Journal of
Information Technology,
Cybersecurity, and Artificial Intelligence

(RESEARCH)

Evaluating the Effectiveness of Cyber Security Frameworks in Preventing Banking Fraud

Jamil Uddin Bhuiyan

Department of Business, Golden Gate University, SanFrancisco, USA

Md. Halimuzzaman

School of Business, Galgotias University, Delhi, India

Dr. Jaideep Sharma

School of Business, Galgotias University, Delhi, India

Mohammad Tofazzal Hossain

School of Business, Bangladesh Open University, Gazipur, Bangladesh

Journal of Information Technology, Cybersecurity, and Artificial Intelligence, 2026, 3(3), 75-94

Article DOI: https://doi.org/10.70715/jitcai.2026.v3.i3.068

Abstract

Banking fraud has become a significant challenge due to the rapid growth of digital financial transactions and evolving cyber threats. Cybersecurity frameworks play a crucial role in mitigating such risks by enhancing detection and prevention capabilities. This study aims to evaluate the effectiveness of different machine learning-based approaches for identifying fraudulent banking transactions within the context of cybersecurity controls. A synthetic yet realistic banking dataset consisting of 12,000 transactions from 3,000 customers was used for analysis. The dataset includes transaction details, behavioral attributes, and security-related features such as authentication methods and risk scores. Several classification models, including Logistic Regression, Random Forest, XGBoost, Support Vector Machine (SVM), and K-Nearest Neighbors (KNN), were implemented. The dataset was split into training (80%) and test (20%) sets, and performance was evaluated using accuracy, precision, recall, F1-score, ROC-AUC, and Precision-Recall metrics. The experimental results indicate that ensemble-based models such as Random Forest and XGBoost achieved higher accuracy (above 98%) and better overall performance compared to other models. However, despite high accuracy, all models struggled to detect minority fraud cases due to class imbalance, as reflected in lower recall and F1 Scores for the fraud class. Logistic Regression provided stable performance with interpretable results, while SVM and KNN showed comparatively lower effectiveness in fraud detection. The findings suggest that while cyber security-inspired feature engineering improves model performance, addressing class imbalance remains critical for reliable fraud detection. The

DOI: https://doi.org/10.70715/jitcai.2026.v3.i3.068

study concludes that advanced ensemble techniques, combined with appropriate data-balancing strategies, can significantly enhance the effectiveness of cybersecurity frameworks in preventing banking fraud.

Keywords: Banking Fraud Detection; Cyber Security Framework; Machine Learning; Random Forest; XGBoost; Fraud Classification.

1. Introduction

The rapid growth of digital banking has transformed the financial sector by enabling faster transactions, remote access, and improved customer convenience through online platforms and automated systems. However, this transformation has also increased financial institutions' exposure to cyber threats, including phishing, malware, identity theft, account compromise, and transaction fraud, making cybersecurity a central concern in modern banking operations (Asakpa, 2023). Because banks handle sensitive customer information, high-value assets, and critical financial infrastructures, they remain prime targets for cybercriminals. To reduce these risks, institutions increasingly rely on cybersecurity and compliance frameworks that support risk governance, data protection, and consumer trust in digital financial environments (Chukwuemeka Iregbu, 2025; Tamrakar & Rajput, 2025). Among the most widely discussed approaches, cybersecurity frameworks such as NIST CSF, ISO/IEC 27001, PCI-DSS, and integrated risk management models provide structured mechanisms for identifying vulnerabilities, strengthening controls, and improving cyber resilience in banking(Azura et al., 2025; Olutimehin, 2025). Broader research also emphasizes that resilient financial institutions require strategic threat mitigation, adaptive defense, and continuous preparedness against evolving attacks (Tope Oladele Jooda et al., 2023; Tran, 2025). At the operational level, machine learning and AI-driven systems are increasingly used to detect fraudulent behavior by analyzing transaction patterns, behavioral indicators, and anomalies more efficiently than traditional rule-based systems. These techniques have shown promise in improving fraud monitoring and supporting real-time detection in banking environments(Agbeve et al., 2025). In addition, studies on internet banking security stress the importance of protecting account holders' personal and transactional information through optimized cybersecurity techniques and layered defense frameworks (Yasir Ali Solangi, 2025). The seriousness of this issue is further reflected in major financial cyber incidents, particularly the Bangladesh Bank cyber intrusion, which demonstrated how weaknesses in financial cybersecurity can create severe legal, institutional, and economic consequences. At the same time, emerging threats continue to push financial institutions toward stronger encryption and more advanced security architectures to safeguard sensitive records (Gbadebo, 2025). Despite growing research in this field, limited empirical studies compare multiple machine learning models within the broader context of cybersecurity frameworks for banking fraud prevention. Therefore, this study evaluates the effectiveness of cyber security frameworks in preventing banking fraud by comparing Logistic Regression, Random Forest, XGBoost, Support Vector Machine (SVM), and K-Nearest Neighbors (KNN) using transaction, behavioral, and security-related features.

2. 2. Literature Review

2.1. Recent Developments in Cyber Security Frameworks for Banking Fraud Prevention

Recent developments in cybersecurity frameworks for banking fraud prevention show a clear movement from conventional static controls toward more intelligent, adaptive, and privacy-aware security models. Earlier discussions on AI in banking security emphasized the growing role of artificial intelligence in strengthening cyber defense, fraud identification, and risk control in financial systems(Soni, 2019). More recent studies have expanded this line of research

by proposing ensemble-based fraud detection models that combine multiple algorithms to improve detection performance and provide stronger countermeasures against financial transaction cyber threats (Alhashmi et al., 2023). At the same time, emerging research highlights that modern fraud prevention frameworks must also address privacy and regulatory compliance, particularly in digital banking environments, where federated learning has been introduced as a promising privacy-preserving approach for collaborative fraud detection without direct data sharing(Umakor et al., 2025). Broader AI-driven cybersecurity research further indicates that advanced machine learning techniques for real-time fraud monitoring, anomaly detection, and risk mitigation increasingly support current financial protection frameworks. However, concerns regarding false negatives, fairness, and governance remain important (Ajayi et al., 2025). In banking-specific fraud analytics, recent work also shows growing interest in unsupervised learning approaches, as traditional rule-based systems often fail to keep pace with rapidly evolving fraud behavior in digital transactions (Karthik Meduri, 2024). In addition, systematic review evidence suggests that machine learning and deep learning have become central to current research on cyber fraud detection in banking, particularly because they offer more flexible and scalable alternatives to conventional fraud monitoring techniques (Marazqah Btoush et al., 2023).

2.2. Theoretical and Practical Foundations of Fraud Detection in Banking

Fraud detection in banking is grounded in both core security controls and adaptive analytical systems. In practice, banks rely on measures such as multi-factor authentication, encryption, monitoring, and awareness programs to reduce fraud risk (Elantheraiyan et al., 2024). At the same time, modern banking increasingly depends on updated digital infrastructure and AI-supported systems to trace suspicious and illegal transactions more effectively (Prakash, 2018). Recent studies further show that machine learning has strengthened fraud detection by enabling anomaly detection, risk assessment, and real-time threat mitigation beyond traditional rule-based methods (Doddipatla & Ramadugu, 2025).In addition, integrated banking security models now combine encryption, biometric authentication, AI-based fraud monitoring, and compliance mechanisms to provide a more practical, layered fraud detection framework (S. Madhumitha & Ms. N. Vaishnavi, 2025).

2.3. Cyber Security and Fraud Detection Challenges in Digital Banking

Digital banking faces growing cybersecurity and fraud-detection challenges as threats become more adaptive, data-intensive, and difficult to identify in real time. Recent studies show that banks must deal with insider threats, phishing attacks, and unusual transaction behavior, for which traditional security methods often fail to detect effectively (Muthukumarasamy & Vanitha, 2025). At the same time, mobile banking systems face major risks related to secure cloud transactions, response time, and balancing strong encryption with operational efficiency(Yuvarani & Mahaveerakannan, 2025a). Authentication also remains a challenge, as online banking platforms must reduce spoofing, identity theft, and unauthorized access while maintaining reliable user verification (Alkhafaji et al., 2025). In mobile banking, behavioral biometrics offer continuous monitoring, but issues such as privacy, model transparency, user variability, and adversarial attacks still complicate secure deployment (Kacheru, 2025). More broadly, AI-powered fraud detection improves risk management, yet false positives, evolving fraud patterns, and the need for real-time, adaptive learning remain persistent challenges in digital finance (Dharmireddi et al., 2025). In addition, IoT-cloud banking environments introduce further concerns related to data breaches, unauthorized access, and transaction

integrity, making secure storage and communication a continuing challenge for financial institutions (Yuvarani & Mahaveerakannan, 2025b).

2.4. Limitations of Current Banking Fraud Detection Research

Current research on banking fraud detection still has several limitations. Existing studies show that many systems struggle to adapt to evolving threats, high false-positive rates, and real-time operational demands in financial environments(Karn et al., 2025). Ensemble and machine learning models improve detection, but their generalizability is often limited by dataset constraints and the need for further validation across broader fraud patterns (Tamanna et al., 2024). Broader review evidence also indicates that explainability, privacy, bias, and the dynamic nature of fraud remain major barriers to the scalable adoption of AI in financial networks (Jahan Sarna et al., 2025). In addition, research on the US financial market highlights that regulatory, ethical, and transparency concerns continue to complicate the sustainable deployment of AI-based fraud detection systems(Chukwu, 2025). Related financial AI research further shows that data privacy risks and algorithmic bias can undermine fairness and trust even when cybersecurity governance is not sufficiently robust (Salami et al., 2025).

2.5. Research Gap

Although previous studies have discussed cybersecurity frameworks and AI-based fraud detection in banking, limited research has empirically compared multiple machine learning models using transaction, behavioral, and security-related features in a single analytical framework. In addition, the challenge of class imbalance in detecting minority fraud cases has received comparatively less attention. Therefore, a clear need exists for a comparative study evaluating the effectiveness of models for banking fraud detection within the context of cybersecurity controls.

2.6. Research Questions

Based on the identified research gap, this study seeks to address the following research questions:

1. How do different machine learning models compare in detecting fraudulent banking transactions?
2. Which machine learning model provides the highest effectiveness in banking fraud classification?
3. How do transaction, behavioral, and security-related features contribute to fraud detection performance?
4. How does class imbalance affect the identification of fraudulent transactions by machine learning models?
5. How can machine learning-based fraud detection support stronger cybersecurity practices in banking systems?

2.7. Research Objectives

The primary objective of this study is to evaluate the effectiveness of cybersecurity frameworks in preventing banking fraud by applying machine learning techniques. Specifically, the study aims to:

1. To compare the performance of different machine learning models in detecting fraudulent banking transactions.
2. To identify the model that provides the highest effectiveness in banking fraud classification.
3. To examine the contribution of transaction, behavioral, and security-related features to fraud detection performance.
4. To assess the impact of class imbalance on the identification of fraudulent transactions.
5. To evaluate how machine learning-based fraud detection can support stronger cybersecurity practices in banking systems.

3. 3. Materials and Methods

3.1. Study Area

This study was conducted within the context of digital banking environments, where cybersecurity controls and fraud-detection mechanisms are integrated into transaction processing systems. The study focuses on banking platforms that conduct financial activities through electronic and online channels. These environments provide an appropriate setting for examining how cybersecurity frameworks and machine learning techniques can help prevent fraudulent banking transactions.

3.2. Study Design

This study employed a quantitative and comparative research design. The objective was to evaluate the effectiveness of different machine learning models for detecting fraudulent transactions within a cybersecurity framework. A structured banking dataset was used to compare model performance using standard classification metrics.

3.3. Sample Size and Selection

The dataset used in this study consisted of 12,000 banking transaction records collected from 3,000 customers. The data were prepared in a synthetic yet realistic format to represent actual banking transaction behavior. The dataset included both legitimate and fraudulent transactions. For model development and validation, the dataset was split into training and test sets at an 80:20 ratio.

3.4. Measures and Variables

The study included transaction, behavioral, and security-related variables relevant to banking fraud detection. These variables included transaction amount, authentication method, device type, and risk score. The dependent variable was fraud classification (normal or fraudulent), while the independent variables served as predictors in the machine learning models.

Feature Selection Justification: Features were selected based on a combination of domain knowledge from the banking fraud detection literature and alignment with established cybersecurity frameworks (such as NIST CSF and ISO 27001). Specifically:

- Security-related features (e.g., risk score, CVV validation, authentication method, IP address flag) were prioritized because they directly correspond to key preventive and detective controls in cybersecurity frameworks. For instance, risk score and authentication method align with the Protect (PR.AC) and Detect (DE.AE) functions of the NIST Cybersecurity Framework.
- Transaction and behavioral features (e.g., transaction amount, device type, account balance, transaction type, location) were selected for their proven predictive power in identifying anomalous patterns, as supported by prior studies on fraud analytics.
- This domain-driven and framework-aligned approach ensures that the selected features are not only statistically relevant but also practically meaningful for real-world cybersecurity governance in banking.

DOI: https://doi.org/10.70715/jitcai.2026.v3.i3.068

Additionally, the Random Forest model's feature importance analysis (see Figure 5) further validated that risk score, CVV validation, and transaction amount were among the most influential variables, confirming the appropriateness of the initial feature selection.

Mapping of Features to Cyber Security Frameworks

To strengthen the connection between the selected features and established cybersecurity practices, the following table maps the key features used in this study to specific controls in the NIST Cybersecurity Framework (CSF) and ISO/IEC 27001.

Table 1: Mapping of Selected Features to Cyber Security Framework Controls

Feature	NIST CSF Function & Category	ISO 27001 Control Example	Rationale
Risk Score	Detect (DE.AE) – Anomalies and Events	A.8.2 Information Classification & Risk Assessment	Identifies potential anomalous behavior in real-time
Authentication Method	Protect (PR.AC) – Identity & Access Management	A.5.17 Authentication Information & A.8.3 System Access Control	Ensures proper user verification and prevents unauthorized access
CVV Validation	Protect (PR.DS) – Data Security	A.8.24 Use of Cryptography	Verifies card authenticity and protects sensitive payment data
IP Address Flag	Detect (DE.CM) – Security Continuous Monitoring	A.12.4 Logging and Monitoring	Helps detect suspicious access locations and potential fraud
Transaction Amount	Detect (DE.AE) + Respond	A.6.1 Internal Organization & Risk Treatment	Supports anomaly detection based on unusual monetary values
Device Type & Location	Protect (PR.AC) + Detect (DE.AE)	A.8.1 Responsibility for Assets	Monitors behavioral context for fraud risk assessment

This explicit mapping demonstrates that the feature engineering in this study is not arbitrary but grounded in recognized cybersecurity governance frameworks. By aligning transaction, behavioral, and security-related features with the NIST CSF's Protect and Detect functions and ISO 27001 controls, the study bridges technical machine learning models with practical cybersecurity implementation in banking environments.

3.5. Data Collection Procedure

The data were organized in a structured format to simulate realistic banking transaction activities. Each record represented a transaction associated with a customer profile and security-related attributes. Before model

implementation, the dataset was cleaned and prepared for analysis. Relevant features were selected, and the fraud label was used as the target variable for classification.

3.6. Research Tools and Techniques

Five machine learning algorithms were applied in this study: Logistic Regression, Random Forest, Support Vector Machine (SVM), XGBoost, and K-Nearest Neighbors (KNN). These models were selected because of their common use in fraud detection and classification studies. The analysis was conducted using Python-based tools for data processing, model training, prediction, and evaluation.

3.7. Data Analysis Techniques

Model performance was evaluated using accuracy, precision, recall, and F1-score. In addition, the Random Forest model was further examined using a confusion matrix, ROC curve, Precision-Recall curve, and feature importance analysis. These techniques were used to compare the models' effectiveness and identify the most influential features in fraud detection. Table 2 summarizes the main components of the research design, including the dataset, data split, target variable, machine learning models, and evaluation metrics.

Table 2: Summary of the Research Design

Item	Details
Data	12,000 transactions; 3,000 customers
Method	Quantitative comparative approach
Split	80:20
Output	Fraud classification
Models	LR, RF, SVM, XGBoost, KNN
Measures	Accuracy, Precision, Recall, F1-score

4. 4. Results and Analysis

4.1. Comparison of Model Performance

This section presents the experimental results and analytical findings obtained from the machine learning models applied in this study. The primary objective of the analysis is to evaluate the performance of different models for detecting fraudulent banking transactions using transaction attributes, behavioral patterns, and security-related features. In this research, five machine learning algorithms—Logistic Regression, Random Forest, Support Vector Machine (SVM), XGBoost, and K-Nearest Neighbors (KNN)—were implemented and tested using the prepared dataset. The dataset consisted of 12,000 transaction records collected from 3,000 customers and included various features such as transaction amount, authentication method, device type, and risk score. The dataset was divided into training and testing sets following an 80:20 ratio. Model performance was evaluated using several statistical metrics, including

DOI: https://doi.org/10.70715/jitcai.2026.v3.i3.068

accuracy, precision, recall, and F1-score. The overall performance comparison of the models based on these evaluation metrics is summarized in Table 3.

Table 3: Comparison of Model Performance

Model	Accuracy	Precision	Recall	F1-score
Logistic Regression	0.9779	0.9838	0.9779	0.9807
Random Forest	0.9896	0.9793	0.9896	0.9844
SVM	0.9854	0.9839	0.9854	0.9846
XGBoost	0.9808	0.9829	0.9808	0.9818
KNN	0.9888	0.9835	0.9888	0.9853

4.2. Most Effective Fraud Detection Model

Figure 1 presents the comparative performance of the machine learning models used in this study based on accuracy, precision, recall, and F1-score. Among the evaluated models, Random Forest achieved the highest overall accuracy of 0.9896, indicating its strong ability to detect fraudulent banking transactions. K-Nearest Neighbors (KNN) and Support Vector Machine (SVM) also demonstrated competitive performance with accuracies of 0.9888 and 0.9854, respectively. XGBoost showed stable performance with an accuracy of 0.9808, while Logistic Regression achieved 0.9779. The precision, recall, and F1-score values further illustrate the comparative behavior of the models across different evaluation metrics. Although most models achieved high overall accuracy, detailed analysis indicates that detecting fraudulent transactions remains challenging due to the dataset's class imbalance. Ensemble-based methods such as Random Forests and XGBoost exhibited better generalization, while Logistic Regression provided consistent, interpretable results.

DOI: https://doi.org/10.70715/jitcai.2026.v3.i3.068

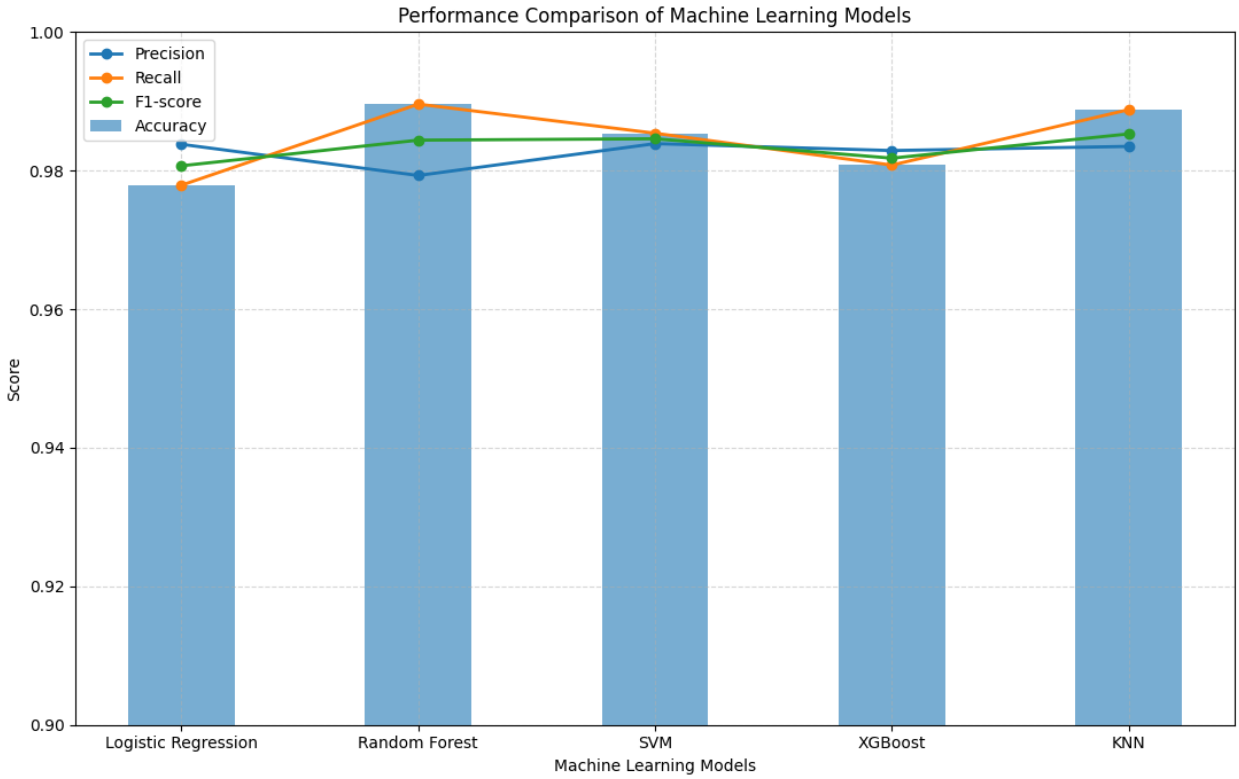

Figure 1: Performance of Fraud Detection Models

Overall, the results indicate that Random Forest provides the most effective and reliable performance for the given dataset, followed closely by KNN and SVM.

4.3. Impact of Class Imbalance on Fraud Detection Performance

The Random Forest model demonstrated superior performance in detecting fraudulent banking transactions compared to other models used in this study. The model achieved an overall accuracy of 0.9896, indicating its effectiveness in classifying transaction data. The evaluation metrics, including precision, recall, and F1-score, were calculated to assess the model's performance in detail, as presented in Table 4.

Table 4: Impact of Class Imbalance on Random Forest Performance

Class	**Precision**	**Recall**	**F1-score**	**Support**
0 (Normal)	0.9896	1.0000	0.9948	2375
1 (Fraud)	0.0000	0.0000	0.0000	25
Accuracy			**0.9896**	2400
Macro Avg	0.4948	0.5000	0.4974	2400
Weighted Avg	0.9793	0.9896	0.9844	2400

Despite achieving high overall accuracy, the Random Forest model failed to correctly identify fraudulent transactions, as indicated by zero precision, recall, and F1-score for the fraud class. This issue arises from severe class imbalance in

the dataset, where normal transactions significantly outnumber fraudulent ones. As a result, the model is biased toward the majority class, resulting in poor fraud-detection performance. Therefore, although Random Forest demonstrates strong overall classification performance, additional techniques such as data resampling, class balancing, or cost-sensitive learning are necessary to improve its effectiveness in detecting fraudulent cases.

4.3.1. Analysis of Class Imbalance and Balancing Techniques

The severe class imbalance in the dataset (only 25 fraud cases out of 2,400 in the test set) caused the models to be heavily biased toward the majority (normal) class. As a result, even the best-performing model (Random Forest) achieved zero recall and F1-score for the fraud class, despite high overall accuracy.

Standard balancing techniques such as SMOTE (Synthetic Minority Over-sampling Technique) and ADASYN (Adaptive Synthetic Sampling) are commonly used to address this issue. SMOTE generates new synthetic fraud samples through linear interpolation between existing minority instances, while ADASYN focuses more on difficult-to-learn borderline examples. However, these techniques may fail or underperform in fraud detection for several reasons:

- They can introduce noise or unrealistic synthetic samples, especially when fraud patterns are highly diverse and evolving.
- In cases of significant class overlap (where some normal transactions resemble fraud), oversampling can worsen model confusion.
- Simple oversampling without proper cleaning (e.g., SMOTE + Tomek links) often leads to overfitting on synthetic data, reducing generalization to unseen real transactions.

To overcome these limitations, this study recommends adopting cost-sensitive learning (e.g., assigning a higher misclassification cost to the fraud class in XGBoost or Random Forest) alongside advanced oversampling. Cost-sensitive approaches directly optimize for the high financial cost of missing fraud cases rather than just balancing the dataset.

Future experiments should include a systematic comparison of SMOTE, ADASYN, and cost-sensitive methods to identify the most effective combination for banking fraud detection.

4.4. Further Evaluation of Random Forest Model

The Random Forest model demonstrated superior performance in detecting banking transactions, achieving a high overall accuracy of 0.9896. This indicates that the model is highly effective in classifying transaction data under general conditions. However, further evaluation using class-wise performance metrics reveals important insights regarding its effectiveness in fraud detection. The model's classification outcomes are further illustrated in Figure 2.

DOI: https://doi.org/10.70715/jitcai.2026.v3.i3.068

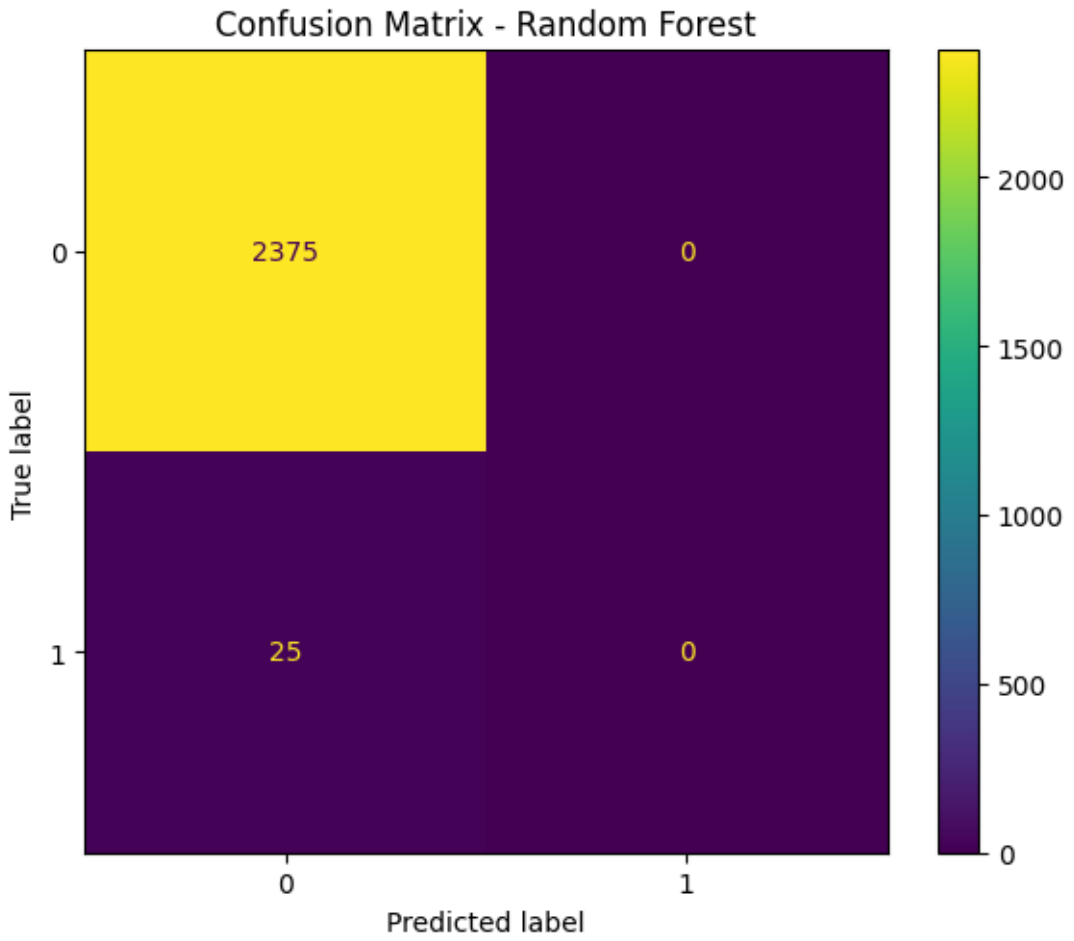

Figure 2: Confusion Matrix of Random Forest Model

The Receiver Operating Characteristic (ROC) curve is used to evaluate the Random Forest model's ability to distinguish between normal and fraudulent transactions. It provides a graphical representation of the trade-off between the true positive rate (TPR) and false positive rate (FPR) at different threshold values. The ROC curve for the Random Forest model is illustrated in Figure 3, along with the Area Under the Curve (AUC) score.

DOI: https://doi.org/10.70715/jitcai.2026.v3.i3.068

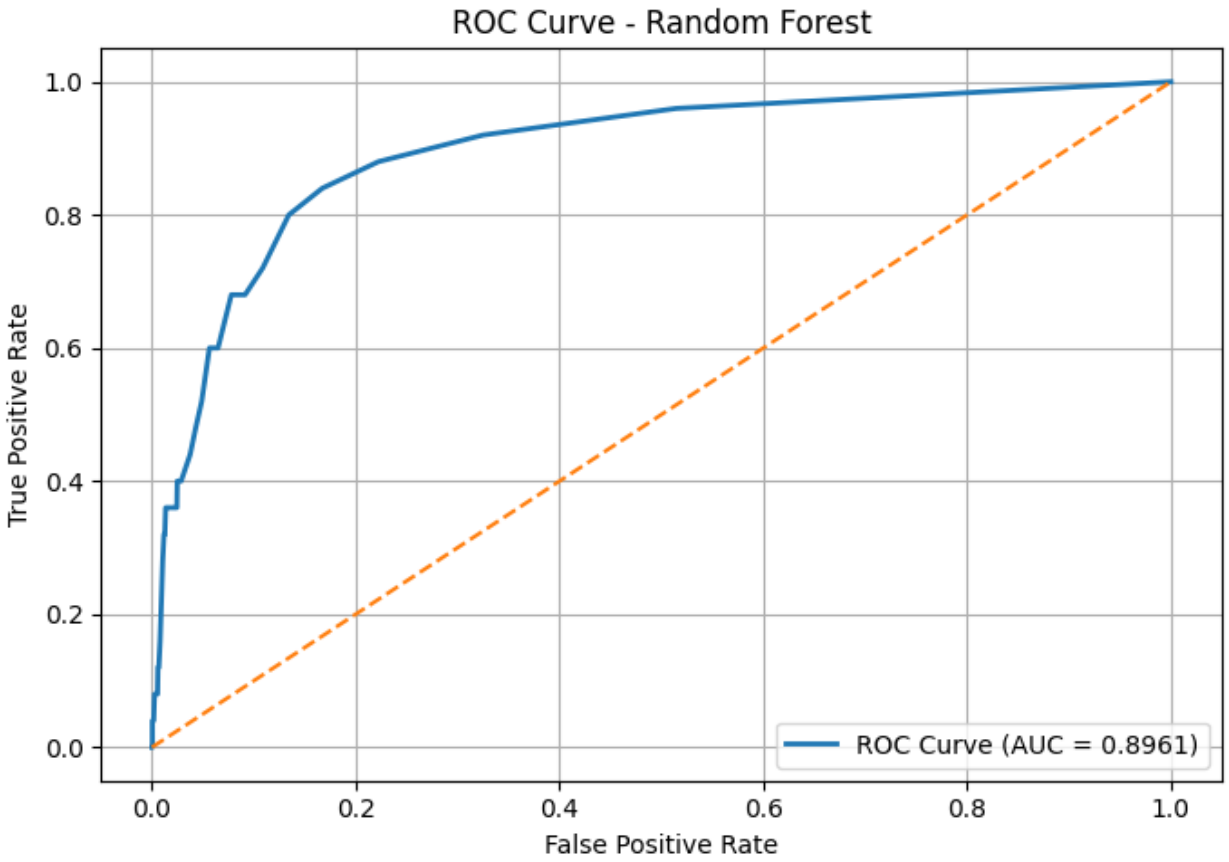

Figure 3: ROC Curve of Random Forest Model

The Precision-Recall (PR) curve is used to evaluate the performance of the Random Forest model, particularly in handling imbalanced datasets where the minority class (fraud) is of greater importance. It illustrates the trade-off between precision and recall at different classification thresholds. The PR curve for the Random Forest model is presented in Figure 4, along with the Average Precision (AP) score.

DOI: https://doi.org/10.70715/jitcai.2026.v3.i3.068

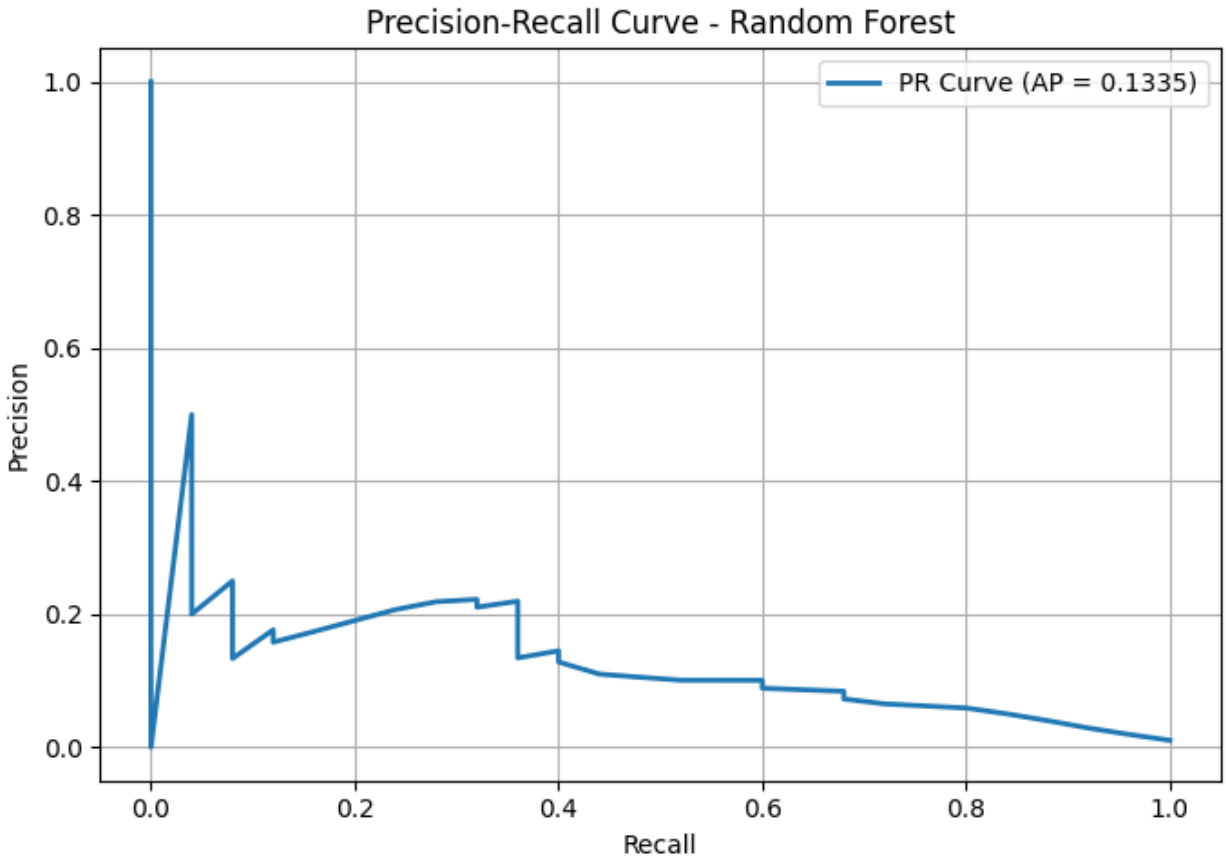

Figure 4: Precision-Recall Curve of Random Forest Model

4.5. Contribution of Features to Fraud Detection

Feature importance analysis is conducted to identify the most influential variables contributing to fraud detection in the Random Forest model. This analysis helps in understanding which transaction attributes and security-related features have the greatest impact on model predictions. The top 20 most important features identified by the model are illustrated in Figure 5.

DOI: https://doi.org/10.70715/jitcai.2026.v3.i3.068

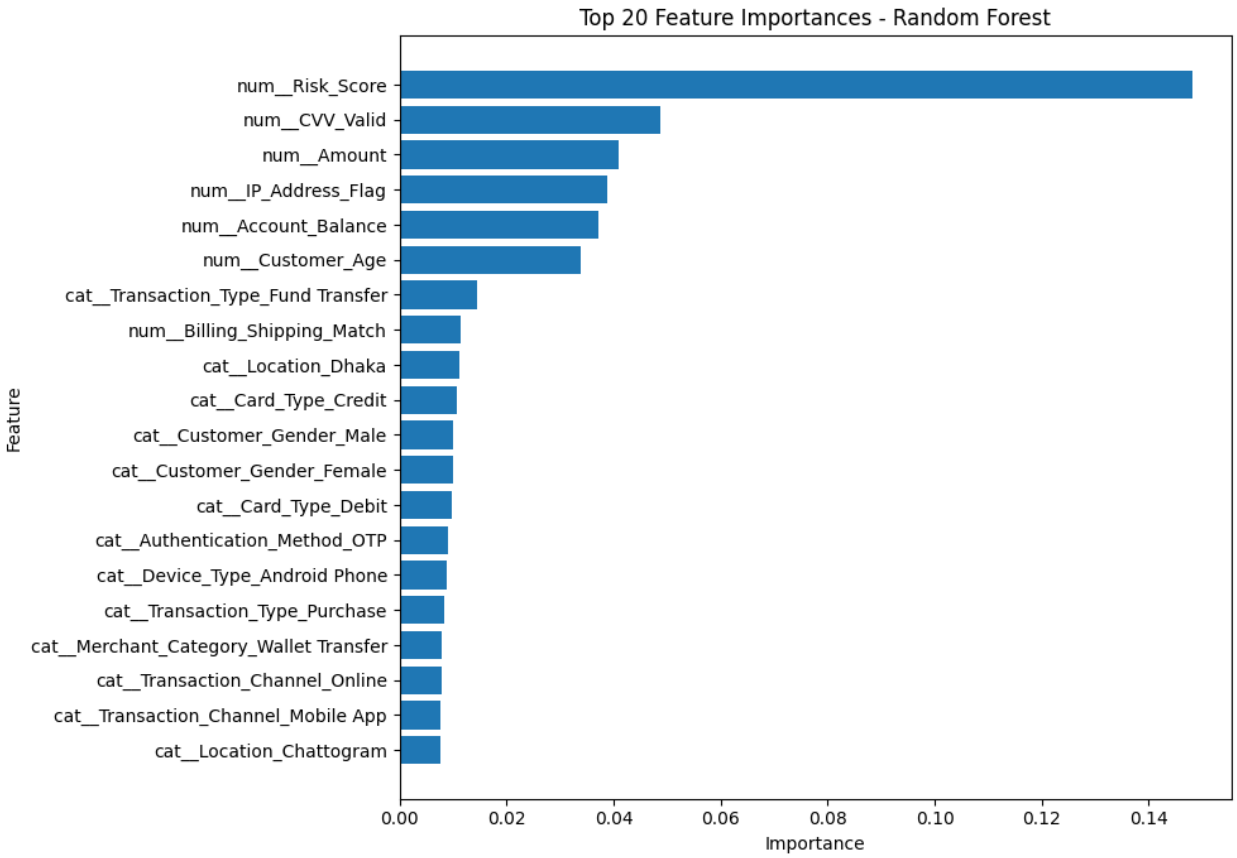

Figure 5: Top 20 Feature Importances of Random Forest Model

As shown in Figure 5, the most significant feature influencing fraud detection is the risk score, followed by CVV validation, transaction amount, IP address flag, and account balance. These features are directly related to transaction security and user behavior, underscoring their strong relevance for identifying fraudulent activity. In addition, demographic and categorical features such as transaction type, location, card type, and authentication method also contribute to the model's decision-making process, although with comparatively lower importance. This suggests that combining numerical risk indicators with contextual transaction information improves the model's predictive capability. The findings of this study demonstrate that machine learning techniques can provide practical support for detecting and preventing fraudulent activities in banking systems. By analyzing transaction patterns, user behavior, and security-related attributes, the proposed approach can help financial institutions identify suspicious transactions more effectively and make faster, more accurate real-time fraud detection decisions. In real-world banking environments, such systems may reduce financial losses, improve transaction security, and enhance customer trust. Therefore, integrating machine learning-based fraud detection systems into banking platforms can significantly strengthen cybersecurity frameworks and support more secure and efficient financial operations.

4.6. Cost Analysis of Classification Errors

Although the evaluated models achieved high overall accuracy (ranging from 97.79% to 98.96%), relying solely on accuracy as a performance metric can be highly misleading in the context of banking fraud detection. In fraud detection tasks, the dataset is severely imbalanced, with fraudulent transactions accounting for less than 1% of total cases. In such scenarios, a model can achieve very high accuracy by predicting almost all transactions as "normal" (the majority class), while completely failing to detect actual fraud cases.

In real-world banking operations, the cost of different types of errors varies significantly:

- **False Negative (FN)**: A fraudulent transaction is incorrectly classified as normal. This results in direct financial losses for the bank and the customer, potential regulatory penalties, reputational damage, and loss of customer trust. The financial impact of a single large fraud case can be substantial.
- **False Positive (FP)**: A legitimate transaction is incorrectly flagged as fraud. This leads to customer inconvenience, declined transactions, increased manual investigation costs, and possible loss of legitimate business. However, the cost is significantly lower than that of False Negatives.

To better reflect the operational reality, future fraud detection systems should incorporate cost-sensitive evaluation metrics. For example, a cost matrix can be defined in which the cost of a False Negative is set 50 to 100 times higher than the cost of a False Positive. This approach prioritizes models that minimize expensive misses (low recall for fraud class) rather than maximizing overall accuracy. The current study acknowledges that ensemble models like Random Forest and XGBoost, despite high accuracy, showed zero recall for the fraud class in the test set. This highlights the urgent need to move beyond traditional accuracy-based evaluation toward business-oriented and cost-aware performance assessment when integrating machine learning into cybersecurity frameworks for banking fraud prevention.

5. Discussion

The findings of this study suggest that machine learning can strengthen cybersecurity frameworks for banking fraud prevention, particularly by improving transaction monitoring and enabling faster decision-making. The strong overall performance of Random Forest, KNN, and SVM is broadly consistent with prior research showing that advanced AI and deep learning models improve fraud detection in banking, especially in real-time and high-volume transaction environments (Khaled Alarfaj & Shahzadi, 2025). However, the present study also shows that high overall accuracy does not necessarily mean effective fraud detection, since the weak identification of minority fraud cases reflects an important practical limitation also emphasized in wider AI-based financial security research, where adaptability, governance, and operational reliability remain essential (Oladipupo Dopamu et al., 2024). In this sense, the results support the view that fraud detection should be integrated with secure enterprise controls, compliance mechanisms, and real-time analytics rather than treated as a standalone prediction task (Anbazhagan, 2025). They also align with broader evidence that effective fraud prevention depends not only on powerful models but also on strong feature engineering, explainability, and the ability to respond to evolving fraud patterns in dynamic systems (Temitope Oluwatosin Fatunmbi, 2024). Finally, the need to evaluate effectiveness beyond simple accuracy is consistent with conceptual work stressing that system quality in financial environments must also consider trust, oversight, and practical reliability under complex operating conditions (Babalola et al., 2022)(Babalola et al., 2022).

Furthermore, the high overall accuracy observed in this study must be interpreted with caution. In highly imbalanced fraud-detection problems, accuracy alone does not adequately reflect a model's practical usefulness or operational value. As demonstrated in the results, even the best-performing model (Random Forest) achieved 98.96% accuracy but failed to detect any fraudulent transactions (recall = 0.000 and F1-score = 0.000 for the fraud class). This highlights a critical limitation: models can appear highly effective by simply classifying the vast majority of transactions as normal, while completely missing the rare but high-impact fraud cases.

In real-world banking environments, the cost of misclassifications is asymmetric. A False Negative (FN) — failing to detect a fraudulent transaction — can lead to substantial direct financial losses, regulatory penalties, reputational

damage, and erosion of customer trust. In contrast, a False Positive (FP) mainly causes customer inconvenience and additional manual review costs, which are significantly lower than the consequences of missed fraud. Therefore, banking institutions should move beyond traditional accuracy metrics and adopt cost-sensitive learning approaches. These methods assign higher penalties to False Negatives during model training and evaluation, thereby prioritizing recall and F1-score for the minority (fraud) class. Such cost-aware evaluation ensures more meaningful and practical outcomes when integrating machine learning models into cybersecurity frameworks for banking fraud prevention.

In conclusion, this study demonstrates that while ensemble machine learning models such as Random Forest and XGBoost can achieve high overall accuracy in detecting banking fraud, relying solely on accuracy metrics is misleading in highly imbalanced datasets. The persistent failure to identify minority fraud cases, driven by severe class imbalance, underscores the critical need for cost-sensitive learning approaches that prioritize minimizing the high financial and reputational cost of False Negatives over False Positives. Furthermore, the explicit mapping of security-related features to NIST CSF and ISO 27001 controls enhances the integration of technical models with established cybersecurity governance frameworks. However, the use of synthetic data limits generalizability, and important ethical concerns, including algorithmic bias and fairness, must be adequately addressed through explainable AI and fairness-aware techniques. Ultimately, enhancing the effectiveness of cyber security frameworks in preventing banking fraud requires a balanced combination of advanced predictive modeling, appropriate data balancing strategies, robust feature engineering, and strong ethical safeguards to ensure reliable, fair, and operationally valuable outcomes in real-world banking environments.

5.1. Ethical Considerations and Algorithmic Bias

The application of machine learning models in banking fraud detection raises important ethical concerns, particularly regarding algorithmic bias and fairness. Since the models rely on features such as location, device type, transaction patterns, and risk scores, there is a risk that certain demographic or geographic groups may be disproportionately flagged as fraudulent. This could lead to unfair treatment of customers, reduced access to financial services, and erosion of trust in banking systems.

Algorithmic bias may arise from imbalanced training data or historical patterns embedded in the features, potentially discriminating against minority groups or customers from specific regions. In addition, the black-box nature of some ensemble models (e.g., Random Forest and XGBoost) reduces transparency, making it difficult for stakeholders to understand and challenge automated decisions.

To mitigate these risks, future implementations should incorporate:

- Fairness-aware machine learning techniques to detect and reduce bias.
- Explainable AI (XAI) methods, such as SHAP or LIME, can improve model transparency.
- Regular bias audits and fairness evaluations before deploying models in live banking environments.
- Compliance with ethical guidelines and data protection regulations (e.g., GDPR principles or relevant local privacy laws in Bangladesh and India).

Addressing these ethical implications is essential to ensure that machine learning-based fraud detection systems not only improve security but also promote fairness, accountability, and public trust in digital banking.

6. Findings

1. Random Forest achieved the highest overall accuracy (0.9896), indicating the strongest general classification performance among the tested models.
2. KNN and SVM also achieved competitive results, while Logistic Regression provided stable, interpretable performance.
3. Despite high overall accuracy, the Random Forest model failed to detect fraud-class transactions, showing zero precision, recall, and F1-score for the minority fraud class.
4. The most influential features in fraud detection were risk score, CVV validation, transaction amount, IP address flag, and account balance.
5. The findings confirm that machine learning can strengthen fraud detection in banking, but class imbalance remains a major challenge in real-world cybersecurity applications.

7. Recommendations

1. Financial institutions should integrate machine learning-based fraud detection systems into digital banking platforms to improve real-time monitoring and transaction security.
2. Cybersecurity frameworks in banking should include transaction-level risk indicators, such as authentication methods, device types, and behavioral anomalies.
3. Data balancing techniques, resampling methods, or cost-sensitive learning should be applied to improve the detection of minority fraud cases.
4. Ensemble-based models may be prioritized in fraud analytics, but they should be combined with additional strategies to reduce bias toward majority-class transactions.
5. Future studies should test the proposed models on larger, real-world banking datasets collected from actual financial institutions. Such validation will enhance the generalizability and practical applicability of the findings in real cybersecurity and fraud-prevention scenarios.

8. Limitations

1. This study used a synthetic dataset of 12,000 transactions. Although designed to be realistic, synthetic data cannot fully capture the complexity, noise, missing values, concept drift, and adversarial behavior observed in real-world banking transactions. As a result, the generalizability of the findings to actual banking environments is limited.
2. The dataset was highly imbalanced, which significantly affected the models' ability to detect fraudulent transactions.
3. Only five machine learning models were examined, while other advanced or hybrid methods were not included in the analysis.

9. Conclusion

This study evaluated the effectiveness of cybersecurity frameworks in preventing banking fraud by applying machine learning models. The results show that Random Forest, KNN, and SVM achieved strong overall classification performance, with Random Forest producing the highest accuracy. The study also found that security-related and behavioral features, such as risk score, CVV validation, and transaction amount, contribute meaningfully to fraud detection in banking environments. These findings suggest that machine learning can provide valuable support in strengthening fraud prevention and improving cybersecurity practices in digital banking systems. However, the study also demonstrates that high overall model accuracy does not necessarily translate into effective fraud identification. The failure of the best-performing model to detect minority fraud cases highlights the critical impact of class imbalance in banking fraud analytics. Therefore, the study concludes that effective cybersecurity frameworks in banking must combine predictive modeling with appropriate data balancing, feature engineering, and adaptive security controls.

Overall, this research contributes to the growing understanding that fraud prevention in banking depends not only on strong algorithms but also on the development of more balanced, practical, and resilient cybersecurity systems.

10. Reference

[1] Agbeve, V., Brakye, K., Samlafo, E. K., Odigie, G. E., & Abbeyquaye, S. (2025). Evaluating the effectiveness of AI-driven fraud detection systems in US commercial banks. *International Journal of Asian Social Science*, *16*(1), 53–59. https://doi.org/10.55493/5007.v16i1.5778

[2] Asakpa, S. T. (2023). *From risk to resilience: Strengthening cyber security in financial institutions*. *International Journal of Advance Research, Ideas and Innovations in Technology, 9*(6), 137–145. https://www.ijariit.com/manuscript/from-risk-to-resilience-strengthening-cyber-security-in-financial-institutions/

[3] Azura, Y. T. Y., Azad, M. A., & Ahmed, Y. (2025). An integrated cyber security risk management framework for online banking systems. *Journal of Banking and Financial Technology*, *9*(1), 85–104. https://doi.org/10.1007/s42786-025-00056-3

[4] Chukwuemeka Iregbu, T. (2025). Examining Regulatory Perspectives on Cybersecurity Compliance and Its Implications for Financial Institutions' Risk Management and Consumer Trust. *International Journal of Science and Engineering Applications*. https://doi.org/10.7753/IJSEA1312.1011

[5] Gbadebo, M. O. (2025). Integrating Post-Quantum Cryptography and Advanced Encryption Standards to Safeguard Sensitive Financial Records from Emerging Cyber Threats. *Asian Journal of Research in Computer Science*, *18*(4), 1–23. https://doi.org/10.9734/ajrcos/2025/v18i4605

[6] Olutimehin, A. T. (2025). Assessing the Effectiveness of Cybersecurity Frameworks in Mitigating Cyberattacks in the Banking Sector and its Applicability to Decentralized Finance (DeFi). *Asian Journal of Research in Computer Science*, *18*(3), 130–151. https://doi.org/10.9734/ajrcos/2025/v18i3583

[7] Tamrakar, P., & Rajput, S. (2025). *Evaluating Regulatory and Compliance Frameworks for Safeguarding Financial Systems Against Cyber Threats*. *12*(8). https://www.jetir.org/papers/JETIRHA06019.pdf

[8] Tope Oladele Jooda, Chukwudi Tabitha Aghaunor, Joseph Darko Kassie, & Peter Oyirinnaya. (2023). Strengthening cyber resilience in financial institutions: A strategic approach to threat mitigation and risk management. *World Journal of Advanced Research and Reviews*, *20*(3), 2166–2177. https://doi.org/10.30574/wjarr.2023.20.3.2424

[9] Tran, T. N. (2025). *Systematic Review of Cybersecurity in Banking: Evolution from Pre-Industry 4.0 to Post-Industry 4.0 in Artificial Intelligence, Blockchain, Policies and Practice*. https://arxiv.org/abs/2503.00070

[10] Yasir Ali Solangi, A. M. (2025). *AN OPTIMIZED FRAMEWORK OF CYBERSECURITY TECHNIQUES FOR PROTECTING THE PERSONAL INFORMATION OF ACCOUNT HOLDERS IN INTERNET BANKING SYSTEM OF PAKISTAN*. https://doi.org/10.5281/ZENODO.16779280

[11] Ajayi, A. J., Joseph, S. A., Metibemu, O. C., Olutimehin, A. T., Balogun, A. Y., & Olaniyi, O. O. (2025). The Impact of Artificial Intelligence on Cyber Security in Digital Currency Transactions. *Archives of Current Research International*, *25*(2), 329–351. https://doi.org/10.9734/acri/2025/v25i21090

[12] Alhashmi, A. A., Alashjaee, A. M., Darem, A. A., Alanazi, A. F., & Effghi, R. (2023). An Ensemble-based Fraud Detection Model for Financial Transaction Cyber Threat Classification and Countermeasures. *Engineering, Technology & Applied Science Research*, *13*(6), 12433–12439. https://doi.org/10.48084/etasr.6401

[13] Karthik Meduri. (2024). Cybersecurity threats in banking: Unsupervised fraud detection analysis. *International Journal of Science and Research Archive*, *11*(2), 915–925. https://doi.org/10.30574/ijsra.2024.11.2.0505

[14] Marazqah Btoush, E. A. L., Zhou, X., Gururajan, R., Chan, K. C., Genrich, R., & Sankaran, P. (2023). A systematic review of literature on credit card cyber fraud detection using machine and deep learning. *PeerJ Computer Science*, *9*, e1278. https://doi.org/10.7717/peerj-cs.1278

[15] Soni, V. D. (2019). *International Engineering Journal For Research & Development*. (1). https://doi.org/10.17605/OSF.IO/JYPGX

[16] Umakor, M. F., Iheanyi, I., Ofurum, U. D., Ibecheozor, U. H. B., & Adeyefa, E. A. (2025). *Federated Learning For Privacy-Preserving Fraud Detection In Digital Banking: Balancing Algorithmic Performance, Privacy, And Regulatory Compliance*. *9*(1). https://www.irejournals.com/paper-details/1709491

[17] Natesan, Dr. G. (2024). PREVENTION OF CYBER FRAUDS IN THE BANKING SECTOR. *International Scientific Journal of Engineering and Management*, *03*(03), 1–22. https://doi.org/10.55041/ISJEM01341

[18] S. Madhumitha & Ms. N. Vaishnavi. (2025). Banking Security System Using Cyber Security. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *11*(2), 1184–1190. https://doi.org/10.32628/CSEIT25112451

[19] Prakash, S. (2018). *Effect of Outdated Technology in Banking Industry & Need of Advance Technology to Eliminate Cyber Security Threats , Track illegal transaction and fraud and To enhance revenue stream—The Clients Enterprise*. https://www.researchgate.net/publication/338342125_Effect_of_Outdated_Technology_in_Banking_Industry_Need_of_Advance_Technology_to_Eliminate_Cyber_Security_Threats_Track_illegal_transaction_and_fraud_and_To_enhance_revenue_stream_-The_Clients_Enterpri

[20] Doddipatla, L., & Ramadugu, R. (2025). Impact of AI Based Security systems on customer satisfaction and engagement of Fintech based companies. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.5104750

[21] Alkhafaji, S. M. S., Abbas, A. F., Banana, M. Z. H., Rammoo, H. M., Hadi, A. A., & Radif, M. (2025). Enhancing Online Banking Security Using CNN-Based Biometric Authentication Techniques for Verification. *2025 3rd International Conference on Cyber Resilience (ICCR)*, 1–6. https://doi.org/10.1109/ICCR67387.2025.11292361

[22] Dharmireddi, S., Hameed, A., Albdairi, M., Samudro, E. G., & Nandy, M. (2025). Cybersecurity in Digital Finance: Artificial Intelligence-Powered Fraud Detection and Risk Management. *2025 International Conference on Computational Innovations and Engineering Sustainability (ICCIES)*, 1–5. https://doi.org/10.1109/ICCIES63851.2025.11032566

[23] Kacheru, G. (2025). Governance of AI-Enabled Behavioral Biometrics in Mobile Banking: Ensuring Security and Trust. *2025 2nd International Conference on Recent Trends in Electrical, Electronics and Computing Technologies (ICRTEECT)*, 1–6. https://doi.org/10.1109/ICRTEECT67512.2025.11448951

[24] Muthukumarasamy, K., & Vanitha, M. (2025). Implement AI to Protect Banks from Cyberthreats: Identify Insider Threats, Phishing Attacks, and Strange Transactions in Banking Systems. *2025 10th International Conference on Smart Structures and Systems (ICSSS)*, 1–6. https://doi.org/10.1109/ICSSS66939.2025.11346282

[25] Yuvarani, R., & Mahaveerakannan, R. (2025a). Enhancing Data Secure Csp Framework Using Hybrid (Ecdh-Aes) Algorithm With Fhfboa Optimization Algorithm in Mobile Banking Transactions. *2025 6th International Conference on Data Intelligence and Cognitive Informatics (ICDICI)*, 422–429. https://doi.org/10.1109/ICDICI66477.2025.11135269

[26] Yuvarani, R., & Mahaveerakannan, R. (2025b). Secure IoT-Cloud Framework for Banking: Enhancing Data Storage and Transactions with Cryptographic Authentication. *2025 International Conference on Inventive Computation Technologies (ICICT)*, 1753–1758. https://doi.org/10.1109/ICICT64420.2025.11004853

[27] Chukwu, B. N. (2025). A Critical Intersection of cybersecurity, AI and fraud detection in the United States financial market. *International Journal of Science and Research Archive*, *17*(1), 289–297. https://doi.org/10.30574/ijsra.2025.17.1.2758

[28] Jahan Sarna, N., Ahmed Rithen, F., Salma Jui, U., Belal, S., Amin, A., Kabir Oishee, T., & Muzahidul Islam, A. K. M. (2025). AI Driven Fraud Detection Models in Financial Networks: A Comprehensive Systematic Review. *IEEE Access*, *13*, 141204–141233. https://doi.org/10.1109/ACCESS.2025.3596060

[29] Karn, A. L., Ghanimi, H. M. A., Iyengar, V., Siddiqui, M. S., Alharbi, M. G., Alroobaea, R., Yousef, A., & Sengan, S. (2025). Applying the defense model to strengthen information security with artificial intelligence in computer networks of the financial services sector. *Scientific Reports*, *15*(1), 30292. https://doi.org/10.1038/s41598-025-15034-4

[30] Salami, I. A., Adesokan-Imran, T. O., Tiwo, O. J., Metibemu, O. C., Olutimehin, A. T., & Olaniyi, O. O. (2025). Addressing Bias and Data Privacy Concerns in AI-Driven Credit Scoring Systems Through Cybersecurity Risk Assessment. *Asian Journal of Research in Computer Science*, *18*(4), 59–82. https://doi.org/10.9734/ajrcos/2025/v18i4608

[31] Tamanna, Kamboj, S., Singh, L., & Kaur, T. (2024). Automated Fraud Detection in Financial Transactions using Machine Learning: An Ensemble Perspective. *2024 2nd International Conference on Artificial Intelligence and Machine Learning Applications Theme: Healthcare and Internet of Things (AIMLA)*, 1–6. https://doi.org/10.1109/AIMLA59606.2024.10531422

[32] Babalola, F. I., Kokogho, E., Odio, P. E., Adeyanju, M. O., & Nwokediegwu, Z. S.-. (2022). Redefining Audit Quality: A Conceptual Framework for Assessing Audit Effectiveness in Modern Financial Markets. *International Journal of Multidisciplinary Research and Growth Evaluation*, *3*(1), 690–699. https://doi.org/10.54660/.IJMRGE.2022.3.1-690-699

[33] Anbazhagan, D. K. (2025). *Secure AI Enabled Enterprise Ecosystems for Fraud Prevention Compliance Automation and Real Time Analytics*. *1*(4). https://doi.org/10.15680/IJMRSETM.2025.0104002

[34] Khaled Alarfaj, F., & Shahzadi, S. (2025). Enhancing Fraud Detection in Banking With Deep Learning: Graph Neural Networks and Autoencoders for Real-Time Credit Card Fraud Prevention. *IEEE Access*, *13*, 20633–20646. https://doi.org/10.1109/ACCESS.2024.3466288

[35] Oladipupo Dopamu, Joseph Adesiyan, & Femi Oke. (2024). Artificial intelligence and US financial institutions: Review of AI-assisted regulatory compliance for cybersecurity. *World Journal of Advanced Research and Reviews*, *21*(3), 964–979. https://doi.org/10.30574/wjarr.2024.21.3.0791

[36] Temitope Oluwatosin Fatunmbi. (2024). Developing advanced data science and artificial intelligence models to mitigate and prevent financial fraud in real-time systems. *World Journal of Advanced Engineering Technology and Sciences*, *11*(1), 437–456. https://doi.org/10.30574/wjaets.2024.11.1.0024