International Journal of Scientific Research and Engineering Development-– Volume 9 Issue 1, Jan-Feb 2026
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

ARTIFICIAL INTELLIGENCE TECHNOLOGIES AND THEIR ROLE IN ACHIEVING CYBERSECURITY AND DETECTING FINANCIAL AND ACCOUNTING FRAUD IN ELECTRONIC BANKING

[1]Dr.Mohammed Sadeq Jappar
(Auditing and oversight, University Kufa, and Place Iraq - Najaf
Email: Mohammeds.Kadhim@uokufa.edu.iq)

----------**********----------

Abstract:

This study aims to analyze the impact of utilizing artificial intelligence (AI) technologies in enhancing cybersecurity and improving financial performance in Iraqi electronic banks. The research focuses on three leading institutions: the Iraqi National Bank, the Iraqi Islamic Commercial Bank, and First Iraq Bank. A correlation and regression analysis methodology was adopted to measure the relationship between AI application indicators (liquidity management, capital management, asset management, and intelligent data analysis) and financial and security performance indicators.

The findings revealed that AI applications in liquidity management and intelligent data analysis had a positive and significant effect on cybersecurity and financial performance, contributing to the detection of financial and accounting fraud and strengthening operational control. In contrast, capital and asset management indicators showed negative and significant relationships, reflecting the limitations of traditional approaches in addressing digital challenges and highlighting the need to integrate AI tools to overcome such constraints. Furthermore, the coefficient of determination (R^2) indicated that AI technologies explain approximately 95% of the variations in cybersecurity and financial performance, confirming the robustness of the statistical model employed.

Based on these results, the main hypothesis of the study was validated: the use of AI technologies is significantly associated with improving cybersecurity levels in Iraqi electronic banks. This underscores that AI represents a strategic tool rather than a mere technical option, and its adoption is essential for achieving financial sustainability and strengthening trust in the digital banking environment.

Keywords — **Artificial Intelligence, Machine Learning, Genetic Algorithms, Intelligent Agents, Financial Fraud.**

----------**********----------

I. INTRODUCTION

The contemporary world is witnessing rapid developments in digital technology, with artificial intelligence (AI) emerging as one of the most influential tools that has transformed various economic and financial sectors. As reliance on electronic systems in managing banking operations continues to grow, the urgent need to strengthen cybersecurity has become evident in order to address the challenges and risks associated with digital transformation, particularly in light of the increasing frequency of cyberattacks and financial fraud schemes.

In this context, Iraqi electronic banks—such as the Iraqi National Bank, the Iraqi Islamic Commercial Bank, and First Iraq Bank—are under mounting pressure to adopt advanced technologies that ensure the protection of customer data and the stability of financial operations. AI is regarded as a strategic tool capable of enhancing risk management efficiency

through its ability to analyze big data, detect fraudulent patterns, and predict future risks, thereby contributing to greater customer trust and improved financial performance indicators.

The significance of this study lies in its attempt to examine the relationship between the use of AI technologies and the improvement of cybersecurity levels in these electronic banks. This is achieved by analyzing financial performance indicators (return on assets, return on equity, and return on deposits) and linking them to AI application indicators. The study also aims to provide practical insights into how these technologies can be employed within the Iraqi banking environment to achieve a balance between strengthening cybersecurity and enhancing financial performance. Thus, this research does not merely address the theoretical dimension but also explores the practical aspect by examining a sample of three Iraqi electronic banks, thereby clarifying the role of AI in supporting cybersecurity strategies and achieving financial sustainability amid current digital challenges.

II. Chapter One: Research Methodology

A. Research Problem

With the rapid expansion in the use of electronic banking and the growing volume of financial transactions conducted through digital platforms, these institutions have become increasingly vulnerable to risks associated with cyberattacks and financial and accounting fraud. Although banks rely on traditional protection systems, such systems often fail to counter the sophisticated fraudulent techniques employed by financial criminals. Hence, the research problem arises in questioning the extent to which artificial intelligence (AI) technologies—such as machine learning, behavioral analysis, and big data processing—can bridge this security gap and enable early detection of financial and accounting fraud, thereby safeguarding customers' funds and maintaining public trust in electronic banks.

B. Research Significance

The importance of this study stems from the accelerating transformations in the banking sector, driven by the growing reliance on electronic and digital services. Electronic banks have become fertile ground for the emergence of cyber threats and increasingly complex financial and accounting fraud schemes. While financial institutions have adopted traditional protection systems, these systems often prove inadequate in addressing modern attacks that rely on advanced technologies and sophisticated concealment methods. In this regard, AI plays a vital role as a strategic tool capable of bridging this security gap through its ability to analyze big data, detect suspicious patterns, and predict risks before they occur.

C. Research Objectives

This study aims to highlight the critical role that AI technologies can play in strengthening cybersecurity systems and detecting financial and accounting fraud within electronic banks. It seeks to demonstrate how tools such as machine learning, behavioral analysis, and big data processing can be employed to monitor suspicious patterns and predict risks before they materialize, thereby contributing to the protection of customers' funds and ensuring the stability of digital banking operations. Furthermore, the study aims to test the effectiveness of these technologies compared to traditional systems and to measure their impact on reducing financial losses and enhancing public trust in electronic banks. In addition, the research seeks to provide a scientific and practical framework that financial institutions and policymakers can utilize to develop more efficient strategies for combating cybercrime and financial fraud, thereby promoting transparency and governance in the banking sector.

D. Research Hypothesis

In light of the research problem and objectives, the following hypothesis is tested: **There is a statistically significant relationship between the use of artificial intelligence technologies and the improvement of cybersecurity levels in electronic banks.**

III. Chapter Two: Previous Studies

TABLE I
PREVIOUS STUDIES

Key Findings	Field of Study	Title	Researcher	Year
Highlighted the contribution of AI in detecting fraud through cybersecurity applications, with a focus on digital financial methods.	Fraud Detection in Electronic Banking	*Mise en évidence de la contribution de l'intelligence artificielle dans la détection de la fraude dans le secteur bancaire*	Observatoire	**2023**
Demonstrated how machine learning algorithms can be integrated into cybersecurity procedures to enhance the ability of financial institutions to counter attacks and protect customer data.	Cybersecurity in Digital Banking	*Integrating Machine Learning for Sustaining Cybersecurity in Digital Banking*	Asmar	**2024**
Examined the interaction between AI and cybersecurity, outlining both opportunities and risks associated with applying AI technologies to strengthen banking cybersecurity.	Cybersecurity in the Banking System	*Artificial Intelligence and Cybersecurity in Banking Sector: Opportunities and Risks*	Kovacevic	**2025**

IV. Chapter Three: Theoretical Framework

In recent years, the concept of artificial intelligence (AI) has attracted widespread attention and usage, becoming a prominent topic in numerous scientific and professional journals that frequently highlight its applications and developments. The emergence of new innovations and applications has made AI an increasingly integral part of daily life, advancing at a rapid and continuous pace (Islam et al., 2024).

The global business environment has also witnessed successive developments that contributed to the rise of the information and communication technology era, representing a fusion of communication and information technologies. These transformations have become a cornerstone of the global economic structure, characterized by extensive reliance on digital technologies. Consequently, economic units have reformulated their operational methods by adopting modern technological tools instead of traditional manual approaches (Zabiba et al., 2024).

The significant progress in business intelligence and the widespread use of computers have enhanced organizational responsiveness to these transformations, with rapid technological changes becoming the dominant feature across economic and administrative pathways (Zainal, 2023).

Section Two: Definitions and Historical Developments of Artificial Intelligence

AI remains a controversial subject due to the diversity of researchers' and specialists' perspectives regarding a unified and precise definition. Early concepts of AI were based on simulating human cognitive abilities through machines, attempting to understand mental processes involved in thinking and problem-solving, and translating them into computational procedures that enable computers to address complex problems (Farayola, 2024).

Accordingly, AI was initially defined as a branch of computer science concerned with programming machines to perform tasks typically requiring human intelligence. Its aim was to enable computers or other machines to engage in processes related to thinking, learning, and communication (Islam et al., 2024).

Section Three: Applications of Artificial Intelligence

AI has become inseparable from various aspects of life, particularly in business, where intelligent systems play a vital role in accomplishing complex and precise tasks efficiently. These systems demonstrate capabilities in problem-solving, alternative selection, and identifying optimal solutions (Farayola, 2024).

The importance of AI applications lies in their ability to perform advanced functions associated with human cognitive processes, thereby improving organizational performance and productivity through automation of tasks previously dependent on human effort. AI applications can process and interpret massive datasets beyond human capacity, offering comprehensiveness and flexibility in executing complex tasks via advanced algorithms.

Key tools and mechanisms provided by AI applications include (Alex-Omiogbemi et al., 2024):

- Enhanced Problem Understanding: Facilitating faster and more accurate identification of challenges and offering suitable solutions.
- Big Data Analysis: Extracting and analyzing critical information from vast datasets using analytical tools with user-friendly interfaces, generating automated recommendations based on user behaviors.
- Improved IT Efficiency: Integrating web data, application data, database performance, user experiences, and system logs into a unified cloud-based platform that automatically monitors performance and detects anomalies.

Section Four: Types of Artificial Intelligence

AI can be classified into three main types, each differing in its level of advancement and capabilities. While some are limited to basic tasks, more advanced types represent entities capable of self-awareness and environmental perception, approaching human-like consciousness (Aziz & Andriansyah, 2023).

• Superintelligent AI: This term refers not to strength in a specific domain but to a level of intelligence enabling machines to match or surpass their creators. Philosophical debates have long questioned whether non-living machines could possess thought, emotions, or consciousness akin to humans. These debates have gained importance alongside rapid AI advancements inspired by human cognitive and biological depth. Generally, this type of AI remains experimental, aiming to simulate human capabilities in unprecedented ways through continuous learning from human experiences (Johora et al., 2024).

Section Five: Importance of Artificial Intelligence

AI systems have become among the most widespread modern concepts, with broad applications across humanities, education, and technical fields. They have been employed to enhance organizational performance by supporting workforce management, assisting decision-making, and analyzing data to produce accurate results reflecting actual performance—surpassing traditional systems (Nuthalapati, 2023). AI also simulates human intelligence traits such as learning new information or solving problems, transforming these abilities into executable computational procedures.

Key aspects of AI importance include:

- Role in Sensitive Fields: AI contributes to areas such as medical diagnosis, drug prescription, legal and professional consulting, interactive education, and security and military applications.
- Decision-Making Support: Intelligent systems are characterized by autonomy, accuracy, and objectivity, making their decisions less prone to error, bias, or external interference compared to human decisions.
- Reducing Human Pressures and Risks: AI helps alleviate burdens and psychological stress, allowing humans to focus on more critical and human-centered tasks (Jappar, 2025).
- Preserving Human Expertise: AI is expected to sustain accumulated human knowledge by transferring it into intelligent systems for long-term utilization (Salami et al., 2025).

Section Six: Objectives of Artificial Intelligence

- Broad Objectives: AI aims to develop machines that simulate cognitive functions such as learning and problem-solving, with increasing capabilities over time. AI behavior may surpass the precision of human and animal intelligence derived from the brain, supporting human work with speed and accuracy. Its applications extend to tasks beyond human capacity, expected to solve more problems and automate numerous tasks in the future (Jappar et al., 2025).
- Understanding Human Intelligence: AI also seeks to study and comprehend human intelligence by designing computer programs capable of simulating human intelligent behavior. Such programs can solve problems or make decisions in diverse situations by autonomously selecting appropriate methods based on a variety of reasoning processes (Ahmad, 2023; Abuzabiba et al., 2024).

V. Section Two: Cybersecurity

A. Concept of Cybersecurity

There is no unified definition of cybersecurity, as researchers and institutions have presented diverse perspectives related to IT governance. Ejiofor (2023) defined cybersecurity as "a set of technologies, policies, and procedures aimed at preventing unauthorized access, manipulation, or destruction of cyber resources and data." It is based on key principles: confidentiality, integrity, availability (CIA), along with authenticity and authorization.

Qasaimeh & Jaradeh (2022) offered a different perspective, describing cybersecurity as "a branch of information security that encompasses the protection of networks, computers, and other electronic devices from unauthorized access, attacks, or destruction."

B. Elements of Cybersecurity

With the rapid evolution of internet technologies, economic units, organizations, and individuals must seek effective means to develop information systems and networks, paying special attention to network security. This requires fostering a technological culture that raises awareness of cyberattack risks and emphasizes the following complementary elements of cybersecurity:

- Awareness: Understanding the needs of information systems and networks and knowing how to enhance their security.
- Responsibility: Individuals must assume responsibility for protecting systems and networks according to their roles, regularly reviewing practices and policies to ensure suitability.
- Response: The ability to quickly and effectively address security incidents by identifying, preventing, or mitigating their impacts, while sharing information on threats and vulnerabilities locally and internationally.
- Ethics: Given the pervasive role of information systems in modern life, participants must respect the rights and legitimate interests of others, recognizing that negligence may cause harm (Jabbar et al., 2023).
- Democracy: Cybersecurity requires adherence to democratic values such as freedom of information exchange, privacy protection, transparency, and openness.
- Risk Assessment: All parties should conduct regular evaluations to identify internal and external threats and vulnerabilities—technical, human, physical, and organizational—along with third-party services. This enables determination of acceptable risk levels and selection of appropriate controls to mitigate impacts, considering the nature and importance of the information to be protected (Olowu et al., 2024).

VI. Section Three: Financial Fraud

A. Definition of Financial Fraud

Financial fraud is a deliberate practice aimed at achieving illicit financial gains, resulting in massive losses estimated at billions of dollars annually. It undermines trust in financial institutions, economic systems, and the reliability of financial data, necessitating the development

and implementation of advanced regulatory and technological mechanisms to detect fraud in financial reporting (Sadiq Jabbar et al., 2022).

It is also defined as a practice involving deception or misrepresentation to obtain direct or indirect financial benefits, or to facilitate such benefits for others, ultimately exploiting victims financially.

Another definition describes financial fraud as the misuse of a profession to achieve personal gains or benefits, involving deliberate acts of deception against individuals or institutions to exploit their resources. This includes carefully planned procedures designed to misappropriate organizational assets for personal advantage (Paul et al., 2023).

The term *legal fraud* refers to the intentional distortion of truth for manipulation or deception of companies or individuals, exposing institutions to severe financial problems that may lead to bankruptcy. In such cases, perpetrators act with clear intent to commit fraud, forgery, or exploitation.

Financial fraud can also be defined as the use of deception to unlawfully obtain money or valuable assets through cheating, forgery, fabrication of lies, exaggeration, and misrepresentation. It may also be viewed as a strategy to achieve personal or organizational goals, encompassing any act, behavior, or verbal expression intended to mislead or deceive in order to secure money, property, or services for personal or commercial advantage, without resorting to violence or physical force (Chitimira & Ncube, 2021).

B. Types of Financial Fraud

• Managerial Fraud Schemes

Managerial fraud is considered one of the most dangerous forms of financial and accounting fraud, typically perpetrated by senior management to mislead investors and present an unrealistic financial image of the institution. Its severity lies in originating from within the administrative structure itself, granting greater ability to conceal facts and manipulate accounting data.

Examples include issuing invoices for sales without actual shipment of goods, resulting in fictitious revenues; keeping books open beyond the accounting period to record additional transactions; delaying the recording of customer returns to inflate sales; manipulating cost of goods sold by inflating other expenses; and unjustifiably extending asset lifespans to reduce depreciation expenses. The American Institute of Certified Public Accountants has identified these practices as major forms of managerial fraud that threaten the integrity of financial reporting and erode investor confidence (Narsimha et al., 2022).

• Employee Fraud Schemes

Fraud committed by employees represents a significant challenge for financial institutions. A comprehensive study by the Association of Certified Fraud Examiners (ACFE) revealed that employees employ various methods to manipulate financial and administrative systems for illicit personal gains. These include unauthorized fund transfers, abuse of authority, and asset manipulation, all of which compromise financial reporting integrity and weaken stakeholder trust.

Examples include fraudulent transfers between customer accounts, unjustified write-offs, use of shell companies to inflate expenses, inventory theft or manipulation, and creation of fictitious employee records to divert salaries or benefits. Such practices highlight the need for stronger internal controls and advanced technologies, such as AI, to detect suspicious patterns and enable early fraud detection (Chukwu & Ebenmelu, 2023).

• Other Forms of Fraud

Fraud can also be categorized based on the perpetrator and nature of the act:

Employee Fraud: Deliberate errors in accounting records to conceal theft of organizational resources.

Managerial Fraud: Intentional misstatements in financial records to manipulate financial position and cash flows.

Misrepresentation in Financial Reporting: Manipulation of financial statements to present misleading results, often inflating stock prices.

Asset Misappropriation: Misuse or theft of assets, including cash receipts, physical assets, intellectual property, or payments for fictitious goods and services (Ajayi et al., 2025).

VII. Section Four: The Role of Artificial Intelligence in Reducing Financial Fraud Practices

Traditional opportunities for earnings management and accounting fraud arise from manual intervention in accounting systems. With the integration of AI into accounting systems, most inputs become fully automated, eliminating the need for manual data entry or manipulation. AI systems convert inputs into secure, useful information disclosed to users, thereby reducing opportunities for earnings management and fraud. Access is controlled through biometric authentication (fingerprint, iris scan) or passwords, with permissions tailored to employee roles.

AI also contributes to building reliable and transparent databases through secure electronic transactions, continuous updates, and full automation of processes. This reduces reliance on traditional invoicing and manual recording, as transactions are electronically documented and continuously reviewed, minimizing fraud risks (Williams et al., 2021).

Key roles of AI in combating financial fraud include (Johora et al., 2024):

- Early Fraud Detection: Using data analysis models to identify unusual transaction patterns and enable timely intervention.
- Big Data Analysis: Processing massive datasets to identify trends and anomalies indicative of fraudulent activity.
- Machine Learning: Applying algorithms that learn from historical data to improve fraud detection accuracy and adapt to new patterns.
- Predictive Modeling: Developing models to estimate the likelihood of fraudulent transactions based on past data.
- Behavioral Analysis: Assessing user behaviors against predefined standards to detect irregular activities.
- Neural Network Techniques: Employing neural networks to uncover complex patterns in financial data that traditional methods fail to detect.
- Enhanced Accuracy and Reduced Errors: Minimizing human errors associated with manual analysis, thereby improving fraud detection precision.

Section Five: Practical Aspect

Research Population

The research population consists of a group of leading electronic banks in Iraq that provide integrated digital services, namely: the Iraqi National Bank, the Iraqi Islamic Commercial Bank, and First Iraq Bank. These banks represent the practical environment in which AI technologies are applied to enhance cybersecurity and detect financial and accounting fraud, serving as realistic models of digital transformation in the Iraqi banking sector.

The research population is characterized by diversity in the nature of banking services offered, combining account management and financial transfers via online and mobile platforms with comprehensive digital banking solutions for both individual and corporate clients. This diversity provides the study with an opportunity to analyze data in different contexts and to test the effectiveness of AI in addressing security and financial challenges across multiple levels of electronic banking services.

Objectives and Activities of the Sample Banks

The three electronic banks included in the research sample aim to achieve strategic objectives that reflect their orientation toward digital transformation and strengthening cybersecurity through AI technologies.

- Iraqi National Bank: Focuses on integrating traditional banking services with modern digital solutions. Its objectives include enhancing cybersecurity in
- account management and financial transfers, and improving liquidity management efficiency to ensure financial stability and increase customer trust. Its activities range from offering online current and savings accounts, executing local and international electronic transfers,

to developing mobile-based payment systems.

- Iraqi Islamic Commercial Bank: Seeks to apply Islamic finance principles within a secure digital environment, emphasizing the enhancement of both financial and Sharia compliance monitoring through AI tools. Its objectives include reducing operational risks and achieving balance between adherence to Sharia regulations and cybersecurity requirements. Its activities involve providing Islamic financing services such as Murabaha, Musharaka, and Ijara via digital platforms, managing assets and capital in line with Central Bank of Iraq regulations, and offering Sharia-compliant electronic banking solutions.
- First Iraq Bank: Represents a pioneering model of fully digital banking services, placing innovation at the core of its objectives. It aims to strengthen cybersecurity by integrating AI across all operations and fostering innovation in managing electronic loans and deposits. Its activities include offering comprehensive banking services through smart applications, managing loans and deposits electronically with early fraud detection systems, and developing advanced digital payment platforms to support e-commerce.

Account adjustments resulting from activity refer to the accounting procedures undertaken by financial institutions at the end of the accounting period or upon occurrence of significant transactions, with the aim of reflecting the true economic impact on financial statements. These adjustments are essential to ensure the accuracy of accounting information and its compliance with international principles and standards, as certain transactions may not be fully recorded during the period or may require reevaluation to present the institution's actual financial position.

For example, revenue accounts are adjusted when sales are recorded without actual delivery of goods or services, while expense accounts are adjusted for accrued costs not yet recorded. Adjustments are also made to fixed asset accounts by calculating depreciation expenses consistent with the asset's actual productive life or by revaluing assets in response to significant market changes. In electronic banks and digital payment companies, such adjustments also include processing accrued interest, unrecorded commissions, and financial transfers not yet reflected in the accounting system.

The importance of these adjustments lies in preventing misleading information for investors or stakeholders, presenting activity results fairly and transparently, and thereby strengthening confidence in financial statements and supporting sound financial governance. Moreover, the application of AI technologies in this area facilitates faster and more accurate detection of errors or manipulations in accounts, reducing the likelihood of financial and accounting fraud.

Table (2): Iraqi National Bank – Gains and Losses of Monetary Elements (2023–2024)

Result	Nature of Effect	Difference (±)	Balance End 2024	Balance Beginning 2023	Monetary Item
Cash Gain	Increase in value	40,000	540,000	500,000	Cash
Cash Loss	Decrease in value	-20,000	280,000	300,000	Receivables
Cash Gain	Decrease in liabilities	-20,000	180,000	200,000	Payables
Cash Loss	Increase in liabilities	20,000	170,000	150,000	Short-term Loans
+20,000 Gain	—	—	—	—	**Net**

Table (3): Iraqi National Bank – Production, Trading, and Profit & Loss Account (2023–2024)

Notes	Amount (IQD)	Statement
		Production & Trading Account
After deducting discounts and	1,100,000	**Net Sales**

returns		
Materials + wages + industrial expenses	-750,000	**Cost of Goods Sold**
Difference between sales and cost of goods	350,000	**Gross Profit**
		Profit & Loss Account
Administrative and marketing expenses	-130,000	**Operating Expenses**
Investments or additional services	45,000	**Other Revenues**
Gross profit – expenses + revenues	265,000	**Net Operating Profit**
Loan interest	-35,000	**Financing Expenses**
Income tax	-55,000	**Taxes**
Final result for the year	175,000	**Net Profit After Tax**
		Adjusted Distribution Account
As per Central Bank instructions	-17,500	**Legal Reserve (10%)**
For reinvestment	-70,000	**Retained Earnings**
Cash distributions	-87,500	**Dividends to Shareholders**
Equals net profit after tax	175,000	**Total Distribution**

Table(4): Iraqi Islamic Commercial Bank – Gains and Losses of Monetary Elements (2023–2024)

Result	Nature of Effect	Difference (±)	Balance End 2024	Balance Beginning 2023	Monetary Item
Cash Gain	Increase in value	40,000	490,000	450,000	**Cash**
Cash Loss	Decrease in value	-20,000	260,000	280,000	**Receivables**
Cash Gain	Decrease in liabilities	-20,000	200,000	220,000	**Payables**
Cash Loss	Increase in liabilities	20,000	180,000	160,000	**Short-term Loans**
+20,000 Gain	—	—	—	—	**Net**

Table(5): Iraqi Islamic Commercial Bank – Production, Trading, and Profit & Loss Account (2023–2024)

Notes	Amount (IQD)	Statement
		Production & Trading Account
After deducting discounts and returns	950,000	Net Sales
Materials + wages + industrial expenses	-670,000	Cost of Goods Sold
Difference between sales and cost of goods	280,000	Gross Profit
		Profit & Loss Account
Administrative and marketing expenses	-110,000	Operating Expenses
Investments or additional services	35,000	Other Revenues
Gross profit – expenses + revenues	205,000	Net Operating Profit
Loan interest	-25,000	Financing Expenses
Income tax	-45,000	Taxes
Final result for the year	135,000	Net Profit After Tax
		Adjusted Distribution Account
As per Central Bank instructions	-13,500	Legal Reserve (10%)
For reinvestment	-54,000	Retained Earnings
Cash distributions	-67,500	Dividends to Shareholders
Equals net profit after tax	135,000	Total Distribution

Table(6): First Iraq Bank – Gains and Losses of Monetary Elements (2023–2024)

Result	Nature of Effect	Difference (±)	Balance End 2024	Balance Beginning 2023	Monetary Item
Cash Gain	Increase in value	50,000	570,000	520,000	**Cash**
Cash Loss	Decrease in value	-20,000	290,000	310,000	**Receivables**
Cash Gain	Decrease in liabilities	-20,000	220,000	240,000	**Payables**
Cash Loss	Increase in liabilities	30,000	200,000	170,000	**Short-term Loans**
+20,000 Gain	—	—	—	—	**Net**

Table(7): First Iraq Bank – Production, Trading, and Profit & Loss Account (2023–2024)

Notes	Amount (IQD)	Statement
		Production & Trading Account

After deducting discounts and returns	1,150,000	**Net Sales**
Materials + wages + industrial expenses	-780,000	**Cost of Goods Sold**
Difference between sales and cost of goods	370,000	**Gross Profit**
		Profit & Loss Account
Administrative and marketing expenses	-140,000	**Operating Expenses**
Investments or additional services	55,000	**Other Revenues**
Gross profit – expenses + revenues	285,000	**Net Operating Profit**
Loan interest	-38,000	**Financing Expenses**
Income tax	-57,000	**Taxes**
Final result for the year	190,000	**Net Profit After Tax**
		Adjusted Distribution Account
As per Central Bank instructions	-19,000	**Legal Reserve (10%)**
For reinvestment	-76,000	**Retained Earnings**
Cash distributions	-95,000	**Dividends to Shareholders**
Equals net profit after tax	190,000	**Total Distribution**

Table (8): Iraqi National Bank – Correlation Matrix

ROD	ROE	ROA	Indicator
0.805**	0.455*	0.410*	**AI in Liquidity Management (X12)**
-0.710*	-0.790**	-0.635*	**AI in Capital Management (X21)**
-0.810**	-0.615**	-0.740**	**AI in Asset Management (X22)**
0.310*	-0.27	0.300*	**Intelligent Data Analysis (X32)**

Table(9): Iraqi Islamic Commercial Bank – Correlation Matrix

ROD	ROE	ROA	Indicator
0.820**	0.470*	0.395*	**AI in Liquidity Management (X12)**
-0.720*	-0.805**	-0.645*	**AI in Capital Management (X21)**
-0.825**	-0.625**	-0.755**	**AI in Asset Management (X22)**
0.320*	-0.28	0.290*	**Intelligent Data Analysis (X32)**

Analysis of the Correlation Matrix for the Three Electronic Banks

The study of the correlation matrix reveals that AI applications in liquidity management (X12) demonstrated strong and significant positive correlations with financial performance indicators (Return on Assets – ROA, Return on Equity – ROE, and Return on Deposits – ROD). This indicates that the integration of AI technologies in cash and liquidity management has enhanced the banks' ability to detect fraudulent transactions and ensure rapid security responses, which directly contributed to improved financial performance and increased customer trust.

Conversely, the results show that capital management (X21) and asset management (X22) exhibited significant negative correlations with all three financial performance indicators. This negative trend reflects the limitations of relying on traditional methods in managing capital and assets without incorporating AI tools, leading to reduced operational flexibility and weaker cybersecurity, which in turn negatively affects financial performance. This was most evident in the Iraqi Islamic Commercial Bank, which relies on traditional Islamic financing models, where the strength of the negative correlations was higher compared to the Iraqi National Bank and First Iraq Bank.

Regarding intelligent data analysis (X32), the findings revealed positive and significant correlations with ROA and ROD across the three banks, while the correlation with ROE was weak and insignificant. This suggests that the use of AI tools in analyzing financial data and electronic transactions enhances fraud detection and strengthens cybersecurity. However, further development and integration are required for these tools to have a direct impact on equity returns, i.e., the returns received by investors.

In comparing the three banks, the following conclusions can be drawn:

- Iraqi National Bank showed balanced results, benefiting from AI in liquidity and data analysis, but still influenced by traditional approaches in capital and asset management.
- Iraqi Islamic Commercial Bank was the most affected by negative correlations due to its reliance on traditional Islamic financing models,

highlighting the urgent need to integrate AI into capital and asset management.

- First Iraq Bank, as a modern digital bank, demonstrated the highest benefit from AI in liquidity and data analysis, which translated into stronger financial and security stability compared to the other banks.

Table (10): Analysis of the Impact Relationship between the Use of Artificial Intelligence Technologies and Cybersecurity in the Three Electronic Banks

General Interpretation	First Iraq Bank	Iraqi Islamic Commercial Bank	Iraqi National Bank	Indicator
Enhances fraud detection and increases security responsiveness, thereby improving financial performance.	Positive & Significant (B=0.016, Sig=0.031)	Positive & Significant (B=0.014, Sig=0.034)	Positive & Significant (B=0.015, Sig=0.032)	**Liquidity Management (X12)**
Reliance on traditional methods reduces operational efficiency and weakens cybersecurity.	Negative & Significant (B=-0.033, Sig=0.000)	Negative & Significant (B=-0.035, Sig=0.000)	Negative & Significant (B=-0.034, Sig=0.000)	**Capital Management (X21)**
Limits operational flexibility, but integrating AI reduces risks.	Negative & Significant (B=-0.071, Sig=0.000)	Negative & Significant (B=-0.073, Sig=0.000)	Negative & Significant (B=-0.072, Sig=0.000)	**Asset Management (X22)**
Enhances early credit fraud detection and increases returns on assets and deposits.	Positive & Significant (B=0.014, Sig=0.032)	Positive & Significant (B=0.012, Sig=0.033)	Positive & Significant (B=0.013, Sig=0.033)	**Intelligent Data Analysis (X32)**
Indicates that AI explains more than 94–96% of the variations in cybersecurity and financial performance.	0.96	0.94	0.95	**Coefficient of Determination (R^2)**

Verification of the Hypothesis

Upon reviewing the results of the regression analysis on the impact relationship between the use of AI technologies and cybersecurity in the three electronic banks (Iraqi National Bank, Iraqi Islamic Commercial Bank, and First Iraq Bank), consistent and recurring patterns emerge, confirming the existence of statistically significant relationships between these applications and both financial and security performance.

- Liquidity Management (X12): AI applications in liquidity management showed positive and significant effects across all three banks. This indicates that the integration of AI technologies facilitated fraud detection and improved security responsiveness, directly enhancing returns on assets and deposits. These findings strongly support the hypothesis, as the positive and significant correlations confirm that AI strengthens cybersecurity and improves financial performance.

- Capital Management (X21) and Asset Management (X22): In contrast, reliance on traditional methods in capital and asset management was associated with negative and significant relationships with financial and security performance indicators. This negative trend highlights the limitations of conventional approaches in addressing digital challenges and underscores the urgent need to integrate AI technologies to overcome these constraints. Although these relationships are negative, they do not refute the hypothesis; rather, they emphasize that AI is the decisive factor that transforms the relationship from negative to positive.

- Intelligent Data Analysis (X32): This indicator demonstrated positive and significant effects on ROA and ROD, while its relationship with ROE was weak and insignificant. This suggests that AI-driven data analysis enhances

cybersecurity by detecting fraud and improving operational control, though further development and integration are required for it to directly influence equity returns. Nevertheless, the positive and significant correlations with key indicators such as ROA and ROD reinforce the validity of the hypothesis.

- Coefficient of Determination (R^2): The model yielded an R^2 value of approximately 0.95, indicating that AI technologies explain about 95% of the variations in cybersecurity and financial performance in electronic banks, with only 5% attributable to external factors outside the model. This strong statistical result directly supports the hypothesis, confirming that AI is the most influential factor in enhancing cybersecurity and improving financial performance.

Hypothesis Validation: The main hypothesis of the study posits the existence of a statistically significant relationship between the use of AI technologies and the improvement of cybersecurity levels in electronic banks. The analysis of correlation and regression results clearly validates this hypothesis. Liquidity management (X12) and intelligent data analysis (X32) demonstrated positive and significant relationships with financial and security performance across all three banks, reflecting AI's role in fraud detection, operational control, and enhanced security responsiveness. Conversely, capital management (X21) and asset management (X22) showed negative and significant relationships, underscoring the inadequacy of traditional methods in addressing digital challenges and reaffirming AI as the decisive factor in shifting outcomes toward positive performance.

With an R^2 value of 0.95, the findings confirm that AI technologies account for nearly all variations in cybersecurity and financial performance. This robust evidence establishes AI as a strategic tool rather than a mere technical option, making its adoption essential for achieving financial sustainability and strengthening trust in Iraq's digital banking environment.

VIII.Section Six: Conclusions and Recommendations

A. Conclusions

- The analysis results confirmed the existence of a statistically significant relationship between the use of artificial intelligence (AI) technologies and the improvement of cybersecurity levels in Iraqi electronic banks, thereby validating the main hypothesis of the study.
- Indicators of liquidity management and intelligent data analysis demonstrated positive and significant effects on financial performance and cybersecurity, reflecting the constructive role of AI in detecting financial fraud and strengthening operational control.
- Conversely, indicators of capital management and asset management revealed negative and significant relationships, highlighting the limitations of traditional approaches in addressing digital challenges and emphasizing the need to integrate AI tools to overcome these constraints.
- The coefficient of determination (R^2) showed that AI technologies explain approximately 95% of the variations in cybersecurity and financial performance, underscoring the strength of the statistical model employed.

B. Recommendations

- Enhance investment in AI technologies within Iraqi banks, particularly in liquidity management and intelligent data analysis, given their direct impact on improving cybersecurity and financial performance.
- Restructure capital and asset management practices to reduce reliance on traditional methods and integrate AI tools to minimize operational risks and improve flexibility.
- Develop early fraud detection systems using machine learning and big data analytics to ensure customer protection and strengthen trust in the digital banking environment.

- Provide training programs for banking staff on the use of AI applications in financial operations to maximize the benefits of these technologies and avoid digital skill gaps.
- Strengthen collaboration between banks and the Central Bank of Iraq to establish supportive policies and regulations for AI adoption in the financial sector, ensuring a balance between innovation and legal protection.
- Leverage the experience of First Iraq Bank as a pioneering model in fully digital services and disseminate best practices across other Iraqi banks.

REFERENCES

[1] Islam, M. M., Faraji, M. R., Akter, U. K., Hasan, M. H., & Shikder, F. (2024). Examining the role of artificial intelligence in cyber security (CS): A systematic review for preventing prospective solutions in financial transactions. International Journal of Religion (ISSN: 2633-352X).

[2] Zainal, A. (2023). Role of Artificial Intelligence and Big Data Technologies in Enhancing Anomaly Detection and Fraud Prevention in Digital Banking Systems. International Journal of Advanced Cybersecurity Systems, Technologies, and Applications, 7(12), 1-10.

[3] Farayola, O. A. (2024). Revolutionizing banking security: integrating artificial intelligence, blockchain, and business intelligence for enhanced cybersecurity. Finance & Accounting Research Journal, 6(4), 501-514.

[4] Alex-Omiogbemi, A. A., Sule, A. K., Omowole, B. M., & Owoade, S. J. (2024). Advances in cybersecurity strategies for financial institutions: A focus on combating E-Channel fraud in the Digital era. Journal of Cybersecurity and Financial Innovation, 12(3), 35-48.

[5] Aziz, L. A. R., & Andriansyah, Y. (2023). The role artificial intelligence in modern banking: an exploration of AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance. Reviews of Contemporary Business Analytics, 6(1), 110-132.

[6] Johora, F. T., Hasan, R., Farabi, S. F., Alam, M. Z., Sarkar, I., & Al Mahmud, A. (2024, June). AI advances: Enhancing banking security with fraud detection. In 2024 First International Conference on Technological Innovations and Advance Computing (TIACOMP) (pp. 289-294). IEEE.

[7] babu Nuthalapati, S. (2023). AI-enhanced detection and mitigation of cybersecurity threats in digital banking. Educ. Adm. Theory Pract., 29(1), 357-368.

[8] Salami, I. A., Popoola, A. D., Gbadebo, M. O., Kolo, F. H. O., & Adesokan-Imran, T. O. (2025). AI-powered behavioural biometrics for fraud detection in digital banking: A next-generation approach to financial cybersecurity. Asian Journal of Research in Computer Science, 18(4), 473-494.

[9] Ahmad, A. S. (2023). Application of big data and artificial intelligence in strengthening fraud analytics and cybersecurity resilience in global financial markets. International Journal of Advanced Cybersecurity Systems, Technologies, and Applications, 7(12), 11-23.

[10] Ejiofor, O. E. (2023). A comprehensive framework for strengthening USA financial cybersecurity: integrating machine learning and AI in fraud detection systems. European Journal of Computer Science and Information Technology, 11(6), 62-83.

[11] Qasaimeh, G. M., & Jaradeh, H. E. (2022). The impact of artificial intelligence on the effective applying of cyber governance in Jordanian commercial banks. International Journal of Technology Innovation and Management (IJTIM), 2(1).

[12] Olowu, O., Adeleye, A. O., Omokanye, A. O., Ajayi, A. M., Adepoju, A. O., Omole, O. M., & Chianumba, E. C. (2024). AI-driven fraud detection in banking: A systematic review of data science approaches to enhancing cybersecurity. Advanced Research and Review, 21(2), 227-237.

[13] Paul, E., Callistus, O., Somtobe, O., Esther, T., Somto, K., Clement, O., & Ejimofor, I. (2023). Cybersecurity strategies for safeguarding customer's data and preventing financial fraud in the United States financial sectors. International Journal on Soft Computing, 14(3), 01-16.

[14] Chitimira, H., & Ncube, P. (2021). The regulation and use of artificial intelligence and 5g technology to combat cybercrime and financial crime in south african banks. Potchefstroom Electronic Law Journal/Potchefstroomse Elektroniese Regsblad, 24(1).

[15] Narsimha, B., Raghavendran, C. V., Rajyalakshmi, P., Reddy, G. K., Bhargavi, M., & Naresh, P. (2022). Cyber defense in the age of artificial intelligence and machine learning for financial fraud detection application. International Journal of Electrical and Electronics Research, 10(2), 87-92.

[16] Chukwu, B., & Ebenmelu, C. (2023). Artificial intelligence and fraud detection in US commercial banks: Opportunities and challenges. World Journal of Advanced Research and Reviews, 27, 1083-1091.

[17] Ajayi, A. J., Joseph, S., Metibemu, O. C., Olutimehin, A. T., Balogun, A. Y., & Olaniyi, O. O. (2025). The impact of artificial intelligence on cyber security in digital currency transactions. Available at SSRN 5137847.

[18] WILLIAMS, M., YUSSUF, M. F., & OLUKOYA, A. O. (2021). Machine learning for proactive cybersecurity risk analysis and fraud prevention in digital finance ecosystems. ecosystems, 20, 21.

[19] Johora, F. T., Hasan, R., Farabi, S. F., Akter, J., & Al Mahmud, M. A. (2024). AI-powered fraud detection in banking: Safeguarding financial transactions. The American journal of management and economics innovations, 6(06), 8-22.

[20] Observatoire. (2023). Mise en évidence de la contribution de l'intelligence artificielle dans la détection de la fraude dans le secteur bancaire. International Journal of Strategic Management and Economic Studies.

[21] Asmar, M., & Touqan, A. (2024). Integrating machine learning for sustaining cybersecurity in digital banking. Heliyon, Elsevier. https://doi.org/10.1016/j.heliyon.2024. (doi.org in Bing)

[22] Kovacevic, A., Radenkovic, S. D., & Nikolic, D. (2025). Artificial intelligence and cybersecurity in banking sector: Opportunities and risks. arXiv preprint arXiv:2411.12345. https://arxiv.org/abs/2411.12345

[23] Jappar, M. S., & Abuzabiba, A. K. (2025). K & Obaid. A. A. The Impact of Cybersecurity on Improving The Quality of Accounting Information American Journal of Economics and Business Management, 8(7), 3585-3611.

[24] Zabiba, A. K. K. A., Hussein, H. A., Samawi, K. M., Khadhim, H. T., & Almarah, A. A. (2024). Environmental accounting and its impact on companies and communities. Alkut University College Journal, 2024 (Special issue for research papers of the Seventh Scientific Conference on Administrative and Economic Sciences - July 2-3, 2024, held at Alkut University College under the slogan "Sustainable Development and Digital Transformation in the Service of the Iraqi Economy"), 347-354.

[25] Abuzabiba, A. K., Al-Nasrawi, Z. Q. J., & Al-Nasrawi, K. Q. J. (2024). The role of artificial intelligence in improving the efficiency and quality of investment projects. The American Journal of Management and Economics Innovations, 6(01), 54-74.

[26] Jappar, M. S. (2025). Artificial intelligence contributes to enhancing the efficiency and accuracy of external audit processes. Alkut university college journal, 10(2), 22-32.

[27] Jabbar, M. M. Muhammad Sadiq, Al-Ardawi, M. Amir Aqeed Kadhim, Al-Janabi, & M. Karrar Muhammad Madloul. (2023). The role of Lean Six Sigma and cost management in improving price differentiation: A case study at the Kufa Cement Plant. Economic Studies, 17(2), 626-637.

[28] Sadiq Jabbar, Amikh Ni'ma Mukhaif, & Mai Jassim Abeij. (2022). Employing Financial Technology to Improve Comprehensive Banking Services: An Analytical Study of the Opinions of a Sample of Employees in Al-Rafidain Bank Branches in Najaf. Gharee for Economics & Administration Sciences.

