International Journal of Academic Multidisciplinary Research (IJAMR)
ISSN: 2643-9670
Vol. 10 Issue 6 June - 2026, Pages: 318-321

Mobile Money Fraud Detection System Using Machine Learning

Gabriel F. Manga, Goodluck A. Nyoni, Athuman R Mganga, Boniface Kadege, Alfred Lukenza, Saul Vyagusa, Nuru Gerson, Neema Mathias, Vincent Bob.

Department of Computer Science, Faculty of Information and Communication Technology, Ruaha Catholic University Iringa-Tanzania
gabrielmang99@gmail.com

Abstract *: The rapid growth of mobile money services has transformed financial transactions, particularly in developing countries, by providing secure, fast, and accessible digital payment solutions. Despite these benefits, the increasing adoption of mobile money platforms has also attracted various forms of fraudulent activities, including identity theft, account takeover, phishing attacks, and unauthorized transactions. Traditional fraud detection methods often rely on predefined rules, making them ineffective against evolving fraud patterns. This review paper examines the application of machine learning techniques in mobile money fraud detection systems. The study explores existing approaches, algorithms, datasets, and challenges associated with fraud detection. The review highlights how machine learning models can analyze transaction behavior, identify anomalies, and improve fraud detection accuracy in real time. Furthermore, the paper identifies research gaps and proposes directions for future improvements in developing intelligent and adaptive fraud detection systems.*

Keywords: Mobile Money, Fraud Detection, Machine Learning, Financial Security, Anomaly Detection, Artificial Intelligence.

1.0 Introduction

Mobile money services have significantly transformed the financial sector by providing convenient, accessible, and costeffective digital payment solutions. These services enable users to transfer funds, pay bills, purchase goods, and access financial services through mobile devices without requiring traditional banking infrastructure.
The rapid growth of mobile money platforms has contributed substantially to financial inclusion, particularly in developing countries where access to conventional banking services remains limited [1].

Despite the benefits of mobile money systems, the increasing volume of digital transactions has attracted cybercriminals who exploit system vulnerabilities for financial gain. Common forms of fraud include account takeover, identity theft, SIM swap fraud, phishing attacks, money laundering, and unauthorized transactions [2]. These fraudulent activities result in significant financial losses, reduce customer trust, and negatively affect the sustainability of mobile financial services [3].

Traditional fraud detection systems primarily rely on predefined rules and expert knowledge to identify suspicious transactions. Although these methods are useful for detecting known fraud patterns, they struggle to adapt to emerging and sophisticated fraud techniques. Fraudsters continuously modify their strategies, making rule-based systems less effective in identifying previously unseen attacks [4].

Machine learning has emerged as a promising solution for addressing these challenges. By analyzing large volumes of transaction data, machine learning algorithms can automatically identify hidden patterns, detect anomalies, and classify transactions as legitimate or fraudulent [5]. Unlike conventional methods, machine learning models continuously improve their performance as new data becomes available, making them highly suitable for dynamic fraud detection environments [6].

Recent studies have demonstrated the effectiveness of various machine learning techniques, including Decision Trees, Random Forests, Support Vector Machines (SVM), Artificial Neural Networks (ANN), and Deep Learning models in detecting financial fraud [7]. These approaches have shown improved detection accuracy and reduced false-positive rates compared to traditional methods [8]. Consequently, machine learning-based fraud detection systems have become an active area of research within financial technology and cybersecurity domains.

This review paper examines existing machine learning approaches for mobile money fraud detection, evaluates their strengths and limitations, and identifies research gaps that require further investigation. The study aims to provide insights into current developments and future directions for intelligent mobile money fraud detection systems.

1.1 Background of the Study

Mobile money services have revolutionized digital finance by allowing users to send and receive money, purchase goods, and access financial services using mobile phones. The adoption of mobile money has significantly increased due to the expansion of mobile networks, smartphone usage, and financial inclusion initiatives [8], [9].

Despite these advancements, fraud remains one of the major threats affecting mobile money platforms. Fraudsters employ techniques such as SIM swap fraud, account impersonation, social engineering, and unauthorized transactions to exploit users and service providers [10]. Traditional fraud prevention mechanisms often rely on manually defined rules and threshold values, which may fail to detect sophisticated or emerging fraud patterns [11].

Recent developments in machine learning have introduced intelligent methods capable of detecting fraudulent activities automatically. Supervised learning algorithms such as Random Forest, Decision Trees, Support Vector Machines, and Logistic Regression have been widely applied in fraud detection systems [12], [13]. Unsupervised learning techniques such as clustering and anomaly detection have also shown effectiveness in identifying unusual transaction behavior [14].

Researchers continue to investigate advanced machine learning approaches capable of processing large-scale transaction data while maintaining high detection accuracy and low false-positive rates [15]. The integration of artificial intelligence into fraud detection systems has become a promising direction for enhancing mobile money security [16],
[17].

1.2 Statement of the Problem

Mobile money services continue to experience increasing levels of fraudulent activities that result in significant financial losses and reduced customer confidence. Existing fraud detection methods primarily depend on static rules and manual monitoring, making them ineffective in detecting sophisticated and evolving fraud techniques.

The increasing volume of mobile money transactions generates large amounts of data that are difficult to analyze manually. As fraudsters continuously modify their strategies, traditional systems struggle to identify new fraud patterns in real time. This creates a need for intelligent fraud detection mechanisms capable of learning transaction behavior and automatically identifying suspicious activities.

Furthermore, many existing systems experience challenges such as high false alarm rates, delayed fraud detection, poor scalability, and limited adaptability. Therefore, there is a need for machine learning-based fraud detection systems that can improve detection accuracy, reduce financial losses, and enhance the security of mobile money platforms.

1.3 Objectives of the Study

1.3.0 Main Objective

To develop an intelligent system that detects fraudulent mobile money transactions in real time using Machine Learning to improve security and reduce financial losses.

1.3.1 Specific Objectives

i. To analyse mobile money transaction data to identify patterns of normal and fraudulent activities.
ii. To develop a model using Machine Learning for detecting fraudulent transactions.
iii. To implement a system that classifies transactions as legitimate or fraudulent in real time.
iv. To evaluate the performance of the system using metrics such as accuracy, precision, and recall.

2.0 Related Work (Literature Review)

Fraud detection in financial systems has been extensively studied due to the increasing sophistication of cybercriminal activities. Researchers have explored various data mining, statistical, and machine learning approaches to improve fraud detection performance and reduce financial losses [18].

Bhattacharyya et al. [19] investigated data mining techniques for fraud detection and reported that machine learning models outperform traditional statistical approaches in identifying fraudulent transactions. Their findings demonstrated that classification algorithms can effectively learn transaction patterns and distinguish between legitimate and fraudulent activities.

Ngai et al. [20] conducted a comprehensive review of data mining applications in financial fraud detection and highlighted the effectiveness of classification, clustering, and anomaly detection techniques. The study concluded that machine learning approaches provide higher adaptability and scalability compared to rule-based systems.

Random Forest algorithms have gained considerable attention due to their high accuracy and robustness. Dal Pozzolo et al. [21] demonstrated that Random Forest models achieve superior fraud detection performance by handling imbalanced datasets effectively. Their work showed that ensemble learning techniques can significantly improve fraud classification accuracy.

Support Vector Machines (SVM) have also been widely applied in fraud detection research. Sahin and Duman [22] reported that SVM models successfully identify fraudulent financial transactions by constructing optimal decision boundaries between legitimate and fraudulent classes. However, their performance may decline when processing extremely large datasets.

Deep learning techniques have recently emerged as powerful tools for fraud detection. LeCun et al. [23] emphasized the capability of deep neural networks to learn complex data representations from large transaction datasets. Similarly, Chalapathy and Chawla [24] highlighted the effectiveness of deep learning models in anomaly detection and fraud identification.

Researchers have also explored unsupervised learning techniques for detecting previously unknown fraud patterns. Ahmed et al. [25] demonstrated that anomaly detection algorithms can identify suspicious transaction behavior without requiring labeled fraud data. This approach is particularly useful in environments where fraudulent transactions are rare or difficult to label accurately.

Carcillo et al. [26] proposed a hybrid fraud detection framework that combines supervised and unsupervised learning techniques. Their findings showed that integrating multiple learning approaches improves fraud detection performance while reducing false positives.

Recent studies have also investigated explainable artificial intelligence (XAI) in fraud detection systems. Ribeiro et al. [27] argued that interpretable machine learning models improve transparency and trust by allowing analysts to understand the reasons behind fraud predictions.

Although significant progress has been made in fraud detection research, several challenges remain unresolved. Data imbalance, privacy concerns, computational complexity, and model interpretability continue to affect the deployment of machine learning-based fraud detection systems [28]. Furthermore, many studies focus on general financial fraud while providing limited attention to mobile money-specific fraud scenarios
[29].

The reviewed literature indicates that machine learning techniques provide promising solutions for mobile money fraud detection. However, further research is needed to develop scalable, explainable, and real-time fraud detection systems capable of adapting to evolving fraud patterns.

3.0 Observation from Related Work

From the reviewed literature, it is observed that machine learning techniques
significantly outperform traditional rulebased approaches in detecting fraudulent mobile money transactions.

Most researchers focus on supervised learning algorithms because of their high classification accuracy. However, these approaches require large amounts of labeled transaction data, which is often difficult to obtain due to privacy restrictions and limited fraud records.

Another observation is that fraud datasets are highly imbalanced, where fraudulent transactions represent only a small percentage of total transactions. This imbalance affects model performance and requires specialized techniques such as oversampling and cost-sensitive learning.

The literature also indicates growing interest in deep learning methods due to their ability to analyze complex transaction patterns. However, these approaches require significant computational resources and large datasets for effective training.

Furthermore, many existing studies prioritize detection accuracy while giving limited attention to explainability, scalability, and real-time deployment. These gaps create opportunities for future research in practical fraud detection systems.

4.0 Conclusion

This review paper examined the application of machine learning techniques in mobile money fraud detection systems. The literature demonstrates that machine learning algorithms provide more effective fraud detection capabilities compared to traditional rule-based methods. Various approaches, including supervised, unsupervised, and deep learning models, have been successfully applied to identify fraudulent transactions.

Despite significant progress, challenges such as data imbalance, privacy concerns, computational requirements, and model interpretability continue to affect system performance. The findings suggest that intelligent fraud detection systems have considerable potential to improve transaction security and reduce financial losses within mobile money platforms.

5.0 Recommendations

i. Mobile money service providers should adopt machine learning-based fraud detection systems to improve transaction security.

ii. Financial institutions should invest in high-quality transaction datasets for model training and evaluation.

iii. Researchers should focus on developing explainable machine learning models to improve transparency and user trust.

iv. Organizations should implement realtime fraud detection mechanisms capable of identifying suspicious activities immediately.

v. Collaboration between regulators, financial institutions, and researchers should be strengthened to enhance fraud prevention strategies.

5.1 Future Work

i. Development of deep learning-based fraud detection systems capable of handling large-scale transaction data.

ii. Integration of explainable artificial intelligence (XAI) techniques to improve model interpretability.

iii. Exploration of federated learning approaches that preserve user privacy while enabling collaborative fraud detection.

iv. Development of hybrid models combining machine learning, blockchain, and cybersecurity technologies.

v. Investigation of real-time fraud detection frameworks suitable for mobile money environments with high transaction volumes.

Acknowledgement

We express sincere appreciation to all researchers, academic supervisors, and institutions whose contributions in machine learning and mobile financial security have provided valuable insights for this review study.

References

[1] Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud detection.

[2] Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection.

[3] Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques.

[4] Dal Pozzolo, A., Caelen, O., Johnson, R., & Bontempi, G. (2015). Calibrating probability with undersampling for fraud detection.

[5] Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). A comprehensive survey of data mining-based fraud detection research.

[6] Chalapathy, R., & Chawla, S. (2019). Deep learning for anomaly detection.

[7] LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning.

[8] Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning.

[9] Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). Why should I trust you? Explaining the predictions of any classifier.

[10] Khandani, A. E., Kim, A. J., & Lo, A. W. (2010). Consumer credit-risk models via machine-learning algorithms.