INNOVARE JOURNAL OF ENGINEERING & TECHNOLOGY

INNOVARE ACADEMIC SCIENCES
Knowledge to Innovation

Vol 13, 2025

ISSN - 2347-1573

Research Article

ANALYSIS OF MACHINE LEARNING METHODS PERFORMANCE IN TRANSACTIONS OF CREDIT CARD FRAUD IN ONLINE BANKING

MANISH JAIN*

Department of Electronics and Communications, Mandsaur University, Mandsaur, Madhya Pradesh, India.
Email: manish.jain@meu.edu.in

Received: 17 September 2025, Revised and Accepted: 22 November 2025

ABSTRACT

In Online Banking, fraud is increasing day by day. The different types of fraud include data breaches, unauthorized access, and authentication-like attacks. The conventional system in which password password-based, has declined in reliability, achieving only moderate performance to enhance to detect fraud. Online banking credit card fraud (CCF) is the basis of this research. The research adhered to the processing steps, which included data cleansing (which involved dealing with missing information and deleting duplicates) and standardization, using CCF data. The following step is label encoding, which enables the model to perform mathematical calculations. Then, it uses IHT to deal with data that contains imbalanced classes. The k-fold cross-validation method then splits the data in half. Multilayer Perceptrons and K-Nearest Neighbors are also part of the Ensemble model, which also includes Decision Trees and Random Forest. Every model in the ensemble contributes something useful, which boosts the overall performance. Outperforming LSTM, GBM, and neural network models, the ensemble model attained the highest accuracy (ACC) of 99.99%. The power of the ensemble model lies in its capacity to integrate numerous models. The results of the model demonstrate its top performance, scalability, and dependability.

Keywords: Credit card fraud, Online banking, Machine learning, Digital payments, Fraud transactions, Deep learning, Predictive analytics.

DOI: http://dx.doi.org/10.22159/ijet.2025v13.57902. Journal homepage: https://innovareacademics.in/journals/index.php/ijet

INTRODUCTION

Digital payments and online banking have expanded rapidly, creating substantial benefits but also enlarging the attack surface for financial fraud [1]. The banking industry is one of the most successful and strong industries in the country. The banking structure is affected by the changing environment of an economy. Internet banking, sometimes called e-banking, is a system that allows customers to do a range of financial activities from any location with an internet connection, whether it's their home, business, or any other secure network [2]. Credit-card and online-banking fraud now account for a large proportion of detected financial crime, and they manifest as highly imbalanced, evolving classification problems where fraudulent events are rare, heterogeneous, and concept-drifting over time.

Credit cards allow customers to make purchases worldwide at their convenience by storing personal information on a piece of plastic that is issued by financial service providers. Credit card fraud (CCF) refers to the theft of another person's funds by making unauthorized purchases using their credit card, and it may happen anywhere, even in person. A lot of money is frequently lost due to CCF. Online purchases do not require physical cards, and the information on the card is sufficient to make a payment, making it easier to perpetrate fraud than in the past [3]. Both customers and financial institutions are vulnerable to the high-stakes financial losses and damaged reputations that can ensue from these kinds of actions. Plus, traditional approaches cannot keep up, which means more cases of fraud going unnoticed or, worse, more cases of FP, when real transactions are incorrectly marked as fraudulent [4]. This can create frustration for consumers and inefficiencies for financial institutions. Financial institutions should therefore prioritize these automated fraud detection systems.

Fraudulent actions in the banking sector have been uncovered by the application of data mining, ML, and AI [5,6]. To forecast fraud activities, both supervised and unsupervised techniques were used. The most widely used technique for identifying financial fraudulent activities has been classification. ML techniques for fraud transactions, such as the stock market and other financial industry fraud detection procedures [7,8]. Supervisory learning algorithms that are frequently employed in fraud detection include DTs, RF, and SVMs. Algorithms are trained to differentiate between valid and fraudulent transactions by analyzing tagged data [9]. Furthermore, the variety of money transaction patterns among financial firms has increased the difficulty of detecting fraud. User demographics and operational conditions can have a substantial impact on fraud behaviors [10]. To lessen losses to a specific cardholder or the bank, the project intends to create and evaluate an ensemble model for fraudulent transaction recognition in credit cards based on ML techniques.

The study is motivated by the growing amount and complexity of financial transactions in digital payment systems, which have greatly broadened the field and scope of fraud detection. Conventional rule-based systems tend to be insufficient to detect the changing fraud patterns, especially in large-scale and extremely imbalanced data, where the valid transaction numbers are significantly higher than the fraudulent transactions. With the increasing online banking and credit card transactions, real-time detection of uncommon and evolving fraud trends has become a major dilemma for financial institutions. To counter this problem, this study offers an all-encompassing ML-driven system for detecting fraud in credit card and internet banking settings. The contributions made in this study are as follows:

- Created a system to mimic conventional fraud detection scenarios using anonymized real-world European cardholder transaction data from the publicly available Kaggle CCF Detection dataset
- Processed missing values, removed duplicates, normalized features through standardization, and encoded labels to clean the data and prepare it for modeling
- Applied data balancing using the IHT undersampling technique to address class imbalance and enhance minority class detection
- During training, feature scaling and transformation are used to improve model stability and convergence

- Created a powerful fraud detection ensemble model by integrating DT, RF, KNN, and MLP to leverage the benefits of many algorithms
- Verified that the models were trustworthy, understandable, and had good generalizability by assessing their ACC, precision (PRE), recall (REC), and F1-score (F1).

Justification and novelty of the paper

The fact that conventional rule-based and single-model approaches frequently fail when used in the extremely unbalanced and ever-changing online banking environment justifies this study's need to find solutions. The current models have challenges in identifying rare classes, concept drift, as well as false-alert explosions that overwhelm the financial institutions. The novelty of this paper consists of combining Instance Hardness Threshold (IHT) balancing with an ensemble of DT, RF, KNN, and MLP classifiers, which combine to produce superior discrimination of minority fraud patterns. It is a single architecture that is tested with strong evaluation metrics to provide much better ACC, stability, and adaptability than standard and DL architectures.

Structure of the paper

This paper follows this format. In Section II, provide a thorough review of the literature on ML approaches for detecting fraud in online banking. Section III presents the characteristics of the dataset, data pre-processing processes, and the suggested ML framework. Section IV gives descriptive results of the experiment, performance analysis, and comparison with other benchmark models. Finally, Section V is the conclusion of the research, and future study is outlined.

LITERATURE REVIEW

This section throws light on recent advancements towards CCF detection with ML algorithms, including RF, DT, LR, KNN, ANN, and XGBoost. Research focuses on improved ACC, robustness as well as real-time detection using hybrid and anomaly-based methods.

Jin and Zhang (2025) use the Stacking ensemble learning technique to the problem of financial fraud detection, which is detailed in this work. Building it was several fundamental learners, including LR, DT, RF, GBT, SVM, and NN. Through the use of methods for feature significance weighting and dynamic weight modification, the model's performance is enhanced. Using over a million actual bank transaction records, the project was built. Increases in ACC (95% vs. 93%) and REC (93% vs. 44%) show that the Stacking model is more stable and generalizable than the standard single model [11].

Gupta *et al*. (2025) work presents the RF Classifier, a comprehensive ML approach for identifying fraudulent credit card transactions. They undersampled, used missing value management, and picked features to remove class imbalance as part of my data preparation approaches using a publicly available dataset. With an AUC-receiver operating characteristic (ROC) score of 0.99%, ACC of 98.7%, REC of 96.6%, and PRE of 97.3%, training a model to identify between legal and fraudulent transactions produced outstanding results. Classification results, a confusion matrix, and ROC curve analysis all corroborated the model's efficacy [12].

Aggarwal *et al*. (2024) set the goal of creating an algorithm that can detect monetary fraud. The study makes use of LR, DTC, and KNN. To improve the models' strength and ACC, statistical tests such as ANOVA are used to pick characteristics. There was a 98.01% success rate in detecting fraud using the logistic regression model. Scores of 91% for F1 and 92.35% for ROC AUC were reported. A fraud detection score of 96.67% was achieved using DTC cross-validation. 90% was the F1 score, and 91% was the ROC AUC. The remarkable performance of KNN in detecting fraud is supported by its ROC AUC score of 97.63%, cross-validation score of 99.34%, and F1 of 97% [13].

Beri *et al*. (2024) study looks at XGBoost and ANNs, two well-known ML methods for finding credit card scams. The ACC, PRE, REC, and F1 of the algorithms are tested in this study using the publicly accessible credit card transaction dataset. The choice about the viability of ANNs and XGBoost for employment in real-time fraud detection systems also takes their computing efficiency and scalability into account. A classifier called XGBoost achieves the greatest results with a rate of 92.7%, whereas artificial neural networks (ANN) achieve the highest rate of ACC across all five methods. The findings give financial institutions trying to install or enhance fraud detection systems direction as well as insights into the strengths and constraints of every method [14].

Geng and Zhang (2023) display a network that can identify fraudulent charges on credit cards by employing dual adversarial learning, a technique that enables unsupervised anomaly detection. By giving equal weight to the initial and intermediate data, this method stands out from the crowd of traditional anomaly detection techniques. The method beats the best fraud detection algorithms currently available, according to experiments conducted on a dataset consisting of information from European cardholders. A 0.9224 ACC, a 0.9208 F1, and a 0.8456 MCC are all displayed in the results [15].

Afriyie *et al*. (2023) analyze the PRE of three distinct ML models (LR, RF, and DT) for the purposes of identifying, predicting, and classifying fraudulent credit card transactions. According to the study's performance comparison of the models, the random forest (RF) model performs the best when it comes to predicting and reporting fraudulent credit card transactions. It achieves a maximum ACC of 96% and an area under the curve value of 98.9%. If they want to prevent and detect fraudulent purchases on credit or debit cards, they should use RF as an ML approach [16].

Table 1 discusses the study gaps in the digital banking system based on CCF. The topics covered include methodology, data, performance, limitations, and future directions.

METHODOLOGY

Fig. 1 displays the study's foundational idea: the methodology offers a systematic process of research that begins with the gathering of data by the dataset, which in this case includes 492 different forms of fraud experienced by European cardholders in September 2013. Under the preprocessing stage, tasks are to have great quality, none of the values have been duplicated, none of the values are missing, and then Standardization steps are done to get the data centered around 0 with a standard deviation of 1. Then, label encoding helps the ML models to perform mathematical operations and analyses after converting categorical data into numerical inputs. Moreover, to address the problem of unbalanced data, the study employed the Instant Hardness Threshold (IHT) method so that the dataset is balanced, and also to avoid the issue of overfitting and underfitting. Data sets are prepared for testing and training purposes. Multiple ML methods, including DT, RF, KNN, and MLP, are subsequently included in the ensemble model. It included the best features of each strategy in their ensemble model. The model's capacity to identify fraudulent transactions was assessed using a variety of performance measures. F1, ACC, PRE, and REC were these measures.

Dataset description

The data collection includes every single purchase made in September 2013 using a credit card across Europe. This dataset spans 2 days' worth of transactions and contains 492 fraudulent ones out of a total of 284,807. The statistic is heavily skewed because frauds make up just 0.172% of all transactions. It does not take any parameters into account other than the numerical output of the PCA transformation. Characteristics V1, V2, Only "Time" and "Amount" have remained unchanged by PCA; otherwise, V28 is the most altered characteristic. The dataset's time feature shows the number of seconds since the initial transaction. In other words, the total of the feature is the same as the total of the transaction. An example of a feature that makes advantage of this is cost-sensitive learning. When there is fraud, the experimental response variable, the "Class" feature, takes on the value 1, and when there is no fraud, it takes on the value 0.

Table 1: Research gap analysis on credit card and online banking fraud detection algorithms

Author (s)	Methodology	Dataset	Performance	Limitations	Future work
Jin and Zhang (2025)	Dynamic weight modification; feature significance weighting; stacking ensemble combining LR, DT, RF, GBT, SVM, and NN	1+million real financial transaction records	Accuracy: 95%, Recall: 93%, F1: 94%	Focuses on large offline datasets; computational complexity high; ensemble may not fit real-time online banking constraints	Explore real-time deployment of stacking; evaluate latency in online banking; incorporate streaming fraud detection models
Gupta *et al.* (2025)	Random Forest Classifier; extensive preprocessing; undersampling for class imbalance	Public credit card dataset	Precision: 98.7%, Recall: 96.8%, AUC: 0.990	Uses publicly available dataset (may not generalize to online banking); undersampling may lose important fraud patterns	Test on real online banking datasets; evaluate cost-sensitive learning; integrate adaptive sampling for evolving fraud patterns
Aggarwal *et al.* (2024)	Logistic Regression, Decision Tree, K-Nearest Neighbors; ANOVA for feature selection	Credit card transaction dataset	LR: Acc 98.01%, F1 91%; DT: Acc 96.67%, F1 90%; KNN: AUC 97.63%, F1 97%	Traditional ML models may not capture complex fraud behaviors; limited evaluation for online transaction speed	Integrate advanced models (XGBoost, deep learning); benchmark performance for real-time online banking transactions
Beri *et al.* (2024)	ANN versus XGBoost comparative study; focuses on accuracy and scalability	Public credit card dataset	ANN: 96.9% accuracy; XGBoost: 92.7% accuracy	Limited focus on online transactional environments; does not evaluate adversarial fraud attempts	Study robustness under adversarial attacks; assess performance in high-frequency online banking systems
Geng and Zhang (2023)	Unsupervised anomaly detection using dual adversarial networks; considers both original and intermediate features	European Cardholder dataset	Accuracy: 0.9224, F1: 0.9208, MCC: 0.8456	Unsupervised model may generate false alarms; dataset limited to the European region	Evaluate cross-regional datasets; hybrid unsupervised+supervised models for online banking environments
Afriyie *et al.* (2023)	Logistic Regression, Random Forest, Decision Trees; comparison of ML models	Public credit card dataset	Random Forest: Accuracy 96%, AUC 98.9%	No analysis of online fraud characteristics; static dataset; lacks real-time testing	Incorporate temporal and behavioral features; test models using live online banking transaction simulations

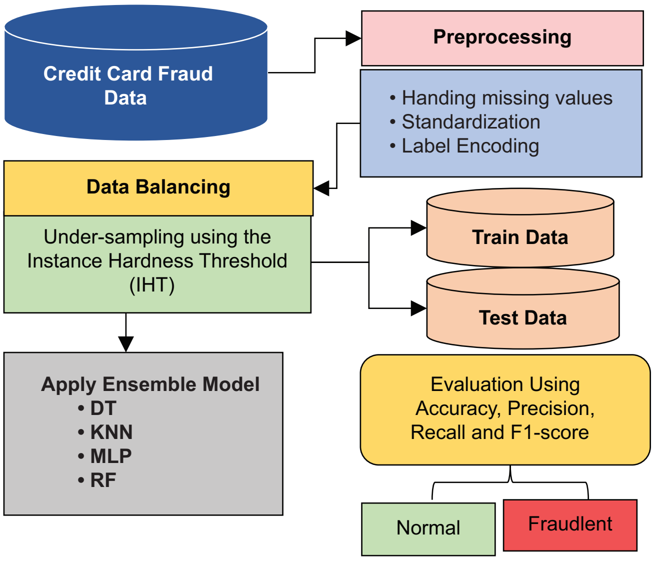

Fig. 1: A machine learning approach to credit card transaction fraud detection algorithms

Exploratory data analysis

EDA is a preliminary study of the data set wherein the key features are summarized using statistical data and visualization.

Features are represented on both the x and y axes of the square matrix that is the heat map. As shown in Fig. 2, the attributes might be associated with a dataset for detecting CCF due to the fact that the x and y axes contain columns for time, amount, and class. A vertical color bar on the right side of the chart represents the correlation coefficient. The shade indicates a strong negative correlation (minimum −1.0) while the color intensity shows a great positive correlation (maximum 1.0). It is not surprising that a variable is always associated with itself (self-correlation = 1.0). The main aim of this map is to unearth the important relations (bright red or dark blue squares off the main diagonal) between the various features and more importantly, the variable of Class, which in most cases is the target (fraudulent or legitimate transaction).

Fig. 3 represents a histogram of the distribution of the Log (1 + Amount) variable and amount probably denotes amounts of transactions (based on the context of the correlation map above). It is commonly referred to as Log1p (Amount), and is typically used to work with data that skews a lot, especially when there is a zero. The distribution of this plot resembles a normal (Gaussian) distribution rather than the distribution of the original data would tend to be, even though it has a slight positive or right skew. The highest number of the mode of the distribution (maximum amount) is 9,000, which is concentrated around the Log1p (Amount) = 3. The amount transformed is plotted on the x-axis, and the count of occurrences at each transformed amount bin is plotted on the y-axis.

Data preprocessing

The process of preprocessing data is an important phase that tries to refine and make the raw dataset ready to be analyzed. Data integrity is ensured by cleaning operations such as deleting null entries and handling missing values. The steps are given below:

Standardization

This technique standardizes the data to a single standard deviation and centers it around zero, resulting in a one-sided mean and variance (Equation (1)). Two types of data standardization functions are considered here: z-score and min–max normalization. This study used the Z-score-based standardization. The standardized formula is:

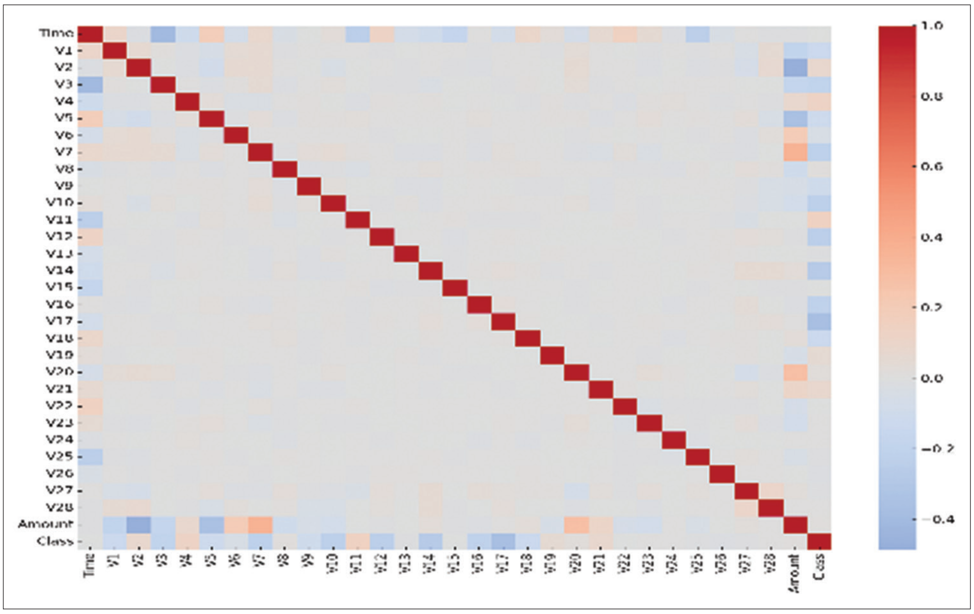

Fig. 2: Correlation heatmap of the dataset

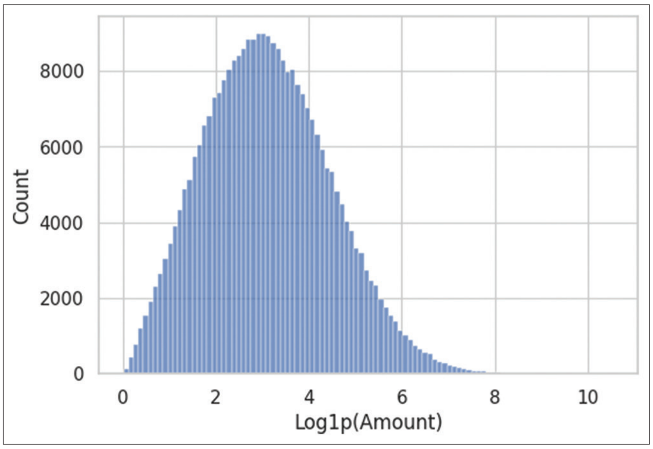

Fig. 3: Log (1+amount) distribution

$$x_{standardized} = \frac{x - mean(x)}{standard\ deviation(x)} \quad (1)$$

The data mean is represented by mean(x), with x being the initial data point. As a measure of how dispersed the observed data is, standard deviation(x).

Label encoding

Label encoding is a method of encoding categorical values by assigning each distinct category a number [17]. Label encoding allows ML models to perform mathematical operations and analysis by processing categorical data as numerical inputs. Label encoding is essentially just giving each data category a numerical value. Equation (2) for label encoding is:

$$x_{encoded} = Label_{(x)} \quad (2)$$

Data balancing

A data-driven method called the IHT gives each instance a hardness score depending on how difficult it is to accurately identify it. As additional complexity or ambiguity is indicated by higher hardness ratings, these occurrences are given more weight during training [18]. One approach that IHT takes to improve the model's performance and resilience to disparities in data is by making it better at classifying occurrences of minority classes, such as fraudulent transactions. To do this, zero in on the most difficult cases [19]. Furthermore, in the study, the IHT is used for the resampling of the dataset to enhance model performance. The definition of the Instance Hardness concerning given by Equation (3):

$$IH_h\ (X_i, Y_i) = 1\text{-}p\ (Y_i \mid X_i, h) \quad (3)$$

Where IH, (X, Yi), $p(Yi|Xi, h)$ represents the Instance Hardness value, training dataset, the probability which h assigns the label Yi, respectively. The class distribution of the data before and after IHT resampling is given in Fig. 4.

Data splitting

Data splitting gives unbiased model assessment by splitting the preprocessed data in an 80:20 ratio, with 80% contributing to model training and learning patterns and 20% being used to test and verify the reliability of the results.

Proposed ensemble model architectures

The Ensemble model is a kind of hybrid that combines DT, RF, KNN, and MLP.

Decision trees

Decision trees, which resemble an inverted tree, use a hierarchical, branching structure for prediction. The final results or forecasts are represented by the leaves at the end of each branch in this structure, which represents the many options or decisions. It was included because it is intuitive and can manage non-linear relationships in data. Decision trees are helpful for locating significant features and relationships in the information since they are simple to see and comprehend [20]. Equation (4) presents the mathematical form:

$$f(x) = \sum_{m=1}^{M} c_m I(x \in R_m) \quad (4)$$

The Equation (4) *f(x)* symbolizes a piecewise constant function, with each region R_m. R_m is given a value of cm. In Decision Tree models, it is frequently used to make predictions according to the leaf (region) that the input x belongs to.

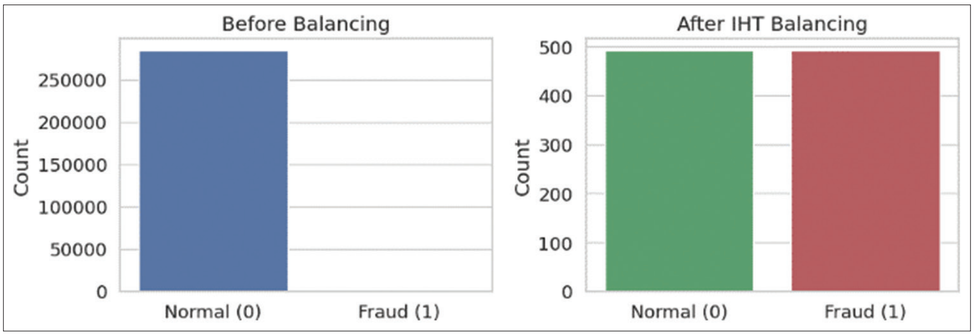

Fig. 4: Class distribution before and after instance hardness threshold resampling

RF

The RF is an ensemble method that pools many tree predictors into a single, uniform distribution, with each tree in the forest drawing its data from a separate, randomly generated dataset. Each tree's strength and the strength of the relationships between several trees define the RF's capacity. When there is less association between several trees and more strength in a single tree, the RF does better. One distinguishing feature of trees is their randomization, which selects some data properties at random using bootstrapped samples [21]. When node Np is divided into c child nodes $N1$., Nc according to the attribute a, the information gain $IG(Np, a)$ is defined by Equations (5) and (6):

$$IG\left(N_p,a\right)=Gini\left(N_p\right)-\sum_{i=1}^{c}\frac{\left|N_i\right|}{\left|N_p\right|}Gini\left(N_i\right) \tag{5}$$

$$Gini\left(N_p\right)=1-\sum_{i=1}^{m}p_j^2 \tag{6}$$

KNN

The KNN algorithm is a classification technique that predicts an information point's relative position to other points. It is characterized using similarity metrics such as the Manhattan distance measure and Euclidean distance [22]. The smallest distance between a data point in the training set and a test point is taken to indicate that the two points share the same unknown characteristic. In this research, the KNN classifier's Euclidean distance metric is used. Equation (7) determines the length of the difference between the two Euclidean (EC) point vectors (x_1, x_2):

$$EC=\sqrt{\sum(x_1-x_1)^2}\ k=1,2,\ldots..n \tag{7}$$

Multi-layer perceptron (MLP)

MLP is an ANN that uses linking weights to connect a group of neurons in a feed-forward fashion. ML produces the required outputs from a given set of inputs. This process begins at the input layer and continues all the way to the output layer by means of the first concealed layer on reception [23]. At each level, there is a fixed number of neurons in each layer. Neurons are connected between layers using weights and biases. For each neurone j in the hidden layer, and may find its output (O_j) using Equation (8):

$$O_j=f\left(\sum_{i=1}^{n}w_ix_i+b\right) \tag{8}$$

A sigmoid activation function is given by Equation (9), where n is the count of neurons in the last layer, w is the weight, x is the input value, b is the bias, and f is the function:

$$f\left(x\right)=\frac{1}{1-e^{-x}} \tag{9}$$

Performance metrics

Analyzing the outcomes is a crucial stage in figuring out how well the process was executed. The performance of the completed calculations was evaluated using the parameters provided:

- True Positive (TP): relationships that were appropriately classified as being of the Normal type
- True Negative (TN): inbound connections that were appropriately classified as Attack type
- False Positive (FP): Mistaking an authorized link for an attack connection
- False Negative (FN): The typical connection was incorrectly thought to be the attack connection.

Accuracy

It is the fraction of the test dataset that was correctly identified as a network connection [24]. A higher ACC score indicates a more effective classification model; the score can take on values between 0 and 1. Equation (10) defines the ACC score as follows:

$$Accuracy=\frac{TP+TN}{TP+TN+FP+FN} \tag{10}$$

Precision

A metric for ACC would involve dividing the total number of positive outcomes by the total number of negative results. One may locate the ACC formula in Equation (11):

$$Precision=\frac{TP}{TP+FP} \tag{11}$$

Recall

The recall is calculated by dividing the total number of TP by the sum of all TP and FN. More formally, Equation (12):

$$Recall=\frac{TP}{TP+FN} \tag{12}$$

F1-Score

Harmonically averaging the values of PRE and REC yields their definition. Equation (13) shows that it is a statistical way for evaluating the correctness of a system that takes into consideration both its REC and PRE.

$$F1=2\times\frac{Precision\times Recall}{Precision+Recall} \tag{13}$$

These assessment criteria are used to compare and assess how well various categorization methods identify different kinds of financial fraud.

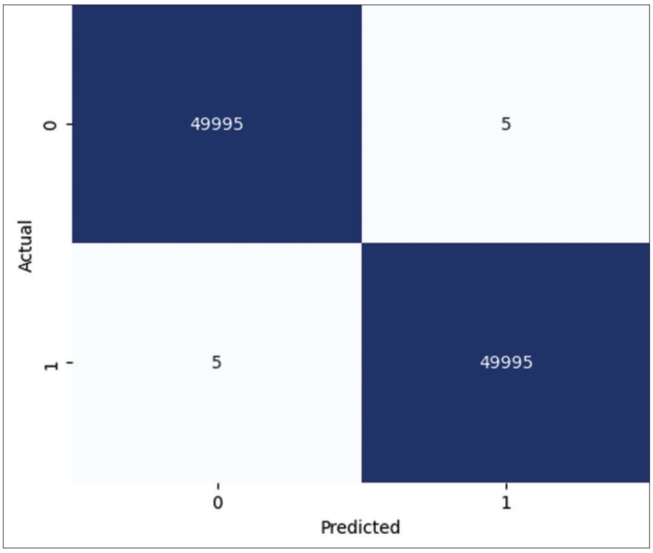

Fig. 5: Confusion matrix of ensemble model for credit card fraud detection

RESULTS ANALYSIS AND DISCUSSION

The research paper examines the execution of an ensemble-based ML-based CCFT detector. A high-performance computer system with an 8-core CPU, 64 GB of RAM, and 100 GB of disc space was used to conduct these tests. Throughout the development process, Jupyter Notebook and Anaconda Navigator were employed. Pandas, NumPy, Matplotlib, Seaborn, TensorFlow, Keras, and Scikit-learn are some of the primary Python libraries that have made data visualization, numerical computation, and ML much easier. Table 2 demonstrates that the ensemble model demonstrated impressive performance figures, as all the ACC, PRE, REC, and F1 hit 99.99%. These findings demonstrate the model's reliability and efficacy in identifying fraudulent credit card activity, indicating that it is well-suited for application in real-world financial security systems.

The Ensemble model's confusion matrices for CCF detection are shown in Fig. 5. The performance of the ensemble model was described in the matrix using TP, TN, FP, and FN variables. The numbers 0 and 1, respectively, represent honest and dishonest deals. The ensemble model has a success rate of 49995, comprised of 49995 true negatives and 5 FP. Based on the facts, it is clear that the Ensemble model is the best and correct alternative.

CCF detection was probably the motivation behind creating the ensemble model's ROC curve, as shown in Fig. 6. As the TPR and FPR are compared at various threshold environments, a curve is drawn. The blue line, when in its ideal location, cuts over the map's upper left corner, showing a model that performs extraordinarily well. AUC comes in at 0.999, which is very near the ideal result of 1.0. The ensemble model completely crushes the competition when it comes to identifying fraudulent from real transactions, with an almost flawless AUC and an incredibly low FPR. The dotted diagonal line representing the performance of a random classifier (AUC = 0.5) is presented.

Comparative analysis

The results of an assessment of the ability of numerous machine learning models to discover credit card fraud are displayed in Table 3. Included in this category are models such as LSTM, GBM, NN, and Ensemble Learning.

The presented evaluation analysis of ML fashions to pick out CCF indicates that the Ensemble version may also attain whole lot better effects than LSTM, GBM, and NN across all key overall performance metrics as provided in Table 3 and Fig. 7. With a low charge of fake positives and fake negatives, the Ensemble model identifies fraudulent transactions pretty nicely, as visible within the graph. Additional evidence for this assertion may be seen in its nearly flawless ACC, PRE, REC, and F1, all of which are 99.99%. Contrarily, LSTM and GBM have lower REC and F1 but are the most precise, suggesting they are less

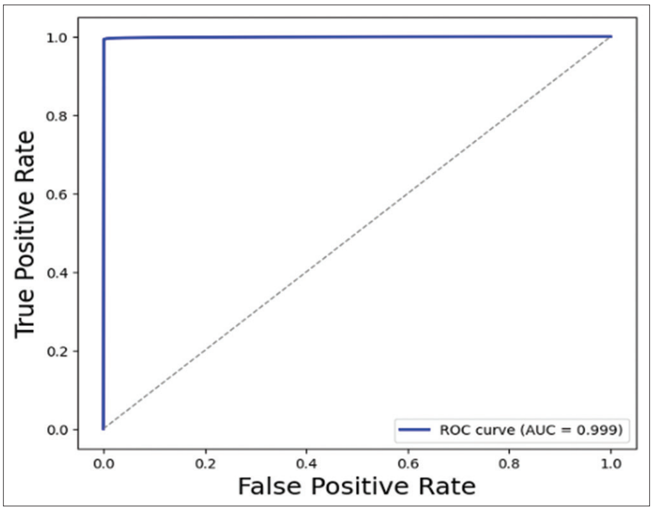

Fig. 6: Receiver operating characteristic curve of ensemble model for credit card fraud detection

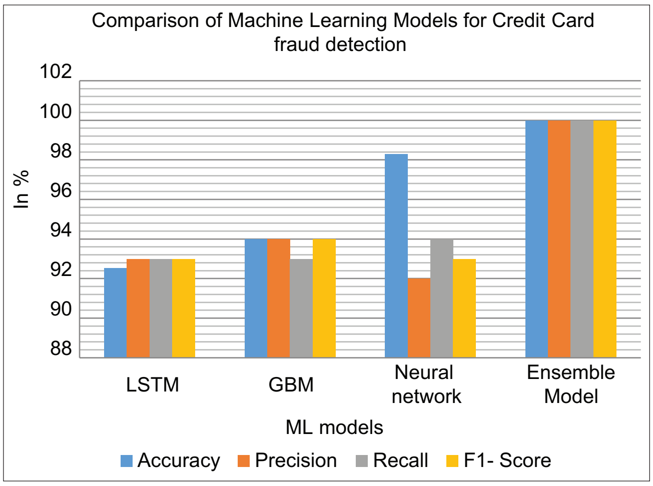

Fig. 7: Bar chart of ensemble model for credit card fraud detection

Table 2: The evaluation metrics of the ensemble model for the determination of CCF

Metrics	Ensemble model
Accuracy	99.99
Precision	99.99
Recall	99.99
F1-Score	99.99

Table 3: The comparison between machine learning models used to detect credit card fraud

Model	Accuracy	Precision	Recall	F1-Score
LSTM [25]	92.54	93	93	93
GBM [26]	94.001	93.998	93.00	93.99
Neural network [27]	98.3	92	94	93
Ensemble model	99.99	99.99	99.99	99.99

susceptible to minority frauds. The neural network model is quite reliable and is only a little less reliable when compared to the Ensemble approach. The strengths of the Ensemble Model comprise the fact that it can incorporate several learners to eliminate weaknesses of each individual model, thus making it very strong, adaptable, and accurate in detecting real-life financial fraud cases.

CONCLUSION AND FUTURE SCOPE

Applying a systematic fraud detection pipeline composed of refined pre-processing, inter-class balancing by the IHT, and a hybrid ensemble framework is showing unprecedented prospects of assuring online banking transactions. The combination of the classifiers, including the DT, the RF, the KNN, and MLP, is suitable and successful in capturing various decision patterns, thus allowing for a greater distinction between genuine and fraudulent transactions. With testing findings showing a 99.99% ACC, PRE, REC, and F1, such a hybrid model surpasses conventional ML and DL models, making it a reliable solution to unusual and unbalanced financial data. A more robust digital payment infrastructure and better decision-making in high-risk financial situations are both made possible by its enhanced performance, which opens up new possibilities for real-time fraud detection without sacrificing operational stability. The future work will be aimed at integrating multi-source transactional data to enhance the ability of models to generalize, integrating temporal and behavioral analytics to track adaptive fraud patterns, and embracing explainable AI systems to enhance decision transparency and regulatory acceptance. Further improvements can involve federated learning to collaborate privately, incremental learning to be learned continuously, and integration with real-time streaming systems to guarantee long-term scalability, operational resilience, and seamless execution and better interpretability of the model in the intricate financial systems.

REFERENCES

1. Shah SB. Advancing Financial Security with Scalable AI: Explainable Machine Learning Models for Transaction Fraud Detection. In: 2025 4th International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE); 2025. p. 1-7.
2. Patel D. Enhancing banking security: A blockchain and machine learning- based fraud prevention model. Int J Curr Eng Technol 2023;13:576.
3. Thakkar KB, Kapadia HP. "The Roadmap to Digital Transformation in Banking: Advancing Credit Card Fraud Detection with Hybrid Deep Learning Model". In: 2025 2nd International Conference on Trends in Engineering Systems and Technologies (ICTEST). IEEE; 2025. p. 1-6.
4. Wawge SJ. "A survey on the identification of credit card fraud using machine learning with precision, performance, and challenges". Int J Innov Sci Res Technol 2025;10:3345-52.
5. Prajapati N. "The role of machine learning in big data analytics: Tools, techniques, and applications". ESP J Eng Technol Adv 2025;5:16-22.
6. Malali N. "Exploring Artificial Intelligence Models for Early Warning Systems with Systemic Risk Analysis in Finance". In: 2025 International Conference on Advanced Computing Technologies (ICoACT). IEEE; 2025. p. 1-6.
7. Ali A, Razak SA, Othman SH, Eisa TA, Al-Dhaqm A, Nasser M, *et al*. "Financial fraud detection based on machine learning: A systematic literature review". Appl Sci 2022;12:9637.
8. Ande BR. "Federated learning and explainable ai for decentralized fraud detection in financial systems. J Inf Syst Eng Manag 2025;10: 48-56.
9. Majumder RQ. "A review of anomaly identification in finance frauds using machine learning systems". Int J Adv Res Sci Commun Technol 2025;5:101-10.
10. AbouGrad H, Sankuru L. "Online banking fraud detection model: Decentralized machine learning framework to enhance effectiveness and compliance with data privacy regulations". Mathematics 2025;13:2110.
11. Jin J, Zhang Y. "The analysis of fraud detection in financial market under machine learning". Sci Rep 2025;15:29959.
12. Gupta I, Kumar RR, Muduli D, Mishra S, Parija S. "A Machine Learning Approach for Credit Card Fraud Detection using Feature Engineering and Ensemble Models". In: 2025 International Conference on Innovations in Intelligent Systems: Advancements in Computing, Communication, and Cybersecurity (ISAC3). IEEE; 2025, p. 1-6.
13. Aggarwal A, Gill KS, Upadhyay D, Dangi S. "Fortifying Financial Security: The Power of Machine Learning in Credit Card Fraud Detection". In: 2024 3rd International Conference for Advancement in Technology (ICONAT). IEEE; 2024. p. 1-5.
14. Beri M, Gill KS, Sharma N. "Enhancing Credit Card Fraud Detection: A Comparative Analysis of Machine Learning Models". In: 2024 4th International Conference on Sustainable Expert Systems (ICSES). IEEE; 2024. p. 449-54.
15. Geng J, Zhang B. "Credit Card Fraud Detection Using Adversarial Learning." In: 2023 International Conference on Image Processing, Computer Vision and Machine Learning, ICICML 2023; 2023.
16. Afriyie JK, Tawiah K, Pels WA, Addai-Henne S, Dwamena HA, Owiredu EO, *et al*. "A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions". Decis Anal J 2023;6:100163.
17. Verma V. "Deep learning-based fraud detection in financial transactions: A case study using real-time data streams". ESP J Eng Technol Adv 2023;3:149-57.
18. Talukder MA, Khalid M, Uddin MA. "An integrated multistage ensemble machine learning model for fraudulent transaction detection". J Big Data 2024;11:168.
19. Trisanto D, Rismawati N, Mulya M, Kurniadi F. "Effectiveness undersampling method and feature reduction in credit card fraud detection". Int J Intell Eng Syst 2020;13:173-81.
20. Wijaya MG, Pinaringgi MF, Zakiyyah AY, Meiliana. "Comparative analysis of machine learning algorithms and data balancing techniques for credit card fraud detection". Procedia Comput Sci 2024;245:677-88.
21. Xuan S, Liu G, Li Z, Zheng L, Wang S, Jiang C. "Random Forest for Credit Card Fraud Detection". In: 2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC). IEEE; 2018. p. 1-6.
22. Adepoju O, Wosowei J, Lawte S, Jaiman H. "Comparative Evaluation of Credit Card Fraud Detection Using Machine Learning Techniques". In: 2019 Global Conference for Advancement in Technology. GCAT 2019; 2019.
23. Kasasbeh B, Aldabaybah B, Ahmad H. "Multilayer perceptron artificial neural networks-based model for credit card fraud detection". Indones J Electr Eng Comput Sci 2022;26:362-73.
24. Sokolova M, Lapalme G. "A systematic analysis of performance measures for classification tasks". Inf Process Manag 2009;45: 427-37.
25. Kali H. "Optimizing credit card fraud transactions identification and classification in banking industry using machine learning algorithms". Int J Recent Technol Sci Manag 2024;9:85-96.
26. Trivedi NK, Simaiya S, Lilhore UK, Sharma SK. "An efficient credit card fraud detection model based on machine learning methods". Int J Adv Sci Technol 2020;29:3414-24.
27. Sundaravadivel P, Isaac RA, Elangovan D, KrishnaRaj D, Rahul VV, Raja R. "Optimizing credit card fraud detection with random forests and SMOTE". Sci Rep 2025;15:17851.