Analysis of Factors Influencing Fraudulent Transactions in Digital Financial Systems Using Machine Learning Models

Jeffri Prayitno Bangkit Saputra[1,*], Muhammad Taufik Nur Hidayat[2]

[1]*Information Systems, Faculty of Computer Science, Amikom Purwokerto University, Indonesia*

[2]*Magister of Computer Science, Amikom Purwokerto University, Indonesia*

(Received: June 15, 2024; Revised: July 31, 2024; Accepted: August 12, 2024; Available online: September 1, 2024)

Abstract

This paper explores the use of machine learning, specifically the Random Forest algorithm, to detect fraudulent transactions in digital financial systems. As digital finance grows, the risk of fraud increases, making effective detection systems crucial for maintaining trust and security. The study focuses on identifying key factors influencing fraudulent transactions, such as transaction amount and type, and evaluates the model's performance using accuracy, precision, recall, F1-score, and AUC-ROC metrics. Results show that Random Forest outperforms traditional methods, achieving high accuracy of 95%, precision of 1.00 for fraudulent transactions, and an AUC of 0.98, indicating excellent discriminatory power. By analyzing transaction data, the model identifies important patterns, offering financial institutions practical insights for enhancing fraud detection systems. The findings suggest that focusing on critical features like transaction amount and transfer type can optimize detection systems. However, limitations include the need for further exploration of additional features, such as user behavior, and the integration of more advanced techniques to address emerging fraud tactics. The study's outcomes provide a robust framework for improving fraud detection in the evolving landscape of digital transactions.

Keywords: Fraud Detection, Machine Learning, Random Forest, Digital Financial Systems, Transaction Analysis

1. Introduction

The growing use of digital financial systems has significantly reshaped the global economy, driven primarily by advancements in information technology. Digital finance encompasses a variety of financial services conducted through digital platforms, such as online banking, mobile payments, and cryptocurrency trading. These innovations have greatly enhanced convenience, accessibility, and operational efficiency in financial transactions, making them more user-friendly and accessible than ever before [1]. Additionally, the rise of fintech solutions has played a key role in improving financial inclusion, particularly for previously underserved populations. By facilitating easier access to financial resources and lowering transaction costs, digital finance is contributing to a more inclusive and equitable financial landscape [2].

The COVID-19 pandemic further accelerated the adoption of digital financial solutions, highlighting their essential role in maintaining business continuity and reducing reliance on traditional financial services during times of disruption [3]. As the digital economy evolves, it is expected to foster continuous innovation in the financial sector, ultimately promoting systemic resilience and economic growth. However, this rapid digital transformation also introduces new challenges, particularly in terms of cybersecurity. With the increasing volume of digital transactions, the risk of cybercrime, including data breaches, phishing, and ransomware, has surged, posing a significant threat to the security of digital financial systems [4].

Governments and institutions have recognized that cyber threats can undermine not only individual organizations but also national security, as breaches in financial systems could disrupt entire economies [5]. Consequently, there is an urgent need for integrated security strategies that combine traditional security measures with advanced technologies

***Corresponding author: author (prayitno.jeffry.b@amikompurwokerto.ac.id)**
DOI: https://doi.org/10.47738/ijaim.v4i3.87

like artificial intelligence (AI) and blockchain. These technologies can safeguard digital transactions more effectively, counteracting evolving cyber threats and ensuring the safety of sensitive financial data [6]. As cybercriminals continually develop new tactics, security frameworks must adapt to address emerging threats and preserve the trust of users in digital financial services [7].

Fraud detection is particularly crucial in ensuring the integrity and trustworthiness of digital financial systems. As digital transactions proliferate, the complexity and frequency of fraudulent activities increase, posing risks not only to consumers but also to the entire financial ecosystem [8]. Effective fraud detection mechanisms are essential for protecting consumer assets and maintaining the reliability of financial service providers, which, in turn, fosters trust between users and digital platforms [9]. The integration of AI and machine learning technologies has significantly enhanced the capabilities of fraud detection systems. These technologies allow for real-time monitoring and analysis of transaction patterns, improving the accuracy of identifying anomalous behaviors that could indicate fraudulent activities [10].

AI-driven approaches have been shown to reduce false positives while maintaining high detection rates, enhancing user confidence in digital financial systems. The adoption of these advanced fraud detection systems is essential to counteract the growing sophistication of fraudsters and sustain the operational integrity of digital finance [11]. By reinforcing fraud detection frameworks, financial institutions can maintain systemic stability and consumer trust in the digital age [12]. However, to design effective fraud detection systems, it is crucial to understand the specific factors contributing to fraudulent transactions. Key factors include identity theft, unauthorized access to payment information, and inadequate security measures [13].

Machine learning techniques, such as CatBoost, leverage feature engineering to enhance fraud detection capabilities, ensuring that financial organizations can quickly respond to emerging threats [13]. The application of ensemble methods further aids financial institutions in assessing fraud risk in digital environments where fraudsters constantly adapt to countermeasures [14]. Big data analytics is also being incorporated into fraud detection systems to facilitate real-time monitoring and provide deeper insights into transaction behaviors, which is crucial for maintaining the integrity of digital financial systems [9]. These technologies underscore the importance of continuous improvement and adaptation in fraud detection techniques to combat the evolving nature of financial fraud.

Detecting fraudulent transactions remains a significant challenge, especially when relying on manual or traditional methods, which often lack the efficiency and adaptability needed to address evolving financial fraud patterns. Traditional rule-based detection systems depend on predefined rules, which may not account for new or sophisticated fraudulent schemes, leading to high rates of false negatives and false positives [15]. Furthermore, manual review processes are time-consuming and labor-intensive, leading to delayed detection and increased vulnerability to fraud [16]. The rise in digital transactions exacerbates these issues, as human analysts struggle to identify patterns indicative of fraud amidst vast amounts of legitimate transactions [17].

To address these challenges, there is a pressing need for advanced, automated systems that leverage machine learning and AI to enhance fraud detection. These technological solutions can analyze complex datasets in real time, adapt to changing fraud patterns, and significantly improve the accuracy of fraud detection [18]. The lack of understanding regarding the specific factors influencing fraud in digital financial systems further complicates detection and prevention efforts. Fraudsters employ increasingly sophisticated methods, making it difficult for traditional detection systems to keep pace with evolving threats [14]. Insufficient regulatory frameworks that fail to adequately capture or analyze user behavior also create opportunities for fraudulent activities [19]. Moreover, the rapid digitization of financial services creates vulnerabilities that can be easily exploited by fraudsters, particularly in environments where user identity information is inadequately verified [20].

In addition to regulatory shortcomings, financial literacy plays a critical role in empowering users to recognize potential fraud. Many individuals remain ill-equipped to navigate the increasingly sophisticated fraud landscape, highlighting the need for public education campaigns focused on safe digital practices [21]. Understanding these factors is essential for designing more effective fraud detection systems capable of adapting to emerging trends and mitigating risks in digital financial environments.

Machine learning techniques are key to addressing the complexities of fraudulent transactions. Research suggests that algorithms such as Decision Trees, Random Forests, and Logistic Regression can be effectively employed to identify fraud patterns [17]. These models can improve their accuracy through methods like oversampling to handle class imbalance, a common challenge when fraudulent transactions are far less frequent than legitimate ones [22]. Furthermore, incorporating advanced deep learning methods, such as Stacked Autoencoders, can improve prediction capabilities, achieving high accuracy and low false positive rates [23]. The continuous adaptation of these models to new fraud patterns is essential for maintaining an effective fraud detection system [24].

Ultimately, this research aims to improve fraud detection systems by identifying the key factors contributing to fraudulent transactions. By leveraging machine learning, financial institutions can enhance their ability to detect and prevent fraud, thereby safeguarding their operations and ensuring consumer trust in digital financial services. Through continuous innovation and the integration of AI-driven fraud detection mechanisms, the security of digital financial systems can be significantly strengthened, fostering a more resilient and reliable financial environment.

2. Literature Review

Financial fraud in digital payment systems has become a significant concern, driven by the rapid expansion of digital platforms that create vulnerabilities cybercriminals can exploit [25]. Traditional fraud detection methods, such as rule-based systems, are becoming increasingly ineffective as they struggle to adapt to the complexity and scale of modern digital transactions. This has prompted a shift towards more advanced techniques like machine learning (ML) and big data analytics, which offer improved fraud detection capabilities by analyzing large datasets, identifying patterns, and enhancing prediction accuracy [26]. Real-time monitoring and predictive analytics have also shown great promise in identifying fraud and mitigating risks [27]. The COVID-19 pandemic has further complicated fraud detection efforts, creating new challenges as organizations must adapt to the rapidly changing cyber threat landscape while ensuring compliance with evolving regulations [19]. As digital financial services continue to evolve, the development of robust fraud detection frameworks remains essential for maintaining the security of financial transactions [28].

Machine learning techniques, including supervised, unsupervised, and reinforcement learning, have significantly enhanced fraud detection capabilities by processing vast amounts of transactional data. Supervised learning methods such as decision trees, random forests, and support vector machines are commonly used due to their high accuracy in predicting fraud [29]. Among these techniques, Random Forest has proven particularly effective in handling classification problems, such as credit card fraud detection, by achieving high accuracy rates and efficiently managing imbalanced datasets, which are a common challenge in fraud detection[30]. Random Forest, an ensemble learning method, combines multiple decision trees to increase the robustness and precision of fraud detection systems, making it a versatile tool in financial applications [31]. The integration of feature engineering and ensemble methods, which combine various models, has further improved fraud detection accuracy by refining input variables and reducing false positives [32]. Recent advancements in deep learning techniques have also played a crucial role by enabling the recognition of more complex patterns in financial data, further enhancing fraud detection in increasingly intricate digital financial environments [33]. As fraud tactics continue to evolve, machine learning algorithms like Random Forest adapt to these emerging risks, ensuring financial institutions can quickly identify and respond to new fraud strategies while maintaining customer satisfaction [34], [35].

The effectiveness of these technological advancements is further supported by regulatory frameworks, which ensure that fraud detection systems comply with legal requirements and industry standards. Legislation such as the Sarbanes-Oxley Act, along with the establishment of the Public Company Accounting Oversight Board (PCAOB), has been crucial in mitigating financial fraud [36]. These regulations not only guide the development of detection technologies but also ensure that they are applied effectively within established legal frameworks [37]. Furthermore, integrating psychological and social factors, such as those outlined in the fraud triangle and fraud diamond frameworks, provides deeper insights into the motivations behind fraudulent behavior, helping to refine detection strategies and make them more adaptive [38]. As financial fraud continues to undermine the stability of financial systems, it is imperative that detection systems not only focus on minimizing losses but also work to restore trust and integrity in financial institutions [39]. The digitization of financial services has introduced new fraud risks, requiring innovative, adaptive fraud detection frameworks to keep pace with these changes.

 ISSN 2776-8007

The risk of fraud in digital transactions is further influenced by several key factors, including transaction amount, type, timing, and user behavior. Larger transaction amounts are often associated with higher fraud risks, as they present more significant targets for cybercriminals [13]. Irregularities in transaction amounts, such as deviations from a user's typical spending patterns, often serve as red flags in fraud detection models [40]. The type of transaction, whether credit card, e-wallet, or bank transfer, also affects fraud risk, with e-commerce transactions being particularly vulnerable due to their complexity and the multiple parties involved [41]. Temporal factors, such as transactions occurring during holidays or late-night hours, further contribute to the likelihood of fraud, as these periods may coincide with lower user vigilance.

User behavior is another crucial determinant of fraud risk. Deviations from normal, established user behavior can be indicative of fraudulent activity. Techniques like sequential pattern mining are essential for identifying anomalies and distinguishing between legitimate and fraudulent transactions [42]. Additionally, user trust in digital payment systems plays a significant role in their engagement with e-commerce platforms, influencing how they interact with these services [43]. By leveraging behavioral analytics and machine learning, more proactive fraud detection systems can be developed that anticipate and identify fraudulent actions more effectively [44]. To address the complexity of fraud in digital transactions, detection frameworks must consider factors such as transaction amount, type, timing, and user behavior, continuously adapting to new challenges in the digital financial landscape.

3. Methodology

This study adopts a quantitative approach to explore and analyze transaction data in the context of detecting fraudulent activities in digital financial systems. The primary objective is to apply machine learning techniques to uncover patterns and anomalies indicative of fraud, improving the accuracy and efficiency of fraud detection in financial transactions. Machine learning is chosen for its ability to identify complex, non-linear relationships within large datasets, making it ideal for detecting fraud, where patterns can be intricate and evolve rapidly. By analyzing historical transaction data, machine learning models can recognize patterns associated with legitimate and fraudulent transactions, enabling the development of automated fraud detection systems. Figure 1 illustrates the research design, outlining the steps involved in data collection, processing, model training and testing, and evaluation for detecting fraudulent activities in digital financial transactions.

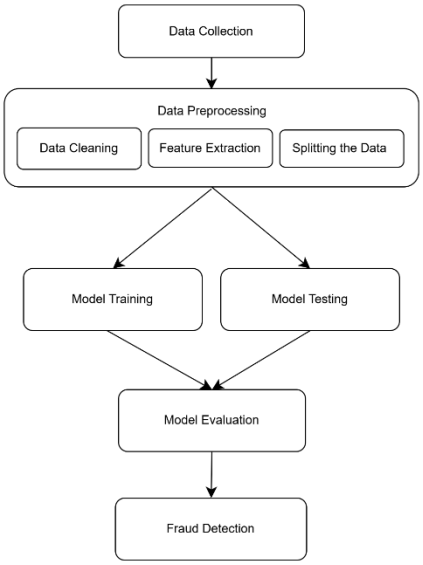

Figure 1. Research Methodology

3.1. Data Collection

The dataset used in this study consists of transaction records from a digital financial system, which captures essential features for each transaction. These include the transaction amount, representing the monetary value of each transaction; the transaction type, which indicates the nature of the transaction, such as purchase, transfer, or withdrawal; the customer ID, a unique identifier assigned to the customer initiating the transaction; the transaction time, which

provides a timestamp for when the transaction occurred; and the fraud flag, a binary variable indicating whether the transaction was fraudulent (1) or not (0). To ensure the data is suitable for analysis, various preprocessing steps are performed. This includes encoding categorical variables, such as the transaction type, to a numerical format, handling any missing values that may be present, and scaling numerical features, like the transaction amount, if necessary, to maintain consistency across the dataset. These preprocessing steps are crucial to preparing the data for effective analysis using machine learning techniques.

3.2. Data Preprocessing

Before training the Random Forest model, several important preprocessing steps will be performed to ensure that the dataset is properly prepared for analysis and model training. First, data cleaning will address any missing or corrupt values in the dataset. Since Random Forest can handle some missing data, imputation techniques, such as filling missing values with the mean or median for numerical features, will be applied, or records with excessive missing data will be removed, depending on their impact on the overall dataset. Next, feature extraction will be employed to create new features that may improve the model's performance. For example, time-based features, like time of day or day of the week, will be extracted from the transaction timestamp to capture potential patterns related to fraudulent behavior. Aggregating customer-level data, such as total spending over a set period, will also help capture behavioral trends that might indicate fraud.

Since Random Forest requires categorical variables like transaction type to be in numerical format, encoding will be performed using techniques like one-hot encoding, where each category is transformed into a binary column, or label encoding, which assigns a unique integer to each category. Finally, while Random Forest is less sensitive to the scale of features compared to other algorithms, data scaling will be applied to numerical features like transaction amounts to ensure that all features are on a comparable scale. This step is particularly important if the model is later combined with other algorithms or used in hybrid models, as it helps prevent outliers from unduly influencing the results. These preprocessing steps will ensure that the dataset is clean, well-structured, and optimized for Random Forest training, allowing the model to effectively identify fraudulent transactions.

3.3. Machine Learning Model

In this study, we focus exclusively on using the Random Forest algorithm to detect fraudulent transactions. Random Forest is an ensemble learning method that builds multiple decision trees and outputs the most frequent class (fraudulent or non-fraudulent) from these trees. This approach is particularly effective for complex datasets with many features, as it captures non-linear relationships and interactions between variables. Recognized for its high accuracy, Random Forest has been shown to achieve an accuracy rate of 98% in mobile money transaction fraud detection, outperforming traditional methods [45]. Additionally, research on a Bayesian-optimized Random Forest classifier demonstrates its ability to efficiently analyze large transaction datasets and identify subtle fraudulent patterns [46].

Random Forest is well-suited for transaction data, as it can handle both numerical and categorical features, such as transaction amounts, types, and customer behavior indicators. One of the key strengths of this model is its ability to reduce overfitting compared to individual decision trees by averaging predictions from multiple trees. This leads to a more stable and reliable classification model, which is crucial for detecting fraud, where patterns can be subtle or variable. To optimize the Random Forest model for fraud detection, several key parameters can be adjusted to control the model’s complexity and performance. Table 1 presents an overview of these essential parameters, along with their descriptions and typical values.

Table 1. Random Forest Parameter

Parameter	Description	Typical Values
n_estimators	The number of decision trees to build in the forest. A higher number improves performance but increases computation time.	100, 200, 500, 1000
max_depth	The maximum depth of each decision tree. Limits how deep the tree can grow. A higher depth can lead to overfitting.	None (no limit), 10, 20, 30
min_samples_split	The minimum number of samples required to split an internal node. Higher values prevent overfitting.	2, 5, 10

min_samples_leaf	The minimum number of samples required at a leaf node. Higher values lead to simpler trees and prevent overfitting.	1, 2, 5
max_features	The number of features to consider when looking for the best split. Fewer features can reduce overfitting.	"auto", "sqrt", "log2"
random_state	Controls the randomness of the model's initialization to ensure reproducibility of results.	Any integer (e.g., 42)

3.4.Model Training and Evaluation

The performance of the Random Forest model will be evaluated using several key metrics, including accuracy, precision, recall, F1-score, and AUC-ROC. Accuracy represents the proportion of correctly classified transactions (both fraudulent and non-fraudulent) out of all transactions, calculated as the sum of true positives (fraudulent transactions correctly identified) and true negatives (non-fraudulent transactions correctly identified) divided by the total number of transactions. It is calculated as:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

Precision measures the proportion of true positives among all transactions predicted as fraudulent by the model, which is particularly important when the cost of false positives is high. Precision is calculated as:

$$Precision = \frac{TP}{TP+FP} \quad (2)$$

Recall, or sensitivity, calculates the proportion of true positives among all actual fraudulent transactions, emphasizing the identification of as many fraudulent transactions as possible. It is given by:

$$Recall = \frac{TP}{TP+FN} \quad (3)$$

The F1-score is the harmonic mean of precision and recall, providing a balanced measure of the model's performance, especially when dealing with imbalanced datasets. The F1-score is calculated as:

$$F1 - Score = 2 \times \frac{Precision \times Recall}{Precision+Recall} \quad (4)$$

Finally, the AUC-ROC curve assesses the model's ability to distinguish between fraudulent and non-fraudulent transactions by plotting the true positive rate (recall) against the false positive rate. A higher AUC value indicates better performance, with a value closer to 1 signifying a highly effective model. The ROC curve is generated by plotting:

$$True\ Positive\ Raate = \frac{TP}{TP+FN} \quad \text{VS} \quad False\ Positive\ Rate = \frac{FP}{FP+TN} \quad (5)$$

To evaluate the model's performance further, a confusion matrix will be generated to visualize the key components: true positives, false positives, true negatives, and false negatives. This matrix provides a clear picture of how well the model distinguishes between fraudulent and non-fraudulent transactions. Additionally, the ROC curve will be plotted to analyze the trade-off between sensitivity (true positive rate) and specificity (1 - false positive rate) at different decision thresholds. The AUC value, derived from the ROC curve, offers an aggregate measure of the model's discriminatory power. Along with evaluating overall performance, we will assess the feature importance in the Random Forest model, which helps identify the key factors influencing fraud detection, such as transaction amount, transaction type, and customer behavior. This analysis will improve model interpretation and highlight the most critical variables for detecting fraudulent activities. Understanding these features can guide future model improvements and assist financial institutions in focusing their efforts on the most significant factors to prevent fraud.

4. Results and Discussion

4.1. Result

Figure 2 highlights the key factors contributing to fraudulent transactions in the machine learning model. The transaction amount emerges as the most significant feature, with a feature importance score close to 0.8. This indicates

that the model heavily relies on the transaction amount to identify fraudulent transactions, as large or unusual transaction amounts are often indicative of fraud. Transaction type (Transfer) also plays an important role in fraud detection, with a feature importance score of around 0.2, suggesting that transfers are more likely to be flagged as fraudulent compared to other types of transactions. In contrast, transaction type (Withdrawal) has the lowest feature importance, indicating that it contributes less to the model's decision-making process. Overall, the analysis highlights that the most critical factors in detecting fraud are the transaction amount and transaction type (Transfer), while Withdrawals have less impact on fraud detection. This insight can help refine fraud detection systems by prioritizing these key features.

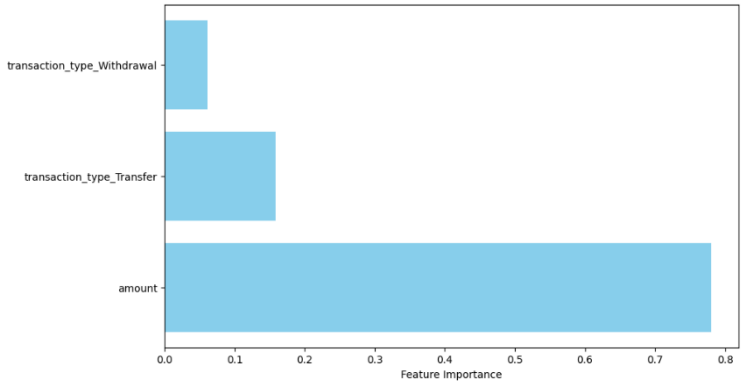

Figure 2. Feature Importance for Fraud Detection

Figure 3 presents the distribution of transaction amounts for both Fraud and Non-Fraud transactions. The chart reveals that fraudulent transactions (red bars) show a distinct peak around the 2.000 transaction amount, suggesting that most fraudulent activities occur in this range. The density plot for fraudulent transactions (red curve) indicates a higher concentration of transactions in the lower to mid-range amounts, with a sharp decline as the transaction amount increases beyond 5,000. In contrast, non-fraudulent transactions (blue bars) exhibit a more evenly distributed pattern across various transaction amounts, with notable concentrations in the 1,000 to 2,000 range, similar to fraudulent transactions. The density plot for non-fraudulent transactions (blue curve) is more spread out, signifying that non-fraudulent transactions occur across a wider range of amounts. This analysis highlights how fraud tends to cluster around specific amounts while non-fraudulent transactions are more diverse, offering insights into patterns that can help detect fraudulent activities in financial systems.

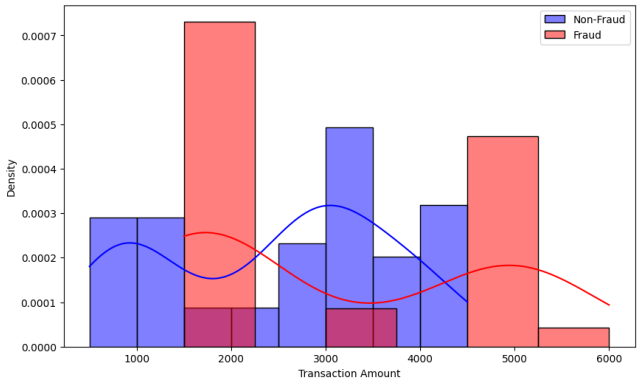

Figure 3. Transaction Amount Distribution for Fraud vs Non-fraud

Table 2 provides several important metrics for evaluating its performance. Precision measures the accuracy of positive predictions. For fraudulent (0) transactions, the model achieves perfect precision (1.00), meaning all predicted fraudulent transactions were correct. For non-fraudulent (1) transactions, the precision is 0.88, indicating that 88% of the transactions predicted as non-fraudulent were indeed non-fraudulent. Recall, which evaluates the model's ability to correctly identify all actual positive instances, is 0.92 for fraudulent (0) transactions, meaning 92% of actual fraudulent

 ISSN 2776-8007

transactions were identified correctly. For non-fraudulent (1) transactions, recall is 1.00, showing that all actual non-fraudulent transactions were correctly identified.

The F1-Score, which balances precision and recall, gives a comprehensive view of the model's performance. The fraudulent (0) class has an F1-score of 0.96, while the non-fraudulent (1) class has an F1-score of 0.93, indicating strong performance in both classes. Accuracy, representing the overall proportion of correct predictions, is 0.95, meaning 95% of all transactions were classified correctly. The Macro Average and Weighted Average provide further insights into the model's performance across all classes. The Macro Average treats each class equally, yielding an average F1-score of 0.95, while the Weighted Average takes into account the distribution of classes, resulting in a slightly adjusted F1-score of 0.95, reflecting a balanced performance across both classes.

Table 2. Classification Report for Fraud Detection Model

Class	Precision	Recall	F1-Score
Fraudulent (0)	1.00	0.92	0.96
Non-Fraudulent (1)	0.88	1.00	0.93
Accuracy			0.95
Macro Avg	0.94	0.96	0.95
Weighted Avg	0.96	0.95	0.95

Figure 4 displays the confusion matrix for the fraud detection model, providing a clear picture of its performance. The matrix shows that the model correctly identified 7 fraudulent transactions as fraud (True Positives, TP) and 12 non-fraudulent transactions as non-fraud (True Negatives, TN). The model also misclassified 1 non-fraudulent transaction as fraudulent (False Positive, FP), but it did not miss any fraudulent transactions, as indicated by the 0 false negatives (FN). This suggests that the model performs effectively, accurately identifying fraudulent transactions without overlooking any and only making a minimal error by incorrectly labeling a legitimate transaction as fraud. The overall performance of the model appears strong, with a low rate of misclassification, which is critical for ensuring the accuracy and reliability of fraud detection in financial systems.

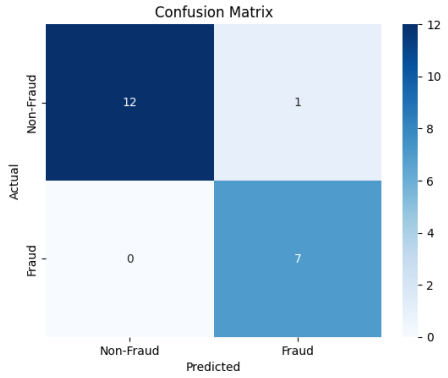

Figure 4. Confusion Matrix for Fraud Detection Model

Figure 5 displays the Receiver Operating Characteristic (ROC) Curve for the fraud detection model, illustrating the trade-off between the True Positive Rate (TPR) and False Positive Rate (FPR). The AUC (Area Under the Curve) score is 0.98, which indicates that the model has excellent performance in distinguishing between fraudulent and non-fraudulent transactions. A value close to 1 for AUC suggests that the model is highly effective, with a very low likelihood of misclassifying fraud as non-fraud and vice versa. The sharp rise in the curve to a high true positive rate without significant increases in the false positive rate shows that the model can effectively detect fraud with minimal errors. The dashed line represents the baseline model, where the AUC is 0.5, indicating random guessing. Since the ROC curve significantly outperforms this baseline, the model demonstrates strong discriminatory power. This suggests that the fraud detection model is well-calibrated and able to provide reliable predictions.

 ISSN 2776-8007

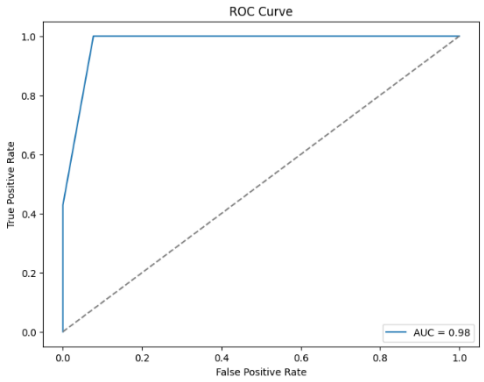

Figure 5. ROC Curve for Fraud Detection Model

4.2. Discussion

The findings from the fraud detection model, as illustrated in Figure 2 and Figure 3, align with the growing body of research on identifying key factors in fraudulent transactions. Transaction amount was found to be the most important feature, with a high feature importance score of 0.8, which emphasizes the significant role transaction value plays in fraud detection. Larger or unusual transaction amounts are often indicative of fraudulent activities, which corroborates findings from previous studies, such as Shi [13], who noted that high-value transactions are attractive targets for fraud. The transaction type (Transfer) also proved to be important, with a score of 0.2, suggesting that transfers are more likely to be fraudulent compared to other types of transactions, such as Withdrawals. This aligns with findings by Alharbi et al. [41], who highlighted the vulnerability of transfer transactions in e-commerce systems.

The distribution of transaction amounts, shown in Figure 3, further supports these insights. Fraudulent transactions were found to concentrate around 2,000, while non-fraudulent transactions displayed a broader distribution across various amounts. This reinforces the conclusion that fraudulent transactions tend to cluster around specific values, while legitimate transactions are more diverse, as noted by [40]. The findings emphasize that understanding these patterns can help improve fraud detection systems by focusing on transaction amount and type, two of the most critical features identified by the model.

The classification report in Table 2 shows strong model performance with an accuracy of 95%, precision of 1.00 for fraudulent transactions, and recall of 1.00 for non-fraudulent transactions. These results suggest that the model is effective at both identifying fraudulent transactions and avoiding misclassifications of legitimate ones. The high F1-score for both classes (0.96 for fraudulent and 0.93 for non-fraudulent) indicates a well-balanced model that minimizes both false positives and false negatives, as also discussed by previous research on machine learning's potential in fraud detection [26].

The confusion matrix in Figure 4 confirms the model's effectiveness, with only one false positive and no false negatives. This low error rate is crucial for ensuring the reliability and trustworthiness of the system, especially in real-world applications where misclassifying fraudulent transactions as non-fraudulent can lead to significant financial losses. The ROC curve in Figure 5, with an AUC of 0.98, further solidifies the model’s strong discriminatory power, demonstrating its ability to distinguish between fraudulent and non-fraudulent transactions with high accuracy. This result is consistent with findings from Kumar & Singh [34] and Mqadi et al. [35]S, who highlighted the effectiveness of machine learning models like Random Forest in fraud detection.

This study suggests that machine learning models, particularly Random Forest, are highly effective in detecting fraudulent transactions within digital payment systems. The model’s reliance on features like transaction amount and transaction type provides important insights for financial institutions. By focusing on these key features, fraud detection systems can be further optimized to minimize false positives and improve the identification of fraudulent activities. These results also highlight the importance of integrating real-time data analysis to maintain high performance in dynamic and complex financial environments.

The research contributes to the body of knowledge on fraud detection by demonstrating the power of Random Forest for financial fraud detection, particularly in digital payment systems. It highlights the importance of specific features such as transaction amount and type in identifying fraud and provides practical insights for improving fraud detection models in real-world applications. The model's strong performance, backed by metrics such as precision, recall, and AUC, reinforces the potential of machine learning for enhancing financial security.

Despite its promising results, this study has several limitations. First, the dataset used may not fully represent the diversity of transactions in all digital financial systems, potentially limiting the model's generalizability to different types of fraud. Additionally, while the model demonstrates strong performance, the accuracy and reliability of fraud detection could be further enhanced by incorporating more features, such as user behavior and historical transaction patterns, which were not explored in this study. Future research could also look into integrating deep learning techniques or hybrid models to improve the identification of complex fraud patterns and adapt to evolving fraudulent tactics. Furthermore, the model's performance might vary with different datasets, and its applicability in larger, real-time environments needs further evaluation.

In conclusion, this study provides valuable insights into the factors influencing fraud detection and demonstrates the efficacy of machine learning models like Random Forest. By considering the transaction amount and transaction type, financial institutions can enhance their fraud detection frameworks, though continuous improvement and adaptation are necessary to keep pace with emerging threats in digital transactions.

5. Conclusion

This study provides valuable insights into the factors influencing fraud detection in digital financial systems and demonstrates the effectiveness of machine learning models like Random Forest. The model's reliance on critical features, such as transaction amount and transaction type (Transfer), underscores the importance of focusing on these variables for more accurate fraud detection. The strong model performance, backed by high accuracy of 95%, precision of 1.00 for fraudulent transactions, and recall of 1.00 for non-fraudulent transactions, highlights the potential of Random Forest to distinguish between fraudulent and non-fraudulent transactions. The model achieved an impressive AUC score of 0.98, indicating excellent discrimination between fraud and non-fraud cases, which suggests that the model performs with high reliability. This signifies that the model is highly effective in real-world applications, providing a promising tool for fraud detection in digital financial systems. However, continuous refinement and adaptation of fraud detection systems are necessary to stay ahead of evolving fraud tactics. This research contributes to the growing field of fraud detection by showing the power of machine learning in digital financial systems and suggesting that further improvements, such as incorporating more behavioral features and exploring hybrid models, could enhance performance even further. Although the model demonstrated robust results, future work should consider real-world challenges such as dataset variability and the need for real-time fraud detection in complex financial environments.

6. Declarations

6.1. Author Contributions

Conceptualization: J.P.B.S., M.T.N.H.; Methodology: J.P.B.S., M.T.N.H.; Software: J.P.B.S.; Validation: M.T.N.H.; Formal Analysis: J.P.B.S.; Investigation: J.P.B.S.; Resources: M.T.N.H.; Data Curation: J.P.B.S.; Writing – Original Draft Preparation: J.P.B.S.; Writing – Review and Editing: M.T.N.H.; Visualization: J.P.B.S.; All authors have read and agreed to the published version of the manuscript.

6.2. Data Availability Statement

The data presented in this study are available on request from the corresponding author.

6.3. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

6.4. Institutional Review Board Statement

Not applicable.

6.5. Informed Consent Statement

Not applicable.

6.6. Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] X. Wu, "The Rise of Digital Finance and Systemic Risk: Implications, Challenges, and Coping Strategies," *Adv. Econ. Manag. Polit. Sci.*, vol. 45, no. 1, pp. 327–333, 2023, doi: 10.54254/2754-1169/45/20230306.

[2] L. Yang and Y. Zhang, "Digital Financial Inclusion and Sustainable Growth of Small and Micro Enterprises—Evidence Based on China's New Third Board Market Listed Companies," *Sustainability*, vol. 12, no. 9, pp. 3733, 2020, doi: 10.3390/su12093733.

[3] A. Sinha, "Digital Technology Improving Financial Inclusion in India: Post Covid Evidence," *Asian J. Econ. Bus. Account.*, vol. 24, no. 2, pp. 107–122, 2024, doi: 10.9734/ajeba/2024/v24i21225.

[4] M. Waliullah, M. J. George, M. T. Hasan, M. K. Alam, M. S. k. Munira, and N. A. Siddiqui, "Assessing the Influence of Cybersecurity Threats and Risks on the Adoption and Growth of Digital Banking: A Systematic Literature Review," *Ajates*, vol. 1, no. 01, pp. 226–257, 2025, doi: 10.63125/fh49gz18.

[5] A. Krysovatyy, O. Desyatnyuk, and O. Ptashchenko, "Digital Innovations and Their Ramifications for Financial and State Security," *African J. Appl. Res.*, vol. 10, no. 1, pp. 431–441, 2024, doi: 10.26437/ajar.v10i1.713.

[6] O. A. Farayola, "Revolutionizing Banking Security: Integrating Artificial Intelligence, Blockchain, and Business Intelligence for Enhanced Cybersecurity," *Financ. Account. Res. J.*, vol. 6, no. 4, pp. 501–514, 2024, doi: 10.51594/farj.v6i4.990.

[7] A. S. Edu, M. Agoyi, and D. Q. Agozie, "Digital Security Vulnerabilities and Threats Implications for Financial Institutions Deploying Digital Technology Platforms and Application: FMEA and FTOPSIS Analysis," *Peerj Comput. Sci.*, vol. 7, no. August, pp. 1–26, 2021, doi: 10.7717/peerj-cs.658.

[8] O. Odeyemi, N. Z. Mhlongo, E. E. Nwankwo, and O. T. Soyombo, "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, doi: 10.30574/ijsra.2024.11.1.0279.

[9] O. Angela, I. Atoyebi, A. Soyele, and E. Ogunwobi, "Enhancing Fraud Detection and Prevention in Fintech: Big Data and Machine Learning Approaches," *World J. Adv. Res. Rev.*, vol. 24, no. 2, pp. 2301–2319, 2024, doi: 10.30574/wjarr.2024.24.2.3617.

[10] B. O. Adelakun, E. R. Onwubuariri, G. A. Adeniran, and A. Ntiakoh, "Enhancing Fraud Detection in Accounting Through AI: Techniques and Case Studies," *Financ. Account. Res. J.*, vol. 6, no. 6, pp. 978–999, 2024, doi: 10.51594/farj.v6i6.1232.

[11] Z. Chen, "The Logic of Digital Finance in the Age of Digital Economy," *Proc. Bus. Econ. Stud.*, vol. 7, no. 2, pp. 53–59, 2024, doi: 10.26689/pbes.v7i2.6605.

[12] B. O. Antwi, B. O. Adelakun, D. T. Fatogun, and O. P. Olaiya, "Enhancing Audit Accuracy: The Role of AI in Detecting Financial Anomalies and Fraud," *Financ. Account. Res. J.*, vol. 6, no. 6, pp. 1049–1068, 2024, doi: 10.51594/farj.v6i6.1235.

[13] J. Shi, "Transaction Fraud Detection by CatBoost Model With Feature Engineering," *Appl. Comput. Eng.*, vol. 48, no. 1, pp. 192–199, 2024, doi: 10.54254/2755-2721/48/20241485.

[14] P. Xia, X. Zhu, V. Charles, X. Zhao, and M. Peng, "A Novel Heuristic-Based Selective Ensemble Prediction Method for Digital Financial Fraud Risk," *Ieee Trans. Eng. Manag.*, vol. 71, no. April, pp. 8002–8018, 2024, doi: 10.1109/tem.2024.3385298.

[15] S. Rout and K. L. Jaiswal, "Fraud Detection Using Deep Learning," *Int. J. Electr. Data Commun.*, vol. 5, no. 1, pp. 7–11, 2024, doi: 10.22271/27083969.2024.v5.i1a.37.

[16] Z. Wang, "Research on the Application of Artificial Intelligence and Big Data Technology in Financial Fraud Detection," *Jtpes*, vol. 4, no. 03, pp. 216–219, 2024, doi: 10.53469/jtpes.2024.04(03).21.

[17] P. Manorom, U. Detthamrong, and W. Chansanam, "Comparative Assessment of Fraudulent Financial Transactions Using the Machine Learning Algorithms Decision Tree, Logistic Regression, Naïve Bayes, K-Nearest Neighbor, and Random Forest," *Eng. Technol. Appl. Sci. Res.*, vol. 14, no. 4, pp. 15676–15680, 2024, doi: 10.48084/etasr.7774.

[18] V. B. Ayoola, U. N. Ugochukwu, I. Adeleke, C. I. Michael, M. B. Adewoye, and Y. Adeyeye, "Generative AI-Driven Fraud Detection in Health Care Enhancing Data Loss Prevention and Cybersecurity Analytics for Real-Time Protection of Patient Records," *Int. J. Sci. Res. Mod. Technol*, vol. 3, no. 11, pp. 89–107, 2024, doi: 10.38124/ijsrmt.v3i11.112.

[19] X. Zhu, X. Ao, Z. Qin, Y. Chang, Y. Liu, Q. He and J. Li, "Intelligent Financial Fraud Detection Practices in Post-Pandemic Era," *Innov.*, vol. 2, no. 4, pp. 1–12, 2021, doi: 10.1016/j.xinn.2021.100176.

[20] A. Zaytsev, R. S. Blizkyi, I. Rakhmeeva, and N. Dmitriev, "Building a Model for Financial Management of Digital Technologies in the Areas of Combinatorial Effects," *Economies*, vol. 9, no. 2, pp. 1–15, 2021, doi: 10.3390/economies9020052.

[21] A. Nursanti and I. Trinugroho, "The Effect of Financial Literacy on the Ability to Detect Investment Fraud," *Int. J. Soc. Sci. Res. Rev.*, vol. 6, no. 12, pp. 323–337, 2024, doi: 10.47814/ijssrr.v6i12.1840.

[22] M. D. V Prasad, "Multi-Entity Real-Time Fraud Detection System Using Machine Learning: Improving Fraud Detection Efficiency Using FROST-Enhanced Oversampling," *Jes*, vol. 20, no. 7s, pp. 1380–1394, 2024, doi: 10.52783/jes.3710.

[23] F. Z. E. Hlouli, J. Riffi, M. Sayyouri, M. A. Mahraz, A. Yahyaouy, K. E. Fazazy, and H. Tairi, "Detecting Fraudulent Transactions Using Stacked Autoencoder Kernel ELM Optimized by the Dandelion Algorithm," *J. Theor. Appl. Electron. Commer. Res.*, vol. 18, no. 4, pp. 2057–2076, 2023, doi: 10.3390/jtaer18040103.

[24] A. Shahapurkar, R. Patil, and K. Tangod, "Class Imbalance Aware Drift Identification Model for Detecting Diverse Attack in Streaming Environment," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 33, no. 2, pp. 981–989, 2024, doi: 10.11591/ijeecs.v33.i2.pp981-989.

[25] E. O. Udeh, P. Amajuoyi, K. B. Adeusi, and A. O. Scott, "The Role of Big Data in Detecting and Preventing Financial Fraud in Digital Transactions," *World J. Adv. Res. Rev.*, vol. 22, no. 2, pp. 1746–1760, 2024, doi: 10.30574/wjarr.2024.22.2.1575.

[26] O. B. Akinnagbe and T. A. Akintayo, "The Impact of Machine Learning on Fraud Detection in Digital Payment," *Asian. J. Of. Sci. Technol. Eng. Art.*, vol. 3, no. 2, pp. 191–209, 2025, doi: 10.58578/ajstea.v3i2.4900.

[27] A. Mutemi and F. Bacao, "E-Commerce Fraud Detection Based on Machine Learning Techniques: Systematic Literature Review," *Big Data Min. Anal.*, vol. 7, no. 2, pp. 419–444, 2024, doi: 10.26599/BDMA.2023.9020023.

[28] V. Gandhi and T. Gajjar, "Enhancing Fraud Detection in Financial Transactions Through Cyber Security Measures," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 10, no. 2, pp. 364–371, 2024, doi: 10.32628/cseit2410281.

[29] M. J. Ahmmed, M. M. Rahman, A. C. Das, P. Das, T. Pervin, S. Afrin, S. S. Tisha, M. M. Hassan, and N. Rahman, "Comparative Analysis of Machine Learning Algorithms for Banking Fraud Detection: A Study on Performance, Precision, and Real-Time Application," *Ijcsis*, vol. 09, no. 11, pp. 31–44, 2024, doi: 10.55640/ijcsis/volume09issue11-04.

[30] O. Balogun, J. A. Kupolusi, and A. Akomolafe, "Credit Card Fraud Detection Using Machine Learning Algorithms," *Br. J. Comput. Netw. Inf. Technol.*, vol. 7, no. 3, pp. 1–35, 2024, doi: 10.52589/bjcnit-ydijnxg2.

[31] L. Guo, R. Song, J. Wu, Z. Xu, and F. Zhao, "Integrating a Machine Learning-Driven Fraud Detection System Based on a Risk Management Framework," *Appl. Comput. Eng.*, vol. 87, no. 1, pp. 80–86, 2024, doi: 10.54254/2755-2721/87/20241541.

[32] S. F. Farabi, M. Prabha, M. Alam, M. Z. Hossan, M. Arif, M. R. Islam, A. Uddin, M. Bhuiyan, and M. Z. A. Biswas "Enhancing Credit Card Fraud Detection: A Comprehensive Study of Machine Learning Algorithms and Performance Evaluation," *J. Bus. Manag. Stud.*, vol. 6, no. 3, pp. 252–259, 2024, doi: 10.32996/jbms.2024.6.13.21.

[33] S. Ray, "Fraud Detection in E-Commerce Using Machine Learning," *Bijamr*, vol. 1, no. 1, pp. 7–14, 2022, doi: 10.54646/bijamr.002.

[34] D. Kumar and S. Singh, "Analyzing the Impact of Machine Learning Algorithms on Risk Management and Fraud Detection in Financial Institution," *Int. J. Res. Publ. Rev.*, vol. 5, no. 5, pp. 1797–1804, 2024, doi: 10.55248/gengpi.5.0524.1135.

[35] N. Mqadi, N. Naicker, and T. Adeliyi, "A SMOTe based Oversampling Data-Point Approach to Solving the Credit Card Data Imbalance Problem in Financial Fraud Detection," *Int. J. Comput. Digit. Syst.*, vol. 10, no. 1, pp. 277–286, Feb 2021, doi: 10.12785/ijcds/100128.

[36] T. V Nguyen and T. H. T. Le, "Financial Reporting Fraud and Models to Assist in Detecting Financial Statement Fraud," *Int. J. Multidiscip. Res. Anal.*, vol. 06, no. 08, pp. 3896–3901, 2023, doi: 10.47191/ijmra/v6-i8-65.

[37] I. W. Othman, "Financial Statement Fraud: Challenges and Technology Deployment in Fraud Detection," *Int. J. Account. Financ. Report.*, vol. 11, no. 4, pp. 1–11, 2021, doi: 10.5296/ijafr.v11i4.19067.

[38] A. Zgarni, "External Audit With a View to Detecting Financial Fraud," *J. Econ. Manag. Trade*, vol. 27, no. 11, pp. 49–54, 2021, doi: 10.9734/jemt/2021/v27i1130377.

[39] X. Feng and S.-K. Kim, "Novel Machine Learning Based Credit Card Fraud Detection Systems," *Mathematics*, vol. 12, no. 12, pp. 1–11, 2024, doi: 10.3390/math12121869.

[40] C. Kuo and S. Tsang, "Detection of Price Manipulation Fraud Through Rational Choice Theory: Evidence for the Retail Industry in Taiwan," *Secur. J.*, vol. 36, no. 4, pp. 712–731, 2022, doi: 10.1057/s41284-022-00360-3.

[41] A. Alharbi, M. Alshammari, O. D. Okon, A. Alabrah, H. T. Rauf, H. Alyami, and T. Meraj, "A Novel Text2IMG Mechanism of Credit Card Fraud Detection: A Deep Learning Approach," *Electronics*, vol. 11, no. 5, pp. 1–18, 2022, doi: 10.3390/electronics11050756.

[42] J. Kim, H. Jung, and W. Kim, "Sequential Pattern Mining Approach for Personalized Fraudulent Transaction Detection in Online Banking," *Sustainability*, vol. 14, no. 15, pp. 1–18, 2022, doi: 10.3390/su14159791.

[43] A. Alhchaimi, "Cloud-Based Transaction Fraud Detection: An in-Depth Analysis of ML Algorithms," *Wasit J. Comput. Math. Sci.*, vol. 3, no. 2, pp. 19–31, 2024, doi: 10.31185/wjcms.253.

[44] B. Mytnyk, O. Tkachyk, N. Shakhovska, C. Федушко, and Y. Syerov, "Application of Artificial Intelligence for Fraudulent Banking Operations Recognition," *Big Data Cogn. Comput.*, vol. 7, no. 2, pp. 1–19, 2023, doi: 10.3390/bdcc7020093.

[45] M. K. G, "Accuracy Analysis for Logistic Regression Algorithm and Random Forest Algorithm to Detect Frauds in Mobile Money Transaction," *Rev. Gestão Inovação E Tecnol.*, vol. 11, no. 4, pp. 1228–1240, 2021, doi: 10.47059/revistageintec.v11i4.2182.

[46] R. PK, S. S, and S. R, "Enhanced Credit Card Fraud Detection: A Novel Approach Integrating Bayesian Optimized Random Forest Classifier With Advanced Feature Analysis and Real-Time Data Adaptation," *Int. J. Innov. Eng. Manag. Res.*, vol. 12, no. 5, pp. 537–561, 2023, doi: 10.48047/ijiemr/v12/issue05/52.