ISSN : 2455-9679
SJIF Impact Factor : 6.190

IJRTSM
INTERNATIONAL JOURNAL OF RECENT TECHNOLOGY SCIENCE & MANAGEMENT

"AN ENSEMBLE LEARNING APPROACH FOR DETECTING FRAUDULENT ACTIVITIES IN DIGITAL BANKING PLATFORMS"

Nisha Golkar [1], Dr. Sanmati Kumar Jain [2]

[1] M.Tech. Scholar, Department of Computer Science and Engineering, Vikrant Institute of Technology and Management, Indore, M.P. India

[2] Associate Professor & HOD, Department of Computer Science and Engineering, Vikrant Institute of Technology and Management, Indore, M.P. India

ABSTRACT

The rapid growth of digital banking has increased the volume of online financial transactions and has also created new opportunities for fraudulent activities such as phishing, identity theft, account takeover, unauthorized fund transfers, and card-not-present fraud. Traditional rule-based fraud detection systems are often unable to identify complex and changing fraud patterns because fraudulent transactions may appear very similar to genuine customer activities. Therefore, this paper presents a machine learning-based fraud detection system for secure digital banking transactions. The study formulates fraud detection as a binary classification problem in which transactions are classified as genuine or fraudulent. Several supervised machine learning algorithms, including Logistic Regression, Decision Tree, Random Forest, Support Vector Machine, K-Nearest Neighbour, Naïve Bayes, XGBoost, and Artificial Neural Network, were developed and evaluated using the same training and testing conditions. Model performance was assessed using accuracy, precision, recall, F1-score, ROC-AUC, PR-AUC, and confusion matrix analysis to address the class imbalance problem commonly found in banking fraud datasets. The results show that XGBoost achieved the best overall performance with 99.967% accuracy, 90.72% precision, 89.80% recall, 90.26% F1-score, 99.10% ROC-AUC, and 91.20% PR-AUC. The model correctly detected most fraudulent transactions while maintaining a low false positive rate. The findings indicate that machine learning, particularly boosting-based ensemble learning, can provide an effective and reliable approach for real-time fraud detection in digital banking systems.

Keywords: Digital banking; fraud detection; machine learning; XGBoost; supervised classification; imbalanced dataset; secure transactions; financial cybersecurity.

I. INTRODUCTION

The use of digital banking transactions has increased significantly due to the expansion of internet access, smartphone usage, online shopping, mobile applications, cashless payment systems, and real-time fund transfer services. Customers now prefer digital banking because it saves time and provides quick access to financial services. Banks and financial institutions also promote digital banking because it improves service efficiency, reduces branch workload, and supports large-scale transaction processing. As a result, digital banking has become a major part of modern financial activity.

The growth of digital banking has created a large volume of transaction data. Each transaction may contain several important attributes, such as transaction amount, transaction time, transaction mode, merchant category, account details, device information, geographical location, and transaction status. This data can be used for banking analytics,

ISSN : 2455-9679
SJIF Impact Factor : 6.190

customer behavior analysis, risk assessment, and fraud detection. However, the increasing number of transactions also increases the difficulty of manually identifying fraudulent activities. Therefore, automated fraud detection systems are required to monitor transactions efficiently. As digital transactions increase, the volume of data increases, and the possibility of fraudulent attempts also increases. Hence, banks require intelligent systems that can process large amounts of data and identify suspicious transactions with minimum delay.

The rise in digital banking has also changed the nature of fraud. In traditional banking, fraud was often associated with forged documents, physical card theft, or unauthorized branch-level activity. In digital banking, fraud can occur through phishing, identity theft, fake websites, account takeover, unauthorized online transfers, card-not-present fraud, malware-based attacks, and social engineering. These frauds are often difficult to detect because they may appear similar to genuine customer transactions. For this reason, digital banking fraud detection must be fast, adaptive, and data-driven.

Machine learning is suitable for handling the growth of digital transactions because it can process large datasets and detect hidden patterns. Instead of depending only on fixed rules, machine learning models learn from past fraud examples and identify abnormal transaction behavior. For example, if a model observes that fraudulent transactions often have unusual transaction amounts, abnormal timing, or repeated transaction attempts, it can use these patterns to classify future transactions. Thus, the growth of digital banking transactions creates both a challenge and an opportunity. The challenge is the increased risk of fraud, while the opportunity is the availability of large transaction datasets that can be used to train intelligent fraud detection models [1-3].

Banking fraud refers to any dishonest or unauthorized activity performed to obtain money, financial benefit, confidential information, or illegal access to a banking system. In the context of digital banking, fraud usually occurs when a fraudster manipulates digital platforms, customer credentials, payment systems, or transaction processes. The objective of such fraud is to transfer money illegally, misuse account information, perform unauthorized purchases, or gain access to sensitive financial data. Banking fraud is a serious problem because it affects customers, banks, merchants, financial institutions, and the overall trust in digital financial systems.

In digital banking, fraud may be committed by external attackers, organized cybercriminal groups, dishonest insiders, or automated malicious software. Fraudsters may use different methods such as phishing messages, fake banking websites, stolen card details, malware, SIM swapping, fake customer support calls, or unauthorized access to mobile banking applications. These methods are continuously changing, which makes fraud detection a complex and dynamic problem. A fraud detection system must therefore identify not only known fraud patterns but also unusual transaction behavior that may indicate new fraud attempts [4].

The concept of fraud detection can be understood as a classification problem. In machine learning, classification means assigning a data record to a particular class. In the case of banking fraud detection, each transaction is generally classified into one of two classes: genuine transaction or fraudulent transaction. A genuine transaction is performed by the authorized customer for a valid purpose, while a fraudulent transaction is performed without proper authorization or with dishonest intention.

Banking fraud detection is challenging because fraudulent transactions are usually very small in number compared with genuine transactions. This creates a class imbalance problem. In a highly imbalanced dataset, a machine learning model may become biased toward the majority class, which is usually the genuine transaction class. For example, if most transactions are genuine, a model may achieve high accuracy by predicting most transactions as genuine, but it may still fail to detect actual fraud cases. Therefore, fraud detection requires evaluation metrics such as precision, recall, F1-score, confusion matrix, receiver operating characteristic curve, and precision-recall curve rather than depending only on accuracy [5].

The concept of banking fraud is also related to risk management. A good fraud detection system must reduce false negatives and false positives. A false negative occurs when a fraudulent transaction is wrongly classified as genuine. This is dangerous because it allows fraud to happen. A false positive occurs when a genuine transaction is wrongly classified as fraud. This creates inconvenience for customers and may reduce trust in banking services. Therefore, an effective fraud detection system must maintain a balance between detecting fraud and avoiding unnecessary blocking of genuine transactions.

ISSN : 2455-9679
SJIF Impact Factor : 6.190

II. METHODOLOGY

2.1 Machine Learning Model Development

The proposed fraud detection system uses supervised machine learning algorithms for binary classification. The selected algorithms include Logistic Regression, Decision Tree, Random Forest, Support Vector Machine, K-Nearest Neighbour, Naïve Bayes, XGBoost, and Artificial Neural Network. These models are selected because they represent different types of classification techniques and allow comparative evaluation.

Logistic Regression is used as a baseline model because it is simple and interpretable. Decision Tree is used because it provides rule-like classification and is easy to understand. Random Forest is included because it combines multiple decision trees and reduces overfitting [6]. Support Vector Machine is used because it can create effective decision boundaries for classification problems [7]. K-Nearest Neighbour is included as a similarity-based model. Naïve Bayes is used as a fast-probabilistic classifier. XGBoost is included because it is a powerful boosting-based model suitable for structured tabular data [8]. Artificial Neural Network is included because it can learn nonlinear patterns from transaction features [9].

All selected models are trained using the same prepared training dataset. After training, each model is tested using the same testing dataset. This ensures fair comparison because each model receives the same input data and is evaluated under the same conditions. The predicted labels are compared with actual labels to calculate evaluation metrics. The model with the best balance between fraud detection and false alarm reduction is selected as the final model. The selected machine learning algorithms are summarized in Table 1.

Table 1: Machine learning algorithms used in the study

S. No.	Algorithm	Type	Reason for Selection
1	Logistic Regression	Linear classifier	Used as a simple and interpretable baseline model.
2	Decision Tree	Tree-based classifier	Provides rule-like classification and easy interpretation.
3	Random Forest	Ensemble classifier	Improves robustness by combining multiple decision trees.
4	Support Vector Machine	Margin-based classifier	Effective for complex class boundaries.
5	K-Nearest Neighbour	Instance-based classifier	Simple method based on similarity between transactions.
6	Naive Bayes	Probabilistic classifier	Fast and computationally efficient baseline model.
7	XGBoost	Boosting-based ensemble classifier	Provides high predictive performance on structured data.

ISSN : 2455-9679
SJIF Impact Factor : 6.190

III. Results and Discussion

3.1 Performance Evaluation of Machine Learning Models

The proposed fraud detection system evaluated eight machine learning models: Logistic Regression, Decision Tree, Random Forest, Support Vector Machine, K-Nearest Neighbour, Naïve Bayes, XGBoost, and Artificial Neural Network. Each model was trained using the prepared training dataset and evaluated using the unchanged testing dataset. The testing dataset contained 56,962 transactions, including 56,864 genuine transactions and 98 fraudulent transactions.

Performance evaluation was performed using multiple metrics. Accuracy was used to measure the overall correct classification rate. Precision was used to measure the reliability of fraud predictions. Recall was used to measure the ability of the model to detect actual fraud cases. F1-score was used to balance precision and recall. ROC-AUC was used to evaluate class separation ability. PR-AUC was used because it is more informative for imbalanced classification problems [10]. The confusion matrix was used to analyze true positives, true negatives, false positives, and false negatives. The comparative performance of all evaluated machine learning models is presented in Table 2.

Table 2: Comparative performance of machine learning models for fraud detection

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	ROC-AUC (%)	PR-AUC (%)
Logistic Regression	99.828	50.00	87.76	63.70	97.50	75.40
Decision Tree	99.916	72.73	81.63	76.92	90.80	72.00
Random Forest	99.953	85.86	86.73	86.29	98.40	87.40
Support Vector Machine	99.896	65.35	84.69	73.78	97.00	76.20
K-Nearest Neighbour	99.919	76.00	77.55	76.77	92.00	73.50
Naive Bayes	98.036	7.07	85.71	13.04	96.30	23.80
XGBoost	99.967	90.72	89.80	90.26	99.10	91.20
Artificial Neural Network	99.949	83.50	87.76	85.57	98.60	86.60

Table 2 shows that most models achieved very high accuracy. However, accuracy values are very close for most models because the dataset contains a very large number of genuine transactions. Therefore, precision, recall, F1-score, ROC-AUC, and PR-AUC provide a better basis for model comparison. XGBoost achieved the highest overall performance with 99.967% accuracy, 90.72% precision, 89.80% recall, 90.26% F1-score, 99.10% ROC-AUC, and 91.20% PR-AUC. Random Forest and Artificial Neural Network also showed strong performance, but their F1-score and PR-AUC values were lower than XGBoost. The accuracy comparison of the machine learning models is shown in Fig. 1.

ISSN : 2455-9679
SJIF Impact Factor : 6.190

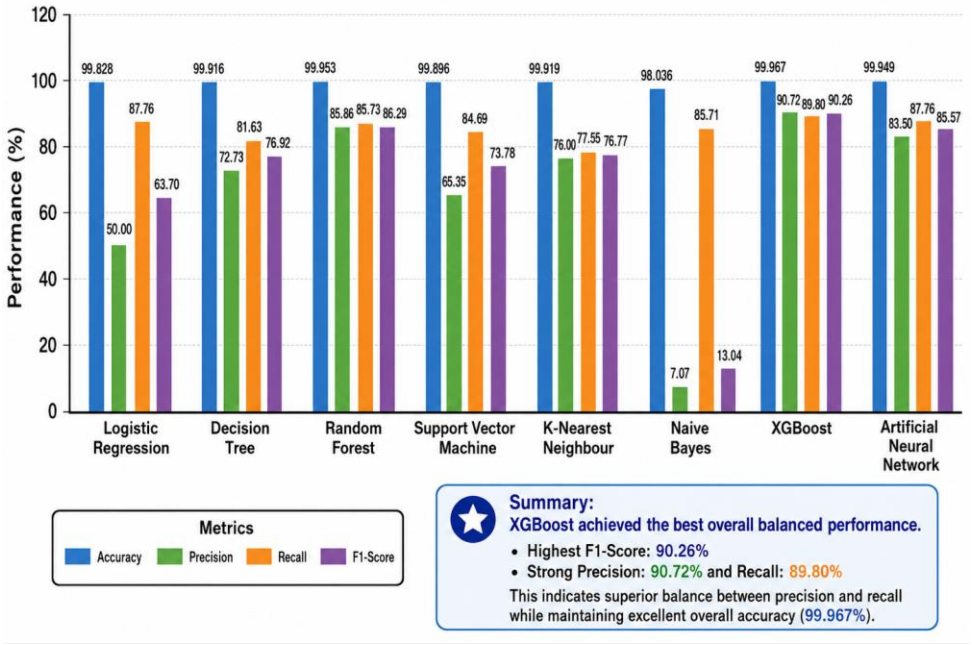

Fig. 1. Accuracy comparison of machine learning models for fraud detection

Figure 1 shows that almost all models achieved high accuracy. XGBoost achieved the highest accuracy, followed by Random Forest and Artificial Neural Network. However, the difference between accuracy values is small. This figure confirms that accuracy alone cannot properly identify the best fraud detection model. A model may show high accuracy because most transactions are genuine, but it may still miss fraud cases. Therefore, fraud-sensitive metrics are required for final model selection. The precision, recall, and F1-score comparison are shown in Fig. 2.

Figure 2 provides a clearer comparison of model performance on the fraud detection task. XGBoost shows the best balance between precision, recall, and F1-score. Logistic Regression achieves good recall but low precision, meaning that it detects many fraud cases but also produces many false positives. Naïve Bayes also shows acceptable recall but extremely low precision, indicating that it wrongly classifies many genuine transactions as fraud. Random Forest and Artificial Neural Network show strong balanced performance, but XGBoost remains superior. The ROC-AUC and PR-AUC comparison of the models is shown in Fig. 3.

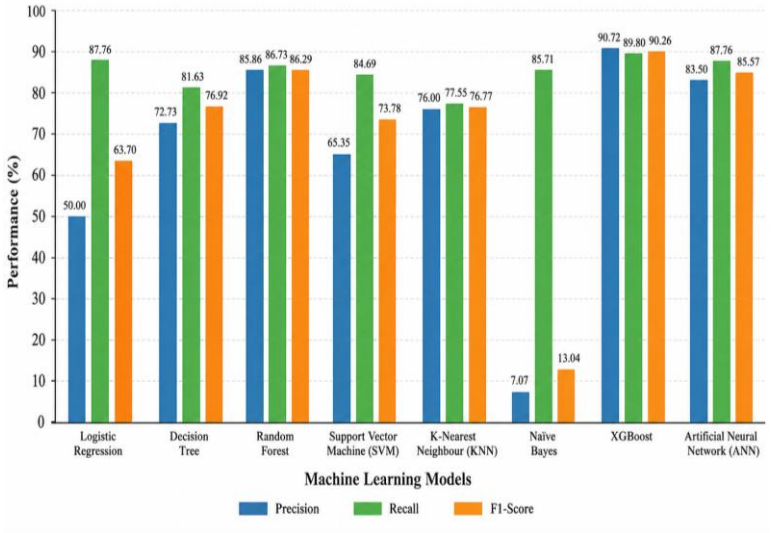

Fig. 3. Precision, recall, and F1-score comparison of machine learning models

ISSN : 2455-9679
SJIF Impact Factor : 6.190

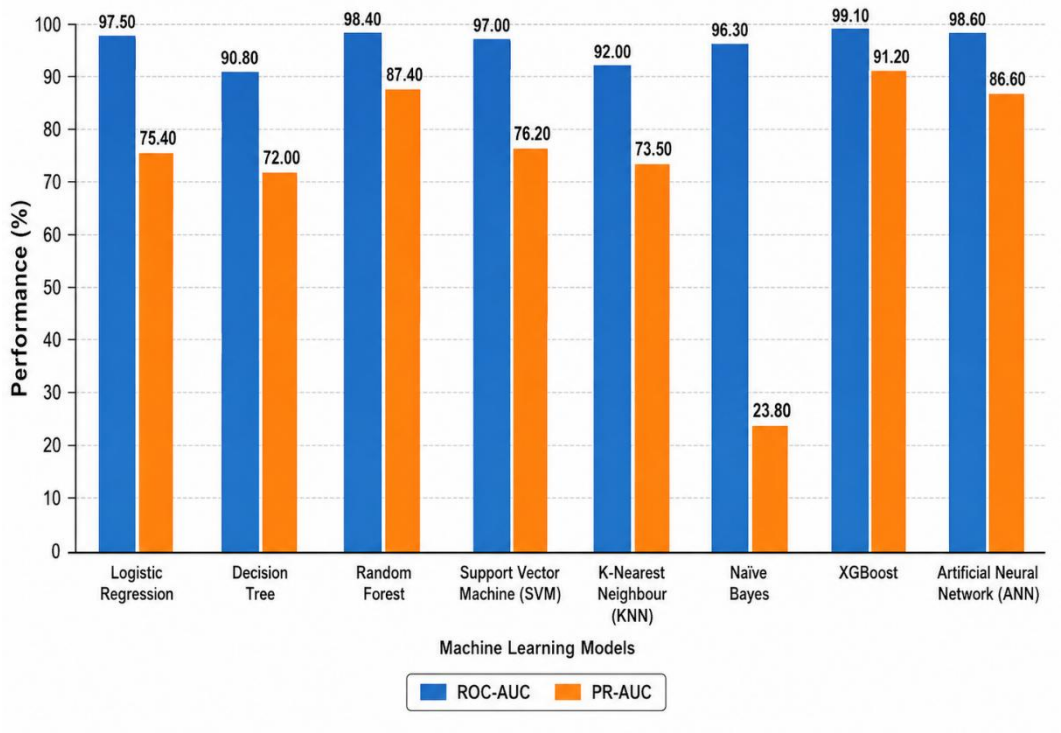

Fig. 4. ROC-AUC and PR-AUC comparison of machine learning models.

Figure 4 compares the curve-based performance metrics of the models. ROC-AUC measures the overall ability of the model to separate genuine and fraudulent transactions. PR-AUC is especially useful in imbalanced datasets because it focuses more directly on the minority fraud class. XGBoost achieved the highest ROC-AUC and PR-AUC values, indicating strong class separation and minority class detection. Random Forest and Artificial Neural Network also performed well, while Naïve Bayes showed poor PR-AUC due to excessive false positives.

3.2 Discussion of Best Performing Model

Based on the comparative evaluation, XGBoost was identified as the best-performing model for the proposed fraud detection system. XGBoost achieved the highest F1-score, ROC-AUC, and PR-AUC among all evaluated models. It also provided the best balance between fraud detection and false alarm reduction. This result indicates that XGBoost is suitable for structured and imbalanced transaction data.

The strong performance of XGBoost can be explained by its boosting-based ensemble structure. XGBoost builds multiple decision trees sequentially, where each new tree attempts to correct the errors of previous trees. This helps the model capture complex and nonlinear relationships between transaction features and fraud labels. Since fraud behavior may be hidden within complex feature interactions, such ensemble learning is useful for fraud detection [11-14]. The performance summary and interpretation of the selected XGBoost model are presented in Table 3.

Table 4: Performance summary and interpretation of the selected XGBoost model

Performance Measure	Value	Interpretation
True Negative	56,855	Genuine transactions correctly classified as genuine
False Positive	9	Genuine transactions wrongly classified as fraud
False Negative	10	Fraudulent transactions wrongly classified as genuine

ISSN : 2455-9679
SJIF Impact Factor : 6.190

Performance Measure	Value	Interpretation
True Positive	88	Fraudulent transactions correctly detected
Accuracy	99.967%	Very high overall classification correctness
Precision	90.72%	Most fraud predictions were actually fraudulent
Recall	89.80%	Most actual fraud cases were detected
F1-Score	90.26%	Strong balance between precision and recall
ROC-AUC	99.10%	Strong class separation ability
PR-AUC	91.20%	Strong minority fraud class detection performance

Table 4 shows that XGBoost correctly detected 88 out of 98 fraud cases in the testing dataset. It missed only 10 fraud cases and generated only 9 false positives. This balance is important for digital banking because false negatives may allow fraudulent transactions to pass, while false positives may inconvenience genuine customers. The high precision indicates that fraud alerts generated by XGBoost are reliable. The high recall indicates that the model detects most fraud cases. The high F1-score confirms that the model maintains balance between fraud detection and false alarm control.

V. CONCLUSIONS

This paper presented a machine learning-based fraud detection system for identifying fraudulent digital banking transactions. The study addressed the growing need for automated fraud detection due to the rapid expansion of internet banking, mobile banking, online payments, and real-time fund transfer services. Since fraudulent transactions are usually much fewer than genuine transactions, the study emphasized the importance of using multiple evaluation metrics rather than relying only on accuracy.

Eight supervised machine learning models were evaluated under the same training and testing conditions. The comparative results showed that although most models achieved high accuracy, their performance varied significantly in terms of precision, recall, F1-score, ROC-AUC, and PR-AUC. Logistic Regression and Naïve Bayes showed good recall but suffered from low precision, which indicates a higher number of false alarms. Random Forest and Artificial Neural Network provided strong and balanced results; however, XGBoost outperformed all other models.

XGBoost achieved the highest overall performance with 99.967% accuracy, 90.72% precision, 89.80% recall, 90.26% F1-score, 99.10% ROC-AUC, and 91.20% PR-AUC. It correctly detected 88 out of 98 fraudulent transactions and produced only 9 false positives. This shows that the model can effectively identify fraud while reducing unnecessary blocking of genuine transactions. The strong performance of XGBoost is mainly due to its ensemble learning structure, which allows it to learn complex and nonlinear relationships in transaction data.

Overall, the study concludes that machine learning is an effective approach for fraud detection in digital banking. Among the evaluated models, XGBoost is the most suitable model for the proposed system because it provides a strong balance between fraud detection capability and false alarm control. The proposed approach can support banks and financial institutions in improving transaction security, reducing financial losses, and maintaining customer trust in digital banking services.

REFERENCES

[1] D. Varmedja, M. Karanovic, S. Sladojevic, M. Arsenovic, and A. Anderla, “Credit card fraud detection: Machine learning methods,” in Proceedings of the 18th International Symposium INFOTEH-JAHORINA,

ISSN : 2455-9679
SJIF Impact Factor : 6.190

East Sarajevo, Bosnia and Herzegovina, 2019, pp. 1–5.

[2] J. M. Johnson and T. M. Khoshgoftaar, "Survey on deep learning with class imbalance," Journal of Big Data, vol. 6, no. 1, article no. 27, Mar. 2019.

[3] A. A. Taha and S. J. Malebary, "An intelligent approach to credit card fraud detection using an optimized Light Gradient Boosting Machine," IEEE Access, vol. 8, pp. 25579–25587, 2020.

[4] K. H. Kalid, K. H. Ng, G. K. Tong, and K. C. Khor, "A multiple classifiers system for anomaly detection in credit card data with unbalanced and overlapped classes," IEEE Access, vol. 8, pp. 28210–28221, 2020.

[5] T. He, G. Cao, and K. Huang, "Using variational auto encoding in credit card fraud detection," IEEE Access, vol. 8, pp. 149841–149853, 2020.

[6] S. Khatri, A. Arora, and A. P. Agrawal, "Supervised machine learning algorithms for credit card fraud detection: A comparison," in Proceedings of the 10th International Conference on Cloud Computing, Data Science and Engineering, Noida, India, 2020, pp. 680–683.

[7] R. Sailusha, V. Gnaneswar, R. Ramesh, and G. R. Rao, "Credit card fraud detection using machine learning," in Proceedings of the 4th International Conference on Intelligent Computing and Control Systems, Madurai, India, 2020, pp. 1264–1270.

[8] Y. Lucas and J. Jurgovsky, "Credit card fraud detection using machine learning: A survey," arXiv preprint arXiv:2010.06479, 2020.

[9] J. Forough and S. Momtazi, "An ensemble deep learning-based approach for credit card fraud detection," Applied Soft Computing, vol. 99, article no. 106883, Feb. 2021.

[10] E. Ileberi, Y. Sun, and Z. Wang, "Performance evaluation of machine learning methods for credit card fraud detection using SMOTE and AdaBoost," IEEE Access, vol. 9, pp. 165286–165294, 2021.

[11] X. Liu, K. Yan, L. B. Kara, and Z. Nie, "CCFD-Net: A novel deep learning model for credit card fraud detection," in Proceedings of the IEEE 22nd International Conference on Information Reuse and Integration for Data Science, Las Vegas, NV, USA, 2021, pp. 9–16.

[12] W. Hilal, S. A. Gadsden, and J. Yawney, "Financial fraud: A review of anomaly detection techniques and recent advances," Expert Systems with Applications, vol. 193, article no. 116429, May 2022.

[13] E. Ileberi, Y. Sun, and Z. Wang, "A machine learning based credit card fraud detection using the GA algorithm for feature selection," Journal of Big Data, vol. 9, article no. 24, Feb. 2022.

[14] F. K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam, M. Ramzan, and M. Ahmed, "Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms," IEEE Access, vol. 10, pp. 39700–39715, 2022.