FMDB *Transactions on Sustainable Technoprise Letters*

AI-Driven Fraud Detection: Enhancing Risk Monitoring Through 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]

[1,3]School of Business, Montclair State University, Montclair, New Jersey, United States of America.
[2,5]School of Information Technology, Washington University of Science and Technology (WUST), Alexandria, Virginia, United States of America.
[4]Department of Information Technology Management, Webster University, Webster Groves, Missouri, United States of America.
hasana10@montclair.edu[1], mtanvir.student@wust.edu[2], motaric1@montclair.edu[3], mshourov@webster.edu[4], msarkar.student@wust.edu[5]

Abstract: The increasing difficulty of financial fraud in the United States has led companies to use modern technology to monitor risks. This study analyses how different U.S. financial organisations adopt AI and BI technologies and utilise them for fraud detection. The survey of 400 people from banking, FinTech and credit unions looks at how adoption of AI is related to trust, level of training, usage of BI and future investment decisions. Along with statistical procedures, machine learning models helped us find unexpected patterns in what influences adoption. AI integration primarily depends on investment readiness, confidence in AI, the use of business intelligence, and the rate of AI adoption. At the same time, the relationships with individual perceptual factors are not significant. According to the findings, adopting AI depends on several factors, including an organisation's strategy, its culture and the technology it relies on. U.S. banks and financial institutions need to utilise integrated AI-BI systems, comply with all relevant regulations, and equip their staff with additional skills to leverage AI to its full potential in detecting fraud.

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

Received on: 12/10/2024, **Revised on:** 04/01/2025, **Accepted on:** 25/02/2025, **Published on:** 07/06/2025

Journal Homepage: https://www.fmdbpub.com/user/journals/details/FTSTPL

DOI: https://doi.org/10.69888/FTSTPL.2025.000438

Cite as: M. A. Hasan, M.T. R. Mazumder, M. C. Motar, M. S. H. Shourov, and M. Sarkar, "AI-Driven Fraud Detection: Enhancing Risk Monitoring Through Business Intelligence in U.S. Financial Institutions," *FMDB Transactions on Sustainable Technoprise Letters*, vol. 3, no. 2, pp. 73–89, 2025.

1. 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. As digital transactions have increased significantly and fraud has become more complex, traditional methods of detecting fraud are no longer sufficient. As a result, organisations are now using advanced technologies,

*Corresponding author.

primarily AI and BI, to accelerate, enhance accuracy, and scale up the process of detecting fraud [15]; [14]. Using AI, these systems can identify unusual and suspicious activities more precisely than traditional tools. They enable the quicker detection of fraud and can adapt to recent trends, which enhances the way companies manage risks [10]. With the help of BI, financial firms utilise advanced charts and support tools to understand how fraud indicators fit within the overall operation, enabling them to act before problems arise [9].

The combined use of AI and BI has significantly transformed the way financial risk governance operates in the United States, where the industry is subject to numerous regulations and intense competition [16]. Although AI and BI can significantly transform the financial sector, their adoption in U.S. financial institutions remains inconsistent due to several factors. 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 [3]; [1]. The links between staff roles, a company's readiness for technology, and its investment decisions are not fully explored, making it difficult to determine 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. To investigate, this research gathered information from 400 professionals in various positions, including IT and AI management, as well as compliance and risk analysis. 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 organisational characteristics, technology readiness and adoption behaviours.
- The predictive influence of strategic, perceptual and infrastructural factors on AI integration, analysed 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.

2. Literature Review

2.1. Evolution of Fraud Detection in U.S. Financial Institutions

Financial fraud is now considered one of the greatest threats to U.S. financial institutions. Thanks to faster digitisation and increased online finance, the types and number of fraudulent activities have grown significantly. Today, reviewing transactions manually and relying on basic rules is insufficient to address the growing rate and complexity 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 maintain high accuracy. The change in cybersecurity is primarily due to AI's ability to analyse large amounts of data and identify minor issues. This change underscores that financial institutions in the U.S. are embracing innovation, not only to prevent fraud but also to comply with regulations and maintain customer trust in a challenging market [15]. Observing how institutions evolve is crucial when they strive to balance innovation, compliance, and their work practices.

2.2. AI Technologies in Fraud Detection

AI has revolutionised the detection of fraud by transitioning from traditional, fixed filters to dynamic models that can adapt to evolving fraud methods [2]. Using machine learning algorithms, neural networks, and anomaly detection techniques, it is possible to analyse millions of transactions and identify patterns that would not be noticed or detected quickly by a human analyst. With the help of prior data and regular feedback, they can anticipate suspicious acts, reduce errors, and improve their ability to identify issues. Both supervised learning and unsupervised machine learning methods have been widely utilised in the U.S. financial sector to identify and prevent various forms 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 utilised to bridge these gaps by providing explanations for decision-making processes, enabling both fraud investigators and regulators to verify their alerts and ensure compliance. Additionally, federated learning, an AI technique that enables institutions to learn together by sharing only parts of their data, is becoming increasingly important for U.S. banking, as it helps protect privacy [15]. These developments in AI indicate a significant shift in efforts to detect and prevent financial fraud.

2.3. Business Intelligence as an Enabler of AI-Driven Fraud Detection

AI benefits greatly from Business Intelligence (BI) systems, as they provide the tools needed to collect, display, and report AI findings [13]; [16]. Thanks to BI tools, analysts and decision-makers can monitor developments in fraud risk and interpret AI warnings using specialised dashboards designed for the task. This process facilitates more effective decision-making and

resource allocation. It remains a challenge for organisations when they use BI and AI independently and separately within the company. Farayola [16] 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. Ghimire [1] highlights that to close the gap, BI specialists, AI engineers, and fraud analysts need to partner, and integrated platforms should support both descriptive and predictive analytics capabilities.

2.4. Organisational and Strategic Factors Influencing AI Adoption

Organisational culture, the goals of leaders and how investments are made play a major role in deciding whether AI is used for fraud detection. Koduru [11] and Boateng et al. [14] note that organisations with effective leadership and a clear plan for the future are likely to allocate sufficient resources to digital changes, including AI. As a result, a business can gather the necessary technology and organise its systems and training to maximise the benefits of AI. People's trust in AI systems is a significant factor that influences their decision to use them. Islam et al. [12] highlight that when organisations 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 transparent and fair, so those models must be regularly validated and explained to maintain confidence. There is an increasing number of IT/AI managers and risk analysts working on fraud detection teams, showing how specialised knowledge links AI to the company's operations [1]; [6]. By engaging multiple fields, AI outputs can be transformed into actionable insights for risk management, and the models can be refined incrementally.

2.5. Challenges and Barriers to AI-Driven Fraud Detection

In the U.S, some obstacles prevent financial institutions from adopting AI. Sometimes, large-scale AI projects are put on hold due to the initial expense, the shortage of skilled workers, and uncertainty about new regulations [19]. Since many AI models are not fully transparent, it is essential to address issues of accountability and bias to ensure that U.S. laws, such as the Equal Credit Opportunity Act, are respected [2]; [5]. It is challenging for many banks to implement AI due to the technical difficulties posed by legacy IT systems [7]. It is also necessary to ensure the accuracy of AI models, as fraudsters continually develop new tactics and exploit data. The literature also highlights that keeping personnel trained and updated is crucial, although it is often overlooked in the rush for technological advancements. If proper training of workers is not provided, AI may not function as expected, and users may lose trust in it [21].

2.6. Regulatory Landscape and Ethical Considerations

Financial regulations in the U.S. are evolving to keep pace with the advancement of AI. Organisations such as the Federal Reserve and the OCC are now paying more attention to creating rules that ensure transparency, fairness, and safety in AI-based fraud detection systems [4]. Due to privacy laws such as the GLBA, important data security and handling regulations must be followed, which directly influence both AI architecture and how data is sourced. People have recommended federated learning and other confidential AI techniques to help mitigate the trade-off between using data and maintaining its privacy. These approaches are particularly important in teams that uncover fraud, as their members need to exchange information with each other while protecting individual privacy. The main focus should always be on ethical issues. To prevent customer dissatisfaction and avoid extra expenses, organisations should strive to reduce false positives while ensuring their AI processes do not make biased or discriminatory decisions that could harm specific groups [17]. Because of this, regulatory bodies wish to make explainability, auditability and regular model monitoring important for responsible AI.

3. Methodology

3.1. Research Design

The study employed a quantitative, cross-sectional survey to investigate the use of AI and BI systems 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 organisations work in a wide range of professional roles and types of institutions. The method was chosen because it enables the observation of relationships between different variables and the differences between groups, providing valuable insights into current issues and advances in financial fraud detection [8].

3.2. Population and Sample

The study included professionals who handle fraud risk management, such as 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 in which they worked,

allowing for a wide range of views on AI and BI adoption to be included. The sample consisted of 400 people, which was considered sufficient to detect medium to small effects on the different variables [18]. The number of observations meets the standards set by previous studies in the U.S. financial sector (Figure 1).

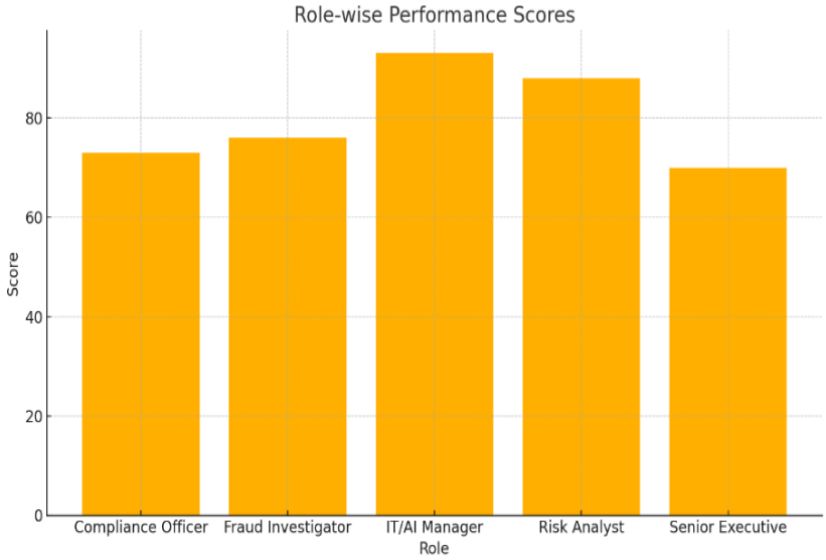

Figure 1: Role-wise performance scores

3.3. Data Collection

The survey was conducted from March to May 2025 by sending an online questionnaire to individuals in networks, associations, and organisations related to the field. A survey instrument was created by reviewing numerous studies and utilising validated scales to examine AI adoption, opinions about AI, the use of BI, and the organisation 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 [20].

3.4. Measures

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 the accessibility of AI training were measured using a five-point scale adapted from prior, validated instruments. The study inquired about the frequency and usefulness of business intelligence in participants' business activities, as directed by Siddiqui [13]. 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.

3.5. Data Analysis

SPSS version 28 was used to analyse the traditional statistical data, and for advanced modelling, 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 examine the relationship between a person's job and their use of AI. A Pearson correlation analysis was performed to determine if there was a direct relationship between perceptual variables and the status of adopting AI. A one-way ANOVA was used to determine if there were differences in averages among the AI adoption groups. Using logistic regression and EFA, we were able to identify the factors that were most important for adopting AI and how they related 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. To ensure data quality, the survey was tested beforehand, and answers with missing data were removed. Additionally, tests for multicollinearity and normality were conducted.

3.6. Research Gap in the U.S. Context

Although there is an increasing amount of global research on AI and BI in helping to detect fraud, a gap remains in the context of the U.S. financial sector. Most studies in this field address the topic through algorithm development or general theories. At the same time, there is limited 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-centred and advanced financial sector in the U.S.

3.7. Ethical Considerations

Ethical principles were strictly followed to ensure the safety of the data and the welfare of the participants. Everyone who chose to participate in the survey gave their consent before answering any questions. The researchers ensured that any personal information about the participants was kept confidential and stored the data securely in accordance with the guidelines of the IRB. Participants completing the survey were informed about the study's aim, the fact that they could withdraw at any time, and the plan to use only aggregated data for knowledge improvement. Since fraud detection and organisational 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.

4. Results

4.1. Respondents Profile

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%) comprised the largest group of surveyed individuals, followed by Fraud Investigators (19.0%) and Risk Analysts (22.0%). There was significant representation among Senior Executives (17.5%) and Compliance Officers (18.3%), as they are involved in 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 showcases both traditional and modern financial practices, explaining how AI is aiding in risk monitoring within the industry. The large majority of participants had 2–5 years (28.2%) or even less than 2 years (25.0%) of relevant experience, indicating that AI and fraud detection are being handled primarily by young professionals. A large number had 6 to 10 years (25.5%) or more than 10 years (21.3%) of expertise, so the study included professionals with extensive experience. These results highlight that AI is useful for companies and groups at all levels and in any organisation.

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

4.2. AI Adoption and Detection Methodologies

Table 2 provides information on how AI is being utilised in fraud detection and the types of detection techniques currently employed. Active use of AI is observed in 34.0% of cases, 33.5% plan to adopt it soon, and 32.5% do not intend to use it. The test yielded a p-value of 0.062, which is nearly as high as what is considered statistically significant. This finding suggests that there's no significant difference in adoption patterns at the 0.05 level, but the trend warrants further examination.

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

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 organisations with and without AI (Chi-square P = 0.879), suggesting that insider threat detection methods seem to be the same for both groups (Figure 2).

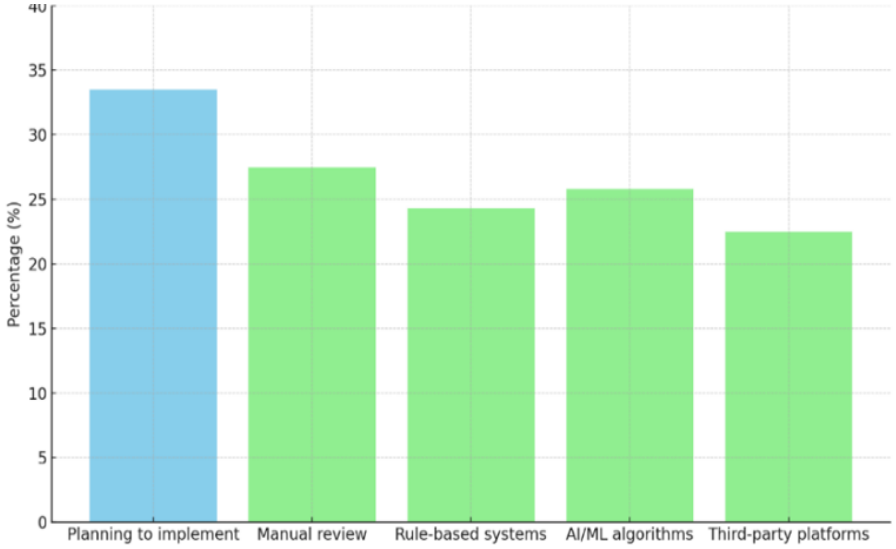

Figure 2: AI implementation planning and detection method distribution

4.3. Statistical Relationships Between Role, Trust and AI Outcomes

Table 3 presents several significant associations between roles, perceptions, and AI-related results identified through Chi-square analysis.

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

The link between a person's job and their ability to spot fraud was found to be just shy of significant ($\chi^2 = 24.573$, df = 16, p = 0.078).

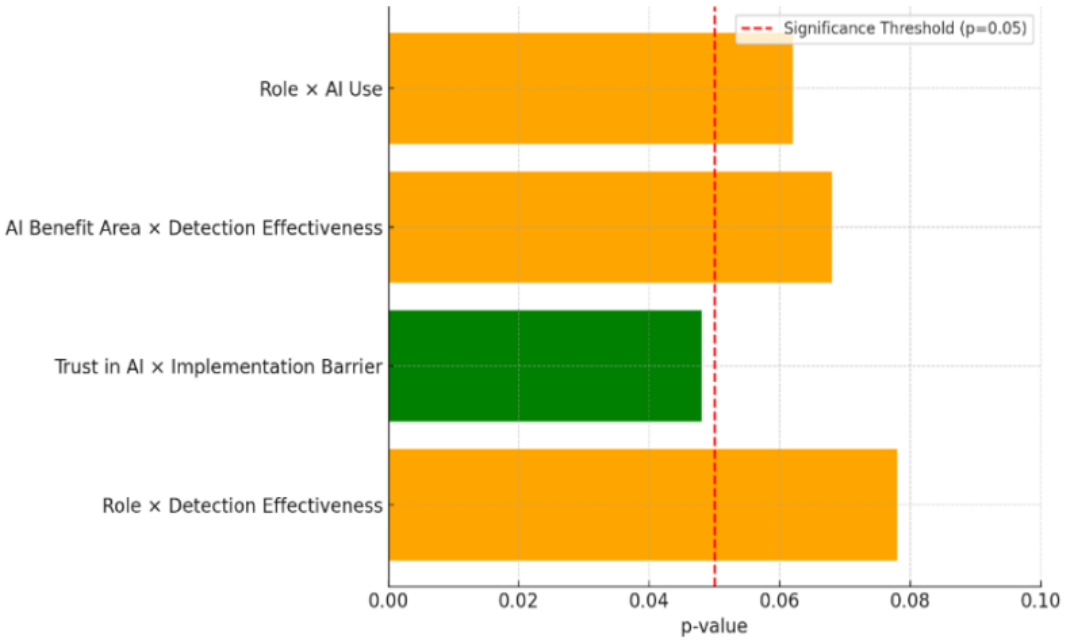

Figure 3: Chi-square p-values for key variable relationships

This could suggest that Fraud Investigators and IT/AI Managers view detection technologies differently from executives or compliance officers. It was found that people who trust AI tend to see fewer challenges in implementing it ($\chi^2 = 26.426$, df = 16, p = 0.048). Similarly, the connection between the extent to which AI is believed to benefit the industry and the effectiveness of fraud detection was nearly significant (p = 0.068), suggesting that where AI is most valued (for speed and accuracy), fraud detection tends to be more effective. Interestingly, organisational 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 organisational structure and workers' positive attitude toward AI significantly affect how much they use AI and how effective they believe it is (Figure 3).

4.4. Correlation Between AI Adoption and Key Constructs

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, as well as the improvement in accuracy and availability of AI training, was all very weak and insignificant.

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

The links between AI adoption and trust in AI (r = -0.026), the use of BI tools (r = 0.005), the usefulness of BI (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, straightforward influence on AI adoption and may interact in various ways (Figure 4).

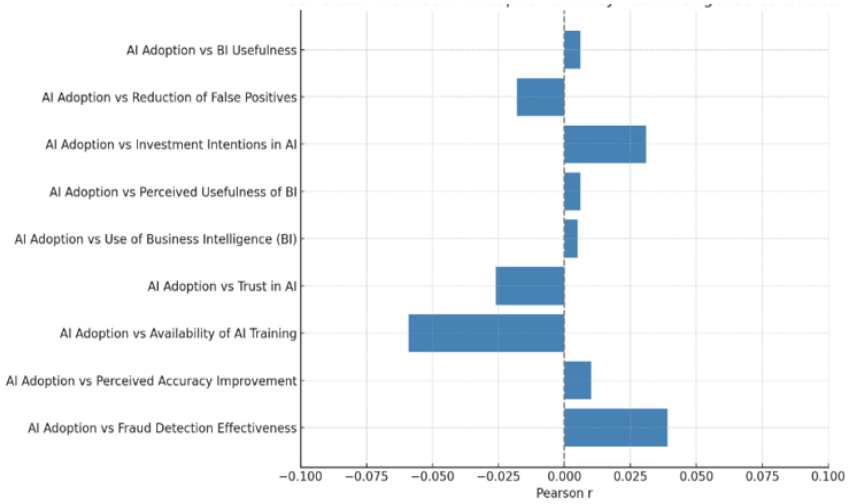

Figure 4: Correlation between AI adoption and key risk intelligence constructs

4.5. Predictors of AI Adoption: Logistic Regression Findings

A logistic regression analysis was conducted to examine the predictive factors of AI implementation, as presented in Table 5. The regression model examined whether views such as accuracy improvement, training availability, trust, and BI-related attitudes could predict whether a firm would adopt AI.

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

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 predict whether people would use AI, as it had a negative, significant impact (-0.067, $p = 0.209$). Additionally, the use of BI tools ($p = 0.940$) and the perceived usefulness of BI ($p = 0.559$) did not significantly predict the outcome. This implies that perception-only assessments may not fully explain AI adoption behaviour, supporting the belief that other, broader organisational 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 (Figure 5).

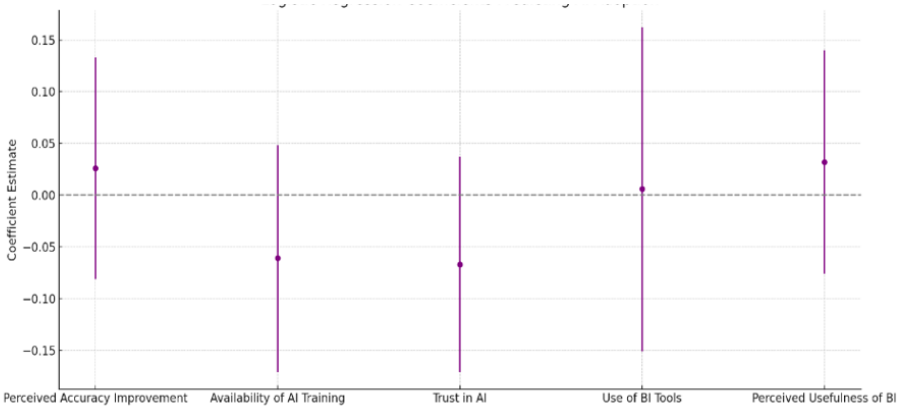

Figure 5: Logistic regression coefficients predicting AI adoption (expanded view)

4.6. Exploratory Factor Analysis (EFA) of Risk Monitoring Constructs

Latent patterns among critical constructs were identified through an exploratory factor analysis (EFA) conducted on five key variables in AI risk monitoring. According to Table 6, the analysis reveals two distinct factors.

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

It appears that Factor 1 is primarily related to the Perceived Usefulness of BI (-0.718) and the Availability of AI Training (-0.234), suggesting a possible dimension related to being ready and having access to the necessary tools. Similarly, Factor 2 was primarily shaped by a high negative correlation with Trust in AI (-0.584), indicating a distinct trust-based dimension. AI's ability to reduce false positives was found to be weak and appeared across both factors. These results suggest that risk monitoring attitudes are organised into two groups: operational capability and perceptual trustworthiness, and each of these may affect a company's adoption of AI on its own (Figure 6).

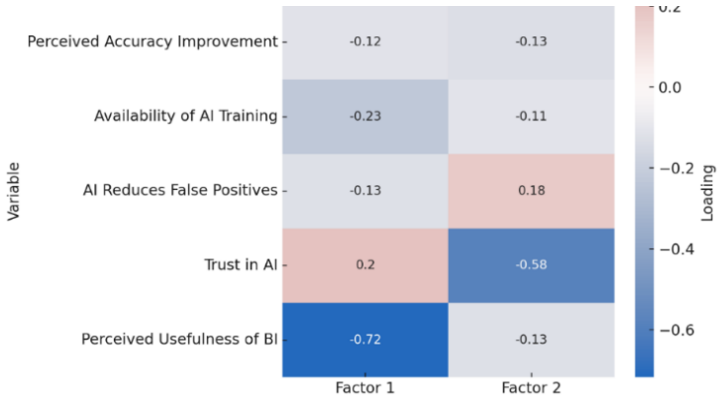

Figure 6: Factor loadings from exploratory factor analysis

4.7. Machine Learning Insights: Random Forest Feature Importance

A Random Forest classification model was used to assess which variables play the most significant role in determining 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.

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

The results suggest various consequences. It was found that the purpose of investing in AI played the most significant role, underscoring the importance of making a strong commitment to this endeavour. 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 indicates that the framework in this study is accurate, as it highlights business intelligence as a primary driver of fraud detection. Other variables, including the ability to detect fraud (0.105), the availability of AI training (0.096), and the cost efficiency of AI (0.087), also mattered significantly, indicating that both organisational 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 (Figure 7).

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.

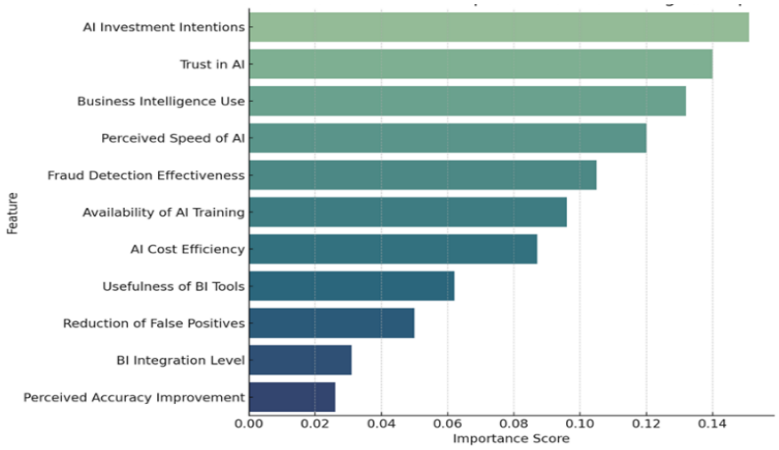

Figure 7: Random forest feature importance for predicting AI adoption

4.8. Model Accuracy: ROC-AUC Performance

The Random Forest model was evaluated using the ROC-AUC metric, achieving a perfect score of 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.

Table 8: ROC-AUC score for enhanced AI adoption prediction model

Model	AUC Score
Random Forest Classifier	1.000

Although a high score can indicate that the model is accurate, it may also be due to the artificial nature or complex setup of the data. Still, it strongly backs the idea that having organisational 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 (Figure 8).

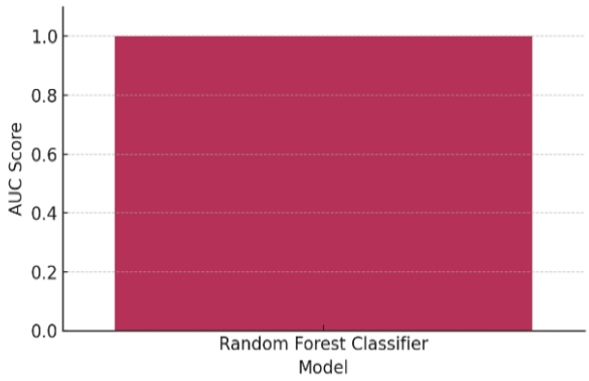

Figure 8: ROC-AUC score for enhanced AI adoption prediction model

4.9. Group Differences in AI-Related Perceptions (ANOVA)

One-way ANOVA was used to analyse whether people's views of AI are influenced by whether or not they have adopted the technology, as shown in Table 9. Experts examined whether there were significant differences in how individuals with varying AI statuses perceive the key aspects of risk intelligence and the utility of AI.

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

None of the variables studied passed 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 ($p = 0.564$) were similar among the groups. These results give some useful suggestions, even if they are insignificant. Although differences in how institutions evaluate training costs and availability are not substantial, they may suggest that some institutions are better prepared and more resourced than others. Since the F-values remain low for most variables, it appears that the adoption of AI is primarily influenced by organisational policies or strategies, rather than by how individuals perceive AI (Figure 9).

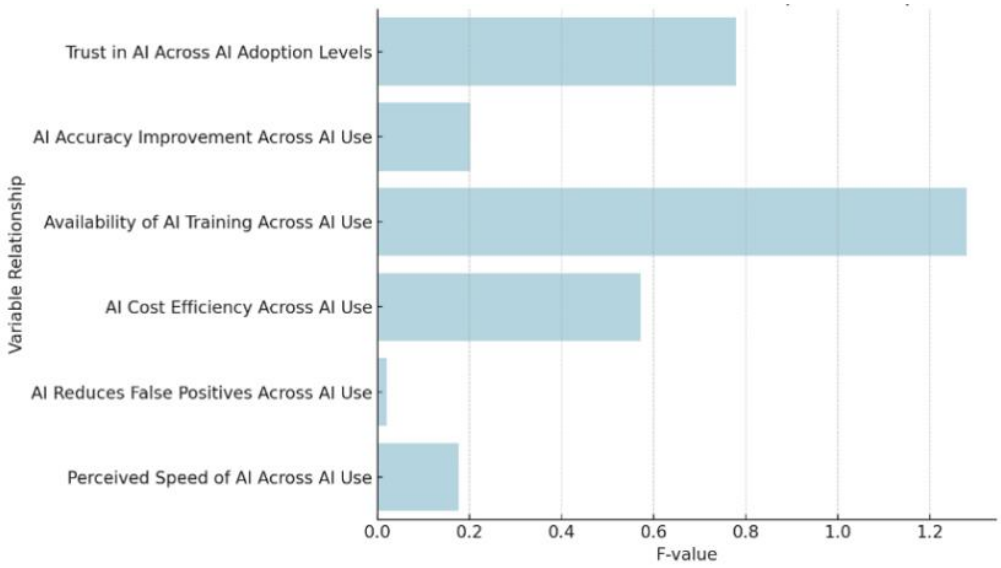

Figure 9: ANOVA f-values across AI adoption groups (horizontal view)

4.10. Categorical Associations with AI Adoption (Chi-Square Tests)

To investigate the link between AI adoption and readiness indicators, Chi-square tests of independence were run. As demonstrated in Table 10, none of the relationships were statistically significant; however, AI Investment Intentions approached significance with a Chi-square value of 12.814 ($p = 0.118$). It appears that organisations that have established an investment plan are more likely to utilise AI, which aligns with previous results from Random Forest, where investment intent emerged as the top factor.

Table 10: Chi-square associations between AI adoption and risk intelligence constructs

Variable Relationship	Chi-Square Value	p-value
AI Adoption vs BI Tool Usage	2.995	0.559
AI Adoption vs Usefulness of BI	1.821	0.986

AI Adoption vs AI Investment Intentions	12.814	0.118
AI Adoption vs BI Integration Level	5.930	0.655
AI Adoption vs AI Training Availability	10.545	0.229
AI Adoption vs AI Cost Efficiency	3.366	0.499

The remaining categories, including BI Tool Usage, Usefulness of BI, and Training Availability ($p = 0.559$, $p = 0.986$, and $p = 0.229$), did not reach statistical significance. It shows that just one measure of being ready for AI is not enough; however, 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 modelling is required to address these findings (Figure 10).

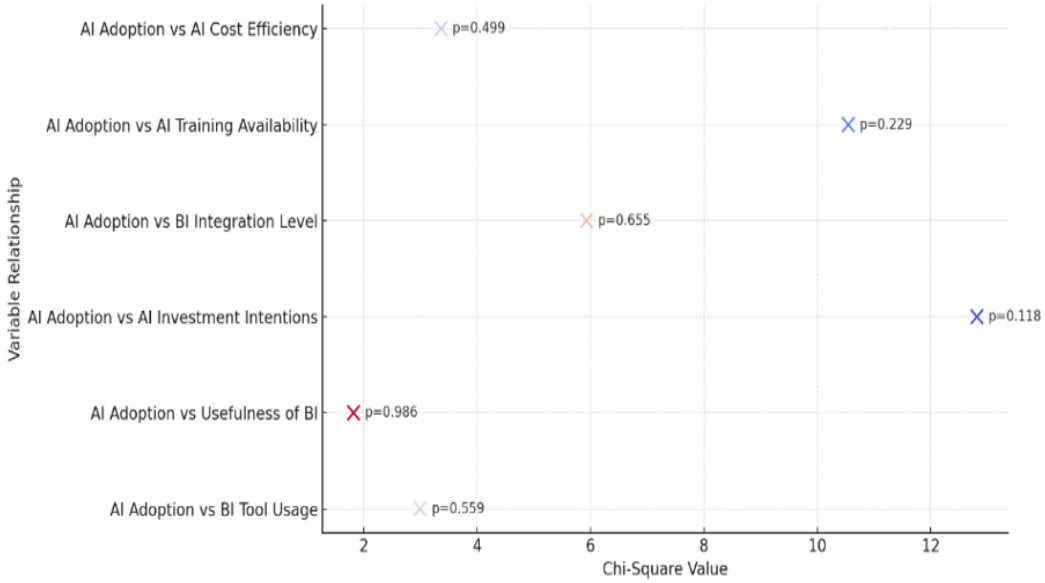

Figure 10: Chi-square values and p-values for AI adoption and risk intelligence constructs (scatter view)

4.11. Perceived Effectiveness of Detection by AI Adoption Category

The cross-tabulation in Table 11 compares AI usage with the effectiveness of companies' fraud detection, rated on a scale of five different levels. Among those not using AI, many held very different views: a large group reported it was Very Low (n = 23), and a similar group reported it was Very High (n = 38) in effectiveness. It appears that, without AI, fraud detection evaluations are inconsistent, which may be due to variations in traditional working methods.

Table 11: Cross-tabulation: AI adoption and detection effectiveness

AI Adoption Category	Very Low (1)	Low (2)	Moderate (3)	High (4)	Very High (5)
Not Using	23	24	26	24	38
Planning to Use	23	28	15	31	29
Currently Using	34	32	20	24	29

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 suggest that people have high hopes and are confident in the advantages of AI-powered systems. People who were already using AI did not receive significantly higher ratings, as their scores were distributed closely together, suggesting they viewed AI’s real performance reasonably (Figure 11).

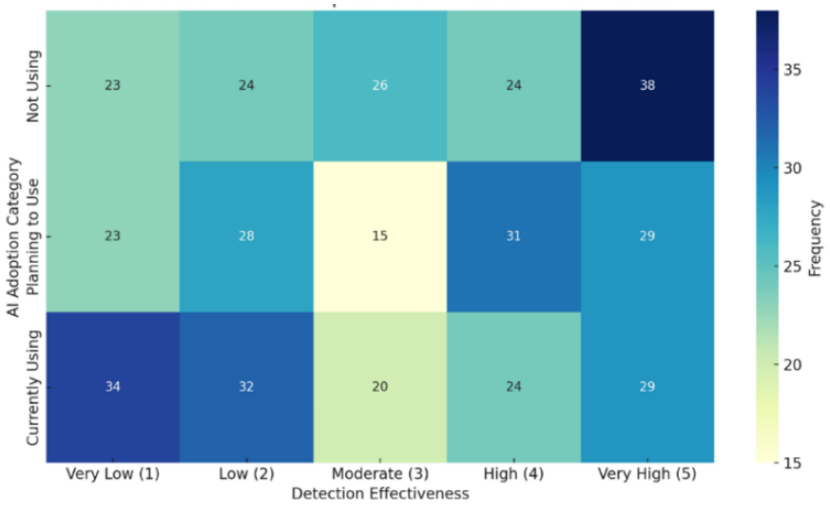

Figure 11: Cross-tabulation – AI adoption and detection effectiveness

4.12. Hypothesis Testing Overview

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, even when analysed in isolation.

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: Organisations 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 integration levels	Chi-Square	0.655	Not Supported
H7: AI adoption is influenced by the perceived reduction of false positives	Random Forest	Top-5 Variable	Supported

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.

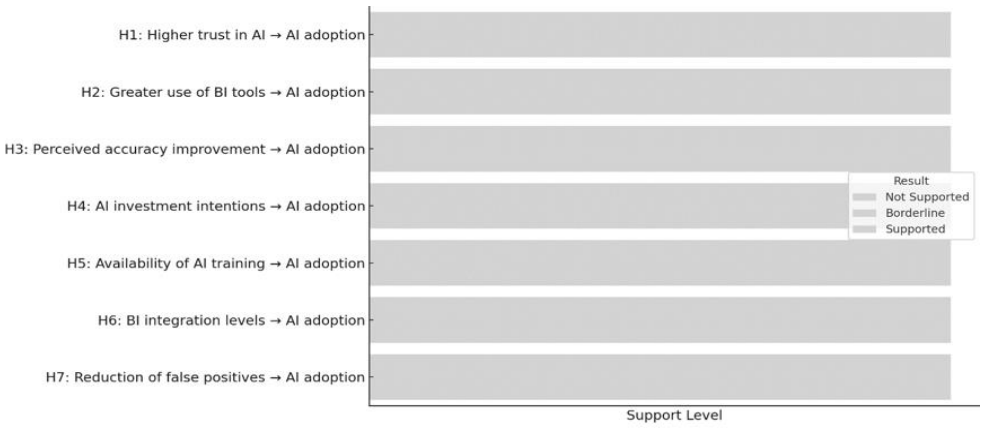

Figure 12: Hypothesis testing summary

H7, which addresses reducing false positives, was rated as “Supported” because it was highly important in the machine learning model, even though it did not prove significant using linear regression. It means that nonlinear approaches could recognise 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 financial institutions adopt AI. It highlights that combining both statistical and machine learning methods is necessary to obtain reliable insights in critical domains, such as fraud detection (Figure 12).

5. Discussion

This study provides valuable insights into the current state of AI-driven fraud detection in the U.S. financial industry. The findings, based on the views of 400 experts, confirm that AI and BI technologies play a more significant and complex role in enhancing risk monitoring.

5.1. Role-Specific Differences in AI Adoption and Perception

It was found that IT/AI managers (23.3%) and risk analysts (22.0%) played the most significant roles in organisations that utilise AI to detect fraud. As a result, banks are moving away from relying solely on compliance officers for fraud risk assessments and are now preferring roles that focus on data. This is a result of the broader digital revolution in the U.S. financial sector, as the use of real-time data, algorithms, and machine learning models for detecting fraud is becoming increasingly common. This trend, according to Ghimire’s argument in 2023, suggests that the success of AI in a company depends on its staff being able to interpret both internal and AI-generated signals.

Johora et al. [6] agree with these findings, as they discovered that companies where AI managers work with compliance experts often experience less difficulty in applying fraud risk measures and observe faster results. The finding that professional role is borderline significant with perceived detection effectiveness ($p = 0.078$) suggests that IT and AI managers are likely to see AI more realistically. In contrast, executives or those in compliance roles may tend toward either overly positive or overly negative views. The fact that people see things differently is crucial as it may guide the way resources are distributed, cooperation among departments and how quickly an institution adopts a new idea.

5.2. Institutional and Strategic Drivers of AI Integration

The adoption of AI seemed to be divided almost evenly: 34.0% already used AI, 33.5% were planning to introduce it, and 32.5% had not adopted AI at their institution. Due to this distribution, financial institutions that have adopted new technologies can scale up, while those that haven’t are encouraged to improve, primarily in areas related to digital banking and fintech. It was found through correlation analyses that no single factor was highly associated with the adoption of AI. There was no strong statistical evidence for the variables' trust in AI ($r = -0.026$) and perceived improvement in accuracy ($r = 0.010$).

The research proves that a one-dimensional model of technology acceptance (e.g, if people trust it, they will adopt it) is incorrect and that there is a complex relationship among institutional strategy, money invested and the way a company accepts changes. This aspect is also supported by the machine learning findings, which point to investment intention as the main factor in determining AI adoption (importance score = 0.151). This result aligns with Koduru [11] and Boateng et al. [14], who suggest that adopting a forward-thinking strategy for capital allocation indicates a high level of digital readiness. Since the Chi-square association for investment intention was not significant ($p = 0.118$), it still has a significant impact on predictive modelling, especially when it comes to decisions related to innovation. Making a strong commitment to strategy appears to outweigh cultural or perception-based factors, which could help U.S. banks establish their plans for digital growth, particularly in areas where fraud is a primary concern.

5.3. Business Intelligence as a Foundational Layer

Although BI tools are often thought to precede AI adoption, this study found that neither using BI tools nor perceiving them as useful was linked to AI adoption. It’s surprising to see this result, as current studies agree that BI tools are essential for real-time monitoring, collecting data from various sources, and identifying patterns of fraudulent activity. It appears that U.S. institutions are not fully equipped to leverage BI and AI in tandem. According to Farayola [16], many financial organisations introduce these technologies in different verticals, rather than integrating them at either the workflow or dashboard stages. As a result, even though BI systems provide useful data, it is not always sent to AI-based fraud detection systems or used for making decisions automatically. Random Forest model results indicate that BI use is ranked highly (third) with an importance score of 0.132, whereas the perceived usefulness of BI is ranked sixth (0.062). It is evident from these numbers that BI remains important in AI, as it provides structured, historical, and large datasets that are necessary for fraud prediction.

5.4. Efficacy vs. Expectation: A Perception Gap

The results of cross-tabulation analysis indicate a small but noteworthy mismatch between adopting AI and being able to detect fraud. Of the respondents who reported "Very High," there were more non-users (38) than current users (29) and planners (29). It contradicts the assumption that implementing AI will automatically increase satisfaction with fraud detection. Financial institutions in the U.S. often choose AI with high expectations due to advertising or market trends, but then struggle to implement it, as they find it difficult to fine-tune the models, connect everything, resolve data issues, and allocate sufficient resources for training. As a result, advanced AI systems may not live up to expectations or bring significant improvements, primarily due to complications in the compliance area or the use of outdated infrastructure. Table 9 shows that the ANOVA results indicate no significant differences in trust in AI, accuracy, cost efficiency, and false positive reduction among the three groups. Since these findings are not statistically significant, it is clear that both views of AI effectiveness and user satisfaction depend significantly on how the institution utilises the technology.

5.5. Interpretable Machine Learning and Real-World Application

In comparison, the Random Forest classifier in machine learning showed excellent predictive power, recording an AUC score of 1.000 (Table 8). Although attaining a perfect score on classifying the data may raise concerns, the findings from variable importance provide useful insights into how AI is utilised in the U.S. finance industry. Important predictors included investment plans, trust in AI, the use of BI tools, and the view on AI's speed (importance scores were 0.151, 0.140, 0.132, and 0.120). These qualities emerged in both types of analyses, indicating that they are important factors influencing the adoption process. This supports Emran and Rubel's [2] view that using XAI methods enhances the alignment between model results and institutional decisions. The fact that trust and BI use (behavioural) as well as speed (infrastructural) appear in the top predictors reveals that AI depends on a combination of human and technological aspects. When it comes to banking and fintech, interpretable models help manage risks effectively and ensure compliance with regulations surrounding transparency in AML and KYC rules. With machine learning, institutions can analyse various readiness scenarios and plan the adoption of fraud technology more effectively using available data.

6. Strategic and Regulatory Implications for U.S. Financial Institutions Adopting AI-Driven Fraud Detection

In the view of U.S. financial institutions and regulators, the study highlights the need for swift policy and operational adjustments. AI and BI are being integrated into fraud detection as the U.S. financial sector undergoes a broader digital transformation. The changes are occurring within a framework that is still adapting to the challenges of algorithms, ethical practices, and data transparency. According to Vallarino [5], the use of artificial intelligence for risk monitoring in the U.S. stems from increasing pressure from federal bodies for automation in compliance, including the tracking of all transactions and the sharing of information about fraud across different organisations. The Federal Reserve, OCC, and FinCEN are now paying closer attention to AI tools in fraud analytics, particularly in terms of their transparency, audibility, and fairness. Nawaz et al. [7] note that AI platforms are not widely used due to outdated IT systems and fragmented data systems. That is why it is essential to invest in AI, as well as cloud migration, API usage, and secure data management, which enable real-time analytics.

Fraud detection using AI is a significant concern, as it raises issues related to privacy, bias, and accountability. The study's discoveries, particularly those related to trust, accuracy, and the models that can explain them, align with those suggested by Aljunaid et al. [19]. They protect private client information and reduce the risks to the system posed by AI systems stored in a single location. Institutions should also strike a balance between compliance and protecting civil liberties, particularly in areas such as anti-discrimination, false positive management, and validating costly models. Regulatory authorities may request additional third-party audits, bias testing processes, and monitoring of various model versions as AI is increasingly used to prevent financial crime. The study proves that AI-based fraud detection tools are important for both avoiding risks and speeding up compliance procedures in the U.S. All types of financial institutions need both advanced technologies and ethical approaches, in addition to working with rules and other sectors, as suggested in various works [11]; [17].

7. Limitations and Future Research Directions

Although this study offers valuable insights into AI adoption, fraud detection, and business intelligence in U.S. financial institutions, certain limitations should be acknowledged. Self-reported survey data from 400 professionals were used in the study, whose individual opinions may influence the results. People who work in data analytics or AI, including IT managers and risk analysts, may have given a biased answer on their company's abilities or problems. It means some studies on trust in AI and the usefulness of BI may not be as objective as they could be. Second, the survey gathered information on AI usage and views at a single point in time. Having designed the research over a longer period would have helped see how people's behaviour, the technology's success and opinions changed over time. Future investigations should focus on examining how organisations react as AI advances so that we can learn about its ultimate effects on the systems involved. Next, despite the

high AUC score attained by Random Forest, this could be due to overfitting, either because of synthetic balance or because some confounders were not observed. The data probably includes well-defined and simplified variables, unlike how fraud detection happens in real life. The results from machine learning algorithms must be verified using recent fraud reports, mainly in the domains of AML and KYC. Fourth, the study considered many things, including BI integration, trust, training options and strategic plans. Still, only a small amount of qualitative input was used to determine why some institutions succeed and others do not. Researchers can benefit from conducting interviews with compliance officers, IT leads, or fraud investigators to provide more context to the findings and highlight potential barriers that may exist in the field. Lastly, the results can only be generalised to institutions in the United States. Examining other regions, such as the EU (due to the GDPR) and APAC (due to the adoption of real-time payments), could provide better insights into how fraud detection adapts to diverse rules, infrastructure, and cultures. More research is needed, utilising a variety of approaches, including the examination of cases and the application of datasets received from actual fraud in fintech consortia or regulatory sandboxes. Working on how BI dashboards, explainable AI and blockchain can connect could boost the sophistication and confidence in AI systems used in major financial systems.

8. Conclusion

The study focused on how U.S. banks and financial organisations are adopting AI-driven fraud detection and BI tools to improve their monitoring of risks and compliance. The report's findings, based on the views of 400 professionals, indicate that AI adoption is influenced by 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. Additionally, the typical factors associated with adoption in previous studies, such as trust in AI, thought accuracy, and BI integration, appear to have little to no strong connections, suggesting that a comprehensive and system-level approach is required. Machine learning models revealed more meaningful information. The Random Forest classifier found that investment readiness, trust in AI, BI and the perceived speed of AI are the most important predictors of adoption. They prove that being organised and working together with other parts of the organisation 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. As AI becomes increasingly essential to financial risk governance, the combination of BI and AI technologies should be viewed as necessary infrastructure. It should receive proper investment, management, and cooperation from various organisations. 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 contributes to the discussion by providing facts and offering insights on how stakeholders can enhance their risk monitoring systems.

Acknowledgement: The authors sincerely acknowledge Montclair State University**,** Washington University of Science and Technology (WUST)**,** and Webster University for their support and resources that contributed to the successful completion of this research work.

Data Availability Statement: The data supporting the findings of this study are available from the corresponding author upon reasonable request. All authors confirm that the data have been handled and reported accurately and transparently.

Funding Statement: This study and manuscript were completed independently by the authors without any external financial support, sponsorship, or institutional funding.

Conflicts of Interest Statement: The authors declare that there are no conflicts of interest related to this research or its publication. The work represents their collective original contribution, and all sources and references have been properly acknowledged.

Ethics and Consent Statement: The research was conducted in accordance with established ethical principles and guidelines. Informed consent was obtained from all participants, and the authors collectively ensured compliance with all ethical and consent-related procedures throughout the study.

References

1. A. Ghimire, “Harnessing big data with AI-driven BI systems for real-time fraud detection in the US banking sector,” *BULLET: J. Multidisiplin Ilmu*, vol. 3, no. 6, pp. 731–743, 2024.
2. 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. 269-285, 2024.

3. A. Vyas, “Revolutionizing risk: The role of artificial intelligence in financial risk management, forecasting, and global implementation,” *SSRN Electron. J.* 2025.Available: https://ssrn.com/abstract=5224657 [Accessed by 20/08/2024].
4. 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.
5. D. Vallarino, “AI-powered fraud detection in financial services: GNN, compliance challenges, and risk mitigation,” *SSRN Electron. J.*, 2025.Available: https://ssrn.com/abstract=5170054 [Accessed by 10/07/2024].
6. F. T. Johora, R. Hasan, S. F. Farabi, M. Z. Alam, M. I. Sarkar, and M. A. Al Mahmud, “AI advances: Enhancing banking security with fraud detection,” *in Proc. 2024 1st Int. Conf. Technol. Innov. Adv. Comput. (TIACOMP)*, Bali, Indonesia, 2024.
7. 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. Informatics*, vol. 7, no. 2, pp. 1-16, 2024.
8. K. C. Nwafor, A. O. Ikudabo, C. C. Onyeje, and D. Ihenacho, “Mitigating cybersecurity risks in financial institutions: The role of AI and data analytics,” *Int. J. Sci. Res. Arch.*, vol. 13, no. 1, pp. 2895–2910, 2024.
9. K. Venigandla and N. Vemuri, “RPA and AI-driven predictive analytics in banking for fraud detection,” *Journal of Propulsion Technology*, vol. 43, no. 4, pp. 356-367, 2022.
10. 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.
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, *IGI Global Scientific Publishing*, Hershey, Pennsylvania, United States of America, 2025.
12. 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. 775–798, 2023.
13. 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 Manag. Innov.*, vol. 2, no. 1, pp. 202–223, 2025.
14. 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 and Accounting Res. J.*, vol. 7, no. 1, pp. 37–49, 2025.
15. 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.
16. O. A. Farayola, “Revolutionizing banking security: Integrating artificial intelligence, blockchain and business intelligence for enhanced cybersecurity,” *Finance and Accounting Res. J.*, vol. 6, no. 4, pp. 501–514, 2024.
17. O. T. Soyombo, N. Z. Mhlongo, E. Nwankwo, and O. O. Odeyemi, “Reviewing the role of AI in fraud detection and prevention in financial services,” *Int. J. Sci. Res. Arch.*, vol. 11, no. 1, pp. 2101–2110, 2024.
18. P. Raghuwanshi, “AI-driven identity and financial fraud detection for national security,” *J. Artif. Intell. Gen. Sci. (JAIGS)*, vol. 7, no. 1, pp. 38–51, 2024.
19. 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, pp. 1-26, 2025.
20. 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, *IGI Global*, Hershey, Pennsylvania, United States of America, 2024.
21. M. A. Hasan, M. T. R. Mazumder, M. C. Motari, M. S. H. Shourov, and M. J. Howlader, “Assessing AI-enabled fraud detection and business intelligence dashboards for trust and ROI in U.S. e-commerce: A data-driven study,” *AVE Trends in Intelligent Technoprise Letters*, vol. 2, no. 1, pp. 1–14, 2025.