Journal of Global Research in Electronics and Communication
Volume 1, No. 6, June 2025
Available Online at: www.jgrec.info
RESEARCH PAPER

Evaluating Machine Learning Systems for Banking Fraud Recognition: A Comprehensive Research

Dr. Parth Gautam
Associate Professor
Department of Computer Sciences and Applications
Mandsaur University
Mandsaur
parth.gautam@meu.edu.in

***Abstract*—Financial institutions must prioritize the detection and prevention of fraudulent activities due to the increasing use of digital banking. Integrating intelligent systems is necessary since conventional rule-based systems can't detect new and complicated forms of fraud. Various machine learning (ML) algorithms for banking fraud detection are covered in this study. These algorithms range from more traditional classifiers like Logistic Regression (LR) and Decision Trees (DT) to more advanced models like Random Forest (RF), AdaBoost (AB), eXtreme Gradient Boosting (XGBoost), Support Vector Machines (SVM), and Artificial Neural Networks (ANN). Class imbalance, idea drift, and real-time fraud detection are some of the issues brought up in the review. Research shows that hybrid and ensemble models greatly improve recall, precision, and accuracy. Hybrid methods that combine models, such as HMM and Gradient Boosting (GB), provide enhanced adaptability, while techniques such as Synthetic Minority Oversampling Technique (SMOTE) handle data imbalance. F1-score, recall, accuracy, and precision are among the common measures used in performance evaluation. The paper concludes by identifying the strengths and limitations of each method. It suggests future directions, including using explainable AI and real-time learning for more effective fraud detection systems.**

Keywords—Banking fraud detection, machine learning, classification, SMOTE, ensemble learning, real-time detection, anomaly detection, performance metrics, credit card fraud, hybrid models.

I. INTRODUCTION

The extensive digitization of banking services has revolutionized the way that financial transactions are carried out, allowing consumers to utilize internet-enabled devices to carry out tasks like cash transfers, deposits, and bill payments from almost anywhere [1]. This evolution has made electronic banking the central operational mode for financial institutions in the global economy. The convenience and speed offered by such digital platforms have significantly improved customer experience and operational efficiency. However, the increased threat of banking fraud coincides with this digital revolution, causing significant financial losses for both institutions and clients. As transactions increase in volume and complexity, so do the methods and frequency of fraudulent activities.

Bank fraud detection encompasses a variety of unlawful actions taken by external or internal actors with the intention of obtaining sensitive financial data without authorization. These types of acts are identity theft, data breaches, malware attacks, and advanced fraud schemes [2]. In order to combat the dynamic and sophisticated techniques used by modern fraudsters, conventional fraud detection methods that mostly use pre-established patterns and static rule-based systems are becoming less successful. The weaknesses in such systems form loopholes that can potentially be exploited by the fraudsters, and are usually realized when it is too late and much has gone to waste [3].

Machine learning (ML) approaches have become prominent in this regard, as they can compute immense inflows of transactional data, identify aberrations [4], and modify as fraud patterns change. ML models are able to learn using historical data, detect weak correlations and make predictive decisions, which are superior to those that could be made by a manual or a rule-based system. In this regard, the combination of ML with IoT systems opens additional opportunities to improve fraud detection precision, performance, and responsiveness [5]. Through real-time data and linked devices, and with the aid of clever algorithms [6]. The financial institutions will be able to spot and mitigate fraudulent behavior before it leads to great loss or reputation loss A comparison of many ML methods for identifying bank fraud is provided in this research. To ascertain which algorithms are best at quickly and consistently identifying financial system fraud, the algorithms' accuracy, precision, recall, and F1-score are assessed.

A. Structure of the Paper

The structure of this paper is as follows: Section II provides an overview of and types of banking fraud. Section III introduces the role of ML in fraud detection. Section IV discusses types and challenges of machine learning. Section V presents a literature review and comparative analysis of ML algorithms. Section VI concludes with future research directions.

II. OVERVIEW AND TYPES OF BANKING FRAUD

Banking fraud manifests in various forms, broadly categorized as internal or external. Internal fraud involves dishonest acts by bank employees, while external fraud is perpetrated by clients or external entities. This paper focuses specifically on external fraud, which poses significant threats to financial institutions through unauthorized access, identity theft, and other illicit activities targeting banking systems and customer data.

A. Money laundering

Fraud is also known to include money laundering. Several governments pursue international legislation against this practice in order to identify and bring criminal charges against those involved. Financial institutions' examination and processing of information pertaining to questionable

transactions is the foundation of the financial industry's battle against money laundering. Only a small percentage of questionable transactions are typically money laundering schemes. But financial organizations need a lot of time to analyze the quantity of activities. These unauthorized operations are produced by complicated socioeconomic situations, making money laundering factors and indices easier to discern [7]. A few money bleaching indices that are utilized in the literature are as follows: The transaction is not justified and is thus suspicious if the amount exceeds a certain threshold set by the bank. For example, you shouldn't use your credit card to make transactions in Ghana that cost more than 5,000 euros. The following are looked at in further detail. 1). Transfer sources 2). The transaction date 3). The address change 4). The timing of the transaction: large-value transfers performed at night are suspicious.

B. Credit Cards Based Fraud

Credit card fraud is still on the rise. Credit card fraud costs financial institutions a pretty penny every year. Not to mention [8]. Several prognosis indications that are often derived from transaction data obtained from the historical database are frequently used as the foundation for the identification of credit card fraud. Look at indicators like how often the card is used [9], the highest frequency of late days, daily transactions, daily shopping, the highest frequency in the historical database, the amount that is still outstanding at the conclusion of each cycle, etc. These features are obtained for each transaction and documented in order to spot patterns in fraudulent transactions. In Figure 1, the fraud detection model is displayed. The proposed algorithm is used to determine whether the result is fake, and the historical data that forms the basis of the suggested data model is already present in the bank's warehouse. The model's efficacy will be predicted using a collection of comparable data. The model assesses a new transaction; if it is accepted, it is executed and entered into the database to improve the model. Instead of being processed, transactions that the model rejects are marked as suspicious.

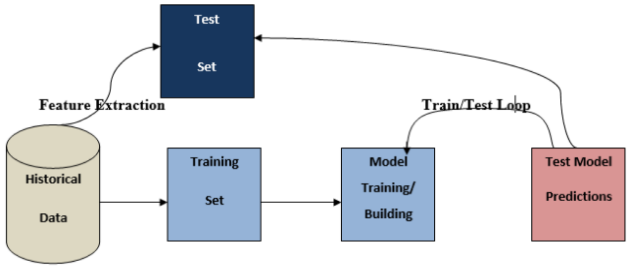

Fig. 1. Fraud Detection Model

C. Forgeries

The practice of forging involves the fraudulent duplication and use of a customer's signature in order to withdraw large amounts of money from their account without the customer's prior authorization. These forgeries may target transfer papers such as drafts, current accounts, savings accounts, or deposit accounts. Experience has shown that most of these forgeries are executed by internal employees or by outside parties collaborating with bank employees, who frequently disseminate the forged specimen signatures.

D. Defalcation

This entails the theft of funds that bankers hold in trust on behalf of their clients [10]. The refusal of customers' deposits, which can happen through conversion or dishonest manipulation of deposit vouchers by the customer or the bank teller, is a common kind of bank fraud. This kind of fraud is usually executed with elegance and is more difficult to uncover when the consumer and the bank teller collude. The clients can only be easily located once their bank accounts have been reconciled. Other examples of dishonesty include collaborating with a customer's agent when the agent transfers funds into the customer's account and taking notes from money that should be paid to unsuspecting clients or customers.

E. Causes of Bank Fraud

Institutional factors and environmental or social variables are the two primary kinds of causes of fraud, according to several scholars. Institutional variables pertain to the internal environment of the bank, whereas environmental or social elements are those that arise from the impact of society or the environment on the banking sector [11]. categorized institutional or endogenous and environmental or external elements as the main causes of bank frauds and forgeries. The external causes he highlighted include low moral norms in society, ineffective deterrents and punishments, and fear of bad press. The endogenous elements include things like a weak internal control system, inexperienced employees, and low compensation. Here are some examples of institutional factors: Poor management, as evidenced by incapacity, insufficient oversight, poor leadership, insufficient controls, etc., and a weak internal control system.

III. Machine Learning in Fraud Detection

As ML can read through lots of information quickly, it is very helpful in spotting signs of fraudulent transactions. ML algorithms, in contrast to traditional rule-based systems, are capable of handling novel types of fraud and identifying difficult-to-notice behaviors [12]. Using methods like classification and anomaly detection, machine learning increases accuracy, lowers the risk of wrongly suspecting someone, and allows real-time detection, so it is effective against financial fraud.

A. Embracing Change: The Intervention of Machine Learning

Machine Learning (ML) emerges as a formidable alternative, steering away from traditional paradigms [13]. By allowing algorithms to identify intricate links and learn from past data [14]. ML introduces numerous advantages:

- **Adaptability:** ML algorithms mitigate the rigidity of static rules by continually learning from current data to adapt to emerging fraud types on their own.
- **Scalability:** ML algorithms excel at processing extensive datasets, effectively scrutinizing intricate patterns across millions of transactions—a task beyond the capacity of manual analysis.
- **Predictive prowess:** Advanced ML techniques may be able to forecast future fraudulent conduct in addition to identifying existing fraud, enabling proactive intervention and preventative measures.

B. Types of Machine Learning

ML algorithms may be divided into four main categories: The differences between learning with and without supervision [15], Figure 2 shows reinforcement learning and semi-supervised learning.

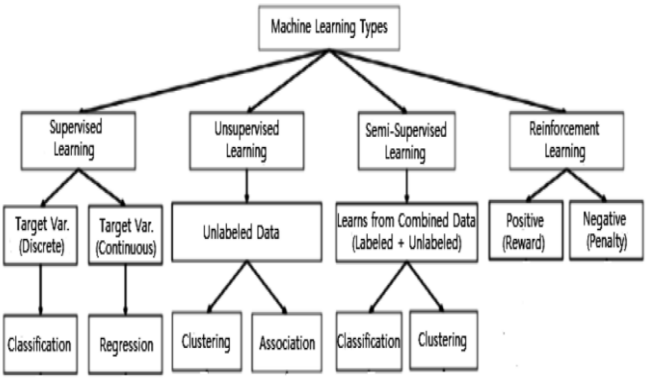

Fig. 2. Types of machine learning

1) Supervised Learning:

Training a function that maps an input to an output usually involves using example input-output pairs in supervised learning in ML. It infers a function from a set of training samples and labelled training data. Supervised learning, often known as a task-driven approach, is employed when specific objectives need to be fulfilled using a predefined set of inputs. In supervised learning, the two most prevalent operations are "regression," which involves fitting the data, and "classification," which involves separating the data. One use of supervised learning with text categorization is the prediction of the class label or mood of textual items like tweets or product reviews.

2) Unsupervised Learning:

A data-driven method known as unsupervised learning evaluates unlabeled data without requiring human involvement. Finding important patterns and structures, doing exploratory research, extracting generative qualities, and aggregating discoveries are all common uses for this. Learning features, dimensionality reduction, clustering, density estimation, anomaly detection, association rule identification, and other unsupervised learning tasks are among the most commonly utilized ones.

3) Semi-Supervised Learning:

Operating on both labelled and unlabelled data, semi-supervised learning combines elements of both supervised and unsupervised approaches. So, it's neither too far from learning "without supervision" nor too far from learning "with supervision." In real-world situations, semi-supervised learning could be highly beneficial when there is an abundance of unlabelled data but a shortage of labelled data. A semi-supervised learning model's end goal is to outperform the model's performance with just the labelled input in terms of prediction accuracy. Several domains employ semi-supervised learning techniques, including machine translation, data labelling, text categorization, and fraud detection.

4) Reinforcement Learning:

Machine learning techniques like reinforcement learning, which use an environment-driven approach, allow computers and software agents to perform at their best by automatically deciding what to do in every given situation [16]. Using the information provided by environmental activists, the end goal of this technique for learning is to take actions that will either raise the reward or decrease the danger. Although it is a great tool for training AI models, it is not recommended to use it to tackle simple or elementary problems. But it might speed up automation or make complex systems like manufacturing, supply chain logistics, autonomous vehicles, and robots even more effective.

C. Challenges in Machine Learning

Despite the promising capabilities of ML in banking fraud detection, several challenges remain that affect the performance and practical implementation of these models. This section discusses key challenges faced when applying machine learning to banking fraud detection, including:

1) Real-Time Fraud Detection:

Recognizing fraudulent activity in real-time is one of the key achievements of this study. A data warehouse, fraud detection models, and application programming interface (API) module comprise the real-time fraud detection system for the most part. Every component is used concurrently in the identification of fraud. Fraudulent transactions are categorized into four classes using three supervised learning classifiers: transactions above $100, ISO-Response Code, Risky MCC, and Unknown Web Address [17]. Transactions between the data warehouse, GUI, and fraud detection model are exchanged in real time using the API module. Important data from ML models, such as real-time transactions and anticipated outcomes, are stored in a data warehouse[18]. The fraud detection system may be accessed by the user using graphical user interfaces (GUIs), which show the fraud history, fraud alerts, and real-time transactions in a graphical style. The API module will get a notification if the fraud detection model finds that a transaction is fraudulent. The end user will then receive a notification and feedback from the API module.

2) Concept Drift

The identification of fraud is particularly difficult for two reasons: frauds only make up a small portion of daily transactions, and their distribution changes over time due to seasonality and emerging attack techniques [19]. Concept drift is the term used to describe this condition, which is extremely relevant for FDSs that must be updated continuously either by using the most current supervised samples or by forgetting old knowledge that may no longer be relevant but is not deceptive.

3) Data Imbalance

The problem with imbalanced datasets is that most ML algorithms assume that the majority and minority classes are similarly distributed. This results in poor predictive modelling performance and erroneous discoveries [20]. Furthermore, in the case of other complicating conditions like class overlap, the imbalance issue seems to be associated to learning with too few minority class instances. One well-known method for dealing with this issue head-on is SMOTE-ENN, or the Synthetic Minority Over-Sampling Technique with Edited Nearest Neighbors. It uses ENN for data cleaning and SMOTE for oversampling to eliminate class, overlap, and produce more distinct class clusters.

IV. Comparative Analysis of ML Algorithms

The goal of ML, a rapidly evolving discipline of computer algorithms, is to imitate human intelligence by learning from its environment. It is believed that ML is the foundation of big data technology [21]. Data science, artificial intelligence, and the fields of computer science and statistics all use ML as its cornerstone. ML is often used in the financial sector to provide algorithm-based forecasts.

A. Machine Learning Algorithms

The detection of financial fraud depends on ML algorithms that automatically recognize complex patterns and anomalies in transaction data. Below is a discussion of a few ML algorithms.

1) Decision Tree

A decision-making process diagram, or DT, is a framework that looks like a flowchart. There are three types of nodes in a decision tree: internal (representing attributes), branching (representing the results of the test), and leaf (representing the final decision or class label) [22]. The structure is composed of nodes and branches: the nodes indicate the attributes being evaluated, while the branches represent the possible values or outcomes of those attributes. DT are very popular in classification due to their interpretation and logical appeal. As shown in Figure 3, the typical structure of a DT is as follows.

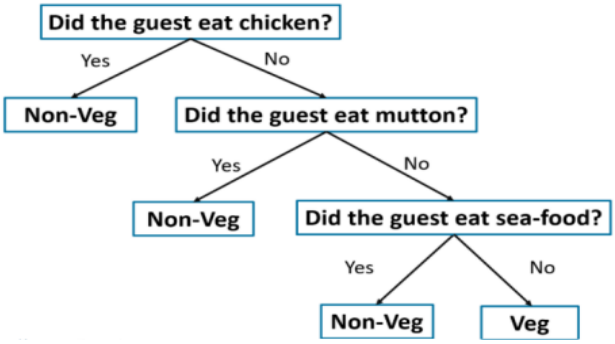

Fig. 3. Decision Tree

2) Naive Bayes

The core tenets of the Bayes-Schrodinger Theorem-based probabilistic taxonomy modality known as NB are the assumption that characteristics are conditionally independent. In this case, the classifier establishes the requirement that a characteristic's presence or absence within a group is unrelated to the presence or absence of other traits. Despite being a simple algorithm, NB performs exceptionally well, particularly in text categorization problems such as spam recognition and sentiment analysis. It is based on the conditional likelihood of feature occurrence given a class and is very useful in classification and clustering procedures. Figure 4 illustrates the formula that represents Bayes' Theorem and the elements that NB Classification entails.

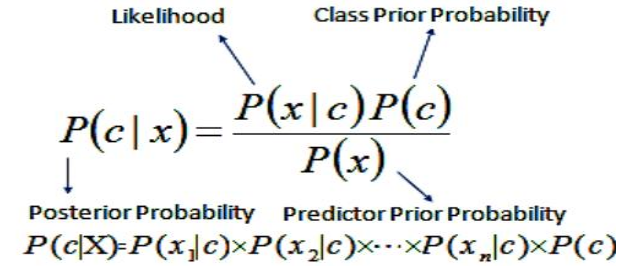

Fig. 4. Naive Bayes

3) Support Vector Machine (SVM)

SVM are the gold standard of supervised ML algorithms when it comes to classification and regression situations. SVM is a technique that searches for a hyperplane that can maximize the distance between the hyperplane and the separated classes in order to identify the best hyperplane within the dataset. By maximizing such a margin, the reduction of classification error and enhancing generalization is achieved [23]. Support vector machines (SVMs) excel in linear classification by assuming the classified problem is linearly separable; however, they may also tackle non-linear problems by employing kernel functions, which implicitly translate the input space to higher-dimensional spaces. Figure 5 shows the simplest idea of SVM, i.e., two different classes are segregated via a border (hyperplane) in between with the biggest possible distances (margin) in between. The data points closest to the margin, or support vectors, are also crucial for identifying this border and offering reliable categorization.

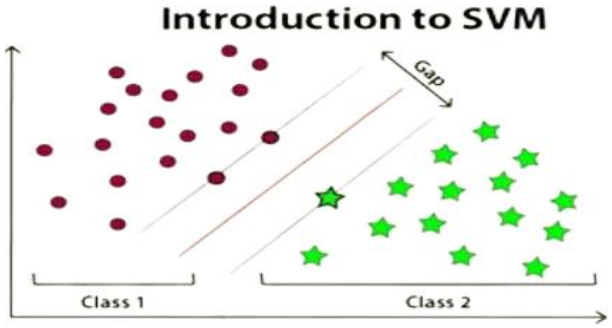

Fig. 5. Support Vector Machine

B. Performance Metrics

The models' performance was evaluated using a performance matrix that contrasted the values produced by the models with the observed values. The performance matrix contained performance parameters, including F1-score, recall, and accuracy [24]. A number of levels were used to calculate the metrics: The number of correctly classified negative cases is called True Negatives (TN), while the number of correctly identified positive occurrences is called True Positives (TP). Whereas False Positives (FP) refer to the frequency of findings that are erroneously classified as positive, False Negatives (FN) refer to the frequency of outcomes that are wrongly categorized as negative.

1) Accuracy

The accuracy score is the ratio of correctly predicted occurrences to all cases [25]. Shown is the model's performance in every category. The given Equation (1) can be seen below:

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

2) Precision

Precision is defined as the ratio of expected positive instances to true positives. Its primary use is in lowering the incidence of FP. Equation (2) displays:

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

3) Recall

The percentage of TP that the model properly detects is known as recall. It is crucial when minimizing false negatives. Equation (3) is shown in:

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

4) F1-Score

The F1-score equalizes FP and FN by averaging recall and accuracy harmonically. It is particularly helpful for assessing models using datasets that are unbalanced. The formula is shown in Equation (4):

$$F1 - SCORE = \frac{Precision * Recall}{Precision + Recall} \quad (4)$$

V. Literature of Review

This literature review section explores various ML techniques for banking fraud detection, highlighting classifiers such as RF, XGBoost, AdaBoost, and neural networks for their accuracy, efficiency, and adaptability.

Mishra, Biswal and Padhy (2025) have used several ML classifiers to detect fraudulent behavior in the banking system. They used classifiers like: - LR, RF, SVM, KNN, GB, AdaBoost, and DT. have calculated the accuracy, precision, recall, and F1-scoire of these classifiers. Result: From the experimental observation they found that RF gives the highest accuracy of 0.985, Recall at 0.985000 and the classifier KNN has the highest score at 0.988937. It indicates that RF is the best classifier in comparison to others for detecting fraud in the banking system Simultaneously the classifiers AdaBoost and Gradient Boosting provide good precision and AUC-ROC values [26].

Murugamani et al. (2025) applied an ML-oriented system for banking data fraud detection. To fix the problem of the groups not being balanced, the Synthesized Minority over-sampling technology (SMOTE) was employed to resample the database. It was found that the Adaptable Booster (AdaBoost) method worked best with these ML techniques when it came to classification. To test the methods, performance matrices were used. The tests showed that using AdaBoost makes the suggested methods work better. In addition, the improved processes led to better results than the old methods. The research's findings support the efficacy of creating fraud identification methods for e-commerce platforms utilizing automated ML techniques [27].

Singh et al. (2024) demonstrate the effectiveness of technology as a standard in detecting fraud. Algorithms process as much data as possible to optimize efficiency, acquire insight, and boost security. When spotting fraudulent transactions on the Internet, these algorithms are useful. The unique internet business dataset may be obtained here. Then, using ML algorithms, anomalies or specific patterns in the data are discovered, aiding in the detection of fraud. For optimal outcomes, the XGBoost algorithm is a DT. Recently, this algorithm was introduced to the machine. Therefore, putting an end to the scammers' actions is essential. The experience becomes more real as additional layers are added [28].

Singh et al. (2024) Evaluate the performance of XGBoost and ANN, two well-known ML methods, in detecting fraudulent credit card purchases. Examine various approaches utilizing a freely available dataset of credit card transactions in terms of accuracy, precision, recall, and F1 score. Another area that the study looks into is the computation performance and scalability of ANNs and XGBoost to identify their applicability in a real-time fraud detection system. ANNs achieve the highest accuracy at 96.9%, surpassing all five methods evaluated, while XGBoost, with an accuracy of 92.7%, outperforms all other classifiers. These findings illustrate the advantages and disadvantages of each strategy, offering financial organizations trying to develop or enhance fraud detection systems useful information [29]

Thar and Wai (2024) intend to do predictive modelling based on ML to enhance fraud detection and prevention inside a public or private economic body. This study's primary objective is to offer a new, intelligent, self-governing ensemble method for identifying fraudulent transactions. To begin with, the Hidden Markov Model (HMM), which is used in order to observe the hidden states of financial transactions, is constructed on a probabilistic representation of a sequence of observations, the underlying process of which is believed to be a Markov process with unobservable states. To categories the fraud, a machine learning model known as the Gradient Boosting Classifier (GBC) is then used. Lastly, they combine GBC and HMM in their hybrid approach. To make sure that HMM and GBC work, experiments are carried out [30].

Dash et al. (2023) Compare more modern ML technologies like neural networks with more traditional methods like LR and DT. The methods are applied to actual banking and financial data, and the outcomes demonstrate that neural networks perform better than the more traditional methods. Moreover, the significance of data compilation and management in fraud detection system development will be the sphere of their study [31].

Table I provides an overview of the literature evaluation, including information on each study's topic, methodology, main conclusions, limitations, and future prospects.

TABLE I. Comparative Analysis of study on Machine Learning Algorithms for Banking Fraud Detection

Reference	Study On	Approach	Key Findings	Challenges	Future Direction
Mishra, Biswal and Padhy (2025)	ML classifiers for fraud detection	LR, RF, SVM, KNN, GBC, AdaBoost, DT; SMOTE for imbalance	RF achieved highest accuracy (98.5%) and recall; KNN highest F1-score; AdaBoost and GBC good AUC	Class imbalance and variance in classifier performance	Explore hybrid models and ensemble learning with further optimization
Murugamani et al. (2025)	SMOTE + AdaBoost for fraud classification	Used SMOTE for balance; applied AdaBoost for classification	AdaBoost performed best among tested models; enhanced classification metrics	Handling imbalance and maintaining generalization	Group models should be improved and used for real-time fraud detection. Apply improved group models to the problem of real-time fraud detection.
Singh et al. (2024)	Fraud detection in online shopping	XGBoost-based decision tree model	XGBoost is effective in detecting anomalies; increases system security	Need for dataset quality and complexity handling	Integrate deeper ensemble methods and scalable ML frameworks
Singh et al. (2024)	ANN vs XGBoost in credit card fraud	Compared ANN and XGBoost using standard metrics	ANN highest accuracy (96.9%), XGBoost second-best (92.7%)	Scalability and computational efficiency	Focus on lightweight ANN models for real-time deployment
Thar and Wai (2024)	Hybrid fraud detection system	HMM for sequences + Gradient Boosting	HMM-GBC hybrid improved detection accuracy and reliability	Sequence modeling complexity and system integration	Refine HMM-GBC integration for dynamic fraud trends

Dash et al. (2023)	Classic vs modern ML in fraud detection	Compared NN to decision trees and logistic regression.	Traditional models are outperformed by neural networks.	Data management and quality issues	Improve data preprocessing pipelines and scalable neural architectures

VI. Conclusion And Future Work

Increased digital banking has posed a great threat to fraud related activities and thus conventional fraud detection systems are no longer effective. This review will give a detailed report into the different ML algorithms applied to the detecting of banking fraud namely LR, DT, RF, SVM, KNN, AdaBoost, XGBoost, and ANN. Researchers state that ensemble algorithms like RF and AdaBoost, DL models like ANN are more precise and stable, especially when they were joined with data-balancing techniques like SMOTE. The HMM-equipped eventualities of GB (hybrid) also enhance the systems to detect frauds as they capture both the series and the classification performance. Nevertheless, there are still some challenges, e.g., imbalance of classes, concept drift, and the inability to develop real-time systems with high accuracy and few false positives.

The goal of future studies should be to develop real-time fraud detection systems that are scalable, lightweight, and capable of adjusting to new fraud techniques. This includes integrating semi-supervised or online learning techniques, exploring explainable AI to improve transparency, and optimizing hybrid models for operational efficiency. In addition, the preprocessing of the data needs to be improved, and computational requirements need to be minimized and models must be made applicable in different banking conditions and types of transactions.

References

[1] F. L. Becerra-Suarez, H. Alvarez-Vasquez, and M. G. Forero, "Improvement of Bank Fraud Detection Through Synthetic Data Generation with Gaussian Noise," *Technologies*, vol. 13, no. 4, 2025, doi: 10.3390/technologies13040141.

[2] M. N. Alatawi, "Detection of fraud in IoT based credit card collected dataset using machine learning," *Mach. Learn. with Appl.*, vol. 19, p. 100603, Mar. 2025, doi: 10.1016/j.mlwa.2024.100603.

[3] S. Tyagi, "Analyzing Machine Learning Models for Credit Scoring with Explainable AI and Optimizing Investment Decisions," *Am. Int. J. Bus. Manag.*, vol. 5, no. 01, pp. 5–19, 2022.

[4] R. Zhang, Y. Cheng, L. Wang, N. Sang, and J. Xu, "Efficient Bank Fraud Detection with Machine Learning," *J. Comput. Methods Eng. Appl.*, no. October 2023, pp. 1–10, 2023, doi: 10.62836/jcmea.v3i1.030102.

[5] K. M. R. Seetharaman, "Internet of Things (IoT) Applications in SAP: A Survey of Trends, Challenges, and Opportunities," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 3, no. 2, pp. 499–508, Mar. 2021, doi: 10.48175/IJARSCT-6268B.

[6] H. Kali, "Optimizing Credit Card Fraud Transactions Identification and Classification in Banking Industry Using Machine Learning Algorithms," *Int. J. Recent Technol. Sci. Manag.*, vol. 9, no. 11, pp. 85–96, 2024.

[7] B. Ramanujam, "Statistical in Sights in to Anti-Money Laundering: Analyzing Large-Scale Financial Transactions," *Int. J. Eng. Res. Technol.*, vol. 14, no. 4, 2025, doi: 10.17577/IJERTV14IS040136.

[8] S. J. Wawge, "A Survey on the Identification of Credit Card Fraud Using Machine Learning with Precision, Performance, and Challenges," *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 4, 2025, doi: 10.38124/ijisrt/25apr1813.

[9] H. Kali, "Diversity, Equity, and Inclusion Analytics in HR : How Workday Enables Data-Driven Decision-Making," vol. 3, no. 2, pp. 162–170, 2023, doi: 10.56472/25832646/JETA-V3I6P113.

[10] E. J. Idolor, "Bank frauds in Nigeria: Underlying causes, effects and possible remedies," *African J. Accounting, Econ. Financ. Bank. Res.*, vol. 6, no. 6, pp. 62–81, 2010.

[11] K. Clementina and I. G. Isu, "Security Challenge, Bank Fraud and Commercial Bank Performance in Nigeria: An Evaluation," *J. Bus. Manag.*, vol. 5, no. 2, pp. 1–21, 2016, doi: 10.12735/jbm.v5n2p01.

[12] R. Q. Majumder, "A Review of Anomaly Identification in Finance Frauds Using Machine Learning Systems," *Int. J. Adv. Res. Sci. Commun. Technol.*, pp. 101–110, Apr. 2025, doi: 10.48175/IJARSCT-25619.

[13] A. Olushola and J. Mart, "Fraud Detection using Machine Learning." 2024. doi: 10.14293/PR2199.000647.v1.

[14] R. Q. Majumder, "Machine Learning for Predictive Analytics: Trends and Future Directions," *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 4, pp. 3557–3564, 2025.

[15] I. H. Sarker, "Machine Learning: Algorithms, Real-World Applications and Research Directions," *SN Comput. Sci.*, 2021, doi: 10.1007/s42979-021-00592-x.

[16] S. Shah and M. Shah, "Deep Reinforcement Learning for Scalable Task Scheduling in Serverless Computing," *Int. Res. J. Mod. Eng. Technol. Sci.*, vol. 3, no. 12, Jan. 2021, doi: 10.56726/IRJMETS17782.

[17] S. P. M Shah, "AI/ML Techniques for Real-Time Fraud Detection," *DZone*, 2025.

[18] A. Thennakoon, C. Bhagyani, S. Premadasa, S. Mihiranga, and N. Kuruwitaarachchi, "Real-time credit card fraud detection using machine learning," in *Proceedings of the 9th International Conference On Cloud Computing, Data Science and Engineering, Confluence 2019*, 2019. doi: 10.1109/CONFLUENCE.2019.8776942.

[19] A. Dal Pozzolo, G. Boracchi, O. Caelen, C. Alippi, and G. Bontempi, "Credit card fraud detection and concept-drift adaptation with delayed supervised information," in *2015 International Joint Conference on Neural Networks (IJCNN)*, 2015, pp. 1–8. doi: 10.1109/IJCNN.2015.7280527.

[20] E. F. Malik, K. W. Khaw, B. Belaton, W. P. Wong, and X. Chew, "Credit Card Fraud Detection Using a New Hybrid Machine Learning Architecture," *Mathematics*, 2022, doi: 10.3390/math10091480.

[21] M. Hasan, A. Hoque, and T. Le, "Big Data-Driven Banking Operations: Opportunities, Challenges, and Data Security Perspectives," *FinTech*, vol. 2, no. 3, pp. 484–509, 2023, doi: 10.3390/fintech2030028.

[22] T. U. Roberts, A. Polleri, R. Kumar, R. J. Chacko, J. Stanesby, and K. Yordy, "Directed Trajectories Through Communication Decision Tree using Iterative Artificial Intelligence," 11321614, 2022

[23] B. Mahesh, "Machine Learning Algorithms - A Review," *Int. J. Sci. Res.*, vol. 9, no. 1, pp. 381–386, 2020, doi: 10.21275/art20203995.

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

[25] T. Al-quraishi, O. Albahri, A. Albahri, and A. Alamoodi, "Bridging Predictive Insights and Retention Strategies : The Role of Account Balance in Banking Churn Prediction," pp. 1–28, 2025.

[26] J. Mishra, B. B. Biswal, and N. Padhy, "Machine Learning for Fraud Detection in Banking Cyber security Performance Evaluation of Classifiers and Their Real-Time Scalability," in *2025 International Conference on Emerging Systems and Intelligent Computing (ESIC)*, 2025, pp. 431–436. doi: 10.1109/ESIC64052.2025.10962752.

[27] C. Murugamani, V. Sivakamy, V. Vimala, P. Dayalan, K. Al-Said, and N. Al Said, "Machine Learning for Fraud Detection in Banking Systems," in *2025 International Conference on Pervasive Computational Technologies (ICPCT)*, 2025, pp. 416–420. doi: 10.1109/ICPCT64145.2025.10941200.

[28] R. Singh, J. Sekar, P. Ahmad, and V. Ahmad, "Online Payments Fraud Detection with Machine Learning Algorithm," in *2024 1st International Conference on Advances in Computing,*

Communication and Networking (ICAC2N), IEEE, Dec. 2024, pp. 371–373. doi: 10.1109/ICAC2N63387.2024.10894819.

[29] A. Singh, K. S. Gill, M. Kumar, and R. Rawat, "Beyond Traditional Methods: Evaluating Advanced Machine Learning Models for Superior Fraud Detection," in *2024 4th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS)*, 2024, pp. 297–300. doi: 10.1109/ICUIS64676.2024.10866102.

[30] K. W. Thar and T. T. Wai, "Machine Learning Based Predictive Modelling for Fraud Detection in Digital Banking," in *2024 IEEE Conference on Computer Applications (ICCA)*, 2024, pp. 1–5. doi: 10.1109/ICCA62361.2024.10532788.

[31] S. Dash, S. Das, S. Sivasubramanian, N. K. Sundaram, H. K. G, and T. Sathish, "Developing AI-based Fraud Detection Systems for Banking and Finance," in *2023 5th International Conference on Inventive Research in Computing Applications (ICIRCA)*, 2023, pp. 891–897. doi: 10.1109/ICIRCA57980.2023.10220838.

