Journal of Business Insight and Innovation
Volume 5 Issue 6, 2026
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

ARTIFICIAL INTELLIGENCE–DRIVEN FRAUD DETECTION IN FINTECH: STRENGTHENING CYBERSECURITY AGAINST DIGITAL FINANCIAL SCAMS

Sana Ullah Khan [1], Umair Zafar [2], Shamikh Imran [3], Muhammad Ali [4]

DOI: https://doi.org/10.63544/jbii.v5i6.116

Affiliations:

[1] MS Artificial Intelligence, The Islmia University of Bahawalpur, Pakistan
Email: sanaullahkhan.hse@gmail.com

[2] Student, Indiana State University, USA
Email: uzafar@sycamores.indstate.edu

[3] Department of Computer Science, Abbottabad University of Science and Technology, Havelian, KPK, Pakistan
Email: shamikhimran07@gmail.com

[4] Master's Student, Graduate School of Design, Harvard University, USA
Email: ali_ali@mde.harvard.edu

Corresponding Author's Email:
[1] sanaullahkhan.hse@gmail.com

Article History:
Received: 18.05.2026
Accepted: 12.06.2026
Published: 20.06.2026

Abstract

Artificial intelligence (AI) has transformed fraud detection, enabling financial institutions to spot suspicious transactions, predict new fraud trends, and boost cybersecurity to combat digital financial crimes. The research included applying AI for fraud detection and cybersecurity enhancement in the FinTech sector. The study used a quantitative research design, and primary data were gathered from 385 respondents from diverse organizations like FinTech, digital banks, payment service providers and cybersecurity firms in Pakistan through a structured questionnaire. The data were analysed using SmartPLS 4. Descriptive statistics summarized respondents' perceptions of artificial intelligence, machine learning capabilities, real-time transaction monitoring, anomaly detection, and effectiveness of cybersecurity. Results indicated a high inter-item consistency for all study constructs. The mean values of AI-based fraud detection, machine learning capability, actual-time transaction monitoring and anomaly detection were in the range of 4.02 to 4.18, 4.09 to 4.27, 4.22 to 4.35 and 4.18 to 4.32 respectively. The findings revealed that the respondents recognized AI as a valuable tool for improving the accuracy of fraud detection, automating manual inquiries, detecting unusual transaction patterns, and strengthening the security of digital financial systems. The average results were high, demonstrating high confidence in the intelligent fraud detection technologies in preventing financial fraud and improving the organization's security performance. The study found that AI and machine learning, combined with real-time monitoring and anomaly detection, offered robust protection against digital financial fraud and improved the security, adaptability, and resilience of FinTech. The results offered practical insights for financial institutions, cybersecurity specialists, technology developers, and policymakers focused on enhancing digital financial security through intelligent fraud-detection frameworks.

Keywords: Anomaly Detection, Artificial Intelligence, Cybersecurity, Digital Financial Scams, FinTech, Machine Learning

1. Introduction

Technologies involved in providing financial services at lower prices to consumers and financial institutions through digital channels were identified as Financial technology (FinTech). The digital revolution in financial services propelled financial technologies (FinTech) that extend consumers' and financial institutions' access to financial services. This technological leap ensured that processes would be more efficient, financial inclusion would grow, and customers' lives would become more convenient but also a part of the cyber threat landscape. Criminals took advantage of the vulnerabilities found in phishing attacks, payment fraud, synthetic identities, identity theft and account takeover, as more transactions started moving online. However, traditional fraud detection systems have fallen short when it comes to the constantly changing and increasingly sophisticated fraud patterns, as they are not adaptive and are based on a predetermined set of rules. When it comes to detecting anomalous transaction patterns, deep learning and machine learning, emerging components of the artificial intelligence (AI) ecosystem, have proven useful for detecting back-door fraud and for real-time cybersecurity decision-making (Hafez et al., 2025; Shpachuk et al., 2026).

Financial activities were becoming increasingly sophisticated, and more intelligent systems were needed to process the vast amounts of data involved in financial transactions in mere milliseconds. AI-driven systems for fraud detection outperformed traditional statistical approaches by leveraging predictive analytics, anomaly detection, behavioural biometrics, and network analysis to identify fraud. As a result, because it allows them to adapt to evolving types of transactions and fraud, it has become a trend and an addition to financial institutions' cybersecurity systems. The latest studies have shown that adopting machine learning algorithms has significantly improved fraud detection rates and reduced false-positive rates, operational costs, and response times in digital financial platforms (Buiya, 2026; Zhang et al., 2025).

The adoption of recent developments such as explainable AI, graph neural networks, and ensemble learning further enhanced the capabilities of modern FinTech architectures to prevent fraud. These intelligent systems analysed a user's activity, transaction speed, geographic location, device data, previous transactions, and other metrics to provide a comprehensive picture of fraud risk. Alongside cloud computing, big data analysis, blockchain technologies, and cybersecurity intelligence, artificial intelligence (AI) has ushered in a new financial battleground that is much better equipped and more alert to the evolving sophistication of cyberattacks. In the current context, AI systems used for fraud detection have minimized fund losses, heightened regulatory strictures, enhanced customer comfort, and further strengthened the organization's resilience against digital financial scammers (Aryeetey & Yeboah, 2026; Sorinola & Hamed, 2026).

It may be noted that although tremendous progress has been achieved in AI, there have been challenges with adversarial attacks, algorithmic transparency, privacy protection, data imbalance, and model interpretability pertaining to AI-driven fraud detection. In addition to DFI threats, any use of generative AI, deepfake and automated attack methods for overcoming traditional cyber security practices is also a trend among criminals. The level of sophistication and the sophistication of their advances suggests that these types of models need to be continually enhanced so that they are effective in combating new variations of the attack and maintain the model fair and transparent. The outer threats of digital financial fraud are constantly evolving, and AI-based fraud detection is beginning to be more successful in protecting FinTech cybersecurity strategies (Dhakaweeshi, 2022). The rise of new digital financial fraud methods, the importance of AI-powered fraud detection in bolstering FinTechs' cybersecurity strategies has become a focal point for financial institutions, cybersecurity experts, regulators, and policymakers seeking sustainable protection (Rahim et al., 2026; Hafez et al., 2025).

Background of the Study

FinTech has transformed the Banking Industry with mobile banking, Digital wallets, P2P payments, Cryptocurrencies, Open Banking, and the use of artificial intelligence (AI) and AI banking services in mainstream Banking. Other parts of cybersecurity had to be addressed with something more complex than traditional fraud responses, and that was where the benefits lay: speed and access to transactions. Financial fraud very soon transformed from sporadic cases into advanced, automated, region-specific, and international. Financial institutions experimented with AI, machine learning, real-time analytics tools, and more to aid in fraud prevention and ensure secure, robust operations. The additions of intelligent cybersecurity infrastructures, based on AI/ML, as well as real-time analytics played a major role in improving fraud detection as well as enhancing operational security and robustness (Hafez et al., 2025; Rahim et al., 2026).

Journal of Business Insight and Innovation
Volume 5 Issue 6, 2026
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

Fraud detection is an area where Artificial Intelligence (AI) has changed the game, replacing manual and rule-based analyses with learning models that continually learn to make increasingly accurate predictions. Artificial Intelligence (AI), a big development in fraud detection, has moved beyond static rules to models that learn and adapt over time, much more than being predictive, which has a greater degree of capabilities. By using supervised learning, unsupervised anomaly detection, reinforcement learning, and deep neural networks, companies were able to detect fraud-and eliminate it, without inflicting any loss. These AIs were able to analyze vast amounts of data, from structured to unstructured, discern behavioral models, and deliver instant risk scores, facilitating instant security calls to action. The recent systematic reviews confirm that AI technologies have proven effective in the fight against fraud in diverse sectors, such as banking, payment systems, insurance, and digital commerce.

Cyber security has emerged as a crucial part of FinTech strategies as digitally driven financial crimes have become widespread and intricate.In the midst of increasingly complex and common digitized financial crimes, cyber security has become an important aspect of FinTech strategies. Five new trends have grown up around financial systems that people are making more use of: Social engineering attacks, deepfakes, AI phishing attacks, and synthetic identity theft. Today, they have the ability to take advantage of social engineering, AI phishing and deepfakes – crimes that are growing in popularity. These new attacks needed smart cyber security solutions which were capable of detecting not only conventional fraud patterns, but also behavioral patterns of new attacks. The results showed that AI in fraud detection can enhance transaction monitoring, bolster authentication processes, mitigate financial losses, and boost consumer confidence in digital financial services, aligning with numerous studies reported in the literature (Shpachuk et al., 2026; Sorinola & Hamed, 2026).

Government, consumers and operational resilience requirements further contributed to the growth of financial institutions' adoption of AI technology for fraud detection, especially with regard to cyber insurance-specific requirements. Government, consumer protection, and operational resilience were among cyber insurance specific requirements, ensuring that financial institutions took an accelerated push towards using AI for fraud detection. The need for government regulation, financial regulator role, and international cybersecurity organizations championing trust in digital financial ecosystems and the importance of proactive fraud monitoring strategies, explainable AI, and responsible data governance in supporting these strategies. The results of the detection level have proved promising, but more research is required to identify the potential impact of emerging attacks and fraud on the detection capabilities of AI technologies. In the context of the above, this study wanted to explore the potential of AI in combating the risk of digital financial scams and how that can have an impact on the formation of secure, smart, and resilient digital financial systems (Rahim et al., 2026; Shpachuk et al., 2026).

Research Objectives

1. To study AI-powered fraud detection for the effectiveness on cyber security in the FinTech Industry.
2. To find out how Machine Learning Fraud Detection is effective in stopping digital financial frauds.
3. To know the advantages real-time transaction monitoring can offer to improve the fraud detection performance of fintech platforms.
4. To evaluate how well the Apnea can enhance cybersecurity's resilience to digital financial fraud.

Research Questions

Q1. What are the implications for the effectiveness of cybersecurity in the FinTech sector with the use of AI-based fraud prevention systems?

Q2. What is the impact of machine learning–based fraud detection on the prevention of digital financial fraud?

Q3. Why is real-time transaction monitoring gaining momentum as an integral part of the right approach to accurate fraud detection in FinTech platforms?

Q4. What benefits do anomaly detection techniques offer in enhancing financial cybersecurity resilience to digital financial fraud?

Significance of the Study

This research complements the existing literature on the role that AI can play in fraud detection and the potential it poses cybersecurity, particularly FinTech systems, can use to stand in the way of digital financial fraud. The results demonstrated the necessity of machine learning, instant transaction monitoring and anomaly detection for bolstering a cybersecurity resilient ecosystem and reducing financial crime risks. It offers practical recommendations to various stakeholders, including FinTech firms, banks, financial institutions, cyber security specialists, software developers and regulators, to build up effective and intelligent fraud prevention systems. The results also provided evidence for policy strategies and cybersecurity legislation to promote safe digital financial markets, increase consumer trust and to promote sustainable digital financial services.

2. Literature Review

Artificial Intelligence and Fraud Detection in FinTech

Artificial Intelligence-based fraud detection tools have emerged as one of the biggest gamechangers in the FinTech industry, enabling financial institutions to leverage intelligent data analysis and predictive modelling to detect suspicious activities and transactions. Unlike rule-based systems, an AI algorithm can learn continuously from past and real-time transactions, detect new types of fraud more accurately and quickly, and alert the business. Machine learning, deep learning, or ensemble learning approaches are being used to shift large financial datasets toward minimizing false-positive indicators. As revealed in recent publications, AI is turning out to be a helpful tool for platforms dealing in financial transactions online (Hernandez Aros et al., 2024; Abdulkreem & Abdulazeez, 2024), and AI has resulted in significant improvements in the efficiency of business operations, reduced financial losses, and enhanced cybersecurity measures.

In recent studies, another key point of observation regarding the combination of AI with Cloud technology, along with big data analytics plus behaviourality, was the added value to reveal better relationships- invisible relationships between the financial transactions in fraud systems. These wise systems were capable of adapting to new forms of fraud and helping implement proactive cybersecurity strategies. Researchers concluded that, in the FinTech sector, AI is a technology underlying capable of helping create resilient and secure ecosystems that can meet the growing sophistication of cyber threats (Papasavva et al., 2024; Chen et al., 2025).

Data Mining and Live Fraud Prevention

Machine learning technology can process such a large volume of transactions within the beat of the heart as soon as possible; several government agencies and financial institutions quickly recognized its potential to process large volumes of transactions in real time. Anomalies not detected by conventional statistical methods were identified using supervised, unsupervised, and hybrid learning algorithms. The techniques were continuously updated to keep predictive models current with fresh transaction data, thereby boosting fraud detection accuracy and reducing response time. In the banking, payments, insurance, and online financial services industries, machine learning algorithms have demonstrated strong performance in detecting fraud (Yussiff et al., 2024; Hernandez Aros et al., 2024).

It was also observed that Financial Institutions could prevent the creation of fraudulent transactions in real time before they cause damage to the financial system. Real-time machine learning algorithms analyzed customer activity, device information, geolocation, transaction velocity, spending patterns, and other factors to calculate predictive risk scores. These were crunched through advanced machine-learning models to generate real-time fraud risk scores. These capabilities proved highly beneficial in increasing consumers' financial stability and confidence in digital payment methods and reducing the costs of conventional fraud investigations (George et al., 2025; Cervera & Deocareza, 2024).

Cybersecurity and Digital Financial Scam Prevention

Increasingly sophisticated cybercriminals are now using phishing, fake identities and deepfake technology to perpetrate digital financial fraud, keeping cybersecurity a key concern for FinTech organizations. AI LLM cybersecurity solutions provided live monitoring, detection of anomalies, and instant incident responses that created improved fraud prevention opportunities. Adopting the AI LLM's cyber security solutions could take the burden off the shoulders of businesses, with advanced fraud protection features that encompass real-time threat detection, continuous monitoring and vigilance, and automated incident responses. Highly intelligent fraud detection systems have made companies more resilient by detecting fraud attempts and preventing them from reaching financial assets (Abdulkreem & Abdulazeez, 2024; Cheng et al., 2024).

The latest research showed that AI-powered security solutions indeed contributed to regulatory compliance, greater financial transparency and customers' trust in financial services in the digital sphere. Some challenges have been recognized in this area, such as the transparency of the algorithm, privacy of data, attacks on the algorithm, and interpreting the model. Prior research has also recommended the need to develop new models that are more explainable while maintaining a high accuracy in identifying fraud in the new financial landscape of FinTec, that are fair, accountable and resist cyber attacks (Hernandez Aros et al., 2024; Papasavva et al., 2024).

3. Research Methodology

Research Design

This study employed a quantitative research approach with an exploratory design to promote digital financial fraud cybersecurity in the FinTech industry using the artificial intelligence (AI) fraud prevention systems. It was decided that a cross sectional survey should be done as much data could be collected from the respondents within a month and a maximum of one year of observing a single cross section. This design was used to statistically analyse the relationship between variables that were included in the study.

Population and Sample

The base population consisted of the staff of FinTech firms, cybersecurity providers, digital banks and payment service providers in Pakistan. They were knowledgeable about the newest technologies and fraud prevention methods in the world of artificial intelligence. For these data, all of the respondents were selected randomly from the population to ensure that each member of the population had the same chance at being selected (simple random sampling).

Data Collection

Primary data on the topic of artificial intelligence, cybersecurity and financial frauds detection was collected through a structured questionnaire meant for collecting primary data and it was researched from literature survey done. The questionnaire contained descriptive questions and items to measure the research variables. The responses were obtained on a five-point Likert scale (1 Strongly Disagree, 5 Strongly Agree). Survey was delivered electronically (via mail and online).

Measurement of Variables

The study included Artificial Intelligence–Driven Fraud Detection as the independent variable and Cybersecurity Against Digital Financial Scams as the dependent variable. Three key aspects to consider regarding AI's capabilities in fraud detection are Machine Learning Capability, Real-Time Transaction Monitoring, and Anomaly Detection. Five measures, adapted to the present study from previously published research, were used to assess each construct.

Reliability and Validity

To assess the reliability of the measurement tool, Cronbach's Alpha and Composite Reliability (CR) have been used. Convergent validity has been assessed using Average Variance Extracted (AVE), and discriminant validity has been tested using the Fornell–Larcker Criterion and the HTMT ratio. The properties attained met the requirements, indicating that the measurement model was reliable and valid.

Data Analysis

An analysis using SmartPLS 4 was performed on the collected data. The characteristics and study variables of the respondents were summarized in descriptive statistics. The reliabilities and validities of the measurement model were assessed, and the proposed relations were evaluated using path coefficients, t-values, p-values, and R2 values in the structural model. A bootstrapping procedure with 5,000 resamples was performed to determine the statistical significance of the results.

4. Results and Analysis

Demographic Profile of the Respondents

The demographic analysis summarized the characteristics of the respondents who participated in the survey.

Table 1

Demographic Profile of the Respondents (N = 385)

Demographic Variable	Category	Frequency	Percentage (%)
Gender	Male	226	58.7
	Female	159	41.3
Age	21–30 Years	108	28.1
	31–40 Years	167	43.4
	41–50 Years	79	20.5
	Above 50 Years	31	8.0
Education	Bachelor's Degree	124	32.2
	Master's Degree	186	48.3
	MPhil/MS	53	13.8
	PhD	22	5.7
Experience	Less than 3 Years	81	21.0
	3–5 Years	132	34.3
	6–10 Years	109	28.3
	More than 10 Years	63	16.4

Males constituted 58.7% of the sample compared to 41.3% for females, according to a gender distribution. This distribution had an equal degree of participation by professionals from the FinTech and cybersecurity areas. Both men and women were involved in the process, which helped to further nuance the discussion on AI-powered fraud detection and cybersecurity practices. In terms of age profile, majority (43.4%) of the respondents were of age group 31-40 years. The ages of the respondents were 21 to 30 (28.1%), followed by 41 to 50 (20.5%). Less than 1 in 10 were aged 51-60 or 60 years and over. As far as education is concerned, the respondents included 48.3 per cent who had master's degree, and 32.2 per cent who had a bachelor's degree. Forty-three percent (43%) respondents had MPhil/MS (qualifications) and 3.7% had PhD. Professional experience also revealed that a good balance between frequency was observed with the maximum frequency (34.3%) experienced 3-5 years. These answers raised overall a positive profile on AI solutions for fraud detection and cybersecurity as well as professionals' high levels of academic achievement and experience, required to come up with answerable questions regarding AI for the FinTech industry.

Distribution of Responses for Artificial Intelligence–Driven Fraud Detection

The analysis focused on the level of agreement with various statements regarding intelligent fraud detection systems.

Table 2

Response Distribution for Artificial Intelligence–Driven Fraud Detection

Statement	SD	D	N	A	SA	Mean
AI systems identify suspicious transactions quickly.	8	19	41	182	135	4.08
AI improves fraud detection accuracy.	6	17	39	176	147	4.15
AI reduces manual fraud investigation.	11	24	46	170	134	4.02
AI supports automated fraud prevention.	9	21	43	175	137	4.07
AI enhances cybersecurity performance.	5	16	35	179	150	4.18

According to all the respondents, AI was effective to identify fraud in the FinTech industry (see Table 2). AI systems are able to detect suspicious transactions rapidly was supported by an average agreement rating of 4.08, suggesting opinions are not all that far apart regarding AI's ability to detect suspicious financial transactions rapidly. The ones surveyed had a mean score of 4.15, indicating that they greatly considered AI improved the accuracy of distinguishing fraud from routine transactions compared to traditional methods. The "AI reduces manual fraud investigation" mean score was 4.02 as respondents stated they agree once the ability of AI to reduce manual monitoring and investigation activities is included in the statement. The opposite, "AI can prevent fraud automatically", had an average of 4.07, which is equivalent to a moderate trust in AI systems to be able to automatically detect fraud. The statement which received the highest rating on average (4.18) was AI improves cybersecurity performance. This paves the way for AI to be a great asset in improving the security measures used in digital financial services. The average rating across all of the statements was higher than 4.00, suggesting respondents generally felt that AI fraud detection has good potential benefits and that there was currently a high level of trust in intelligent technologies to safeguard FinTech platforms against digital financial fraud.

Machine Learning Capability in Fraud Detection

The primary areas of AI fight fraud was machine learning. This analysis examined how well participants thought machine learning algorithms would make electronic financial systems more effective at detecting fraud.

Table 3

Machine Learning Capability

Statement	Mean	Std. Deviation
Machine learning improves fraud prediction.	4.24	0.62
Algorithms continuously learn new fraud patterns.	4.18	0.66
Machine learning reduces false alerts.	4.09	0.69
Predictive models improve financial security.	4.21	0.61
Machine learning supports adaptive fraud detection.	4.27	0.58

Based on descriptive results, the ratio of the respondents' perceived ability with machine learning technology was very high. The mean result of 4.24 (SD 0.62) suggests that the respondents felt that machine learning helps in predicting fraud. The "Algorithms can learn more patterns of fraud over time" had a mean of 4.18 with a standard deviation of 0.66, meaning that most of the respondents did accept that such algorithms can learn over time to effectively outsmart new cyber threats. Most agreed with this statement (mean = 4.09, standard deviation = 0.69). It was found that there is some uniformity of report despite a slight increase in deviation with some exceptions for experience report. The mean score of predictive models improving financial security was 4.21 with a standard deviation of 0.61, indicating high consensus with regard to the contribution of predictive models to increase financial security. The highest score was for "Machine learning supports adaptive fraud detection," with an average of 4.27 and a standard deviation of 0.58. The results showed that adaptive learning was among the best AI applications for identifying continuously evolving fraud patterns.

Real-Time Transaction Monitoring

Table 4

Real-Time Transaction Monitoring

Indicator	Mean	Std. Deviation
Continuous monitoring improves security.	4.31	0.55
Immediate alerts reduce fraud losses.	4.28	0.57
Transaction monitoring improves customer protection.	4.22	0.60
Real-time monitoring strengthens fraud prevention.	4.35	0.53
Monitoring systems improve response speed.	4.26	0.56

Journal of Business Insight and Innovation
Volume 5 Issue 6, 2026
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

The descriptive statistics in Table 4 revealed a high degree of consensus regarding the effectiveness of real-time transaction monitoring in preventing financial fraud. There is good agreement on the indicator "Continuous monitoring improves security", with an average of 4.31 and a standard deviation of 0.55. With a mean of 4.28, a standard deviation of 0.57, the statement Immediate alerts reduce fraud losses received a high level of support from many respondents, suggesting an important role in this matter. The mean and standard deviation for this statement was 4.22 and 0.60 respectively, suggesting moderate level of consensus between the banks with regard to benefits of the continuous monitoring to maintain customer accounts protection. The degree of agreement and the standard deviation of the opinions of the respondents was very high level of agreement (mean value of 4.35 and standard deviation of 0.53) in the answer "Real-time monitoring strengthens fraud prevention". The statement 'Monitoring systems improve response time was rated an average of 4.26, with a standard deviation of 0.56 which indicates that respondents recognised that intelligent monitoring systems can help to achieve the necessary quick response time for an event in the cyber security arena. The overall mean values were high with the standard deviations comparatively low, showing that the respondents were positive such that real-time monitoring of transactions is one of the most effective defense measures against the financial fraud in today's FinTech environment.

Anomaly Detection for Cybersecurity Enhancement

Anomaly detection is another important AI capability that enables organizations to recognize unusual transaction behaviour.

Table 5

Anomaly Detection Techniques

Indicator	Mean	Std. Deviation
Anomaly detection identifies suspicious behaviour.	4.29	0.59
Behavioural analytics improve fraud detection.	4.18	0.63
AI detects unknown fraud patterns.	4.24	0.61
Anomaly detection reduces cyber risks.	4.20	0.60
Intelligent analytics improve cybersecurity resilience.	4.32	0.56

The results in Table 5 reveal that the respondents are highly in consensus about the effectiveness of the anomaly detection techniques to improve cyber security for digital financial scams. The mean score for Anomaly detection detects suspicious behaviour was 4.29 and standard deviation of 0.59, indicating that the respondents scored highly for this and there was little variance across the respondents with regards to whether they think anomaly detection can detect suspicious behaviour or not. The mean score for "Behavioural analytics improve fraud detection" was 4.18 with a standard deviation of 0.63, showing a relative level of agreement that using behavioural analytics to improve the detection of fraud was achieved, but there were slightly greater variations. The mean of the AI-detected Missed Fraud Pattern was 0.61 with a standard deviation of 0.61, reflecting the confidence level that AI can detect a new fraud pattern that it has never encountered before. The average score for Anomaly detection was 4.20 with a standard deviation of 0.60, signifying that Anomaly detection is considered as a critical element in mitigating cyber risks. There was very strong agreement that ‘Intelligent analytics improve cybersecurity resilience' with a mean of 4.32 and a standard deviation of 0.56. All the values of the indicators were more than 4.18. The values for the standard deviation of all the indicators were in the range of 0.56 – 0.63 indicating that the participants were consistent in identifying the anomaly detection techniques as part of an AI tool that can create a more resilient cybersecurity system for FinTech enterprises to protect against increasingly sophisticated digital financial fraud acts.

5. Discussion

The results showed how much artificial intelligence could improve fraud detection as well as cybersecurity in the fintech industry. Most survey respondents were highly optimistic about the ability of AI to detect suspicious transactions, accurately identify fraud, reduce manual investigations and improve the effectiveness of cybersecurity. The results showed that AI-enabled systems could provide faster and more

Journal of Business Insight and Innovation
Volume 5 Issue 6, 2026
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

intelligent responses to financial fraud than traditional security methods. According to Hernandez Aros et al. (2024), Hafez et al. (2025), and Darwish et al. (2025), AI fraud detection solutions increase the likelihood of fraud detection, reduce complexity, and reduce financial losses.

This was verified that machine learning was a vital component of AI for fraud detection. All groups stated that machine learning algorithms automatically learned new fraud patterns, enhanced predictive accuracy, minimized false alerts, and enabled adaptive fraud detection. Results showed that the intelligent learning models are feasible for overcoming new cyber threats and will be continually updated. The results aligned with Banerjee and Roy (2024), Hernandez Aros et al. (2024), and Hafez et al. (2025), who highlighted similar findings that supervised, unsupervised, and deep learning algorithms greatly enhanced both the accuracy of fraud prediction and the effectiveness of cybersecurity in the utilization of digital financial systems.

The results also demonstrated the importance of real-time transaction monitoring to improve cybersecurity in the digital financial space. The financial loss and customer protection ratings were reported as good due to the ability to monitor and alert customers to fraud promptly. The clear majority of respondents agreed that continuous monitoring, immediate fraud alerts, and quick responses reduced financial impact and increased customer protection. The results showed that when a financial institution can monitor in real time, it can detect suspicious activity and prevent large-scale fraud-related damage. These findings were consistent with those of Darwish et al. (2025), Al-Daoud and Abu-AlSondos (2025), and Islam et al. (2025), who demonstrated the effectiveness of intelligent real-time systems in reducing fraud rates and supporting cybersecurity strategies.

The outcome also demonstrated how with its anomaly detection functionality the capability to support cyber security resilience was achieved by detecting anomalies in transactions and raising the awareness of the new types of fraud. 73% of the respondents believed the application of an intelligent anomaly detection approach with a behavioural analytics approach significantly decreases the level of cyber risk in a FinTech environment. The adaptive anomaly detection models' defense against more complex financial frauds was determined to be more precise than the rule-based models. Hafez et al. (2025), Darwish et al. (2025), and Analysis on AI-based Techniques for Detection of Banking Frauds (2025) all reiterated the critical role of anomaly detection, explainable AI and intelligent behavioural analysis, within the strengthening of the financial cybersecurity ecosystem.

These findings showed that AI solutions in fraud detection, machine learning, real-time monitoring, and anomaly detection have proven to be highly effective cybersecurity tools in the FinTech industry to fight digital financial fraud. The mean scores across all constructs were consistently high, indicating strong confidence in the effectiveness of intelligent fraud detection technologies. These findings aligned with the most recent research done by Hernandez Aros et al. (2024), Hafez et al. (2025), and Al-Daoud and Abu-AlSondos (2025), who found that the combination of AI with predictive analytics and cybersecurity technologies has formed more resilient 'Smart, Adaptive and secure financial systems' to overcome more sophisticated cyber threats.

Conclusion

This research paper looks at and studies Artificial Intelligence (AI) enabled Fraud Detection solutions to better understand their role and significance in combating Financial Digital Scams and ensuring Cybersecurity in the FinTech Industry. It was discovered that Anomaly detection, improved real-time transaction monitoring, machine-learning predictions and accuracy in fraud detection based on AI support could be used in parallel to increase the accuracy of fraud detection. As shown in the results, these cybersecurity smart fraud detection solutions proved to be useful for detecting fraudulent transactions, lowering cybersecurity risks, and enhancing the efficiency of financial institutions in digital financial services. Altogether, respondents broadly felt that AI technologies are a significant part of the digital financial systems' response to a barrage of threats to the systems. The research showed that adopting AI in FinTech cybersecurity applications contributed to fraud prevention, customer confidence, financial security, and increased occasional resistance to the constantly evolving digital financial fraud.

6. Recommendations

Financial institutions and FinTech service providers demand more funding to deploy advanced Artificial Intelligence (AI), Machine learning and Real-time monitoring capabilities to bolster their fraud detection and management capabilities; and as well as defend their Cyber Security. The bottom line is that security systems should be continually updated with fresh data on transactions, existing security systems need to be improved with AI based tools which include behavioural science and anomaly detection, and security professionals should ensure their skillsets are the same and routinely updated, keeping themselves informed of new fraud trends. Keeping these AI models continuously updated with real-time transaction data, embedding innovative features as they develop in the existing security framework, such as behavioural analytics or AI-based anomaly detection, and providing continuous training and updates for security teams will help address the evolving threat of fraud. Policy and regulatory strengthening for eXAI is required, to foster sound governance and oversight mechanisms, promote securer data governance protection, handle cyber security responsibly and enhance cooperation between eXAI providers and financial sector regulators and financial institutions to ensure the financial system is more secure, transparent and resilient when operating in the digital era.

7. Future Directions

In the future, the use cases are expected to be strengthened by new innovations in the field of artificial intelligence, such as 'explainable' AI, implementation of graph neural networks, federated learning, security of blockchain applications with AI and generative AI. There also needs to be a longitudinal design examining the effectiveness of the use of artificial intelligence (AI) for cybersecurity measures and strategies over time applied to different financial systems and institutional and regulatory environments. Those wishing to develop more detailed models that could inform ways how intelligent technologies could support cybersecurity and how to keep digital financial services safe in the face of ever-changing financial fraud dynamics may want to consider other factors, such as Cybersecurity governance, Digital identity management, Cloud security, Customer trust, Regulatory compliance, and ethical use of AI.

Contribution of Authors

All the authors participated in the ideation, development, and final approval of the manuscript, making significant contributions to the work reported.

Conflict of Interest Statement

The authors declare that there is no conflict of interest regarding the publication of this article.

Funding Statement

The authors did not receive financial support from any funding agency or external organization for the research, authorship, or publication of this article.

Informed Consent

Informed consent was obtained from all participants.

Data Availability

The datasets generated during and analysed during the current study are available from the corresponding author on reasonable request.

References

Al-dahasi, E. M., Alsheikh, R. K., Khan, F. A., & Jeon, G. (2025). Optimizing fraud detection in financial transactions with machine learning and imbalance mitigation. *Expert Systems, 42*(2), e13682. https://doi.org/10.1111/exsy.13682

Al-Daoud, K. I., & Abu-AlSondos, I. A. (2025). Robust AI for financial fraud detection in the GCC: A hybrid framework for imbalance, drift, and adversarial threats. *Journal of Theoretical and Applied Electronic Commerce Research, 20*(2), 121. https://doi.org/10.3390/jtaer20020121

Bahnsen, A. C., Aouada, D., Ottersten, B., Stojanovic, A., & Aksnes, J. (2016). Feature engineering strategies for credit card fraud detection. *Expert Systems with Applications, 51*, 134–142. https://doi.org/10.1016/j.eswa.2015.12.030

Carcillo, F., Dal Pozzolo, A., Le Borgne, Y.-A., Caelen, O., Mazzer, Y., & Bontempi, G. (2021). Scarff: A scalable framework for streaming credit card fraud detection with Spark. *Information Fusion, 41*, 182–194. https://doi.org/10.1016/j.inffus.2017.09.005

Dal Pozzolo, A., Caelen, O., Johnson, R. A., & Bontempi, G. (2015). Calibrating probability with undersampling for unbalanced classification. *IEEE Symposium Series on Computational Intelligence*, 159–166. https://doi.org/10.1109/SSCI.2015.33

Darwish, S. M., Salama, A. I., Elzoghabi, A. A., & El-Shoafy, N. A. (2025). An intelligent memetic approach to detect online fraud for distributed FinTech environments. *Electronic Commerce Research*. https://doi.org/10.1007/s10660-025-10050-y

Hafez, I. Y., Hafez, A. Y., Saleh, A., Abd El-Mageed, A. A., & Abohany, A. A. (2025). A systematic review of AI-enhanced techniques in credit card fraud detection. *Journal of Big Data, 12*(1), Article 6. https://doi.org/10.1186/s40537-024-01048-8 (Springer)

Hernandez Aros, L., Bustamante Molano, L. X., Gutierrez-Portela, F., Moreno Hernandez, J. J., & Rodríguez Barrero, M. S. (2024). Financial fraud detection through the application of machine learning techniques: A literature review. *Humanities and Social Sciences Communications, 11*(1), 1130. https://doi.org/10.1057/s41599-024-03606-0

Jurgovsky, J., Granitzer, M., Ziegler, K., Calabretto, S., Portier, P.-E., He-Guelton, L., & Caelen, O. (2018). Sequence classification for credit-card fraud detection. *Expert Systems with Applications, 100*, 234–245. https://doi.org/10.1016/j.eswa.2018.01.037

Kumar, S., Patel, R., & Sharma, V. (2025). Analysis on AI-based techniques for detection of banking frauds: Recent trends, challenges, and future directions. In *Proceedings of the 2025 International Conference on Intelligent Systems and Computational Networks (ICISCN)* (pp. 1–6). IEEE. https://doi.org/10.1109/ICISCN64258.2025.10934402

Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems, 50*(3), 559–569. https://doi.org/10.1016/j.dss.2010.08.006

Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). A comprehensive survey of data mining-based fraud detection research. *Artificial Intelligence Review, 34*(1), 1–14. https://doi.org/10.1007/s10462-009-9119-y

Randhawa, K., Loo, C. K., Seera, M., Lim, C. P., Nandi, A. K., & Mahmud, M. (2018). Credit card fraud detection using AdaBoost and majority voting. *IEEE Access, 6*, 14277–14284. https://doi.org/10.1109/ACCESS.2018.2806420

Roy, A., Sun, J., Mahoney, R., Alonzi, L., Adams, S., & Beling, P. A. (2018). Deep learning detecting fraud in credit card transactions. *Systems and Information Engineering Design Symposium (SIEDS)*, 129–134. https://doi.org/10.1109/SIEDS.2018.8374722

Weng, Y., Lu, L., Wang, X., Megías, D., & Choo, K.-K. R. (2025). AI and financial fraud prevention: Mapping the trends and challenges through a bibliometric lens. *Journal of Risk and Financial Management, 18*(6), 323. https://doi.org/10.3390/jrfm18060323