fields. Artificial intelligence includes machine learning methods, including supervised, unheard, and reinforcement learning, within the information safety domain. Supervised learning completes training models using labeled datasets to create tasks that combine inputs with specified results. Uncontrolled learning examines the pattern in unbelled data, facilitating the automated organization of data in the cluster without previous classification or classification (Alloghani, 2020). Strengthening Learning (RL) employs a reward-based structure to make an option in dynamic settings, addresses adaptation challenges by adapting adaptation challenges through environmental interactions. Later Figure (1) depicts the primary categories of machine learning. This study examines important safety hazards associated with the use of artificial intelligence in information protection, including sensitivity to adverse attacks (Chakraborty, 2021)

Figure 1

Types of ML algorithms



Methodology

Study Design

This study is descriptive and interpretive, aiming to understand the phenomenon as it exists in its natural environment. A quantitative approach was adopted to collect and analyze data. In terms of timescale, this study is classified as cross-sectional, meaning it analyzes data at a specific point in time.

Population and data collection

The research relied on collecting primary data from a questionnaire as the primary tool for the study, addressing various analytical aspects related to its topics. The questionnaire included a number of statements that reflected the study's variables, thereby achieving its objectives. The questionnaire reflected the study's variables and dimensions, including the independent variable (artificial intelligence technologies) and the dependent variable (information security). It was distributed to Technical and accounting staff working in commercial bank branches in Babil Governorate, numbering (247) employees distributed over 10 branch banks in Babylon.

Sample Of Study

The study population is represented by a sample of commercial bank branches in Babil Governorate, consisting of (247) Technical and accounting staff working in commercial bank branches in Babil Governorate. A random sample of (152) out of (247) was selected. However, the researcher intended to distribute (152) questionnaires as a precautionary measure to ensure the representation of the community. (150) questionnaires were retrieved and were valid for statistical analysis. Table No. (1) shows the distribution of the study population and the study sample among commercial banks. Table No. (1) shows the number of employees in the branches of commercial banks in Babil Governorate.

Table 1

The Sample and Population Size

NO.	Bank name	IT employee	Sample size
1	Rafidain Bank 299	45	29
2	Rashid Bank	39	26
3	Trade Bank of Iraq	22	12
4	Bank of Baghdad	14	9
5	Gulf Commercial Bank	13	8
6	Real Estate Bank	33	20
7	Al-Tayf Islamic Bank	12	7
8	Industrial Bank	34	21
9	Agricultural Bank	26	13
10	National Bank of Iraq	9	7
Total		247	152

Testing Measurement Model

Cronbach's alpha is used to calculate reliability and stability coefficients for survey instruments that use Likert-type response sets. Cronbach's alpha estimates the reliability of the tool's responses (questionnaire) as assessed by the subjects, indicating overall reliability of the tools. In this regard, (Sekaran ,2003) indicates that there is consensus that research requires a Cronbach's coefficient greater than or equal to 0.70. The results in Table (2) indicate that the artificial intelligence techniques axis recorded a high reliability value of 0.898, while the information security axis also recorded a high reliability value of 0.857. The overall reliability value reached 0.967. Hence, it is clear that the variables met the requirements for all items.

Table 2

Testing Measurement Model

Items	Conbach's alpha	Reliability coefficient
Artificial Neural networks	0.908	0.952
Artificial Immune Systems	0.938	0.968
Machine learning	0.879	0.937
Fuzzy logic and fuzzy sets	0.891	0.943
Genetic Algorithms	0.882	0.939
Intelligent agents	0.895	0.946
AI techniques	**0.898**	0.947
Integrity	0.826	0.928
Confidentiality	0.887	0.941
Availability	0.860	0.927
Information Security	**0.857**	0.925

Deceptive Statistics

This paragraph is concerned with stating the level of response of the individuals of the researched sample to the questionnaire axes in an attempt to answer the study questions, where the five-point Likert scale was used, with 5 being the highest value and 1 being the lowest value.

Deceptive Statistics for AI Techniques

Table 3

Deceptive Statistics for AI Techniques

Items	Mean	SD	Significance
Artificial Neural networks	3.891	0.861	77.40
Artificial Immune Systems	3.919	0.865	78.38
Machine learning	3.909	0.892	78.17
Fuzzy logic and fuzzy sets	3.959	0.910	79.18
Genetic Algorithms	3.977	0.909	79.53
Intelligent agents	3.943	0.908	78.86
TOTAL	78.58	0.890	3.933

Based on Table 3, the results highlight a positive and high evaluation of all the studied technologies. Overall, all dimensions received high average scores approaching 4, indicating that participants view these technologies as important and valuable. Genetic Algorithms received the highest average score (3.977) and the highest importance score (79.53), making it the most important of all the mentioned technologies. Fuzzy Logic came in second in importance with an average score of 3.959 and an importance score of 79.18, confirming its role as a key component of the study. Artificial Neural Networks (ANNs) appeared: Despite receiving the lowest average score (3.891), it still achieved a high importance score (77.40), indicating its importance despite its slightly lower rating compared to the other technologies. Intelligent learning, machine learning, and artificial immune systems received ratings very close to each other, indicating their close and perceived importance. Standard Deviation: The standard deviation for all dimensions was

relatively low, approaching 0.900, meaning that participants' opinions were relatively close to each other regarding the importance of each dimension, and there was not much variation in the answers.

Deceptive Statistics for Information Security

Table 4

Deceptive Statistics for Information Security

Items	Mean	SD	Significance
Integrity	3.801	0.88	76.02
Confidentiality	3.943	0.907	78.86
Availability	3.829	0.898	76.57
TOTAL	3.857	0.895	77.15

Table 4 shows the results of an analysis of three main dimensions of information security: integrity, confidentiality, and availability. These dimensions were measured using mean, standard deviation (SD), and significance. Confidentiality also showed the highest mean score of 3.943, indicating that study participants consider confidentiality the most important element of the three dimensions. The importance score of 78.86, the highest in the table, confirms this conclusion. The standard deviation of 0.907 indicates moderate variance in participants' opinions on this dimension. Availability came in second with a mean of 3.829, indicating that it is also considered important, but slightly less important than confidentiality. The importance score was 76.57, reinforcing its position as second most important. The standard deviation of 0.898 indicates that participants' opinions were relatively close. Integrity had the lowest mean score of 3.801 and the lowest importance score of 76.02. This does not mean that it is unimportant, but it is considered relatively less important compared to confidentiality and availability in the context of this study. The standard deviation of 0.880 is the lowest among the three dimensions, indicating greater agreement among participants on the assessment of this dimension.

Hypothesis Testing and Analysis

This section is concerned with testing the hypotheses of influence in order to determine the possibility of judging them as acceptable or rejected. Regression coefficients and structural modeling will be relied upon for the purpose of testing simple regression and structural modeling.

i. **There is a statistically significant effect between artificial neural network and information security.**

Table 5

The Impact of Artificial Neural Networks on Information Security

Independent Variable	α	β	(R^2)	F	P-Value	Dependent variable
Artificial Neural network	1.746	0.52	0.459	137.331	0.000	Information security

Depend on Table (5) Beta coefficient (β) = 0.52: This coefficient indicates a strong direct relationship between the two variables. This means that the greater the interest or application in artificial neural networks, the greater the interest in information security. Coefficient of determination (R^2) = 0.459: This coefficient shows that 45.9% of the variance in information security can be explained by artificial neural networks. This result indicates that artificial neural networks are an important and influential factor in determining the level of information security, and that the remaining factors (about 54.1%) are due to other variables not included in this model. F-value = 137.331: This high value shows that the regression model is statistically significant, meaning that the relationship between the two variables is not due to chance. P-value = 0.000: Since this value is lower than the standard significance level (0.05), we conclude that the relationship between the two variables is very statistically significant. This allows us to reject the null hypothesis that there is no relationship between the two variables, and accept the alternative hypothesis that there is a relationship.

ii. **There is a statistically significant effect between Artificial Immune Systems and information security**

Table 6

The Impact of Artificial Immune Systems on information security

Independent Variable	α	β	(R^2)	F	P-Value	Dependent variable
Artificial Immune Systems	1.438	0.616	0.517	173.2	0.000	Information security

The statistical analysis results presented in Table (6) indicate a positive and statistically significant relationship between artificial immune systems and information security. Beta coefficient (β) = 0.616: This figure demonstrates a strong direct relationship. This means that with every increase in the use or development of artificial immune systems, the level of information security increases. Coefficient of determination (R2) = 0.517: This coefficient indicates that 51.7% of the variance in information security can be explained by artificial immune systems. This is a high percentage and confirms that artificial immune systems are a significantly influential factor in achieving information security. F-value = 173.2: The high F-value confirms that the statistical model as a whole is statistically significant, meaning that the relationship is not the result of chance. P-value = 0.000: Since this value is less than the significance level (0.05), the relationship between the two variables is very statistically significant. This confirms the real and tangible impact of artificial immune systems on information security.

iii. **There is a statistically significant effect between Machine learning and information security**

Table 7

The Impact of Machine Learning on Information Security

Independent Variable	α	β	(R^2)	F	P-Value	Dependent variable
Machine learning	1.66	0.616	0.545	194.158	0.000	Information security

Based on the results of the linear regression analysis shown in Table 7, the relationship between machine learning (as an independent factor) and information security (as a dependent factor) can be analyzed. Analysis of the Results Beta coefficient (β) = 0.616: This value indicates a strong positive relationship between the two variables. This means that the greater the interest in or application of machine learning, the higher the level of information security. Coefficient of determination (R^2) = 0.545: This coefficient shows that 54.5% of the variance in information security can be explained by the variance in machine learning. This is a very high percentage and confirms that machine learning has a significant and specific impact on information security. F value = 194.158: A very high F value indicates that the statistical model is highly statistically significant, meaning that the relationship between the two variables is not due to chance. P-value = 0.000: Since this value is less than the standard significance level (0.05), we conclude that the relationship between the two variables is very strongly statistically significant. This allows us to reject the null hypothesis that there is no relationship.

iv. **There is a statistically significant effect between Fuzzy logic and fuzzy sets and information security**

Table 8

The Impact of Fuzzy Logic and Fuzzy Sets on Information Security

Independent Variable	α	β	(R^2)	F	P-Value	Dependent variable
Fuzzy logic and fuzzy sets	1.48	0.6	0.567	212.512	0.000	Information security

According to Table (8), accurate conclusions can be drawn about the relationship between fuzzy logic and fuzzy sets as the independent variable, and information security as the dependent variable. Analysis of the results Beta coefficient (β) = 0.6: This coefficient indicates a strong direct relationship. In other words, the more fuzzy logic is applied or used, the higher the level of information security. Coefficient of determination (R^2) = 0.567: This value shows that 56.7% of the variance in information security can be explained by the variance in fuzzy logic and fuzzy sets. This high percentage indicates that the independent variable has a significant and specific effect in predicting changes in information security. F value = 212.512: The very high F value indicates that the statistical model is highly statistically significant, meaning that the relationship between the two variables is not due to chance. P-value = 0.000: Since this value is less

than the standard significance level (0.05), we conclude that the relationship between the two variables is very strongly statistically significant. This allows us to reject the null hypothesis that there is no relationship.

v. There is a statistically significant effect between Genetic Algorithms and information security

Table 10

The Impact of Genetic Algorithms Sets on Information Security

Independent Variable	α	β	(R^2)	F	P-Value	Dependent variable
Genetic Algorithms	1.46	0.5	0.627	216/422	0.000	Information security

The statistical analysis results in Table 9 indicate a strong, direct relationship between genetic algorithms and information security Analysis of the results: Beta coefficient (β) = 0.5: This coefficient shows that there is a strong, direct relationship between the two variables. The more genetic algorithms are used, the higher the level of information security. Coefficient of determination (R^2) = 0.627: This value shows that 62.7% of the variance in information security can be explained by genetic algorithms. This very high percentage confirms that genetic algorithms have a significant and influential impact on information security. F-value = 216.422: A high F-value indicates that the statistical model is highly statistically significant, meaning that the relationship between the two variables is not due to chance. P-value = 0.000: Since this value is lower than the standard significance level (0.05), we conclude that the relationship between the two variables is very strongly statistically significant.

vi. There is a statistically significant effect between Intelligent agents and information security.

Table 11

The Impact of Intelligent Agents Sets on Information Security

Independent Variable	α	β	(R^2)	F	P-Value	Dependent variable
Intelligent agents	1.539	0.484	0.570	197.131	0.000	Information security

Based on the results of the linear regression analysis shown in Table 10, the relationship between Intelligent agents as the independent variable and information security as the dependent variable can be interpreted. The results show a beta coefficient (β) = 0.484: This value indicates a strong direct relationship. This means that the greater the attention or application of Intelligent agents, the higher the level of information security. Coefficient of determination (R^2) = 0.570: This value shows that 57.0% of the variance in information security can be explained by the variance in Intelligent agents. This high percentage confirms that Intelligent agents have a significant and specific impact on information security. F-value = 197.131: This very high F-value indicates that the statistical model is highly statistically significant, meaning that the relationship between the two variables is not due to chance. P-value = 0.000: Since this value is lower than the standard significance level (0.05), we conclude that the relationship between the two variables is very strongly statistically significant.

vii. There is a statistically significant effect between AI techniques and information security

Table 12

The Impact of AI Techniques on Information Security

Independent Variable	α	β	(R^2)	F	P-Value	Dependent variable
AI techniques	0.918	0.735	0.673	333.765	0.000	Information security

Table 11, which explains the relationship between the independent variable, artificial intelligence technologies, and the dependent variable, information security, reveals that the beta coefficient (β) = 0.735: This value indicates a very strong direct relationship. This means that the greater the application or use of artificial intelligence technologies, the greater the level of information security. The coefficient of determination (R^2) = 0.673: This value shows that 67.3% of the variance in information security can be explained by the variance in artificial intelligence technologies. This very high percentage confirms that artificial intelligence technologies have a significant and specific impact on information security. The F-

value = 333.765: This very high F-value indicates that the statistical model is very statistically significant, meaning that the relationship between the two variables is not due to chance. The probability value (P-value) = 0.000: Since this value is less than the standard significance level (0.05), we conclude that the relationship between the two variables is very statistically significant. This allows us to reject the null hypothesis that there is no relationship.

Result and Discussion

The results show that each dimension of the analyzed AI technologies (neural networks, immune systems, machine learning, fuzzy logic, genetic algorithms, and intelligent agents) has a positive and significant impact on information security. This impact is not merely a coincidence; it is statistically proven through P-values, which were always 0.000, confirming the significance of the results. Beta Coefficients (β): The beta coefficient values range between 0.484 and 0.735, indicating a strong positive relationship between each AI technology and the level of information security. The more these technologies are implemented, the more organizations are able to enhance their information security. Coefficient of Determination (R^2): The coefficient of determination values range between 0.459 and 0.673. This means that between 45.9% and 67.3% of the variance in information security can be explained by the aforementioned independent variables. This high percentage confirms that AI technologies are not merely facilitators, but rather essential determinants of the level of information security. Ranking by Impact AI technologies can be ranked according to their impact on information security, from most to least, based on R^2 values: AI technologies (combined): have the highest impact with R^2 = 0.673. This confirms that using these technologies together yields the best results in enhancing information security. Genetic algorithms: R^2 = 0.627. Considered among the most influential individual technologies. Fuzzy logic and fuzzy sets: R^2 = 0.567. They have a strong impact similar to that of intelligent agents. Intelligent agents: R^2 = 0.570. Machine learning: R^2 = 0.545. Artificial immune systems: R^2 = 0.517. Artificial neural networks: R^2 = 0.459. Although they have the least impact, their effect is still strong and statistically significant. Conclusion: Overall, the results show that AI technologies combined have the greatest impact on information security, reflecting the importance of integration between these technologies. Each technology individually contributes to enhanced security, with genetic algorithms considered the best performer. These results confirm that integrating AI technologies into information security strategies is not an option, but rather a necessity to enhance protection against growing threats.

Recommendations

1. Commercial banks should continue to support and integrate AI technologies. This ensures advanced and continuous protection against evolving cyber threats, enhancing customer confidence and preserving the integrity of their financial and personal data.
2. Banks are required to improve the ability of their security systems to analyze big data related to network traffic using AI technologies. This enables them to detect suspicious activities or potential attacks in real time and respond to them proactively and effectively.
3. Banks must invest in training their employees on how to use and manage AI-based information security systems. This includes understanding how to analyze the alerts generated by these systems and making sound decisions based on their recommendations, to ensure the full potential of these technologies is fully utilized.
4. It is recommended to establish specialized information security units or teams within banks, whose primary mission is to implement, monitor, and manage AI-based security solutions. This ensures clear channels for maximizing the benefits of these technologies and developing them to meet emerging threats.

References

Al-Kilani, M. A. (2015). *Information Security Management*. Dar AlThaqafah for Publishing and Distribution.

Al-Najjar, F. J. (2018). *Management information systems, an administrative perspective*. Dar Al-Hamid for Publication and Distribution.

Alghizzawi, M., Ahmed, E., Alshaketheep, K., Alkhlaifat, B. I., & Alnawafleh, H. (2023). Rival influences of Airbnb digital platforms on the Jordanian hotels market. *Migr. Lett*, *20*(8), 134–144.

Alloghani, M., Al-Jumeily, D., Mustafina, J., Hussain, A., & Aljaaf, A. J. (2020). A systematic review on supervised and unsupervised machine learning algorithms for data science. *Supervised and unsupervised learning for data science*, 3-21. https://doi.org/10.1007/978-3-030-22475-2_1

Angelopoulos, A., Michailidis, E. T., Nomikos, N., Trakadas, P., Hatziefremidis, A., Voliotis, S., & Zahariadis, T. (2019). Tackling faults in the Industry 4.0 era-A survey of machine-learning solutions and key aspects. *Sensors (Basel, Switzerland)*, *20*(1), 109. https://doi.org/10.3390/s20010109

Aziz, A. S. A., Salama, M., ella Hassanien, A., & Hanafi, S. E. O. (2012, September). Detectors generation using genetic algorithm for a negative selection inspired anomaly network intrusion detection system. In *2012 Federated Conference on Computer Science and Information Systems (FedCSIS)* (pp. 597-602). IEEE.

Barman, D., & Kumar, G. (2012). Design of intrusion detection system based on artificial neural network and application of rough set. *International Journal of Computer Science and Communication Networks*, *2*(4), 548–552.

Bivens, A., Palagiri, C., Smith, R., Szymanski, B., & Embrechts, M. (2002). Network-based intrusion detection using neural networks. *Intelligent Engineering Systems through Artificial Neural Networks*, *12*(1), 579–584.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., ... & Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. *arXiv preprint arXiv:1802.07228*. https://doi.org/10.48550/arXiv.1802.07228

C. Liu, J. Yang, Y. Zhang, R. Chen and J. Zeng, "Research on immunity-based intrusion detection technology for the Internet of Things," Seventh International Conference on Natural Computation, 2011.

Chakraborty, A., Alam, M., Dey, V., Chattopadhyay, A., & Mukhopadhyay, D. (2021). A survey on adversarial attacks and defences. *CAAI Transactions on Intelligence Technology*, *6*(1), 25-45. https://doi.org/10.1049/cit2.12028

Chapple, M., Stewart, J. M., & Gibson, D. (2018). *ISC) 2 CISSP certified information systems security professional official study guide*. John Wiley & Sons.

Chimphlee, W., Abdullah, A. H., Sap, M. N. M., Srinoy, S., & Chimphlee, S. (2006, November). Anomaly-based intrusion detection using fuzzy rough clustering. In *2006 International Conference on Hybrid Information Technology* (Vol. 1, pp. 329-334). IEEE.

Chowdhary, K. R. (2020). *Fundamentals of artificial intelligence.* Springer. https://doi.org/10.1007/978-81-322-3972-7

Deng, L., & Yu, D. (2014). Deep learning: methods and applications. *Foundations and trends® in signal processing*, *7*(3–4), 197-387. http://dx.doi.org/10.1561/2000000039

Dhingra, M., Jain, M., & Jadon, R. S. (2016). Role of artificial intelligence in enterprise information security: A review. *2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC)*.

Forrest, S., Hofmeyr, S. A., & Somayaji, A. (1997). Computer immunology. *Communications of the ACM*, *40*(10), 88–96. https://doi.org/10.1145/262793.262811

Golovko, V. A. (2017). Deep learning: an overview and main paradigms. *Optical Memory and Neural Networks*, *26*, 1–17. https://doi.org/10.3103/S1060992X16040081

Immannavar, M., Pujar, P. M., & Suryavanshi, M. (2015). An Intrusion Detection Model Based on Fuzzy Membership Function Using GNP. *International Journal of Research in Engineering and Technology*, *4*(8), 27-32.

Ji, H., Alfarraj, O., & Tolba, A. (2020). Artificial intelligence-empowered edge of vehicles: architecture, enabling technologies, and applications. *IEEE Access*, *8*, 61020-61034. https://doi.org/10.1109/ACCESS.2020.2983609

Jongsuebsuk, P., Wattanapongsakorn, N., & Charnsripinyo, C. (2013, May). Real-time intrusion detection with fuzzy genetic algorithm. In *2013 10th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology* (pp. 1-6). IEEE.

Juma, S., Muda, Z., Mohamed, M. A., & Yassin, W. (2015). MACHINE LEARNING TECHNIQUES FOR INTRUSION DETECTION SYSTEM: A REVIEW. *Journal of Theoretical & Applied Information Technology*, *72*(3).

Juma, S., Muda, Z., Mohamed, M. A., & Yassin, W. (2015). MACHINE LEARNING TECHNIQUES FOR INTRUSION DETECTION SYSTEM: A REVIEW. *Journal of Theoretical & Applied Information Technology*, *72*(3).

Kaloudi, N., & Li, J. (2020). The ai-based cyber threat landscape: A survey. *ACM Computing Surveys (CSUR)*, *53*(1), 1-34. https://doi.org/10.1145/3372823

Kritzinger, E., & Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. *Computers & Security*, *27*(5–6), 224–231. https://doi.org/10.1016/j.cose.2008.05.006

Li, J. H. (2018). Cyber security meets artificial intelligence: a survey. *Frontiers of Information Technology & Electronic Engineering*, *19*(12), 1462-1474. https://doi.org/10.1631/FITEE.1800573

Li, W. (2004). Using genetic algorithm for network intru sion detection. *Proceedings of the United States department of energy cyber security group*, *1*(1), 8. http://bit.csc.lsu.edu/~jianhua/krish-1.pdf

Luck, M., McBurney, P., & Preist, C. (2003). *Agent technology: enabling next generation computing (a roadmap for agent based computing)*. AgentLink. https://eprints.soton.ac.uk/257309/1/al2roadmap.pdf

McIlwraith, A. (2021). *Information security and employee behaviour: How to reduce risk through employee education, training and awareness* (2nd ed.). https://doi.org/10.4324/9780429281785

Moradi, M., & Zulkernine, M. (2004, November). A neural network based system for intrusion detection and classification of attacks. In *Proceedings of the IEEE international conference on advances in intelligent systems-theory and applications* (pp. 15-18). IEEE Lux-embourg-Kirchberg, Luxembourg.

Novikov, I. (2018). How AI can be applied to cyberattacks. *Retrieved Novemb*, *25*, 2019.

Ojugo, A. A., Eboka, A. O., Okonta, O., Yoro, R., & Aghware, F. (2012). Genetic algorithm rule-based intrusion detection system (GAIDS). *Journal of Emerging Trends in Computing and Information Sciences*, *3*(8), 1182-1194.

Panda, M., Abraham, A., Das, S., & Patra, M. R. (2011). Network intrusion detection system: A machine learning approach. *Intelligent Decision Technologies*, *5*(4), 347–356. https://doi.org/10.3233/idt-2011-0117

PK, F. A. (1984). What is artificial intelligence?. *Success is no accident. It is hard work, perseverance, learning, studying, sacrifice and most of all, love of what you are doing or learning to do*, *65*, 85-108.

Tipton, H. (2019). *Information security management handbook: Volume IV* (H. Tipton & M. KrauseBoca Raton, Eds.; 4th ed.). https://doi.org/10.1201/9780203325438

Trifonov, R., Nakov, O., & Mladenov, V. (2018, December). Artificial intelligence in cyber threats intelligence. In *2018 international conference on intelligent and innovative computing applications (ICONIC)* (pp. 1-4). IEEE. https://doi.org/10.1109/ICONIC.2018.8601235

Veselý, A., & Brechlerova, D. (2009). Neural networks in intrusion detection systems. *Agricultural Economics*, *50*, 35-50. https://www.agriculturejournals.cz/pdfs/age/2004/01/06.pdf

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, *38*, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Wang, P. (2019). On defining artificial intelligence. *Journal of Artificial General Intelligence*, *10*(2), 1–37. https://doi.org/10.2478/jagi-2019-0002

Yuan, X. (2017, May). Phd forum: Deep learning-based real-time malware detection with multi-stage analysis. In *2017 IEEE International Conference on Smart Computing (SMARTCOMP)* (pp. 1-2). IEEE. https://doi.org/10.1109/SMARTCOMP.2017.7946997