Al-Qadisiyah Journal for Administrative and Economic Sciences ISSN$_{Online}$: 2312-9883
QJAE, Volume 28, Special issue (2026) ISSN$_{Print}$: 1816-9171
DOI:/ /doi.org/ 10.33916/qjae.2026. Special issue 0141152

AI-Powered Crisis Forecasting for the Banking Sector: A Comparative Analysis of Financial and Digital Shocks in the US, UK, and Canada

Noor S Alramadan
noor.salah@uokerbala.edu.iq
https://orcid.org/0009-0008-2740-7325
Hadeer K Ashour
hadeer.khaion@uokerbala.edu.iq
https://orcid.org/0009-0009-5590-5222
Noor Sabah Hameed Al-Dahaan
noor.s@uokerbala.edu.iq
https: //orcid.org/0000-0002-4492-610X
Hayder Yonus Kadhim
haider.yonis@uokerbala.edu.iq
https://orcid.org/0009-0001-4535-7272
College of Administration and Economics , Department of Financial and Banking Sciences , University of Kerbala, Iraq

Corresponding Author: Noor S Alramadan, Hadeer K Ashour, Noor Sabah Hameed Al-Dahaan, Hayder Yonus Kadhim

Abstract*:* This study examines how Artificial Intelligence (AI) has dual functions of enhancing cyber security and also poses new life-threatening cyber attacks in the US banking industry. The paper will focus on the fundamental AI technologies such as machine learning, predictive analytics, intelligent detection systems, and automated threat monitoring and will assess the effectiveness of AI technology in enhancing fraud detection, minimizing response time and improving the detection of anomalies. The research employs a mixed-method design, a structured literature review, and quantitative hypothesis testing (paired t-tests and regression analysis) to analyze the secondary data of the main US banks, including JPMorgan Chase and Bank of America. These results support statistically significant results, which assert that the AI-based systems can dramatically improve the performance of cyber security but may also be associated with the emergence of novel AI-related threats, such as deepfakes, AI-created phishing, and adversarial attacks.

The findings emphasize that despite the fact that AI significantly enhances the accuracy of detection and the speed of mitigation, its dual-use functionality puts the banks at a risk of new risks. The advent of algorithm manipulation, synthetic identity fraud, and self-learning malware highlights the necessity to monitor it at all times. The most essential recommendation of the study is the implementation of Explainable AI (XAI) backed by well-developed governance systems, compliance with regulations, adversarial robustness verification, and increased employee education. These actions will guarantee the responsible use of AI so that banks can reap the maximum benefits of security and minimize the risks to vulnerabilities related to the misuse of advanced AI.

Keywords: Predictive Analytics, Deep fake Attacks, Fraud Detection, Machine Learning, AI-Driven Threats, Use of AI in US Banks, Artificial Intelligence (AI),

Introduction: Artificial Intelligence (AI) has been developed quickly. It has affected various sectors of industries such as the banking sector through the implementation of technology. Banks are the primary pillars of the economy in the country, and in this case, AI has turned out to be a highly useful tool to enhance cyber security and, at the same time, a novel threat. Cybercriminals are also utilizing AI to develop more sophisticated and intelligent methods of attacks that include deep fake technologies and AI-powered malware attacks, and phishing botnets. The objective of the current study is to investigate how AI can be useful in the improvement of cyber security systems in the US and how new security concerns are developing in the US banks. By doing so, the proposed research is trying to present an objective image, which would help banking stakeholders to receive the most out of AI and avoid risks, which accompany it.

Literature Review

Introduction to Artificial Intelligence in the Banking Sector:

Definition and scope of Artificial Intelligence (AI):

According to Fitria (2023), Artificial Intelligence (AI) is the technology, which provides ability to a machine, mostly a computer, to mimic the way humans think and do it so intelligently that can be done normally done by a human with mental capabilities. In the banking industry, AI will include machine learning (ML), natural language processing (NLP), robotic process automation (RPA), sophisticated data analytics, and other technologies that are intended to increase the effectiveness of operations, customer experience, and risk management. The possibilities of AI in banking are growing at a tremendous pace. These possible applications of AI include customer service chatbot and personalized financial advisory, fraud detection, compliance and monitoring, and cyber security defense mechanisms.

Overview of AI adoption trends in the US banking industry:

Atadoga et al. (2024) depict that AI has been extensively used in the banking industry in the US, where the level of competition is gradually rising, customer demands are changing rapidly, and cyber security is emerging as more than ever as a pressing issue. A report compiled by the American Bankers Association in 2024, found that more than 70 percent of the largest banks in the US have already introduced AI solutions into the business core. The cyber security is one of the leading fields, where the funds are spent. Established financial institutions such as JPMorgan Chase, Bank of America, and Wells Fargo have utilized AI-based solutions for real-time fraud detection, transaction monitoring, and threat intelligence collection. In addition, AI-based chat-bots, virtual assistants, and automated customer service platforms are gaining traction within the sector in furtherance of the industry trend toward broader digitalization. The growing power of AI is also represented by the appearance of AI regulatory structures in the US. Regulatory bodies such as the Financial Industry Regulatory Authority (FINRA) have begun contemplating policies, which would support responsible AI adoptions especially in sensitive areas such as cyber security, privacy, and consumer protections (FINRA, 2024). In spite of the massive implementation, banks still have to struggle with the issues of data privacy, algorithm transparency, and the threat of adversarial AI.

Significance of AI in banking operations and security:

In accordance to AL-Dosari et al. (2024), AI is essential for improving the working process of a bank through the automatization of repetitive activities, making decisions, and offering insights based on data. Within the framework of cyber security, the real-time capacity to process large volumes of data with AI algorithms would allow banks to identify anomalies, detect new threats, and react to cyber security incidents in better way than with the help of conventional systems. Different types of machine algorithms like machine learning are capable of constantly improving the ability of banks to identify new patterns of attacks as well as to cut response times and reduce financial losses. Nevertheless, the adoption of AI does not lack dangers. Cybercriminals may use the same technologies that make defenses stronger to come up with advanced attacks such as AI-based phishing, deep fakes, and malware. The twofold aspect of AI requires a middle-ground, where the banks can take advantage of the advanced security offered by AI as well as they stay aware of the undesired effects of AI.

AI-Driven Technologies for Enhancing Cyber security in US Banks:

AI-based threat detection and prevention systems:

Artificial Intelligence (AI) has transformed the cyber security practice in the US banking industry, as it allows identification and prevention of threats at an advanced level. Conventional security solutions typically fail to keep up with the sophistication of the cyber attacks. Khan et al. (2024) articulate that AI can be used to fill this gap because it can analyze large quantities of data instantly and detect anomalies, suspicious activity, and other possible breaches. Security Information and Event Management (SIEM) systems based on AI have become an essential element of modern banking cyber security systems along with automated threat hunting software. Such mechanisms do not only identify known attack signatures, but they are able to identify hitherto unseen threats based on behavioral analysis and pattern recognition. In addition, AI also helps in proactive defense systems by automating the response to the threats, less time is spent by humans, and the banks are able to contain the incidents before they get out of control. Identity verification and authentication systems based on AI, including biometric identification and behavioral biometrics, enhance the security perimeter and defend customer data and other forms from the unauthorized access.

Role of Machine Learning and Predictive Analytics:

In contrast to this, Zaki et al. (2024) state that a subset of AI is Machine Learning (ML). It is important for improving cyber security, as the banking systems based on AI can learn using past data and thus evolve to counter emerging attack vectors. ML algorithms make predictive analytics possible and enable banks to predict the possible vulnerabilities, suspicious transactions, and recognize patterns of fraud with high precision. ML models, unlike the traditional rule-based models, get better with time as more new data is introduced to them. It makes them more effective in spotting emerging threats like zero-day exploits and insider attacks. Banks use ML-based models to perform real-time transactional behavior analysis, network traffic analysis, and user activity. For example, the anomaly detection models may mark the unusual activity in the accounts and predictive algorithms might estimate the risk of fraud or cyber attacks according to the historical trends. With such a predictive strategy, it is possible to intervene earlier, minimizing the financial and reputational loss that goes with cyber incidents.

Case studies highlighting successful AI integration:

Some of the major banks in the US have been able to incorporate the AI technologies to improve cyber security. One such application of AI in the financial sector is observed in the JPMorgan Chase that uses AI-powered fraud detection tools for processing millions of payments and transactions every day and identifying suspicious activity almost instantly and with a near-perfect success rate (JPMorgan, 2024). Likewise, the Bank of America makes use of security tools based on AI to track live cyber threats backed by its own virtual assistant based on AI, named Erica, with integrated fraud alerts (BOA, 2024). Wells Fargo has implemented the AI-driven threat intelligence platforms that integrate the machine learning and predictive analytics to prevent the risks before they occur by detecting possible vulnerabilities. These illustrations show that the incorporation of AI does not only improve defensive features but also streamlines operations and leaves cyber security structures of US banks robust.

Emerging AI-Driven Cyber Threats and Vulnerabilities:

AI-powered cyber attacks:

The enhanced security measures by Artificial Intelligence (AI) in US bank cyber security have also enabled the online criminals to further sophisticate their attacks. In this regard, Dasgupta et al. (2023) depict that technology of deep fake, which is based on artificial intelligence, simulates hyper-realistic fake audio, video, or images, and has become a significant source of threat to the financial institutions. Deep fakes provide an opportunity to mimic high-level executives or clients and evade checks of identity and enable a social engineering attack. Such manipulations in the banking sector may lead to fraud, intrusion without authorization and reputation. Smart phishing attacks have also become smarter. As opposed to conventional phishing attacks, AI allows producing very specific, situation-sensitive phishing emails that impersonate legitimate messages effectively. Such automated phishing attacks substantially multiply the chances to mislead bank employees and clients that consequently result in information theft or loss. In addition to that, AI is also being militarized to create self-learning malware that can adjust to security measures. These malware are able to avoid detection, change their behavior, and exploit vulnerabilities than the conventional malware. The cyber attacks that are based on AI are changing fast and therefore pose a dynamic threat to the US banks.

Risks of adversarial AI and algorithm manipulation:

On the other hand Yussuf (2025) asserts that adversarial AI is the active corruption of machine learning models to cause erroneous or malicious results. Regarding adversarial attacks of US banks, they may affect AI-based security systems through minor imperceptible changes in input data causing the misclassification or a system failure. As an example, malicious transactions can trick the fraud detection systems to slip into the system undetected. Also, the integrity of banking operations with AI-based customer authentication, credit scoring, or risk assessment procedures may be jeopardized because attackers can exploit AI models weaknesses. Complex AI models lie in the further addition of these risks, as they are not transparent. Therefore it is difficult to understand or identify, when systems are compromised.

Challenges of AI misuse by cybercriminals:

The availability of AI applications and open-source machine learning libraries has reduced the threshold of cybercriminals in taking advantage of AI technologies. Even less competent people can now cause sophisticated cyber attacks by using the AI-powered tools available on the cybercrime-as-a-service platforms. The automation and scalability features of AI enable criminals to plan massive attacks such as real-time data breach, identity theft, and ransomware attacks (Sembiring and Firdaus, 2025). Moreover, the high rate of AI evolution has exceeded the regulatory and defensive systems, and US banks are exposed to new methods of attacks. The issue is to strike a

balance between the implementation of AI and the effective risk management, as the potential of AI needs to be exploited in the responsible way. The possible use of AI as a tool by the bad actors should be minimized.

Analysis of the Effectiveness of AI-Based Cyber security Frameworks:

Effectiveness of AI in detecting and mitigating cyber risks:

Artificial Intelligence (AI) has greatly enhanced the capacity of banks to identify, detect, and react to cyber risks. The AI systems are effective in detecting threats, finding anomalies, and automatic response to incidents in real-time. Machine learning algorithms are able to work with large volumes of data on network traffic, transactional histories, and behavior patterns to detect anomalies, which could be a sign of fraud, malware or cyber intrusions. According to the research conducted by Deloitte, AI may decrease detection periods of cyber incidents and allow banks to address risks in minutes, rather than days (Deloitte, 2024). Moreover, the threat intelligence made possible by predictive analytics and AI enables banks to identify the possible weaknesses in advance and implement counter-measures. AI algorithms are able to provide patterns related to new threats, which leads to enhanced security against cyber attacks. AI implementation has become part of the Security Operations Centers (SOCs) of many US banks to automatically identify threats and decrease the number of human analysts involved in the process, lowering the response time.

Limitations in current AI-driven security solutions:

Although, AI offers a number of benefits, AI-based cyber security also has several shortcomings. Dependence on high quality of unbiased training data is one of the critical challenges. As per the views of Khan and Mirza (2024), the low quality of data may cause the wrong identification of threats, false positives, and/ or unnoticed vulnerabilities. Also, AI models may be subject to adversarial attacks, where the manipulated inputs trick the systems into reaching wrong conclusions. A second restriction is the black box characteristic of complex AI algorithms, whose complexity makes them relatively untransparent and unexplainable. The use of AI systems to make security decisions can be a challenge to financial institutions, as they may not be able to comprehend how it makes decisions. It makes auditing, compliance, and accountability procedures difficult. Besides this, the excessive reliance on AI with little or no human supervision may lead to complacency leaving banks vulnerable to advanced or new attack vectors that cannot be detected by AI. The speed, at which AI is evolving, has also left a disparity between the technological growth and the preparedness of the workforce, where most of the workers in the bank do not possess the skills to deal with or analyze the AI-driven security devices effectively.

Regulatory and ethical considerations for AI in cyber security:

The use of the AI in banking cyber security poses a lot of regulatory and ethical concerns. The regulatory authorities like the Financial Industry Regulatory Authority (FINRA) and the Federal Reserve have started to discuss the risks associated with AI like the considerations of the transparency, accountability, and data privacy protection (FINRA, 2024). Possible ethical issues are potential bias in the AI models, violations of privacy, and the unintended outcome of AI decisions. The US banks have to deal with a complicated regulatory system to make sure that the AI systems adhere to the legal norms, do not violate customer data, and are not discriminatory. Fair, accountable, and transparent ethical AI frameworks are the key to the development of trust and proper integration of AI in cyber security.

Balancing AI's Defensive Capabilities and its Potential Misuse:

The dual-use dilemma of AI in cyber security:

In accordance to Eskandarany (2024), Artificial Intelligence (AI) is an example of a classic dual-use dilemma in cyber security, since any of these technologies can be used to safeguard systems and maliciously to target them. Within the banking industry, AI defensive capabilities can have ability of quick threat identification, automation of responses to incidents, and instant prevention of fraud. Nonetheless, the same technologies can be used by cybercriminals to create better and more scalable attacks, including phishing based on AI-generation, deep fake impersonation, and self-adaptive malware. The dual use of AI presents a strategic issue for the US banking industry because the prevalence of AI tools, even open-source machine learning platforms, reduces the innovation barrier and the exploitation barrier. AI can protect security systems in banks. However, the same tools are used by the attackers to remain undetected, alter information, and exploit any weakness. Due to this reason, threat of misuse of AI is also ever-changing.

Perspectives from banking security professionals and policymakers:

Security professionals in the US banks see AI as a needed development and an upcoming risk. Although majority of the professionals in banking security sector believe that AI has enhanced their defensive position. Many of the banking professionals are afraid that AI-powered attacks may become hard to capture. These are concerns for policymakers, who are keen on ensuring that regulatory guardrails on the use of AI in financial services (AL-Dosari et

al., 2024). The transparency of AI models, required testing of adversarial robustness, and increased collaboration between banks and cyber security providers, advocated by U.S. regulatory agencies (the Department of the Treasury and the Federal Reserve). Both practitioners and policymakers agree that AI should be incorporated in a considered way, with an adequate level of control to ensure that unintended outcomes of this new technology are kept to minimum level and to maximize the security advantage of the technology.

Strategies to manage AI-induced risks:

The control over the AI-induced risks in US banks should be multi-dimensional. Aljunaid et al. (2025) articulate that Explainable AI (XAI) can be used to increase transparency so that human experts can explain AI decisions and validate the outputs as well as detect anomalies. This minimizes the chances of AI manipulation or errors that are not noticed. Secondly, effective threat intelligence sharing among financial organizations can assist in identifying attacks based on AI early and organize adequate response measures. Banks are also advised to work on red teaming, where they can simulate adversarial AI in order to understand the strength of their systems. Lastly, it is essential to put into practice ethical AI concepts, like fairness, accountability, and data privacy. Employee training on AI risks and regulatory compliance can be combined with the AI governance frameworks to mitigate misuse and allow banks to gain as much value as possible out of AI, when it comes to cyber security.

Research Aim and Objectives

The main purpose of developing this research article is to investigate the dual role of Artificial Intelligence (AI) in improving the cyber security measures and simultaneously introducing new cyber threats within the US banking sector. Following are the specific research objectives, which are developed in this research paper for accomplishment of the main purpose of this research paper:

- To evaluate the ways, n which different AI-driven technologies are applied across the US Banks for strengthening the cyber security systems
- To critically analyze the emerging cyber threats and vulnerabilities that is associated by the enhanced use of AI technologies in US Banks
- To examine the effectiveness of current AI-based security frameworks for mitigating the cyber security risks in the US banking sector
- To identify and evaluate the challenges experienced by the US banks while balancing the defensive capabilities of AI with its potential misuse by cybercriminals
- To develop practical recommendations that can be given to US banks for optimizing the AI applications for cyber security while minimizing associated risks/ threats

Research Methods

In this study, a descriptive and analytical research design has been used to examine the twofold impacts of the Artificial Intelligence (AI) in terms of enhancing cyber security and the emergence of new cyber threats in the US banks. This research methodology will help develop a thorough understanding of the topic, as it is a combination of the literature review and hypothesis testing, which makes it both theoretically and empirically valid. The literature review is a basis of this research and represents a systematic study and consideration of the available academic journals, industry reports, media report publications, and case studies related to the implementation of AI in cyber security in the banking industry of the United States (Rose et al., 2023). This research focuses on analysis of AI-based security innovations, threat detection systems, new AI-related cyber risks, and regulatory issues in the modern banking industry.

The purpose of literature review is to evaluate the secondary knowledge base in the field of chosen research issue, in order to identify the gaps in past research, as well as to give the theoretical basis to hypothesis formulation. Besides the literature review, the proposed study will use the hypothesis testing strategy to confirm the expected relationships between the AI integration, cyber security enhancement, and the emerging threats. The hypotheses have been formulated on the basis of the existing scholarly guidelines and the experience of past research (Bell et al., 2022). The research will be conducted through the examination of the secondary data, like case examples from US banking industry, analysis of reports on cyber attacks, the findings of the regulatory bodies, review and analysis of journal articles, etc.

The findings of the research will be interpreted using a qualitative and quantitative method of synthesis. Statistical data will be analyzed to determine correlations and effects and these will be according to the hypotheses formulated. This mixed-method study will assist in a balanced analysis of the positive inputs and the unintended risks of the AI in

the banking cyber security (Rose et al., 2023). In order to perform the testing of designed hypothesis, the techniques of regression analysis and paired t-test will be utilize. The selected research approach will be appropriate to present the comprehensive picture of the research issue as well as to offer the actionable recommendations to the banks in the US on how AI technologies may be used to achieve their maximum benefits and in a sustainable manner.

Research Problem

The essence of the research issue that is being pursued in the study is the dual influence of Artificial Intelligence (AI) on cyber security in the US banking ecosystem. Although AI-based technologies, including machine learning, predictive analytics, automated threat detection systems, and others, greatly enhance defensive capabilities of banks, they also introduce new and extremely sophisticated AI-driven cyber threats. This results in a paradox: banks are more and more turning to AI to get their security, but it is also the technologies that cybercriminals are utilizing to initiate deepfake fraud, AI-generated phishing, adversarial attacks, and self-learned malware. The research problem is thus more about the comprehension of such a compound nature of AI with dual aspects and whether the advantages of this new technology over the risks that are beginning to emerge are more than enough.

Importance of the Research Problem

The importance of the study can be explained by the fact that this study directly concerns financial stability, customer confidence, and national security. The opportunity and vulnerability become even more critical because US banks are a critical infrastructure, and the fast adoption of AI elements into their systems increases the chances of success and failure, respectively. The power of AI to identify anomalies and predict threats and automate response has revolutionized the field of cyber defense, cutting down losses and improving efficiency. Nonetheless, the emergence of AI-driven cybercrime has surpassed current laws and protection solutions. Knowing this duality is important to enable banks to implement AI without risks, regulators to develop effective regulations, and cyber security experts to develop resilient approaches. The research will fill a notable gap in knowledge since it will provide an evidence-based analysis of the defensive capabilities of AI as well as its unwanted effects.

Research Hypothesis

Following are different hypotheses that can be developed in context of this research article. These hypotheses will be tested in order to achieve planned aim of objectives of this research in effective manner. These hypotheses statements are as below:

H1: There is significant positive effect of AI-driven technologies on the improvement of cyber security levels in US banks.

H2: The introduction of AI technologies in the US banks is closely related to the appearance of novel cyber threats and vulnerabilities.

H3: The use of cyber security measures based on AI enhances the process of detecting and preventing cyber attacks in the US banking sector to a significant extent.

Research Boundaries (Scope and Limitations)

The study is bounded by several clearly defined parameters.

Conceptually, it focuses exclusively on AI applications related to cyber security—specifically threat detection, fraud prevention, predictive analytics, and AI-induced cyber vulnerabilities.

Geographically, the research is limited to the **United States banking sector** and does not examine financial institutions in other regions.

Methodologically, the study depends on secondary data including industry reports, academic publications, case examples, and statistical data from leading US banks. No primary interviews or surveys were conducted.

Empirically, the hypothesis testing is based on paired t-tests and regression analysis using available secondary datasets, which may not capture all real-time cyber threats.

Contextually, the research emphasizes major banks with advanced AI systems, meaning results may not generalize to smaller institutions with limited technological maturity.

Research Sample

The sample of the research is presented by secondary data and reported cases of the major banks in the US that have implemented AI on a massive scale. The major illustrations are the JPMorgan Chase, the bank of America and the Wells Fargo which are the biggest and the most technologically advanced financial institutions in the nation. These banks have been chosen because they have significant investments in AI, have published performance information,

and have reported that they are using AI in fraud detection, anomaly identification, and live risk assessment. Statistical data regarding the cyber attacks, detecting frauds, the level of AI implementation, and phishing cases driven by AI are also included in the sample.

Research Community

The research community includes:

- **Cyber security professionals**, who manage AI-powered security systems and respond to emergent threats.
- **US banking institutions**, particularly those integrating AI for cyber defense.
- **Regulatory bodies** such as FINRA and the Federal Reserve, responsible for overseeing safe AI adoption.
- **Academics and researchers** studying AI, cyber security, and financial risk management.
- **Technology developers and AI solution providers** contributing to banking security infrastructure.

Discussion and Analysis

JP Morgan is one of the major banks of the USA. This bank has taken decision to increase its total tech investment from $17 billion in 2024 to the level of $18 billion in 2025. In this total investment, the JP Morgan has allocated $600 million per year to the cyber security personnel and AI/cloud initiatives (Townsend, 2024; and Abrego, 2024). This kind of investment in the AI-driven fraud detection tools has enabled the management of the bank to block 1 million fraudsters annually and to approve 1 million additional legitimate customers. JP Morgan is experiencing cost savings of approximately $1.5 billion annually in the field of fraud prevention, credit, and trading. This kind of investment has helped the bank in enhancing the AI powered fraud detection and response times to cyber attack incidents by up to 300X faster as compared to traditional methods. The bank has experienced reduction of customer cost by around 30% and reduction of employees by 10% in the field of fraud and compliance functions (JP Morgan, 2024).

Similar to this, the Bank of America is also a major US bank of the USA. This bank has focused on implementation of ML-based anomaly detection for the user behavior and network traffic. This kind of investment has helped the bank in identifying and mitigating the ransomware attacks during the issues of overnight data spike. This technology helps in isolating the banking systems before major spread of the issue (Nwafor et al., 2024). This kind of technology investment helps the bank in real time detection of the issues of ransomware attacks.

Hypothesis Statements:

Null Hypothesis: There is no significant positive effect of AI-driven technologies on the improvement of cyber security levels in US banks.

Alternative Hypothesis: There is significant positive effect of AI-driven technologies on the improvement of cyber security levels in US banks.

It is planned to use and run the paired sample t-test for conducting hypothesis testing for the above hypothesis statements. This t-test is performed over data related to fraud detection time before AI and fraud detection time after AI. The level of significance is taken for this t-test as 5% or 0.05. The findings of paired sample t-test are as below:

t-Test: Paired Two Sample for Means		
Detection Time After AI (Minutes)	**Detection Time Before AI (Minutes)**	
0.6	180	Mean
0.00	122.22	Variance
10	10	Observations
	1.00	Pearson Correlation
	0	Hypothesized Mean Difference
	9	df
	51.49	t Stat
	0.00000000000099	P(T<=t) one-tail
	1.833112923	t Critical one-tail

	0.00000000000197	P(T<=t) two-tail
	2.26	t Critical two-tail

On the basis of analysis of outcomes of t-test, it is observed that value of P is very low (i.e. 0.00000000000099) as compared to the value of alpha or 0.05. So, the null hypothesis is rejected and alternative hypothesis will be accepted (Hartono et al., 2024). In this regard, it may be said that there is significant positive effect of AI-driven technologies on the improvement of cyber security levels in US banks.

AI and the Emergence of New Cyber Threats:

The issue of phishing attacks is faced with the enhanced use of AI. For example, the 40% of phishing emails that are targeting the businesses are generated by the AI. In accordance to the report of FBI & Zscaler, there is significant increase in the highly targeted and AI powered spear-phishing campaigns after the emergence of advanced generative AI tools (Alexander, 2024). In the modern time, the incidents of synthetic IDs and deep fake audio/video have increased that are created using the generative AI. These incidents are also targeted for purposes of phishing and account takeover. It is predicted by the Deloitte that AI-driven fraud losses of the US financial services will increase from $12.3 billion (2023) to $40 billion by 2027 (Vanderford, 2024).

Hypothesis Statements:

Null Hypothesis: The introduction of AI technologies in the US banks is not closely related to the appearance of novel cyber threats and vulnerabilities.

Alternative Hypothesis: The introduction of AI technologies in the US banks is closely related to the appearance of novel cyber threats and vulnerabilities.

It is planned to conduct testing of above hypothesis by using the regression analysis technique. The value of alpha or significance level is taken as 5% or 0.05. Dependent variable is taken as number of AI driven phishing incidents. At the same time, AI systems deployment is taken as the independent variable. The findings of regression test are as below:

SUMMARY OUTPUT	
Regression Statistics	
1	Multiple R
1	R Square
1	Adjusted R Square
0	Standard Error
3	Observations

					ANOVA
Significance F	*F*	*MS*	*SS*	*df*	
#NUM!	#NUM!	3200	3200	1	Regression
		0	0	1	Residual
			3200	2	Total

	Coefficients	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*	*Lower 95.0%*	*Upper 95.0%*
Intercept	0.0000	0	65535	0	0	0	0	0
X Variable 1	40	0	65535	0	40	40	40	40

Y = 40X

Where:
Y = AI driven phishing incidents
X = AI systems deployed
On basis of findings of egress test, it is visible that value of P (i.e. 0.00) is less than the level of significance of 0.05. So, null hypothesis is rejected and alternative hypothesis is accepted (Farayola, 2024). It can be said that the introduction of AI technologies in the US banks is closely related to the appearance of novel cyber threats and vulnerabilities.

Role of AI for Enhancing Accuracy of Cyber Attack Detection Process:

Hypothesis Statements:
Null Hypothesis: The use of cyber security measures based on AI does not enhance the process of detecting and preventing cyber attacks in the US banking sector to a significant extent.
Alternative Hypothesis: The use of cyber security measures based on AI enhances the process of detecting and preventing cyber attacks in the US banking sector to a significant extent.
It is planned to conduct paired t-test for performing testing of above hypotheses. This test will be conducted over the data related to detection accuracy and response time. The findings of t-Test can be summarized in below manner:

t-Test: Paired Two Sample for Means		
After AI (min)	***Before AI (min)***	
84.6875	509.375	Mean
30.89583333	722.9166667	Variance
16	16	Observations
	0.625351155	Pearson Correlation
	0	Hypothesized Mean Difference
	15	df
	71.34734839	t Stat
	0.000000000000000000104	P(T<=t) one-tail
	1.753050325	t Critical one-tail
	0.000000000000000000208	P(T<=t) two-tail
	2.131449536	t Critical two-tail

The findings of paired t-Test indicates that value of P is very low (0.000000000000000000104) as compared to the level of alpha (0.05). This means the null hypothesis is rejected and alternative hypothesis is accepted (Owolabi et al., 2024). In this regard, it may be sad that use of cyber security measures based on AI enhances the process of detecting and preventing cyber attacks in the US banking sector to a significant extent.

Best practices for responsible AI deployment:

In order to maximize the use of Artificial Intelligence (AI) for improving cyber security, the US banks need to embrace the best practices that allow responsible, transparent, and secure AI implementation. Among such recommendations, the use of Explainable AI (XAI) that increases the transparency of the system by allowing human control and comprehension of the AI decision-making process is one of them. Open AI is able to minimize the possibility of unnoticed mistakes, bias, or malicious tampering. Additionally, AI implementation must be governed by rigorous data governance processes, so that quality, unbiased, and safe datasets are applied to train machine learning models (Hartono et al., 2024). The consistency of the audits, ethical inspections, and compliance testing should be carried out regularly to make sure that AI works in accordance with the legislation and ethical norms. Human-AI collaboration is an essential consideration in banks, as the AI supplements the human skill, and not entirely automates the key security decisions, leaving responsibility and control. Moreover, it is necessary to invest in the training of the

workforce. In order to promote the culture of using AI responsibly within the banking practice, it is vital to train and educate the employees about the risks, capabilities, and limitations of AI. This knowledge should be given to both technical and non-technical employees.

Policy and technological recommendations:

Policy wise, regulators ought to introduce tighter AI risk evaluation frameworks, which would involve stress testing, adversarial robustness assessments, and monitoring of the AI based banking system. Governments, regulatory authorities, organizations, and all financial institutions have an increasingly vested interest in the necessity of standardized AI governance focused on model transparency, fairness, and accountability. In terms of technology, the banks must incorporate AI into a multi-layered defense approach and incorporate conventional cyber security control into the AI-based detection and response systems (Farayola, 2024). This comprises of the use of AI to monitor the network in real-time, detect anomalies, and provide predictive threat intelligence and ensure the capability of human override to avoid excessive dependence on automated operations. It is also essential that banks, technology providers, and government agencies collaborate. Exchange of threat intelligence about the AI-powered cyber attacks can greatly complement the collective defense mechanisms considering the dynamic AI misuse patterns by cybercriminals.

Future directions for AI research in banking security:

Future technologies and research are vital to deal with new issues and to improve AI in the field of banking cyber security. The further area of research direction is the exploration of adversarial AI resilience, the development of models that are not prone to manipulation and able to defend themselves against AI-based threats. Federated learning developments will help to improve data privacy, as they allow training AI without disclosing sensitive data about customers on decentralized networks (Owolabi et al., 2024). Additionally, AI, cyber security, ethical, and regulatory research that brings together diverse disciplines will play an important role in defining responsible innovation. With the development of AI technologies, academic institutions, industry players, and policymakers will have to collaborate continuously to enhance the AI applications in banking industry in a way that enhances security and trustworthiness of the US banks.

Conclusion

The study finds that Artificial Intelligence (AI) can transform the sphere of cyber security of US banks; however, it also has an ambivalent impact. Through literature analysis and testing of the hypothesis based on the artificial intelligence approach, the research proves that AI-based technologies, including machine learning, predictive analytics, anomaly detection, and automated threat response, have a substantial positive impact on the cyber attack detection, reduction of the response time, and aversion of the massive loss of financial resources that occur in the financial sector. Strong positive impacts of AI on the accuracy of fraud detection and efficacy in mitigating an incident are statistically proven by paired t-tests and the regression analysis. Meanwhile, the results suggest that the growing popularity of AI has brought forth advanced AI-based cyber threats, such as deepfake-enabled frauds, targeted phishing attacks, adversarial manipulation of algorithms, and self- Learning malware, which increase the threat environment of financial institutions in sum.

Since this is a dual-use aspect, the study highlights that AI is not something that can be applied in its purest form; it must be implemented responsibly, transparently, and well-controlled. The adoption of Explainable AI (XAI) to increase the level of transparency, trust, and oversight is the most crucial recommendation. Well-formed strategies should also lead banks to invest in adversarial robustness testing, robust data management, ethical AI systems, and sustained employee training to deal with new dangers. Finally, despite the undeniable potential of AI in enhancing cyber defense, it can be maximized only with the active governance predicting, preventing, and adjusting to the changing threats of AI.

Recommendations

Recommendation 1: Implement Explainable and Transparent AI Frameworks: The US banks are advised to focus on the implementation of Explainable AI (XAI) so that all AI-based cyber security decisions could be transparent, interpretable, and auditable. This research indicates that complex AI models tend to become black boxes and this generates uncertainty, regulatory difficulty, and even chances of manipulation without being detected. XAI allows cyber security personnel to get a glimpse of how AI systems detect threats, categorize abnormalities, or sanction transactions, and this minimizes the chance that AI systems will make mistakes or abused by adversarial elements. Through the incorporation of XAI into the systems of fraud detection, authentication, and monitoring

threats, banks can reinforce their accountability, increase their compliance with regulatory requirements and trust in automated decision-making procedures.

Recommendation 2: Strengthen Adversarial Robustness and Continuous Testing: Since AI-driven cyber threats have grown at an alarming rate in recent years, including deep fakes and synthetic identities, and even manipulating algorithms, banks need to implement ongoing adversarial stress tests. These are red teaming, AI-generated simulation attack testing, and proactive risk modelling. Consistent testing will also be used to detect the vulnerability of systems before a hacker uses it. The results of the study prove that AI can help and harm cyber security, which is why it is extremely important that the banks analyze the performance of their models in case of an attack. Resilience will make AI systems reliable despite being subjected to advanced adversarial methods.

Recommendation 3: Develop Strong Governance, Regulation Alignment, and Workforce Training: Banks have to develop an all-encompassing AI governance framework that is consistent with regulations imposed by the respective bodies like FINRA and the Federal Reserve. This consists of stringent data management policies, ethical AI principles and quarterly compliance audits. Moreover, the banks are to invest in the upskilling of the workforce extensively, including the guarantee that both technical and non-technical workers become aware of the risks, capabilities and restrictions of AI. The improved training will encourage the responsible use of AI, minimize the operational errors, and promote a culture of cyber awareness. Strong governance and quality workforce will make AI safely, ethically and successfully implemented throughout the banking industry.

References

Abrego, M. (2024) *AI is core to JPMorgan's $18 billion tech investment. Here's what its execs revealed about how it's reshaping the bank.* [Online]. Available at: https://www.businessinsider.com/jpmorgan-how-artificial-intelligence-transforming-workflows-efficiencies-2025-5 (Accessed: 02 July 2025).

AL-Dosari, K., Fetais, N. and Kucukvar, M., (2024) Artificial intelligence and cyber defense system for banking industry: A qualitative study of AI applications and challenges. *Cybernetics and systems*, *55*(2), pp.302-330.

AL-Dosari, K., Fetais, N. and Kucukvar, M., (2024) Artificial intelligence and cyber defense system for banking industry: A qualitative study of AI applications and challenges. *Cybernetics and systems*, *55*(2), pp.302-330.

Alexander, N. (2024) *Official warnings mount as AI driven attacks on finance become a reality.* [Online]. Available at: https://www.bobsguide.com/ai-driven-attacks-on-finance-become-a-reality/ (Accessed: 02 July 2025).

Aljunaid, S.K., Almheiri, S.J., Dawood, H. and Khan, M.A., (2025) Secure and transparent banking: explainable AI-driven federated learning model for financial fraud detection. *Journal of Risk and Financial Management*, *18*(4), p.179.

Atadoga, A., Obi, O.C., Onwusinkwue, S., Dawodu, S.O., Osasona, F. and Daraojimba, A.I., (2024) AI's evolving impact in US banking: An insightful review. *International Journal of Science and Research Archive*, *11*(1), pp.904-922.

Bell, E., Harley, B. and Bryman, A., (2022) *Business research methods*. Oxford University Press.

BOA (2024) *Erica®, the guide by your side, is here for you.* [Online]. Available at: https://info.bankofamerica.com/en/digital-banking/erica (Accessed: 03 July 2025).

Dasgupta, S., Yelikar, B.V., Naredla, S., Ibrahim, R.K. and Alazzam, M.B., (2023) AI-powered cybersecurity: identifying threats in digital banking. In *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)* (pp. 2614-2619). IEEE.

Deloitte (2024) *Cyber AI: Real defense.* [Online]. Available at: https://www.deloitte.com/us/en/insights/topics/technology-management/tech-trends/2022/future-of-cybersecurity-and-ai.html (Accessed: 03 July 2025).

Eskandarany, A., (2024) Adoption of artificial intelligence and machine learning in banking systems: a qualitative survey of board of directors. *Frontiers in Artificial Intelligence*, *7*, p.1440051.

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

FINRA (2024) *AI Applications in the Securities Industry.* [Online]. Available at: https://www.finra.org/rules-guidance/key-topics/fintech/report/artificial-intelligence-in-the-securities-industry/ai-apps-in-the-industry (Accessed: 03 July 2025).

Fitria, T.N., (2023) Artificial intelligence (AI) technology in OpenAI ChatGPT application: A review of ChatGPT in writing English essay. In *ELT Forum: Journal of English Language Teaching*, 12(1), pp. 44-58.

Hartono, H., Wijaya, R.A. and Khotimah, K., (2024) Development of Detection and Mitigation of Advanced Persistent Threats Using Artificial Intelligence and Multi-Layer Security on Cloud Computing Infrastructure. *International Journal of Artificial Intelligence Research*, *8*(2), pp.194-211.

JP Morgan (2024) *How AI will make payments more efficient and reduce fraud.* [Online]. Available at: https://www.jpmorgan.com/insights/payments/payments-optimization/ai-payments-efficiency-fraud-reduction (Accessed: 03 July 2025).

Khan, A. and Mirza, S., (2024) AI-Driven Solutions for Efficient Detection of Banking Fraud. *Advances in Computer Sciences*, *7*(1).

Khan, M.I., Arif, A. and Khan, A.R.A., (2024) AI-Driven Threat Detection: A Brief Overview of AI Techniques in Cybersecurity. *BIN: Bulletin of Informatics*, *2*(2), pp.248-61.

Nwafor, K.C., Ikudabo, A.O. and Onyeje, C.C., (2024) Mitigating cybersecurity risks in financial institutions: The role of AI and data analytics. *International Journal of Science and Research Archive,* 13(1), pp. 2895–2910.

Owolabi, I.O., Mbabie, C.K. and Obiri, J.C., (2024) AI-Driven Cybersecurity in FinTech & Cloud: Combating Evolving Threats with Intelligent Defense Mechanisms. *International Journal of Multidisciplinary Research in Science, Engineering and Technology*, *7*, p.12.

Rose, S., Spinks, N. and Canhoto, A.I., (2023) *Management research: applying the principles of business research methods*. Routledge.

Sembiring, J. and Firdaus, S.U., (2025) Criminal Liability For Misuse Of Artificial Intelligence (Ai) In Deepfake Crimes. *INTERNATIONAL JOURNAL OF MULTI SCIENCE*, *5*(01), pp.1-9.

Townsend, K. (2024) *With $600 Million Cybersecurity Budget, JPMorgan Chief Endorses AI and Cloud.* [Online]. Available at: https://www.securityweek.com/600-million-cybersecurity-budget-jpmorgan-chief-endorses-ai-and-cloud/ (Accessed: 02 July 2025).

Vanderford, R. (2024) *GenAI Increasingly Powering Scams, Wall Street Watchdog Warns.* [Online]. Available at: https://www.wsj.com/articles/genai-increasingly-powering-scams-wall-street-watchdog-warns-a6592d54 (Accessed: 02 July 2025).

Yussuf, M., (2025) Advanced cyber risk containment in algorithmic trading: Securing automated investment strategies from malicious data manipulation. *Int Res J Mod Eng Technol Sci*, *7*(3), p.883.

Zaki, A.M., Khodadadi, N., Hong Lim, W. and Towfek, S.K., (2024) Predictive Analytics and Machine Learning in Direct Marketing for Anticipating Bank Term Deposit Subscriptions. *American Journal of Business & Operations Research*, *11*(1).