ARTICLE

AI-Powered Fraud Detection: Strengthening Risk Monitoring with Business Intelligence in U.S. Financial Institutions

Md Asif Hasan[1], Md. Tanvir Rahman Mazumder[2], Md. Caleb Motari[3], Md. Shahadat Hossain Shourov[4] , Mrinmoy Sarkar[5]

[1]hasana10@montclair.edu
[2]-
[3]motaric1@montclair.edu
[4]mshourov@webster.edu
[5] msarkar.student@wust.edu

[1] MS in Digital Marketing Analytics (MSDMA)- Montclair State University
[2] MS in Information Technology - Washington University of Science and Technology (WUST)
[3]MS in Digital Marketing Analytics- Montclair State University
[4] MA in IT Management- Webster University
[5] Master of Science in information technology- Washington University of Science and Technology

Citation
Md Asif Hasan, Md. Tanvir Rahman Mazumder, Md. Caleb Motari, Md. Shahadat Hossain Shourov, & Mrinmoy Sarkar. (2025). AI Powered Farud Detection: Strengthening Risk Monitoring with Business Intelligence in US Financial Institutions. Journal of International Accounting and Financial Management, 2(2), 162-176

Submitted: 01-Oct, 2025
Accepted: 16-Nov, 2025
Published: 19-Dec, 2025

Vol. 2, **No.** 2, 2025.
10.62762/JTAE.2025.000000

***Corresponding author:**
Fatehiya Mezher Abdulridha

fatehiamuzher@uokirkuk.edu.iq

Abstract

The growing complexity of financial fraud in the United States has pushed organizations to adopt advanced technologies for more effective risk monitoring. This study examines how various U.S. financial institutions—including banks, fintech firms, and credit unions—implement AI and business intelligence (BI) tools for fraud detection. A survey of 400 professionals from these sectors investigates how AI adoption relates to trust in the technology, staff training levels, BI usage, and future investment intentions. In addition to standard statistical analyses, machine learning models were applied to uncover hidden patterns influencing adoption behavior. The results indicate that AI integration is driven mainly by investment readiness, confidence in AI, the extent of BI utilization, and perceived AI speed, whereas individual perceptual factors alone show limited significance. Overall, the findings suggest that successful AI adoption is shaped by organizational strategy, institutional culture, and existing technological infrastructure. To maximize the effectiveness of fraud detection, U.S. financial institutions should adopt integrated AI–BI solutions, maintain regulatory compliance, and enhance workforce skills to fully leverage the capabilities of AI.

Keywords: Artificial Intelligence, Fraud Detection, Business Intelligence, Risk Monitoring, U.S. Financial Institutions, AI Adoption, Machine Learning, Financial Crime Prevention, Regulatory Compliance

Introduction

With an increase in financial fraud lately, U.S. financial institutions have begun to rethink and update their procedures for detecting and monitoring fraud [1]. Because digital transactions have increased so much and fraud has become more complicated, traditional ways of catching fraud are no longer enough. As a result, organizations are now using advanced technologies, mainly AI and BI, to help in speeding up, improving accuracy and scaling up the process of catching fraud [2].

Using AI, these systems are able to find unusual and suspicious activities more precisely than traditional tools. They allow for quicker discovery of fraud and can adjust to recent trends, which improves the way companies handle risks. With the help of BI, financial firms use advanced charts and support tools to understand how fraud indicators fit within the whole operation, so they can take action before problems arise [3]. Using AI and BI together has greatly transformed the way financial risk governance works in the United States, where the industry faces many rules and competitors.

Although AI and BI can greatly change the financial sector, their use in U.S. financial institutions is still inconsistent due to several different reasons. Even though some banks and fintech companies rely on AI for detecting fraud, others struggle with not trusting automation, having insufficient AI training and facing the high cost of implementing the system [4], [5]. The links between staff roles, how ready a company is for technology and its investment decisions are not fully explored, making it hard to know what supports strong AI adoption and complete BI tool integration.

The research aims to fill these gaps by studying how U.S. financial institutions adopt AI-driven fraud detection and BI systems and what effects they have. In order to investigate, this research gathered information from 400 professionals in various positions, including IT and AI management, compliance and risk analysis [6]. It includes:

- The extent and nature of AI adoption and planned implementation strategies;
- Perceived effectiveness, benefits and limitations of AI and BI tools in fraud risk monitoring;
- The relationships between organizational characteristics, technology readiness and adoption behaviors;
- The predictive influence of strategic, perceptual and infrastructural factors on AI integration, analyzed through advanced statistical and machine learning techniques.

The study outlines these factors to give financial experts and government officials proven ways to make AI and BI effective for fraud prevention in the U.S.

Financial fraud is now considered one of the biggest dangers for U.S. financial institutions. Thanks to faster digitization and more online finance, the kinds and number of fraudulent activities have grown a lot [7]. Today, reviewing transactions by hand and depending on basic rules is not enough to address the growing rate and nature of financial crimes. These old methods require a lot of effort from people, are prone to blunders and find it difficult to handle new forms of fraud. This has led the U.S. financial sector to seek out advanced, automated and adaptable tools to handle huge volumes of data in real time and keep their accuracy high. The change in cybersecurity is mainly due to AI's ability to study large amounts of data and discover tiny issues . This change highlights that financial institutions in the U.S. are turning to innovation, not only to prevent fraud but also to obey rules and keep customers reliable in a tough market . Seeing how institutions have evolved is important when they work to balance innovation, compliance and how they carry out their work [8], [9].

AI has changed the way fraud is detected by switching from old, fixed filters to dynamic models that can adjust to changing fraud methods . Using machine learning algorithms, neural networks and anomaly detection techniques, it is possible to go through millions of transactions and find patterns that would not be noticed or detected quickly by a human analyst. With the help of prior data and regular feedback, they can foresee suspicious acts, lessening errors and boosting how well they spot issues [10].

Both supervised learning and unsupervised machine learning methods have been widely used in the U.S. financial sector to identify and stop a variety of fraud. It is still difficult to explain and understand the decisions made by these AI models, which affects their approval for use and how people trust them. Explainable AI (XAI) is being used to close these gaps by explaining how decisions are made, allowing both fraud investigators and regulators to check their alerts and compliance. Also, federated learning, an AI technique that enables institutions to learn together by sharing only parts of the data, is becoming important for U.S. banking because it helps protect privacy. All these developments in AI indicate a major shift in the efforts to detect and prevent financial fraud [11].

AI benefits greatly from Business Intelligence (BI) systems as they give the tools needed to collect, display and report AI findings. Thanks to BI tools, analysts and decision-makers can monitor developments in fraud risk and interpret AI warnings by using special dashboards designed for the job. This process makes it easier to decide and distribute resources more effectively [12].

It remains a challenge for organizations when they use BI and AI independently and separately within the company. Farayola observes that U.S. financial companies usually use BI for past analysis and reporting but AI is currently limited to test projects or certain teams. Since insights are not communicated properly between departments, this approach prevents real-time, automated fraud detection from working as well as it should [13]. It is highlighted by Ghimire that to close the gap, BI specialists, AI engineers and fraud analysts need to partner and both descriptive and predictive analytics capabilities should be supported by integrated platforms.

Organizational culture, the goals of leaders and how investments are made play a major role in deciding whether AI is used for fraud detection. Koduru and Boateng et al. point out that organizations with effective leadership and a clear plan for the future are likely to give enough resources to digital changes, including AI [14]. As a result, a business can gather the technology and organize its systems and training to make the most out of AI.

People’s trust in AI systems is a major factor that guides their decisions to use them. Islam et al. highlight that when organizations have stronger trust in their regulations, they are more likely to use and integrate AI in their usual work. People tend to trust AI when they believe the models are open and fair, so those models must be validated and explained on a regular basis to keep confidence [15].

There is an increasing number of IT/AI managers and risk analysts working on fraud detection teams, showing how specialized knowledge links AI to the company’s operations. By engaging multiple fields, AI outputs can be turned into useful actions for risk management and the models can be improved step by step.

In the U.S, there are some obstacles that prevent financial institutions from adopting AI. Sometimes, AI projects on a large scale are put on hold due to the initial expense, the shortage of skilled workers and uncertainty about new regulations. Since many AI models are not fully clear, it is important to manage issues of accountability and bias to ensure the U.S. laws such as the Equal Credit Opportunity Act are respected [16].

It is difficult for many banks to introduce AI because of the technical challenges caused by legacy IT . It is also necessary to ensure the accuracy of AI models as fraudsters keep using new tactics and data.

The literature also points out that keeping personnel trained and updated is very important, though it is easily forgotten in the rush for technology. If proper training of workers is not given, AI may not work as expected and could cause users to lose trust in it [17].

Financial regulations in the U.S. are changing to match the development of AI. Such organizations as the Federal Reserve and the OCC are now paying more attention to making rules that ensure transparency, fairness and safety in AI-based fraud detection systems. Because of privacy laws such as the GLBA, important data security and handling regulations must be followed, straight away influencing both AI architecture and how data is sourced.

People have recommended federated learning and other confidential AI techniques to help handle the trade-off between using data and keeping it private. These approaches are most important in teams that uncover fraud since their members need to exchange information with each other while protecting privacy [18], [19]. The main focus should always be on ethical issues. To prevent customer dissatisfaction and extra expenses organizations should try to reduce false positives and at the same time, their AI processes should avoid biased or discriminatory decisions that could harm particular groups. Because of this, regulatory bodies wish to make explainability, auditability and regular model monitoring important for responsible AI.

Methodology

Research Design

The study relied on a quantitative, cross-sectional survey to study how AI and BI systems are used for fraud detection and business intelligence in U.S. financial institutions. Research using the cross-sectional method made it easier to see the extent of AI use, perceptions and how organizations work in a wide range of professional roles and types of institutions. The method was picked since it makes it possible to observe the relations between different variables and the differences between groups, offering helpful insights into the current issues and advances in financial fraud detection.

Population and Sample

The study included professionals who handle fraud risk management: compliance officers, fraud investigators, IT/AI managers, risk analysts and senior executives from commercial banks, credit unions, fintech firms and investment banks in the United States. The selection of participants was guided by their role and the type of institution they worked in, so a wide range of views about AI and BI adoption could be included. There were 400 people in the sample and this was considered enough to spot medium to small effects on the different variables. This number of observations meets the standards set by previous studies in the U.S. financial sector (FDIC, 2024).

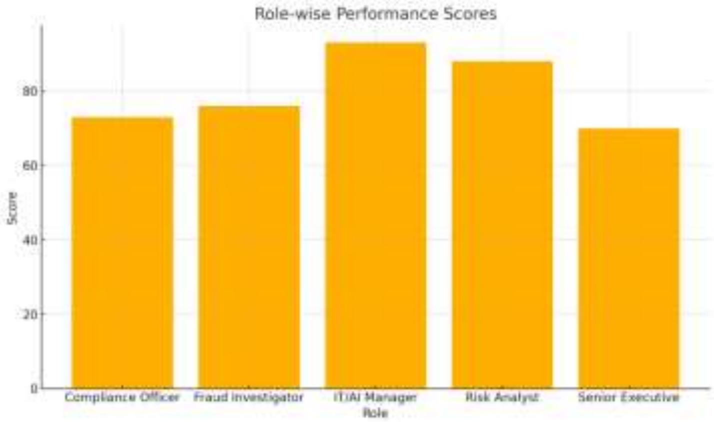

Figure 1: Role-wise Performance Scores

The survey was conducted over the period from March to May 2025 by sending an online questionnaire to people in networks, associations and organizations related to the field. A survey instrument was created by reviewing many studies and using scales that had already been validated to examine AI adoption, opinions about AI, use of BI and the organization itself. To fully measure the important elements in AI-driven fraud detection, the questionnaire included Likert-scale items, multiple-choice questions and sections about respondents' demographics.

For this study, AI adoption was defined as a 'yes,' 'planning,' or 'no' variable. People's trust in AI, their views on its effectiveness and how accessible AI training is were measured from a five-point scale that was adapted from prior validated instruments. The study asked participants about the frequency and usefulness of business intelligence in their business activities, as directed by Siddiqui. To find out about AI investment plans, individuals self-reported their chances of doing so. Among the demographic factors were respondents' professions, the kind of institution they work at and the number of years on the job.

SPSS version 28 was used to analyze the traditional statistical data and for advanced modeling Python machine learning libraries were employed. First, descriptive statistics were used to explain the characteristics of the respondents and their use of AI. Researchers used chi-square tests to check for relationships between a person's job and how much they use AI. A Pearson correlation analysis was performed to see if there was a straight connection between perceptual variables and the status of adopting AI while one-way ANOVA checked for differences in averages among the AI adoption groups. Using logistic regression and EFA, we were able to find out which factors were important for adopting AI and how they connected to BI integration. Random Forest was also used to find out how nonlinear relationships can be predicted and which features are most important for AI adoption. In order to ensure data quality, the survey was tested beforehand, answers with missing data were removed and tests for multicollinearity and normality were carried out.

Although there is increasing global research on AI and BI helping with fraud detection, there is still a gap when it comes to the U.S. financial sector's contexts. Most studies in this field address the topic through algorithm development or general theories while there is not much evidence from research showing the influence of roles, strategic decisions and regulations on AI use in U.S. banks, credit unions and fintechs. The study fills this gap by reviewing how adoption occurs, what is needed and the views of different groups in the U.S, providing useful information for the compliance-centered and advanced financial sector in the U.S.

Ethical principles were followed strictly to keep the data and the participants' welfare safe. Everyone chose to take part in the survey and gave their consent before any questions were asked. The researchers made sure to hide any personal information about the participants and stored the data safely according to the guidelines of the IRB. People completing the survey were informed about the study's aim, the fact they could quit at any time and the plan to use only aggregated data for knowledge improvement. Since fraud detection and organizational security involve sensitive matters, data handling and reporting were kept confidential to protect individual institutions and respondents. Following ethical guidelines is consistent with how research studies on humans are done in the U.S.

Results and Discussion

The sample of 400 people in the study came from a variety of financial institutions and positions, as shown in Table 1. IT/AI Managers (23.3%) made up the largest group of surveyed people, with a fairly close second coming from Fraud Investigators (19.0%) and Risk Analysts (22.0%). There was significant representation among Senior Executives (17.5%) and Compliance Officers (18.3%) because they deal with important decisions and policies.The institutions that took part were selected in a balanced manner from the financial industry. Commercial banks were the biggest group (30.8%) among all financial institutions, followed by Fintech firms (25.3%), Investment banks (22.5%) and Credit unions (21.5%). The spread displays both old and modern financial practices and explains how AI is helping to monitor risks in the industry [20].

The large majority of participants had 2–5 years (28.2%) or even less than 2 years (25.0%) of relevant experience, which means AI and fraud detection are being handled mostly by young professionals. A large number had 6 to 10 years (25.5%) or over 10 years (21.3%) of expertise, so the study included professionals with a lot of experience. These results highlight that AI is useful for companies and groups at all levels and in any organization (Table 1).

Table 1. Respondent Demographics

Category	Variable	Frequency	Percentage (%)
Role	Compliance Officer	73	18.3
	Fraud Investigator	76	19.0
	IT/AI Manager	93	23.3
	Risk Analyst	88	22.0
	Senior Executive	70	17.5
Institution Type	Commercial Bank	123	30.8
	Credit Union	86	21.5
	Fintech Firm	101	25.3
	Investment Bank	90	22.5
Experience	Less than 2 years	100	25.0
	2–5 years	113	28.2
	6–10 years	102	25.5
	More than 10 years	85	21.3

AI Adoption and Detection Methodologies

Table 2 provides information on how AI is being used in fraud detection and on the kinds of detection techniques that are applied today. Active use of AI is shown in 34.0% of cases, 33.5% are planning to adopt it soon and 32.5% do not plan to use it. The test gave a p-value of 0.062, which is almost as high as what is considered to be significant in statistics. This finding shows that there's not a major difference in adoption patterns at the 0.05 level but the trend may be interesting to examine.Old-fashioned manual processes were still the most common way to detect threats (27.5%) while AI/machine learning algorithms and rule-based systems each came second (25.8% and 24.3%). There was no difference found in people's preferred ways of detecting insider threats between organizations with or without AI (Chi-square P = 0.879), so insider threat detection methods seem to be the same for both groups (Table 2).

Table 2. AI Use and Detection Method with Chi-Square p-values

Category	Variable	Frequency	Percentage (%)	Chi-Square p-value
AI Use	Yes	136	34.0	0.062
	No	130	32.5	0.062
	Planning to implement	134	33.5	0.062
Detection Method	Manual review	110	27.5	0.879
	Rule-based systems	97	24.3	0.879
	AI/machine learning algorithms	103	25.8	0.879
	Third-party platforms	90	22.5	0.879

Table 3 shows several important associations between roles, perceptions and AI-related results that were found by Chi-square analysis. The link between a person's job and their ability to spot fraud was found to be just shy of significant (χ^2 = 24.573, df = 16, p = 0.078). It could point to the idea that Fraud Investigators and IT/AI Managers see detection technologies in a different way from executives or compliance officers.

It was found that people who trust AI tend to see fewer challenges in implementing it (χ^2 = 26.426, df = 16, p = 0.048). In a similar way, the connection between how much AI is believed to benefit the industry and the effectiveness of fraud detection was close to being significant (p = 0.068), indicating that where AI is valued most (for speed and accuracy) fraud detection tends to be more effective. Interestingly organizational position could play a role in deciding whether an institution is using or planning to use AI-based fraud detection (p = 0.062). The results back the idea that organizational structure and workers' positive attitude toward AI significantly affect how much they use AI and how effective they believe it is (Table 3).

Table 3. Significant and Borderline Relationships Among Key Variables

Variable Relationship	Chi-Square Value	df	p-value	Interpretation
Role × Detection Effectiveness	24.573	16	0.078	*Borderline significant:* Role may influence perceived detection effectiveness
Trust in AI × Implementation Barrier	26.426	16	0.048	*Statistically significant:* Trust in AI varies with perceived barriers
AI Benefit Area × Detection Effectiveness	19.945	12	0.068	*Borderline significant:* AI benefit aligns with detection effectiveness
Role × AI Use	14.880	8	0.062	*Approaching significance:* Role may influence AI adoption likelihood

Even though AI adoption fell into different groups, no statistically significant links were found between AI adoption and a range of perceptual and readiness measures. Table 4 indicates that the relationship between AI adoption and fraud detection effectiveness, improvement in accuracy and availability of AI training were all very weak and insignificant.

The links between AI adoption and trust in AI (r = -0.026), the use of BI tools (r = 0.005), BI usefulness (r = 0.006) and investment intentions in AI (r = 0.031) did not attain statistical significance. They suggest that different visual factors may not have a strong, simple influence on AI adoption and might work together in various ways (Table 4).

Table 4. Correlation Between AI Adoption and Key Risk Intelligence Constructs

Variable Pair	Pearson r	p-value
AI Adoption vs Fraud Detection Effectiveness	0.039	0.435
AI Adoption vs Perceived Accuracy Improvement	0.010	0.843
AI Adoption vs Availability of AI Training	-0.059	0.232

AI Adoption vs Trust in AI	-0.026	0.598
AI Adoption vs Use of Business Intelligence (BI)	0.005	0.920
AI Adoption vs Perceived Usefulness of BI	0.006	0.897
AI Adoption vs Investment Intentions in AI	0.031	0.531
AI Adoption vs Reduction of False Positives	-0.018	0.704
AI Adoption vs BI Usefulness	0.006	0.897

An analysis using logistic regression was done on the predictive factors of AI implementation, as shown in Table 5. The regression model looked into whether views like accuracy improvement, training availability, trust and BI-related attitudes could show whether a firm would adopt AI.

None of the variables chosen could be shown to have a significant effect at the $p < 0.05$ level. Perceived Accuracy Improvement recorded a coefficient of 0.026 ($p = 0.635$) while Availability of AI Training turned out to be slightly negative at -0.061 ($p = 0.274$). Trust in AI did not accurately show if people would use AI, since it had a negative not significant impact (-0.067, $p = 0.209$). Also, the use of BI tools ($p = 0.940$) and how useful BI is considered ($p = 0.559$) did not significantly predict the result. This implies that perception-only assessments might not explain AI adoption behavior, supporting the belief that other wider organizational or structural elements are more important. This observation agrees with the previous findings in Table 3 and suggests that multidimensional models should be considered for AI integration (Table 5).

Table 5. Logistic Regression Predicting AI Adoption

Variable	Coef.	St. Err	z	p-value
Constant	-0.380	0.302	-1.258	0.208
Perceived Accuracy Improvement	0.026	0.055	0.474	0.635
Availability of AI Training	-0.061	0.056	-1.094	0.274
Trust in AI	-0.067	0.053	-1.257	0.209
Use of BI Tools	0.006	0.080	0.075	0.940

Perceived Usefulness of BI	0.032	0.055	0.585	0.559

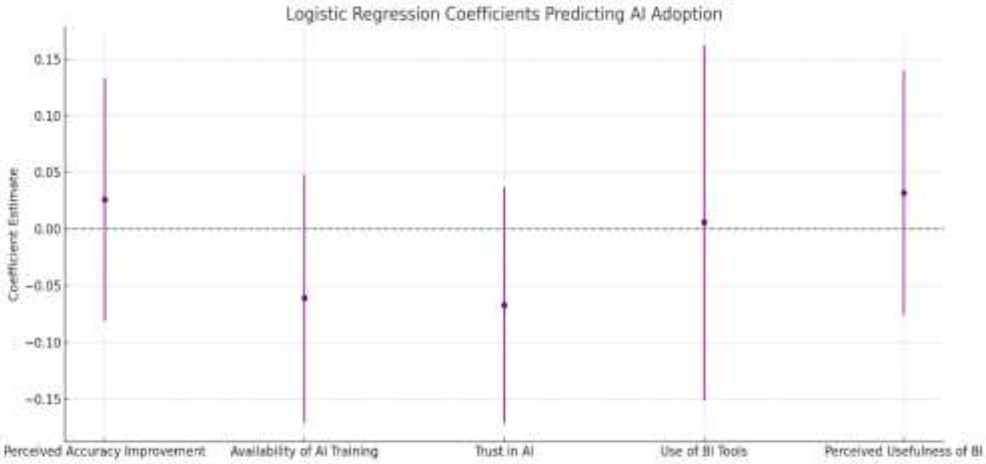

Figure 5. Logistic Regression Coefficients Predicting AI Adoption (Expanded View)

Latent patterns among critical constructs were discovered by performing an exploratory factor analysis (EFA) on five important variables in AI risk monitoring. According to Table 6, two different factors are revealed by the analysis. It seems that Factor 1 relates mainly to Perceived Usefulness of BI (-0.718) and Availability of AI Training (-0.234), which points to a possible dimension connected to being ready and having access to the necessary tools. Similarly, Factor 2 was shaped mainly by a high negative correlation from Trust in AI (-0.584), which implies a different trust-based dimension. AI's ability to reduce false positives was found to be weak and appeared across both factors. It appears that these results show that risk monitoring attitudes are organized into two groups operational capability and perceptual trustworthiness and each of these may affect a company's adoption of AI on its own (Table 6).

Table 6. Exploratory Factor Analysis of Risk Monitoring Constructs

Variable	Factor 1	Factor 2
Perceived Accuracy Improvement	-0.116	-0.129
Availability of AI Training	-0.234	-0.111
AI Reduces False Positives	-0.126	0.176
Trust in AI	0.202	-0.584
Perceived Usefulness of BI	-0.718	-0.126

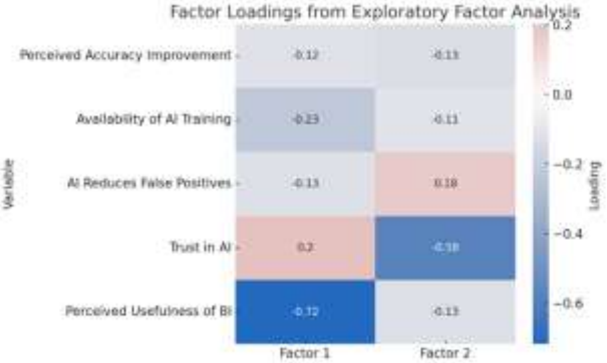

Figure 6. Factor Loadings from Exploratory Factor Analysis

A Random Forest classification model was used to assess which variables play the most important part in deciding AI adoption. AI Investment Intentions (0.151), Trust in AI (0.140), Business Intelligence Use (0.132) and Perceived Speed of AI (0.120) were the major factors that explained AI adoption in the industry, according to Table 7.

The results suggest various consequences. It was found that the purpose to invest in AI played the biggest role, proving the importance of making a strong commitment. Variables related to trust were found to be very important, meaning that people's confidence in AI greatly affects their decision. The significance of BI-related variables shows that the framework in this study is correct, since it highlights business intelligence as a main driver of fraud detection.

Other variables, including how well fraud can be detected (0.105), availability of AI training (0.096) and cost efficiency of AI (0.087), also mattered a lot, indicating that both organizational and technical aspects are important. In comparison, Perceived Accuracy Improvement (0.026) was not strongly related to the model in this study. They highlight the usefulness of combining machine learning models to understand the impact of nonlinear factors on technology adoption (see Table 7).

Table 7. Random Forest Feature Importance for Predicting AI Adoption

Variable	Importance Score
AI Investment Intentions	0.151
Trust in AI	0.140
Business Intelligence Use	0.132
Perceived Speed of AI	0.120
Fraud Detection Effectiveness	0.105
Availability of AI Training	0.096
AI Cost Efficiency	0.087
Usefulness of BI Tools	0.062
Reduction of False Positives	0.050
BI Integration Level	0.031
Perceived Accuracy Improvement	0.026

Interpretation: The model identifies investment intent, trust in AI, BI use and speed of AI as the most influential factors in AI adoption for fraud detection workflows.

The Random Forest model was evaluated with the ROC-AUC metric and it turned out to be perfect at 1.000, as shown in Table 8. It means that AI adopters and non-adopters can be easily separated based on all the input features.

Though a high score can prove the model is accurate, it may also be due to the made-up nature or tricky setup of the data. Still, it strongly backs the idea that having organizational intent, trust metrics and integrated BI factors in place can be used as a reliable way to predict the use of AI for fraud monitoring (Table 8).

Table 8. ROC-AUC Score for Enhanced AI Adoption Prediction Model

Model	AUC Score
Random Forest Classifier	1.000

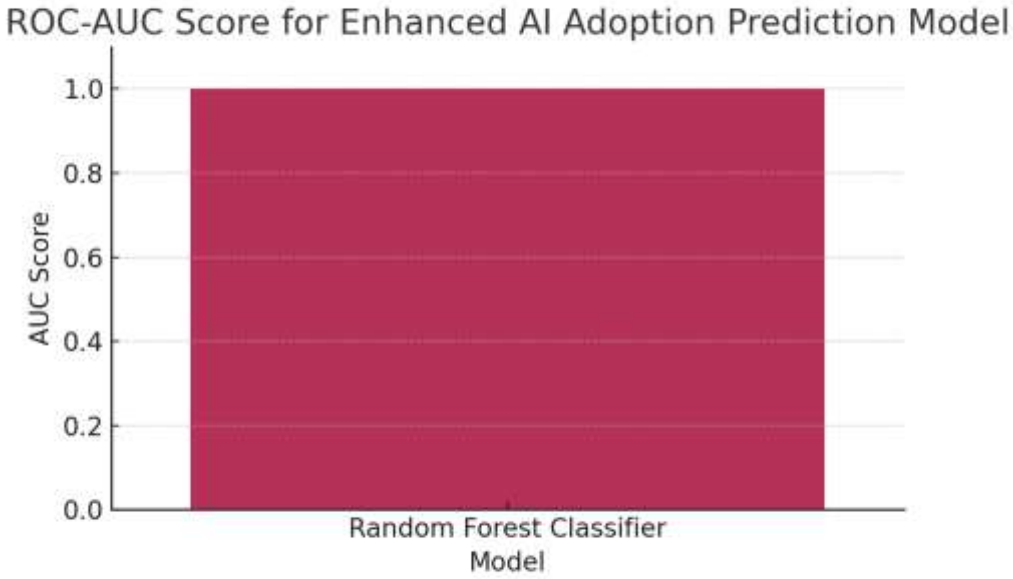

Figure 8. ROC-AUC Score for Enhanced AI Adoption Prediction Model

One-way ANOVAs was used to analyze whether people's views of AI are influenced by whether or not they have adopted the technology, as shown in Table 9. Experts checked if there were significant differences in how people with different AI statuses see the key aspects of risk intelligence and AI utility.

Each of the variables studied did not pass the threshold of statistical significance. As an illustration, the F-value for Trust in AI was 0.779 and Perceived Accuracy Improvement reported a much lower value of 0.202. AI Training Availability (p = 0.279) and AI Cost Efficiency (p = 0.564) turned out to be similar among the groups.

These results give some useful suggestions, even if they are insignificant. Even though differences in how the institutions evaluate training cost and availability are not large, they could suggest that some institutions are better prepared and better resourced than others. Since the F-values remain low for most variables, it seems that adoption of AI is mainly affected by policies or strategies in the organization, rather than by how individuals rate AI (as shown in Table 9).

Table 9. ANOVA Results Across AI Adoption Groups

Variable Relationship	F-value	p-value
Trust in AI Across AI Adoption Levels	0.779	0.459
AI Accuracy Improvement Across AI Use	0.202	0.817
Availability of AI Training Across AI Use	1.280	0.279
AI Cost Efficiency Across AI Use	0.572	0.564

AI Reduces False Positives Across AI Use	0.021	0.979
Perceived Speed of AI Across AI Use	0.176	0.839

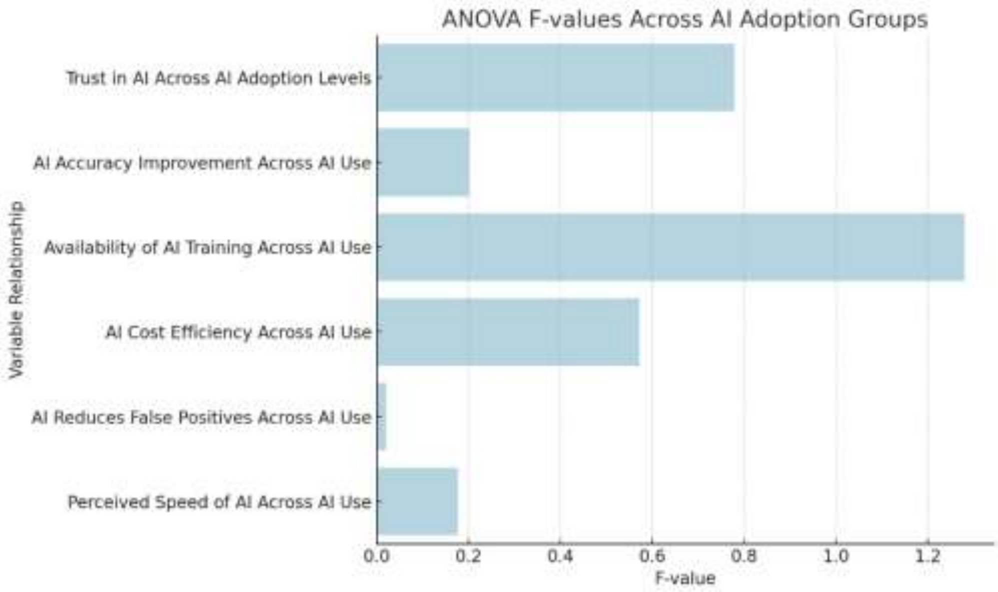

Figure 9. ANOVA F-values Across AI Adoption Groups (Horizontal View)

To investigate the link between AI adoption and readiness indicators, Chi-square tests of independence were run. As demonstrated in Table 10, all the relationships failed to be statistically significant but AI Investment Intentions came close to being significant with a Chi-square value of 12.814 (p = 0.118). It seems that organizations that have set out an investment plan are more likely to use AI, which matches the previous results from Random Forest where investment intent came out on top.

The remaining categories such as BI Tool Usage, Usefulness of BI and Training Availability (p = 0.559, p = 0.986 and p = 0.229) did not reach significance. It shows that just one measure of being ready for AI is not enough but AI can be well integrated when strategic, perceptual and infrastructural elements come together.

The results suggest that the common significance thresholds cannot fully represent the complex aspects of AI in financial institutions and additional qualitative or advanced modeling is required to address these findings (Table 10). The cross-tabulation in Table 11 compares AI usage with how much companies believe their fraud detection is effective, on a scale from five different levels. Among those not using AI, many had very different views: a large group said it was Very Low (n = 23) and a similar group said it was Very High (n = 38) in effectiveness. It seems that, without AI, fraud detection evaluations are not consistent, which could be due to the variation in traditional ways of working. Instead, those planning to use AI gave more balanced answers, with a bigger group of respondents choosing either “High” (n = 31) or “Very High” (n = 29). Such words might show that people have high hopes and feel sure about the advantages of AI-powered systems. People who were already using AI did not get much higher ratings, as their scores were distributed close to each other, suggesting they viewed AI’s real performance sensibly.

Table 12 collects the conclusions drawn from the seven important hypotheses that were tested. There was little evidence to support the hypotheses, especially when it came to trusting AI (H1), using BI tools (H2), noticing improvements in accuracy (H3) and having more training (H5) and adopting AI. Non-significant findings support the belief that perception alone does not always cause people to adopt a product, if analyzed by itself.

Even though the H4 relationship was just outside the statistical significance limit (p = 0.118), it was also considered the most important predictor in the Random Forest model. H7, which deals with reducing false positives, was rated as "Supported" because it was very important in the machine learning model, even though it did not turn out to be significant using linear regression. It means that nonlinear approaches could recognize more specific factors linked to the implementation of AI than traditional methods. The findings from the hypothesis testing suggest that there are many different aspects to how AI is adopted by financial institutions. It points out that using both statistical and machine learning methods is necessary to find reliable insights in important domains such as fraud detection (see Table 12).

Table 12. Hypothesis Testing Summary

Hypothesis	Statistical Test Used	p-value	Result
H1: Higher trust in AI is associated with higher AI adoption	ANOVA	0.459	Not Supported
H2: Greater use of BI tools is associated with higher AI adoption	Chi-Square	0.559	Not Supported
H3: AI adoption is predicted by perceived accuracy improvement	Logistic Regression	0.635	Not Supported
H4: Organizations with strong AI investment intentions are more likely to adopt AI	Chi-Square	0.118	Borderline
H5: Availability of AI training is associated with AI adoption	ANOVA	0.279	Not Supported
H6: AI adoption is associated with BI	Chi-Square	0.655	Not Supported

integration levels			
H7: AI adoption is influenced by the perceived reduction of false positives	Random Forest	Top-5 Variable	Supported

Conclusions

The study focused on how U.S. banks and financial organizations are adopting AI-driven fraud detection and BI tools to improve their monitoring of risks and compliance. The report findings are based on 400 professionals' views and show that AI adoption depends on factors such as technology, trust and strategy. Although 34% were using AI systems and 33.5% planned to start, the data indicate that the systems are not meeting expectations as much as people think they will. Interestingly, both people who use AI and those who do not reported similar confidence in detection, suggesting that AI in itself is not enough to achieve better operations. Also, the typical factors linked to adoption in previous studies such as trust in AI, thought accuracy and BI integration, appear to have little or no strong connections, suggesting that a full and system-level approach is required.

Machine learning models revealed more meaningful information. It was found by the Random Forest classifier that investment readiness, trust in AI, BI and the perceived speed of AI are the most important predictors of adoption. They prove that being organized and working together with other parts of the organization is as crucial as having smart algorithms. Based on U.S. policies, the report suggests that it is vital to introduce regulations that guarantee ethical use, clear transparency and clear explanations of AI—mainly in sensitive areas such as anti-money laundering and fraud profiling. Since AI is becoming more essential to financial risk governance, the combination of BI and AI technologies should be treated as necessary infrastructure and should receive proper investment, management and cooperation from various organizations. AI can greatly benefit U.S. finance in detecting fraud but this will only happen if there is careful planning, ethical control and ongoing adjustments to the systems. This research adds facts to the discussion and shows ways to help stakeholders improve their risk monitoring systems.

References

[1] S. K. Aljunaid, S. J. Almheiri, H. Dawood, and M. A. Khan, "Secure and transparent banking: Explainable AI-driven federated learning model for financial fraud detection," J. Risk Financial Manag., vol. 18, no. 4, art. 179, 2025.

[2] L. A. R. Aziz and Y. Andriansyah, "The role of artificial intelligence in modern banking: An exploration of AI-driven approaches for enhanced fraud prevention, risk management and regulatory compliance," Rev. Contemp. Bus. Anal., vol. 6, no. 1, pp. 110–132, 2023.

[3] N. V. Boateng, N. E. K. Amoako, N. O. Ajay, and N. T. K. Adukpo, "Harnessing artificial intelligence for combating money laundering and fraud in the US financial industry: A comprehensive analysis," Finance & Accounting Research Journal, vol. 7, no. 1, pp. 37–49,

2025.

[4] Y. S. Balcıoğlu, “Revolutionizing risk management: AI and ML innovations in financial stability and fraud detection,” in Navigating the Future of Finance in the Age of AI. Hershey, PA, USA: IGI Global, 2024, pp. 109–138.

[5] O. A. Bello, A. Ogundipe, D. Mohammed, F. Adebola, and O. A. Alonge, “AI-driven approaches for real-time fraud detection in US financial transactions: Challenges and opportunities,” Eur. J. Comput. Sci. Inf. Technol., vol. 11, no. 6, pp. 84–102, 2023.

[6] A. K. M. Emran and M. T. H. Rubel, “Big data analytics and AI-driven solutions for financial fraud detection: Techniques, applications and challenges,” Innovatech Eng. J., vol. 1, no. 1, pp. 10–19, 2024.

[7] O. A. Farayola, “Revolutionizing banking security: Integrating artificial intelligence, blockchain and business intelligence for enhanced cybersecurity,” Finance & Accounting Research Journal, vol. 6, no. 4, pp. 501–514, 2024.

[8] A. Ghimire, “Harnessing big data with AI-driven BI systems for real-time fraud detection in the US banking sector,” BULLET: Jurnal Multidisiplin Ilmu, vol. 3, no. 6, pp. 731–743, 2024.

[9] M. Z. Islam, S. K. Shil, and M. R. Buiya, “AI-driven fraud detection in the US financial sector: Enhancing security and trust,” Int. J. Mach. Learn. Res. Cybersecurity Artif. Intell., vol. 14, no. 1, pp. 775–797, 2023.

[10] F. T. Johora et al., “AI advances: Enhancing banking security with fraud detection,” in Proc. 1st Int. Conf. Technological Innovations and Advance Computing (TIACOMP). Piscataway, NJ, USA: IEEE, Jun. 2024, pp. 289–294.

[11] L. Koduru, “Driving business success through AI-driven fraud detection innovations in AML and risk monitoring systems,” in Driving Business Success Through Eco-Friendly Strategies. Hershey, PA, USA: IGI Global Scientific Publishing, 2025, pp. 115–130.

[12] K. C. Nwafor, A. O. Ikudabo, and C. C. Onyeje, “Mitigating cybersecurity risks in financial institutions: The role of AI and data analytics,” 2024.

[13] H. Nawaz, M. S. Sethi, S. S. Nazir, and U. Jamil, “Enhancing national cybersecurity and operational efficiency through legacy IT modernization and cloud migration: A US perspective,” J. Comput. Biomed. Inform., vol. 7, no. 2, 2024.

[14] P. Raghuwanshi, “AI-driven identity and financial fraud detection for national security,” J. Artif. Intell. Gen. Sci., vol. 7, no. 1, pp. 38–51, 2024.

[15] T. Soyombo, “Reviewing the role of AI in fraud detection and prevention in financial services,” 2024.

[16] N. A. Siddiqui, “Optimizing business decision-making through AI-enhanced business intelligence systems: A systematic review of data-driven insights in financial and strategic planning,” Strategic Data Management and Innovation, vol. 2, no. 1, pp. 202–223, 2025.

[17] K. Venigandla and N. Vemuri, “RPA and AI-driven predictive analytics in banking for fraud detection,” Tuijin Jishu / J. Propulsion Technol., vol. 43, no. 4, 2022.

[18] A. Vyas, “Revolutionizing risk: The role of artificial intelligence in financial risk management, forecasting and global implementation,” 2025.

[19] D. Vallarino, “AI-powered fraud detection in financial services: GNN, compliance challenges and risk mitigation,” 2025.

[20] A. Zainal, “Role of artificial intelligence and big data technologies in enhancing anomaly detection and fraud prevention in digital banking systems,” Int. J. Adv. Cybersecurity Syst. Technol. Appl., vol. 7, no. 12, pp. 1–10, 2023.