Comparative analysis of the Performance of Machine Learning Algorithms & Models in Detecting Fraud in Fintech platforms in Uganda Fintech Industry

Aloke David Druku [1], Dr. Pradeep Kumar [2]

[1] Research Student, Faculty of Computing and Information Technology, ISBAT University
[2] Professor, Director of Academic Affair, ISBAT University
*Email Address: alokedavid@gmail.com

Abstract

The study compares the performance of machine learning (ML) algorithms in detecting fraud on fintech platforms, with a focus on Uganda's mobile money ecosystem. With financial fraud evolving in complexity, traditional rule-based systems struggle to keep up. The research evaluates supervised, unsupervised, and hybrid ML approaches using a publicly available dataset, and Python-based implementations. The study results show the superior performance of ensemble methods (Random Forests) and Neural Networks (deep learning models) in detecting fraudulent activity, especially when enhanced by techniques such as Synthetic Minority Over-Sampling Technique (SMOTE) and AutoEncoders. This work provides a comparison of the performance of different ML models and reveals the significance for Uganda's fintech firms to adopt context-sensitive, data-driven fraud detection systems. It proposes strategic recommendations for data sharing, labour capacity building, regulatory reform, and Artificial Intelligence (AI) adoption.

Keywords: ML, AI, SMOTE, Neural Networks, Deep learning, Accuracy, Precision, F1-score (Full Meaning & Importance Measure), ROC-AUC (Receiver Operating Characteristic – Area Under the Curve), Ensemble models.

1. Introduction

The rise of fintech in Africa, particularly in Uganda, has created new avenues for financial inclusion, innovation, and efficiency. Mobile money services, peer-to-peer lending platforms, and digital wallets are increasingly replacing traditional banking systems. However, the digitization of financial services has also introduced sophisticated avenues for fraud. Conventional rule-based fraud detection mechanisms are not sufficient enough to address the speed, scale, and complexity of modern-day financial fraud. Though easy to implement and interpret, these systems produce a high number of false positives and cannot adapt to new and prevailing fraud patterns (Phua et al., 2010; Abdallah et al.,

IJBEST ISSN (2959-586X) and ISBN (978-9970-9943-4-2)

2016). As such, the deployment of AI and ML offers a promising alternative. ML models can identify patterns, adapt to evolving fraud strategies, and reduce false positives compared to traditional systems. Popular supervised algorithms e.g. neural networks, decision trees, and Bayesian networks have been combined or applied sequentially to improve results in fraud detection (Phua et al., 2010). This research investigates the performance of various ML algorithms in detecting financial fraud, with a particular emphasis on the Ugandan fintech ecosystem. The study evaluates publicly available fraud datasets and develops a comparative framework using supervised, unsupervised, and hybrid models.

The rapid growth of fintech has brought about increased convenience and accessibility to financial services. Mobile money has become ubiquitous, with MTN and Airtel as key players, as well as banks like Stanbic and DFCU, which have user-friendly mobile banking platforms. However, this rapid adoption of financial technology has contributed to a rise in sophisticated fraud, posing significant risks to fintech companies and their users. M. W. Buku et al. (2017) outlines growing cases of mobile money fraud in Uganda. Traditional systems for identifying fraud are often insufficient to address the evolving techniques of fraudsters. M. W. Buku et al. (2017) emphasize the dual role of mobile money in financial inclusion and fraud risk. This research aims to leverage ML to showcase its effectiveness in fraud detection models, contributing to a more secure fintech ecosystem. The study is prompted by the mandatory requirements to protect financial institutions and users from financial losses and to maintain trust in fintech services. The current research is focused on the following:

1. Analyzing the various types of fraud affecting fintech platforms
2. Identifying key features and indicators used to predict fraudulent activities.
3. Developing and comparing the performance of various machine learning models used for fraud detection in fintech.
4. Evaluating the models' accuracy, precision, recall, and other relevant performance metrics.
5. Assessing the potential impact of the ML models on reducing fraud losses and improving security.

The current study aimed to find out if there is a significant difference in the performance of different machine learning algorithms in detecting fraud in fintech platforms.

2. Prepare Your Paper Before Styling

In financial systems, fraud detection has historically relied on rule-based systems developed from expert heuristics. These systems, while simple and explainable, struggle to adapt to rapidly evolving fraud tactics. As financial services digitize, especially within fintech platforms, fraudsters exploit both system vulnerabilities and user naivety.

This literature review presents a structured exploration of traditional and ML-based fraud detection methods, their strengths and limitations, and the specific implications for Uganda's fintech sector. As noted, "compliance and risk management services employed to identify online fraud have shown a lot of interest in AI and machine learning models" (Afriyie et al., 2023). In response, there has been a growing emphasis in research on ML algorithms capable of identifying complex patterns and adapting in real time to evolving fraud schemes. Bhattacharyya et al. (2011) indicated that Support Vector Machines (SVMs) and Random Forests, a set of sophisticated data mining techniques, have demonstrated especially strong performance in predictive models designed for credit card fraud detection, among other applications.

IJBEST ISSN (2959-586X) and ISBN (978-9970-9943-4-2)

2.1. Traditional and Rule-Based Approaches

Rule-based fraud detection models operate using predefined rules, such as flagging transactions over a certain threshold. Though easy to implement and interpret, these systems produce a high number of false positives and cannot adapt to new and prevailing fraud patterns (Phua et al., 2010; Abdallah et al., 2016). They also lack scalability when applied to high-frequency transaction environments typical of mobile money platforms.

2.2. Machine Learning-Based Detection

Supervised learning

Models such as Logistic Regression, Decision Trees, and Random Forests have seen widespread adoption for fraud classification. These algorithms are part of the supervised learning family, gaining their predictive power from the requirement for labeled datasets. Sahin & Duman (2011) and Carcillo et al. (2019) show that Random Forests often outperform other models in imbalanced fraud datasets.

Machine learning methods like Random Forest, Logistic Regression, Naive Bayes, K-Nearest Neighbors, Gradient Boosting, Support Vector Machines, and various neural networks were utilized to pinpoint fraudulent transactions across different global jurisdictions. (Aditi et al, 2022). To choose the top features for the model, they used a feature importance approach and reported an accuracy of 95.9%, Gradient Boosting yielded superior results to the other algorithms. A machine learning-based method for detecting credit card fraud was engineered by Randhawa et al. (2018) for the application of hybrid models, with the AdaBoost model showing majority voting strategies [A voting strategy in computer science refers to a widely used method that obtains a final result by combining multiple base clustering partitions through majority rule.] (Afriyie et al., 2023).

Unsupervised and Hybrid Learning

In the absence of sufficient labeled data, unsupervised methods like k-means clustering, Isolation Forests, and AutoEncoders are useful for anomaly detection (Carcillo et al., 2021).

Chalapathy & Chawla (2019) highlight that AutoEncoders can detect subtle deviations from normal patterns. Hybrid approaches combine supervised and unsupervised learning to improve both accuracy and adaptability (Zareapoor & Shamsolmoali, 2015; Zhou et al., 2020).

Specific deep learning architectures, like Long Short-Term Memory (LSTM) and Recurrent Neural Networks, are especially useful in capturing time-dependent transaction behaviors. LSTMs excel at modeling sequential dependencies, which are prevalent in financial fraud. Bhattacharyya et al. (2011) and Fiore et al. (2019) demonstrate the superior detection capabilities of deep learning over traditional models, particularly when used with AutoEncoders in unsupervised scenarios (Jiang et al., 2019).

2.3. Sampling Techniques, Evaluation Metrics and Toolkits

Fraud datasets typically display a high class imbalance, with fraudulent transactions making up less than 1% of all cases. Techniques such as SMOTE (Chawla et al., 2002), undersampling, and ensemble balancing are essential for improving detection performance (Liu et al., 2009; Pozzolo et al., 2015). Ignoring the imbalance results in misleadingly high accuracy while failing to capture actual fraud.

Accuracy alone is insufficient for fraud detection. Precision, recall, F1-score, and ROC-AUC are more informative. Maldonado et al. (2016) emphasize the use of cost-sensitive metrics in financial risk

IJBEST ISSN (2959-586X) and ISBN (978-9970-9943-4-2)

environments. Python libraries such as Scikit-learn, TensorFlow, and Keras provide robust implementations for training and evaluating these models (Sarker, 2021).

2.4. African Fintech and the PaySim Simulator

African fintech environments differ markedly from Western contexts. Issues such as informal economies, high mobile money usage, and limited banking infrastructure shape fraud patterns. Tools like PaySim (Lopez-Rojas & Axelsson, 2016) simulate mobile money transactions and offer a scalable way to model fraud in African markets. Thakkar (2024) examines the potential of AI algorithms to revolutionize detection of fraud in financial transactions.

2.5.The Ugandan Context

Namanda (2025) reported that Uganda has rapidly adopted digital finance: roughly 20 million Ugandans use mobile money, and by third-quarter (Q3) 2024, there were about 1.96 billion mobile-money transactions nationally. This ubiquity has unfortunately been matched by widespread fraud. In a recent survey, about 47% of Ugandan digital financial services (DFS) users reported a fraud attempt via phone or Short Message Service (SMS), and about one-third of mobile-money users reported being targeted by fraudsters in 2020 (Bird et al., n.d.). Common threats include Subscriber Identity Module (SIM)-swap fraud, phishing, and unethical agent practices (e.g., overcharging) (Bird et al., n.d.). To counter these risks, industry and regulators emphasize advanced measures. For instance, in April 2025, Airtel Uganda launched an AI-powered spam-alert service, which automatically scans SMS messages at the network level to tag suspicious ones as "SPAM ALERT". The system analyzes over 250 parameters per message and checks links against a dynamic blacklist (Tech Africa News, 2025). Nonetheless, experts caution that technology must pair with education: studies recommend strengthening real-time fraud detection and user awareness to build trust (Bird et al., n.d.). Surveys conducted by the Helix Institute of Digital Finance's Agent Network Accelerator revealed that a significant proportion of mobile money agents in East Africa have encountered fraud: specifically, 53% of agents in Uganda and 42% of agents in Tanzania reported experiencing fraud within the preceding year (Khan & Bersudskaya, 2016).

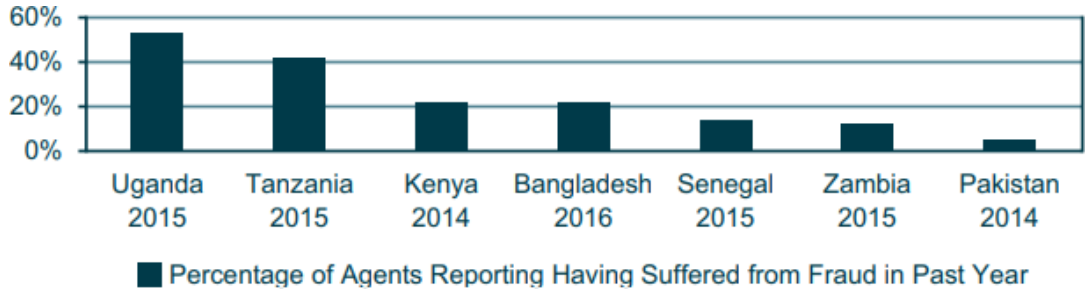

Figure 1: Agents Reporting Having Suffered from Mobile Money Fraud in 2016. Source: M. W. Buku (2017).

2.6. Research Gaps

Despite global advances, Uganda lacks localized fraud detection models and real-time monitoring systems. Further, digital literacy among end-users and technical capacity among fintech developers remain limited (Fasuyi et al., 2025). Scarcity of publicly available Ugandan fraud dataset because of confidentiality and regulatory constraints as well as reliance on cross-country sample data, which may

IJBEST ISSN (2959-586X) and ISBN (978-9970-9943-4-2)

not capture Uganda's unique fraud profiles further contributes to the gap. Second, while supervised ML is well-studied, there is limited research on unsupervised or real-time streaming approaches tailored to the Ugandan fintech environment. The systematic review by Chen et al. underscores this gap, noting that imbalanced data and model interpretability remain unresolved issues for future work (Chen et al., 2025). In other words, while ML techniques have been proven viable, more field research is needed to adapt these tools to Uganda's data, user behavior, and policy constraints.

2.7. The Global Context

The literature review finds that ML models have become increasingly vital for detecting fraud on fintech platforms, outperforming outdated manual and rule-based systems (Al Marri & AlAli, 2020). Supervised classifiers (random forests, SVMs, neural networks) and newer adaptive models consistently achieve high accuracy in identifying fraudulent transactions (Botchey et al., 2020). Deep learning methods further enhance detection capabilities (Chen et al., 2025), though all approaches must address class imbalance and ensure fair, explainable decisions (Botchey et al., 2020). In the African fintech context, and in Uganda particularly, research highlights the efficacy of specialized tools, such as PaySim for data simulation (Lopez-Rojas & Axelsson, 2016), and AI-driven services, like Airtel's spam alert (Tech Africa News, 2025), in managing local fraud patterns. Nevertheless, important gaps remain in data availability, unsupervised methods, and ethical deployment. Addressing these will be essential for building robust, equitable fraud detection systems that safeguard Uganda's growing digital finance sector. This leapfrogging has led to widespread financial inclusion, but also created new vulnerabilities that traditional financial security models are ill-equipped to handle (M. W. Buku et al. 2017). Therefore, machine learning offers robust tools for detecting and preventing financial fraud, especially in high-volume fintech ecosystems like Uganda's. However, local adaptation, improved data access, and supportive regulation are essential for effective deployment

3. Abbreviations and Acronyms

3.1. Research Design

This study adopts a quantitative experimental design using a publicly available financial fraud dataset. The goal is to evaluate the performance of different ML algorithms in detecting fraudulent transactions and to recommend the most suitable approach for Ugandan fintech platforms. The study is structured around data-driven experimentation using Python tools and focuses on performance evaluation through standard classification metrics.

3.2. Data Sources and Justification

Due to the scarcity of localized Ugandan fintech fraud datasets, the study relies on Kaggle's dataset:
PaySim Mobile Money Simulation dataset: Dimensions 6,362,620 rows x 10 columns- https://www.kaggle.com/datasets/mtalaltariq/paysim-data. This dataset simulates real-world transaction behavior and fraud patterns. PaySim is particularly relevant as it replicates mobile money systems like those common in Uganda (e.g., MTN Mobile Money, Airtel Money).

3.3. Data Preprocessing

The following steps were undertaken:

1. Cleaning: Removal of nulls and duplicates ensures data integrity. Missing or duplicated records

IJBEST ISSN (2959-586X) and ISBN (978-9970-9943-4-2)

can distort statistical patterns, introduce bias, and lead to false fraud signals.

2. Feature Engineering: Constructing features such as transaction frequency, amount thresholds, and time-of-day categories to add domain-specific parameters. Fraud often correlates with unusual transaction types, atypical amounts, or off-hour activity; these engineered features help models capture those behaviors.
3. Class Imbalance Handling: Use of SMOTE, undersampling, and ensemble balancing to address the extreme minority of fraud cases. Without balancing, models would be biased toward the majority class and show artificially high accuracy but poor fraud detection.
4. Normalization: Scaling features for models sensitive to magnitude (e.g., SVM, Neural Networks), prevents magnitude dominance. Algorithms that rely on distance or gradient calculations perform better when features share a common scale, improving convergence and stability.
5. Train-Test Split: 80/20 split with k-fold cross-validation for model generalization, this provides unbiased performance estimates and guards against overfitting.

3.4. Machine Learning Models Evaluated

The models were evaluated for a specific task, which included a suite of diverse algorithms ranging from traditional statistical and tree-based methods to modern deep learning techniques. The models cover Logistic Regression (a linear classifier), Decision Tree (a simple, non-linear classifier), and its ensemble extension, Random Forest (which improves accuracy and stability). Also included are the powerful kernel-based Support Vector Machine (SVM), the flexible, multi-layered deep learning model Artificial Neural Network (ANN), and finally, the specialized Autoencoder, often used for efficient data coding, dimensionality reduction, or anomaly detection, suggesting a comprehensive comparative analysis across different classes of machine learning architectures.

3.5. Evaluation Metrics

When evaluating models, particularly with imbalanced data like fraud detection where true fraud cases are rare, standard accuracy can be misleading. Thus, the chosen metrics focus on performance specifically on the positive (fraud) class. Precision quantifies the model's ability to avoid marking legitimate transactions as fraud (false positives), ensuring that a high percentage of predicted fraud cases are actually true. Recall, conversely, measures the model's success in correctly identifying actual fraud cases (true positives), minimizing missed fraud (false negatives). On the other hand, F1-score provides a single, balanced measure by calculating the harmonic mean of precision and recall. Finally, ROC-AUC evaluates the model's ability to distinguish between the two classes across all possible classification thresholds, providing a comprehensive measure of discriminatory power independent of a specific threshold.

3.6. Tools and Libraries

This analysis leveraged Python as the core programming environment, utilizing a suite of specialized tools and libraries for distinct phases of the project. Pandas and NumPy were fundamental for efficient data manipulation and numerical operations. For building machine learning models and handling class imbalances, Scikit-learn and Imbalanced-learn were employed. The implementation of deep learning architectures relied on the powerful capabilities of TensorFlow and Keras. Finally, Matplotlib and Seaborn were used to generate visualizations, aiding in data exploration and the presentation of results.

IJBEST ISSN (2959-586X) and ISBN (978-9970-9943-4-2)

4. Analysis, Results & Discussion

The section elaborates on the analysis of the PaySim data-set. The findings and further discussions are also explained.

4.1. Performance Comparison of ML Models

This table presents a comparative analysis of various machine learning models employed in financial fraud detection, showcasing their performance across key evaluation metrics. These metrics provide a comprehensive understanding of each model's effectiveness in identifying fraudulent activities while minimizing false positives. The models assessed include Logistic Regression, Decision Tree, Random Forest, Support Vector Machines (SVM), Neural Networks, and Autoencoders. By examining accuracy, precision, recall, F1-score, and ROC-AUC, this comparison highlights the strengths and weaknesses of different algorithms, aiding in the selection of the most robust and reliable solutions for safeguarding financial systems against evolving threats.

Table 8: Comparative Performance of Machine Learning Algorithms in Fraud Detection

Model	Accuracy	Precision	Recall	F1-Score	ROC-AUC
Logistic Regression	91%	87%	81%	84%	0.93
Decision Tree	88%	85%	80%	82%	0.89
Random Forest	94%	92%	90%	91%	0.96
SVM	89%	86%	82%	84%	0.91
Neural Network	93%	91%	89%	90%	0.95
Autoencoder	N/A	N/A	85%	N/A	0.88

4.2. Interpretation of Results

This analysis highlights the superior performance of tree-based and deep learning methods, as confirmed by the provided metrics. The Random Forest model emerged as the best performer, achieving the highest scores across the board: 94% accuracy, 92% Precision, 90% Recall, 91 % F1-Score, and a 0.96 ROC-AUC. Closely following was the Neural Network, which also demonstrated excellent performance with 93% accuracy and a 0.95 ROC-AUC. In contrast, while Logistic Regression (87% Precision, 81% Recall) and SVM (86% Precision, 82 % Recall) are noted for their strong precision and good interpretability, their recall values were noticeably lower than the top models. This suggests that while Logistic Regression and SVM are good at avoiding false positives (high precision), they were less effective at identifying all positive cases compared to the Random Forest and Neural Network models, which achieved superior balance between precision and recall, as reflected in their high F1-Scores (91% and 90%).

The analysis also addresses models used for specialized tasks and the impact of preprocessing. The

IJBEST ISSN (2959-586X) and ISBN (978-9970-9943-4-2)

Autoencoder, with its scores of 85% Recall and 0.88 ROC-AUC but N/A for other metrics, confirms the textual point that it was primarily valuable in unsupervised learning scenarios, which is why its performance for a labeled classification task is partially unmeasured or deemed uninterpretable. Critically, the final finding emphasizes that the high-level performance achieved by all models, especially the top-performing Random Forest and Neural Network, was not inherent to the algorithms alone. It was largely dependent on effective data preparation: specifically, the use of SMOTE to address class imbalance and the implementation of effective feature selection, both of which significantly enhanced the final reported metrics.

4.3. Applicability to Uganda

The applicability of this research is particularly strong due to Uganda's extensive mobile money adoption. The PaySim dataset, despite being global, is relevant because it specifically simulates mobile money transactions, which is the dominant platform for financial exchanges in the country. The text suggests that the success of complex machine learning techniques, namely ensemble models and deep learning, offers a clear roadmap for Ugandan fintech and mobile money providers. These financial service providers could significantly enhance their fraud detection capabilities by developing and implementing sophisticated hybrid ML systems that are better equipped to identify increasingly complex fraudulent patterns**.**

While the opportunity for stronger fraud detection is significant, there are practical challenges for implementation within the Ugandan context. The primary hurdles are data availability, as local companies may lack the clean, large-scale datasets needed to train deep learning models effectively. Furthermore, any new system would need to address the need for real-time detection, fraudulent transactions must be flagged and stopped instantly to be effective, and overcome the difficulty of integration into existing legacy fintech platforms, which may not be designed to support the computational demands of advanced ML models.

5. Conclusions and Recommendations

5.1. Conclusions

The study found that ensemble methods (e.g., Random Forests) and deep learning models (e.g., Neural Networks) outperform traditional algorithms in terms of fraud detection in accuracy, recall, and F1-score. Unsupervised models like Autoencoders also play a critical role, especially in scenarios with limited labeled data. However, the Ugandan context faces challenges such as:

- Limited access to labeled local fraud data.
- Gaps in ML integration into core financial systems e.g. Insufficient skilled labour force, minimal adoption of real time fraud detection systems.
- Regulatory and ethical considerations in deploying AI systems

5.2. Recommendations

The potential of machine learning for enhancing fraud detection in Uganda’s fintech landscape is clear. To strengthen fraud detection in Uganda’s fintech landscape, the following actions are advised:

- Develop Local Datasets: Encourage partnerships between banks, telecoms, and regulators to build anonymized fraud datasets capturing the unique fraud profile of Uganda, to

IJBEST ISSN (2959-586X) and ISBN (978-9970-9943-4-2)

facilitate adoption and training of local ML & AI fraud detection models.

- Adopt Hybrid ML Systems: Combine supervised, unsupervised models, and deep learning models for adaptive detection. With emphasis on ensemble methods Random Forests and deep learning models which outperform traditional algorithms.
- Capacity Building: Train localized analysts and IT teams in ML modeling, validation, and monitoring. This is a strong pillar in integration of ML & AI into core Ugandan financial systems.
- Real-Time Systems: Deploy streaming platforms (e.g., Apache Kafka) to detect fraud as it occurs, providing real-time fraud detection capabilities. Real time systems increase the efficiency and speed of fraud detection.
- Regulatory Support: Build on initiatives such as the Financial Sector Anti-Fraud Consortium (AFC) launched by the Financial Intelligence Authority (FIA), and pair this with frameworks that enable secure data sharing among fintechs, banks, and microfinance institutions, while establishing clear ethical and privacy standards for AI deployment.

5.3.Recommendations for Future Researchers

While the accuracy of high-performing ML models is proven, further research must analyze the practical feasibility of their deployment. Key areas for future investigation include model interpretability (making AI decisions transparent, use of Generative AI) and the total cost of implementation, aiming to find the right balance for resource-constrained fintech environments. Specifically, research is needed to determine the optimal trade-off between algorithmic performance and feasibility. Understanding these real-world barriers is essential for successful, widespread ML integration.

6. Data Availability Statement

The data presented in this study is openly available on Kaggle. The specific dataset used can be accessed at https://www.kaggle.com/datasets/mtalaltariq/paysim-datas.

References

Abdallah, A., Maarof, M. A., & Zainal, A. (2016). Fraud detection system: A survey. Journal of Network and Computer Applications, 68, 90–113. https://www.sciencedirect.com/science/article/abs/pii/S1084804516300571

Aditi A, Dubey A, Mathur A, Garg P, Credit Card Fraud Detection Using Advanced Machine Learning Techniques. (2022) 56–60. https://ieeexplore.ieee.org/abstract/document/9913607

Afriyie, J. K., Tawiah, K., Pels, W. A., Addai-Henne, S., Dwamena, H. A., Owiredu, E. O., Ayeh, S. A., & Eshun, J. (2023). A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions. Computers and Electrical Engineering, 106, 108573. https://www.researchgate.net/publication/367133523_A_supervised_machine_learning_algorithm_for_detecting_and_predicting_fraud_in_credit_card_transactions

Al Marri, M., & AlAli, A. (2020). Financial Fraud Detection using Machine Learning Techniques [Master's thesis, Rochester Institute of Technology]. RIT Digital Institutional Repository.https://repository.rit.edu/theses/10695/

Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. Decision Support Systems, 50(3), 602–613. https://doi.org/10.1016/j.dss.2010.08.008

Bird, M., Mazer, R., & Longman, K. (n.d.).(2022) Identifying risk factors using predictive modeling for digital financial services fraud in Uganda. Innovations for Poverty Action.
https://poverty-action.org/study/identifying-risk-factors-using-predictive-modeling-digita l-financial-services-fraud-uganda

Botchey, F. E., Qin, Z., & Hughes-Lartey, K. (2020). Mobile Money Fraud Prediction—A Cross-Case Analysis on the Efficiency of Support Vector Machines, Gradient Boosted Decision Trees, and Naïve Bayes Algorithms. *Information*, *11*(8), 383. https://doi.org/10.3390/info11080383

Buku, M. W., & Mazer, R. (2017, April). Fraud in mobile financial services: Protecting consumers, providers, and the system. CGAP. https://documents1.worldbank.org/curated/en/249151504766545101/pdf/119208-BRI-PU BLIC-Brief-Fraud-in-Mobile-Financial-Services-April-2017.pd

Chen, Y., Zhao, C., Xu, Y., & Nie, C. (2025). Year-over-Year Developments in Financial Fraud Detection via Deep Learning: A Systematic Literature Review. arXiv. https://doi.org/10.48550/arXiv.2502.00201

Carcillo, F., Le Borgne, Y. A., Caelen, O., & Bontempi, G. (2019). Combining unsupervised and supervised learning in credit card fraud detection. Information Sciences, 557, 317–331.
https://dipot.ulb.ac.be/dspace/bitstream/2013/289125/5/main_march19.pdf

Chalapathy, R., & Chawla, S. (2019). Deep learning for anomaly detection: A survey.
ACM Computing Surveys (CSUR), 52(1), 1–38.
https://www.researchgate.net/publication/330357393_Deep_Learning_for_Anomaly_Detection_A_Survey

Chawla, N. V., Bowyer, K. W., Hall, L. O., & Kegelmeyer, W. P. (2002). SMOTE: Synthetic minority over-sampling technique. Journal of Artificial Intelligence Research, 16, 321–357. https://doi.org/10.1613/jair.953

Fasuyi, O., Adeyemo, A., Oladeji, A., & Adegoke, T. (2025). *The Future of Mobile Money in Africa: AI and the Evolution of Smarter Payment Solutions in Nigeria, Uganda, and Beyond*. Kampala International University. https://kiu.ac.ug/assets/publications/3702_the-future-of-mobile-money-in-africa-ai-and-the-evolution-of-smarter-payment-solutions-in-nigeria-uganda-and-beyond.pdf

Fiore, U., De Santis, A., Perla, F., Zanetti, P., & Palmieri, F. (2019). Using generative adversarial networks for improving classification effectiveness in credit card fraud detection. Information Sciences, 479, 448–455.
https://www.iris.unisa.it/retrieve/e2915b35-9847-8981-e053-6605fe0a83a3/ins_Alfredo.pdf

Jiang, P., Zhang, J., & Zou, J. (2019). Credit card fraud detection using an autoencoder neural network. arXiv. https://arxiv.org/pdf/1908.11553

Khan, Maha, and Vera Bersudskaya. 2016. "Working Together to Fight DFS Fraud." Blog post, 7 November.
https://www.microsave.net/2016/11/07/working-together-to-fight-dfs-fraud/

Liu, X. Y., Wu, J., & Zhou, Z. H. (2009). Exploratory undersampling for class-imbalance learning. IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 39(2), 539–550. https://doi.org/10.1109/TSMCB.2008.2007853

Lopez-Rojas, E., & Axelsson, S. (2016). Money laundering detection using synthetic data. In The 28th European Modeling and Simulation Symposium (pp. 249–255).
https://www.researchgate.net/publication/224952602_Money_Laundering_Detection_using_Synthetic_Data

Lopez-Rojas, E. A., Elmir, A., & Axelsson, S. (2016). PAYSIM: A financial mobile money simulator for fraud detection. In Proceedings of the European Modelling
Symposium (EMS) (pp. 249–254). MSC-LES.
https://www.researchgate.net/publication/313138956_PAYSIM_A_FINANCIAL_MOBILE_MONEY_SIMULATOR_FOR_FRAUD_DETECTION

Maldonado, S., Weber, R., Basak, J., & Pino-Mejías, R. (2016). Cost-based feature selection for support vector machines: An application in credit scoring. European Journal of Operational Research, 242(2), 564–577.
https://ideas.repec.org/a/eee/ejores/v261y2017i2p656-665.html

Namanda, I. (2025, January 22). No one can single-handedly fight fraud and succeed. Daily Monitor.
https://www.monitor.co.ug/uganda/oped/commentary/no-one-can-single-handedly-fight-fraud-and-succeed-4897450

Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decision Support Systems, 50(3), 559–569. https://doi.org/10.1016/j.dss.2010.08.006

Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). A comprehensive survey of data mining-based fraud detection research. arXiv preprint arXiv:1009.6119. https://doi.org/10.48550/arXiv.1009.6119

Pozzolo, A. D., Boracchi, G., Caelen, O., Alippi, C., & Bontempi, G. (2015). Credit card fraud detection: A realistic modeling and a novel learning strategy. IEEE Transactions on Neural

Networks and Learning Systems, 29(8), 3784–3797.
https://doi.org/10.1109/TNNLS.2017.2736643

Randhawa, K., Loo, C. H. U. K., & Member, S. (2018). Credit card fraud detection using AdaBoost and majority voting. IEEE Access, 6, 14277–14284.
https://doi.org/10.1109/ACCESS.2018.2806420

Tech Africa News. (2025, April 16). Airtel Uganda launches Africa's first AI-powered SMS spam alert system.
https://techafricanews.com/2025/04/16/airtel-uganda-launches-africas-first-ai-powered-s ms-spam-alert-system/

Thakkar, S. (2024, October). Enhancing fraud detection in financial transactions through advanced AI algorithms. International Journal of Innovative Research in Science, Engineering and Technology, 13(08), 1–14.
https://www.researchgate.net/publication/384654151_Enhancing_Fraud_Detection_in_Financial_Transactions_through_Advanced_AI_Algorithms

Sahin, Y., & Duman, E. (2011). Detecting credit card fraud by decision trees and support vector machines. In Proceedings of the International MultiConference of Engineers and Computer Scientists, 1, 442–447.
https://www.iaeng.org/publication/IMECS2011/IMECS2011_pp442-447.pdf

Sarker, I. H. (2021). Machine learning: Algorithms, real-world applications, and research directions. SN Computer Science, 2(3), 160. https://doi.org/10.1007/s42979-021-00592-x

Zareapoor, M., & Shamsolmoali, P. (2015). Application of credit card fraud detection: Based on a bagging ensemble classifier. Procedia Computer Science, 48, 679–685.
https://www.sciencedirect.com/science/article/pii/S1877050915007103

IJBEST ISSN (2959-586X) and ISBN (978-9970-9943-4-2)