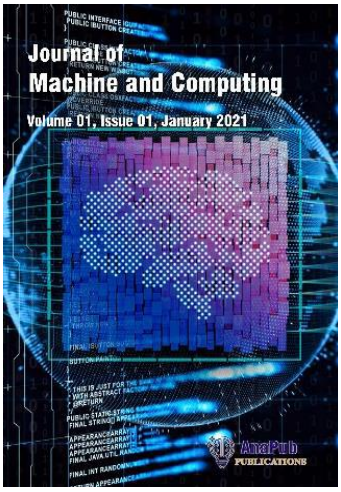
Fraud Detection in Financial Transactions Using Gradient Boost with Hybrid Optimization

Renukadevi S, Manujakshi B C, Shashidhar T M and Sivakumar N



DOI: 10.53759/7669/jmc202505181

Reference: JMC202505181

Journal: Journal of Machine and Computing.

Received 23 May 2025

Revised from 08 July 2025

Accepted 02 August 2025

AnaPub
PUBLICATIONS

Fraud Detection in Financial Transactions Using Gradient Boost with Hybrid Optimization

Dr Renukadevi S[1*], Dr. Manujakshi B C[2,] , Dr Shashidhar T M[3], Dr.N.Sivakumar[4]

[1]Assistant professor, Department of cloud Technology and Information Security, School of CS&IT, JAIN (Deemed-to-be- University), Bengaluru, Karnataka, India*

[2]Associate Professor, Department of Artificial Intelligence and Machine Learning, School of Computer Science and Engineering, Faculty of Engineering and Technology, JAIN (Deemed-to-be-University),Bengaluru, Karnataka, India

[3]Professor and Principal, Department of Electronics and Communication Engineering,, Harsha Institute of Technology, Bengaluru, Karnataka, India.

[4]Associate professor, Department of Computer Engineering, Marwadi University, Rajkot , Gujarat, India

[1]Corresponding author email: renukadevis163@gmail.com*

Abstract

In recent years, the banking sector has faced increasing challenges from fraudulent activities in online transactions. According to survey reports, annual losses due to such frauds exceed $1 trillion. Even while financial fraud unsafe for entire organizations, it may be recovered with the help of intellectual solution like Machine Learning (ML) models, Artificial Intelligence (AI) etc. Also, leveraging big data analytics ML algorithm van improves the identification and mitigation performance of fraudulent activities efficiently. Therefore, this article has developed the hybridized algorithm for predicting financial fraud by integrating metaheuristic optimization-based ML model hyperparameter tuning with suitable classifier logics. Name of the developed model is an intelligent Gradient Boost based Whale Hawk's Optimization with Bayesian (GB-WHOB) framework. Moreover, Banksim dataset has been collected for detecting the fraudulent transactions. This dataset includes payment transaction of numerous customers made in various time periods and amounts. Then, data pre-processing function applied on the collected dataset to messy raw data into readable and clean language formats. Here, convolution kernel function was enabled to altering the data before entering the next stage. Then, feature extraction is performed to extract the fraudulent features from the pre-processed data using. then, the developed model was enabled to analyse the anomaly actions using that Gradient Boost Tree (GBT) algorithm. This model establishes a baseline for normal transactions and detects deviations from this baseline to identify potential fraud. After that, user behavioural is important for detecting the fraud therefore Whale Optimization (WO) fitness function and Harris Hawk's Optimization (HHO) fitness was combined the residual blocks and new decision tree was designed to trained the above residual block function then analyse the frauds accurately. In addition, Bayesian optimization function was adapted to enhance the current best observation in fraudulent activities. The proposed algorithm was modelled and implemented in the Python tool, and the proposed model achieved exceptional performance, recording 99.76% accuracy, 99.72% precision, 99.78% recall, 99.77% F-measure, 99.92% specificity, and a minimal 0.24% error rate. These results significantly outperform other optimization techniques, demonstrating its superior capability in accurately detecting fraudulent financial transactions with minimal false positives and false negatives.

Keywords: fraudulent transactions, residual block, function, anomaly actions, fraudulent features, convolution kernel function

1. Introduction

Financial transaction with fraud encompasses a wide range of fraudulent tactics which are intended to illegally attain more funds, products or facilities [1]. To protect themselves against this possible losses, people and administrations must be aware of the numerous forms of contract fraud [2]. One dominant type is when scammers access a victim's online account, usually using identification they have taken, and continue with unapproved consumptions or connections [3]. Furthermore, criminals may use fictitious identities to open new accounts, make new purchases and then disappear without paying the money [4]. Using stolen gift card numbers to make purchases or reduce balances is additional strategy. In addition, scammers pretend to be responsible for all internet merchants in order to cheat the customers into purchasing goods that are actually delivered by reputable businesses while retaining the money for themselves [5]. In order to attain items with no intention of paying, some scammers take advantage of "buy now, pay later" process which is alternatives by providing fake evidence. Numerous methodologies involving imitation payment information, such as forged checks or hacked Electronic Fund Transfers (EFT), fall under this broad area of fraudsters [6]. When a scammer uses someone else's personal information to take the transactions and get credit in their name, it is identity theft [7]. The manipulation of digital payment systems to carry out illicit operations is the online payment fraud. Deceptive tactics used to transfer money unlawfully through electronic communication are referred to as wire fraud [8]. Lastly, dishonest online shopping tactics, like utilizing credit cards that have been stolen or false identities, are included in e-commerce fraud [9]. In order to identify and stop fraud in financial transactions, big data and ML algorithms must be integrated to perform the functions. Moreover, these technologies can enhance the precision and effectiveness of fraud detection models by using large amount of structured and unstructured data [10].

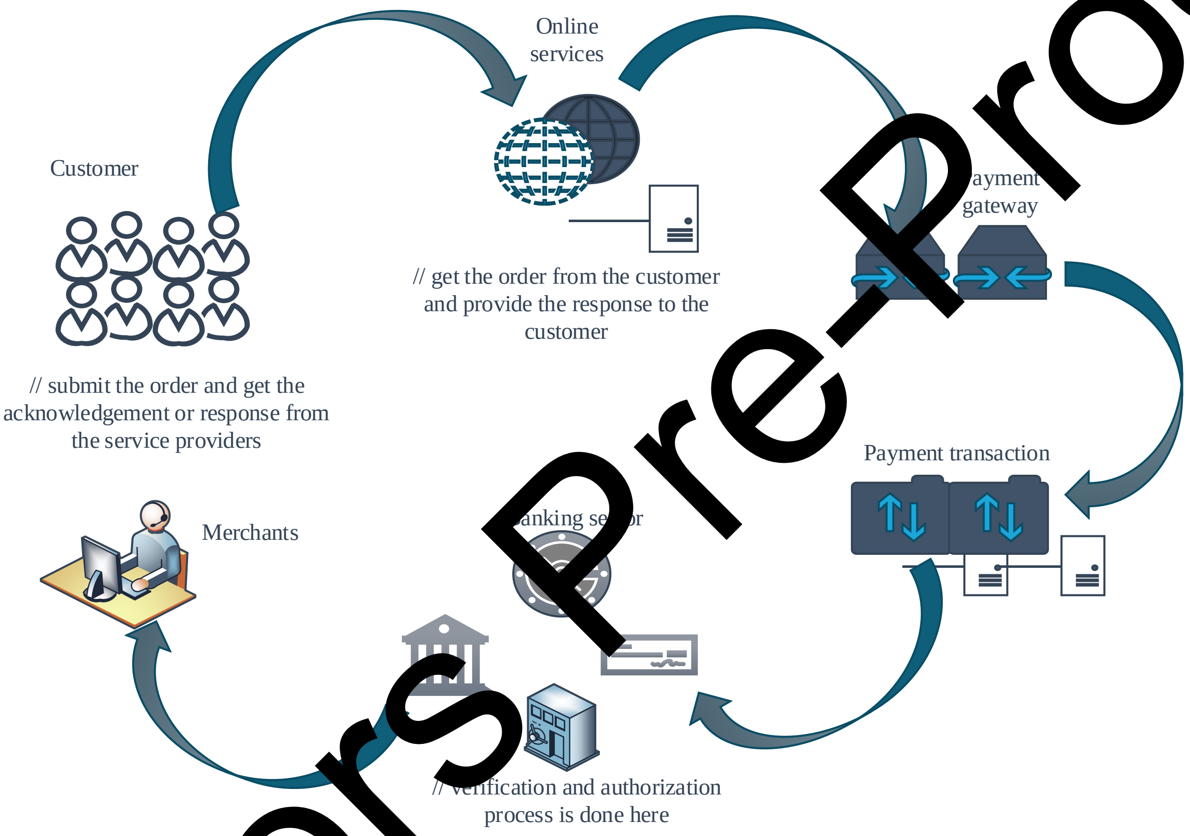

Online services
// get the order from the customer and provide the response to the customer
Customer
// submit the order and get the acknowledgement or response from the service providers
Payment gateway
Payment transaction
Merchants
Banking sector
// verification and authorization process is done here

Fig.1 Basic system representing of online transaction

Moreover, Figure 1 demonstrates the online transaction process between the customer to merchant. Initially, the customer places the order via online services and online service providers can communicate to the customer. Once the order is placed the acknowledgement message received from both side and move to the payment gateway. Then, verification and authorization are completed customer get the response from service provides the conformation was fulfilled. Big data analytics makes it possible to analyse complicated transaction patterns in enormous databases and commercial designs which are connected to fraudulent activity [11]. The capacity of ML and DL models to identify new fraud trends is always being enhanced by their training on historical data. These models may swiftly identify anomalies that might indicate fraudulent activity by setting a baseline for typical user behavior [12]. This is especially important in online banking and e-commerce, where prompt detection is crucial [13].

Big data-powered real-time transaction monitoring enables financial institutions to identify questionable activity as it occurs, assisting in the prevention of fraud before it gets out of hand [14]. Organizations may rapidly examine incoming transactions with streaming data processing, ensuring irregularities are addressed in real time and bolstering security overall [15]. The accuracy of fraud forecasts is increased by this all-encompassing strategy. Machine learning models improve their detection skills and cut down on pointless transaction blocks over time, in contrast to conventional rule-based systems that frequently produce large rates of false positives [16].

In past, numerous techniques are incorporated into the risk assessment frameworks of machine learning classifiers, such as Support vector Machine (SVM) [17], K-Nearest Neighbour (KNN) [18], Decision Tree (DT) [19], random Forest (RF) [20], etc. These models are takes transaction history, location, device information, and behavioural patterns for the training purpose. But in some cases, the model is trained specific data only and failed to process the real-world data. Moreover, temporal feature patterns are cannot capture the dynamic behaviour. To overcome the issues here we have developed the hybrid optimization based ML algorithms.

This research is organised in the following way. Predicting online sales is the focus of Section 2, which summarises current approaches. The approach, including data management and model application, is described in Section 3. The outcomes of the experiments are detailed and discussed in Section 4. Section 5 presents the important findings and suggests areas for further research.

2. Related works

Here, this section discussed the literatures review of exiting studies related to fraudulent behavior of online transaction,

Hou and Xuechen [21] have proposed a reinforcement learning theory to detect the financial anomalies and constructs the nontemporal methods. This method is also used for transforming the nontemporal indicators to temporal indicators of intelligent assessment. Moreover, CNN with four hidden layers is constructed to classify and estimate the financial data fraudsters. Multidimensional correlation analysis is incorporated with this model for further improving the accuracy of the financial data.

Fraudsters activities are increased day by day during the mobile payment transactions specially for smartphones. The extant studies have utilized supervised learning models to detect the financial fraud from the labelled data. However, the detection performance has negatively identified the financial fraud from the class imbalance data. Here, Petr Kajek, et al, [22] have suggested the XGBoost fraud detection strategy to find the financial consequence. Furthermore, this model has validated under random and sampling methods to achieve the better solutions.

Electronic Funds Transfer (EFT) is one of the most online financial system, which is mainly depends on the public internet. Moreover, various internet traffics are created for this online platform. Som of the analysis are failed to control the anomalies from financial transactions. Thus, A.Asad Arfeen, et al, [23] have introduce the ML based multi-layer network topology is applied on the application layer to detect the anomaly action from the finial transactions. Also, this model gas effectively classified the intrusions, online frauds and financial service providers.

Banking sector fraud is the most important and serious problems for monetary losses, bank brand damages, etc. in an e-commerce sector, retail industries and financial managements has taken the major remedy to avoid the fraudulent activities. But those are getting disappointed is such situation. Therefore, Astha Vashistha et al, [24] have developed the hybrid ML models to perform the fraud detection performance. Here nearly 20, 000 dataset was collected through the Kaggle database which includes 114 attributed related o banking sectors.

Cybercrime is one of the most anomaly activity is financial services and their entire loss problems. Also, thus would happens mainly on online transaction, credit card fraudulent activities etc. Therefore, Ahmed Younes Shdefat te al, [25] have developed the six algorithms with various cross validation layers. After the rigorous analyses decision tree with 10-fold cross validation framework has achieved better performance while comparing he models. Also, this ML model has 98.47% accuracy for predicting the financial frauds and cyberthreats.

Digital as well as internet payment transaction is the rapid advancement in a modern technological world. However, financial fraud detection is one of the most operational risks is the era of digital transaction. Therefore, AI-Dahasi et al, [26] have suggested the six ML model and their hyper parameters are tuned to enhance the predictive performance financial fraud detection. And finally, perform the comparative assessment for verifying the valuable insights and efficiency.

Regulatory compliance, reputation management, financial stability are crucial irrelevant attributes of the banking sector. therefore, Sorour et al, [27] have developed the ML with Brown

Bear Optimization (ML_BBO) algorithm to improve the accuracy and eliminate the negative impact of the fitting features. here, the developed model was used the classifier such as SVM and KNN to identify the CCF transaction and improve the capabilities of exploration as well as exploitation. Also, 10 benchmark dataset are used to validate the efficiency of the proposed models.

Yu, Gui, et al, [28] have introduced a Quantum Optimization with deep belief Network to overcome the challenges such as economic landscape, marketing losses, etc. Also, the developed model has combined Grap network and long short terms network to enhance the manual and statistical analysis of the model. Moreover, the hybrid model illustrates better training time and efficiency through the financial market data solutions. In addition, tis model mitigates the computation efficiency and economic losses.

To enhance the fraud transaction and identification process Taluder, et al, [29] have introduced a combined multi-stage ensemble bagging classifier. These techniques have mitigated the data imbalance problems includes higher cost payment transaction, missing payments transaction etc. Moreover, the investigation is mainly focused to reduce the missing transaction as well as false alarm rates while providing the warnings. Moreover, table.1 Shows that the summary of all exiting works.

3. System model and Motivation

In the ML development process starts with data collection from standard web source and prepare the data into the next level such as handling the missing values. Then, processed data is prepared to the training and testing process. After that, trained data is moved to the classification and prediction stage to classify the fraud or not. Finally, the performance measured in terms of various metrics, which is demonstrated in figure.2. While existing studies on fraud detection have demonstrated significant advancements with various methodologies such as NN-based unsupervised learning, meta-heuristic optimization, and deep learning techniques, there remains a notable research gap in generalizing these methods across diverse datasets and real-world scenarios [23].

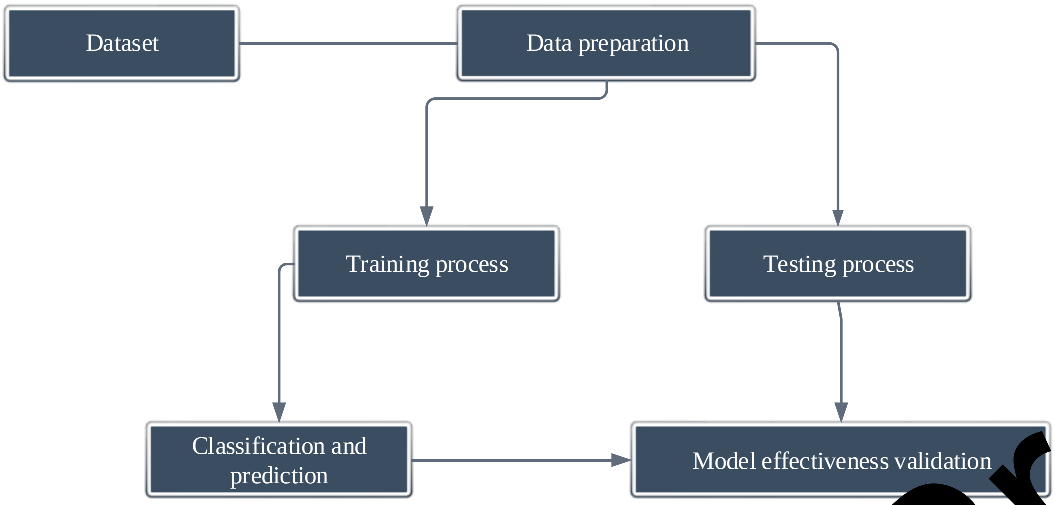


Figure.2 System model

Many approaches are optimized for specific datasets, such as mobile money transactions or financial statements, limiting their applicability to broader contexts [24]. Additionally, the complexity of tuning and preprocessing methods, along with the variability in performance metrics like accuracy and precision, indicates a need for more robust and adaptable frameworks [25]. Future research should focus on developing universal models that integrate advanced techniques and improve generalization, while also addressing the resource intensive nature of current optimization processes.

4. Proposed methodology

The system begins with a dataset which is BankSim, also, this dataset includes synthetic transactional dataset used to model the banking operations. Then, the dataset was kept in a structured database for processing and retrieval the further performance easily. In order to attain high-quality input for the model, the pre-processing step enables to clean the data by addressing missing values and identifying outliers. After that, feature extraction phase can enhance the predictive performance, pertinent characteristics are taken out of the dataset. These attributes are categorised in features that are based on transactions such as amount and frequency, and user behavior such as login patterns and transaction habits, features that are dependent on history, such as previous fraud records finally, relational-based features, such as user and account relationships.

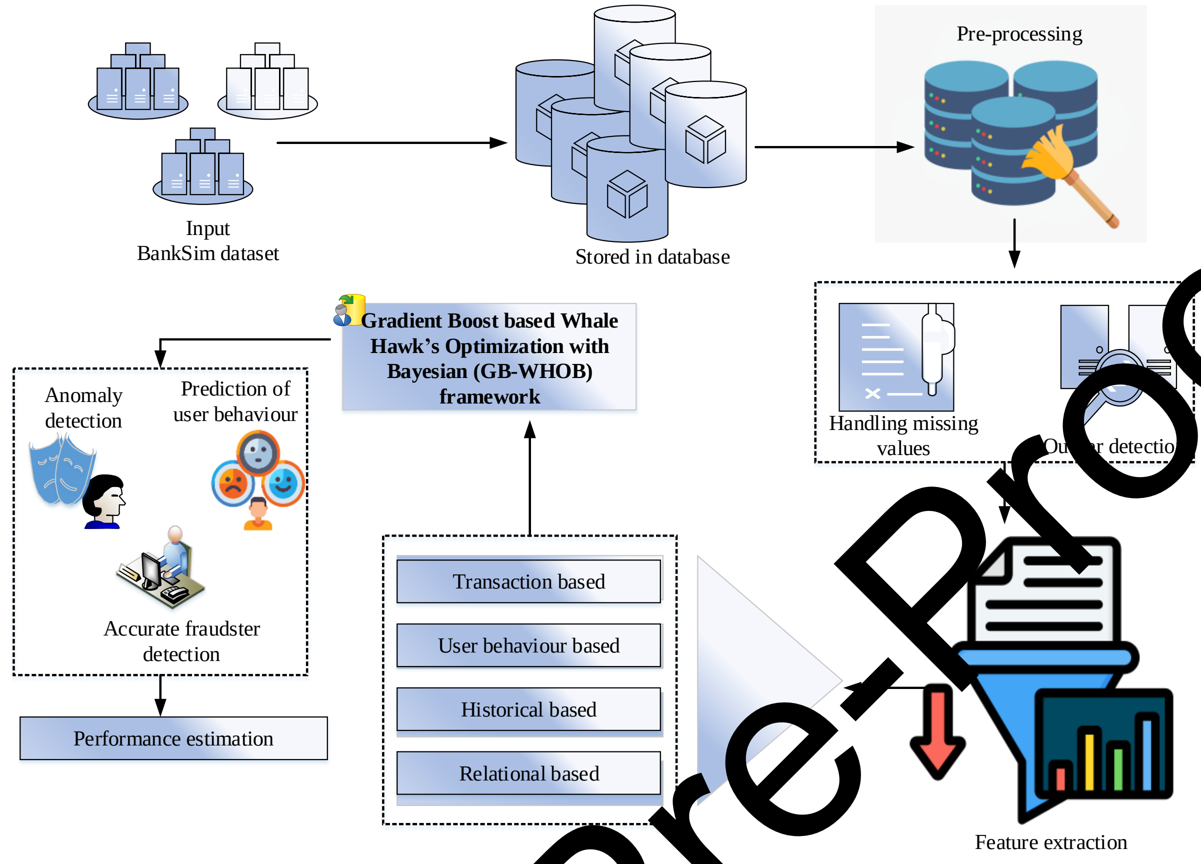


Fig. 3 Proposed GB-WHOB architecture

In order to improve predictive performance, the suggested model combines an ensemble approach which is gradient boosting with an advanced machine learning model. A metaheuristic algorithm for feature selection and optimization which is Whale Hawk Optimization. Bayesian Optimization, which increases accuracy by fine-tuning model parameters. Moreover, fraud Identification and behavior forecasting is analysing the data to identify irregularities and fraudulent activity, the trained model makes predictions about user behavior based on transaction patterns. At last, estimating performance which is the accuracy of the model assessed to gauge how well it detects fraud by using the developed GB-WHOB which is to produce more accurate predictions, this technique improves the fraud detection capability. Moreover, the proposed system model is illustrated in figure.3.

4.1 Process of the GB-WHOB methodology

- **Pre-processing**

Initially, the gathered dataset is transformed into the data pre-processing stage to clean, understandable, and structured format for additional analysis. Statistical imputation such as mean, median, mode and sophisticated methods like interpolation are used to fill in missing or incomplete data. Moreover, to avoid bias in model training, unusual or extreme values are recognized and also eliminated. Consequently, the data is modified and improved using a convolution kernel function before moving the next phase. The dataset becomes more structured for using kernel function with pattern recognition, noise reduction, and feature augmentation process. A kernel function in data preprocessing is essentially a mathematical filter used to transform the raw dataset before it is passed to a machine learning model. Its main purpose is to highlight important patterns, reduce noise, and enhance features so that the data becomes more meaningful for analysis. The expression for convolution is given in following eqn. (1),

$$c(x,y) = \sum_{m=-i}^{i} \sum_{n=-j}^{j} q(m,n)\, p(x+m, y+n) \tag{1}$$

Where, $c(x,y)$ is denoted as filtered data using the kernel function, $q(m,n)$ is represented as original collected data, kernel filter is denoted as q with each function was represented as $-i \le m \le i \ and \ -j \le n \le j$. Moreover, the convolution function integrates two element and that produce third pattern which includes combination of input data with filter function. But this combination can provide output data. Then, apply the small matrix function between the two-function such as $c \ and \ p$ which is mentioned in following eqn. (2),

$$(c*p)(t) = \int_{-\infty}^{\infty} c(\tau)\, p(t-\tau)\, d\tau \tag{2}$$

Where, $(c*p)(t)$ is represented as output of the convolution operation, $c(\tau)$ is denoted as input function and $p(t-\tau)$ is expressed as filter function which are used for analysis. Using this function, we can get noise reduced data.

- **Feature extraction and selection**

In order to detect financial fraud features such as transaction, user behaviour, historical and relation-based features are extract the Hidden Markov Model (HMM) is used to simulate the steps involved in processing credit card transactions. By examining user expenditure, it assists in identifying fraudulent transactions. The HMM is represented by patterns that include data on money spent, time since the last transaction, and common purchase categories. When these patterns are broken, it may be a sign of danger. a limited number of states connected by probability distributions. After that, a potential result or observation is produced in a certain state that is connected to a probability distribution observation symbol. Following that, certain probabilities known as transition probabilities control changes between these states. Consequently, user expenditure profiles can be categorized into low, moderate, and high-profile groups. Here, HMM is denoted by the tuple which is mentioned in eqn. (3),

$$\alpha = \{H(s), O(s), A(t), \delta\} \tag{3}$$

Where, $H(s)$ is represented as hidden states which are termed as finite set $H(s) = \{H(s_1), H(s_2), H(s_3) \ldots\ldots\ldots\ldots\ldots\ldots H(s_n)\}$, is denoted as parameter representation of extracted feature from the pre-processed data $O(s) = \{O(s_1), O(s_2), O(s_3) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots O(s_n)\}$. Then, $A(t_{mn})$ is expressed as state transition probability matrix which is termed as following eqn. (4),

$$A(t_{mn}) = \overline{P}(\bar{s}_{r+1} = \bar{s}_n \mid \bar{s}_r = \bar{s}_m) \tag{4}$$

Where, $\overline{P}$ is denoted as probability function with state transition from $\bar{s}_m$ and $\bar{s}_n$ at the transition $1 \le m, n \le I$ level . Moreover, apply the state probability distribution function to the initial set of observing feature using eqn. (5),

$$\beta_m = \overline{P}(\bar{s}_1 = \bar{s}_m) \tag{5}$$

Where, β_m is denoted as state probability distribution function at $1 \le m \le I$. After that, form the observation sequence using the pre-processed data features as $f = \{f_1, f_2, f_3 \ldots . f_4\}$. Here, HMM has starts the training process using the Baum-Welch principle and also determined the hidden state features which are significantly observed. Consequently, the extracted features are again refined and compressed from the hidden states. The process begins with feature extraction where raw financial transaction data is transformed into meaningful attributes that can effectively represent user behavior. Features such as transaction amount, frequency, time of day, merchant category, device ID, and geolocation are extracted. Advanced preprocessing methods, including kernel-based filtering, are applied to enhance patterns and reduce noise. This step ensures that the dataset captures both routine transaction behavior and subtle variations, forming a structured foundation for the subsequent anomaly detection process.

- **Anomaly detection using GBT**

In the gradient Boost algorithm initially set the objective function based on the loss function using the additive strategy in eqn. (6),

$$T_m(u) = T_{m-1}(u) + \lambda_m \phi_m(u) \tag{6}$$

Where, $T_m(u)$ is denoted as parameter of the objective function also this the interactively performed each solution, $T_{m-1}(u)$ is previous interactively performed each solution. Moreover, gradient Boost algorithm has the learning rate which is mentioned in λ_m, also, it has decision tress so it has fitted in weak learners in ϕ_m. Then apply the decision rule to the tree structure using eqn. (7),

$$\phi_m(u) = \sum_{n=1}^{N} b_n 1(u \in r_n) \tag{7}$$

Where, N is denoted as total number trees designed the gradient Boost algorithm, weightage factor of each trees denoted as b_n, then, finally indicator function is termed as $1(u \in r_n)$. In the final stage this model is anomaly score prediction from the fraudulent transactions using final fraud prediction score $(f(u))$ in eqn. (8),

$$f(u) = \frac{1}{1 + e^{-f_J(u)}} \tag{8}$$

Where, $e^{-f_J(u)}$ is represented as probability function predicted fraud classes, then apply the threshold function γ which is trained under transactions using below conditions,

$$\overline{P}(u) = \begin{cases} A(u) \approx 0 & lower\ proability\, of\ \ fraud\ score \\ A(u) = 1 - \overline{P}(u)_{new} & higher\ proability\, of\ \ fraud\ score \\ A(u) > \gamma & improper\, proability\, of\ \ fraud\ score \end{cases} \tag{9}$$

GBTs improve weak learners, usually decision trees, to create classifiers and prediction models efficiently. Iteratively, each succeeding tree try to find and reduce the errors and enhance the developed model's entire performance.

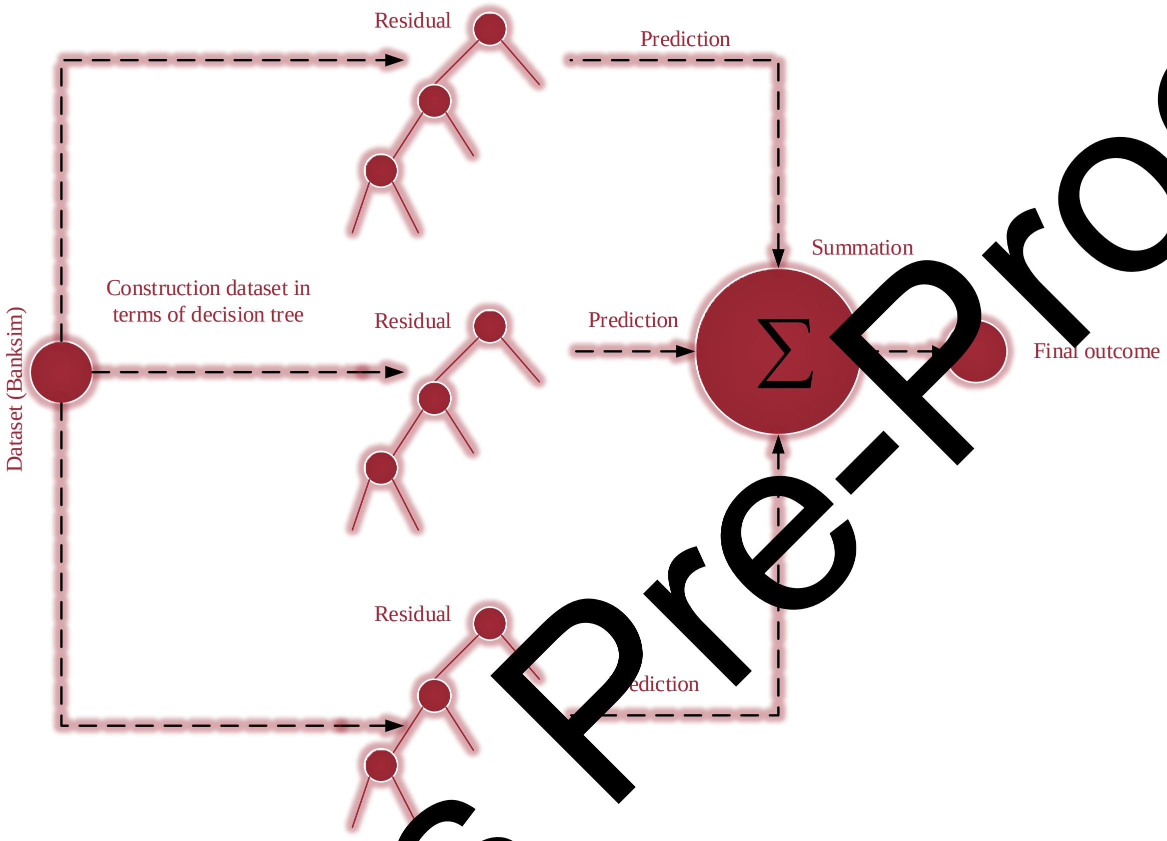


Figure 4 Internal structure of XGB

Once meaningful features are obtained, the system proceeds to anomaly detection, where extracted features are compared against a baseline of normal transaction behavior. The proposed model uses Gradient Boosting Trees (GBT) with integrated residual blocks, allowing it to learn deviations between predicted and actual outcomes iteratively. Hybrid optimization techniques, including Whale Optimization (WO) and Harris Hawks Optimization (HHO), fine-tune the detection process to identify even subtle and complex fraud patterns. This stage flags transactions that exhibit unusual patterns for further analysis in the classification stage.

Prediction of accurate user behaviour

In the proposed system, residual blocks are integrated into the Gradient Boosting Trees (GBT) framework to iteratively learn and refine the residual errors between predicted and actual outcomes, enabling the capture of complex fraud-related behavioral patterns. Each residual block's learning process is enhanced using a hybrid optimization approach: the Whale Optimization Algorithm (WO) identifies optimal fraud-behavior thresholds during the exploration stage, Harris Hawks Optimization (HHO) fine-tunes residual learning parameters for better exploitation, and Bayesian Optimization (BO) further adjusts hyperparameters by maximizing Expected Improvement (EI) for optimal exploration–exploitation balance. This integration ensures that residual blocks are not only more accurate in detecting subtle fraudulent patterns but also improve the overall generalization, stability, and precision of the GBT-based fraud detection model.

Transactions flagged as anomalous are passed to the **classification** stage, where the optimized decision tree within the GBT framework determines whether each transaction is fraudulent or legitimate. Bayesian Optimization (BO) further fine-tunes hyperparameters to maximize classification accuracy and balance false positives with false negatives. By leveraging the refined outputs of the anomaly detection stage, the classification process delivers accurate, stable, and generalizable predictions, completing the fraud detection pipeline from raw data transformation to final decision-making.

In the financial fraud detection system includes, behaviour assessment of each user which are predicted using residual block training process of the GBT algorithm. This also refine the prediction results and enhance the hyperparameter tunning progress with the help of hybrid optimization algorithms. The model can discover more complex patterns in user behavior that point to fraud by including these optimization strategies into decision tree training. The decision tree can make better predictions about possible fraudulent transactions thanks to the residual blocks created using WO and HHO, which provide deeper insights into intricate data linkages. Consequently, residual block decision tree has to predict the financial frauds accurately. Initially, design the residual block layer using residual learning parameter with final fraud prediction score ($F(u)$) in eqn. (10),

$$R(u) = O(u) - O_{i-1}(u) \tag{10}$$

Where, $O(u)$ is denoted as output of the newly designed decision tree, previous decision tree output mentioned in $O_{i-1}(u)$ and residual block parameter is represented as $R(u)$ which is complex fraud behaviours. So, update the position of each whales using eqn. (11),

$$W(t+1) = W' - X.A \tag{11}$$

Where, W' is the finest solution attained from the exploration stage, X is the controlling the coefficient vector function from an exploration stage and A is the distance from current position to update position. After that take the fitness function of the HO and tune the hyperparameter using eqn. (12),

$$H'(u+1) = H'_r - d.\left[H'_r - H'(u)\right] \tag{12}$$

Where, H'_r is denoted as finest solution attained from the exploration stage, d is the energy controlling parameter. Finally, accurate fraudsters detection is performed using BO with Expected Improvement (EI) in eqn. (13),

$$EI(\vartheta) = [\alpha(\vartheta) - f(u) - \chi]\Phi(Y) + \varepsilon(\vartheta)\phi(Y) \tag{13}$$

Where, $\alpha(\vartheta)$ and $\varepsilon(\vartheta)$ is represented as mean and standard deviation, Φ and ϕ is cumulative and probability distribution of each financial transaction. Moreover, balance between exploration and exploitation fitness solution parameter is denoted as χ. As a result, there are fewer conditions are taken to valid the transactions and more dependable and effective systems that can precisely detect fraudulent activity.

Algorithm:1 GB-WHOB framework

```
        Input: BankSim dataset
        Output: Finest prediction results
Start
        Initialization
           {
                      Parameters of GBT, WO, HHO, BO
           }
        Pre-processing
           {
                      convolution kernel function $\Rightarrow q$
                      $c(x, y) \Rightarrow q(m, n)$
                          Apply small matrix function
```

```
                $(c*p)(t) \Rightarrow c(\tau)$    // $c(\tau)$ input function
    }
Feature extraction
    {
        HMM $\Rightarrow H(s)$
            $A(t_{mn}) \Rightarrow \overline{P}\ \bar{s}_m$ and $\bar{s}_n \Rightarrow 1 \le m,n \le I$
            $\beta_m \Rightarrow 1 \le m \le I$    // state probability distribution function
        $f = \{f_1, f_2, f_3 \dots f_4\}$    // extracted feature Baum-Welch principle
    }
Anomaly detection using GBT
    {
        Set objective function $\Rightarrow T_m(u)$
        Iteratively perform $\Rightarrow T_{m-1}(u)$, $\lambda_m$, $\phi_m$
        anomaly score prediction $\Rightarrow f(u)$    // probability function predicted fraud classes
    }
Prediction of accurate user behaviour
    {
        Update the population of WO and HHO at residual block
        Update Newly designed decision tree $O(u)$
        $W' \Rightarrow$ obtained from WO with exploration stage
        $H'_r \Rightarrow$ obtained from WO with exploration stage
        accurate fraudsters detection    // using BO
Stop
```

5. Result and discussion

This study develops an integrated strategy utilizing the combined strengths of WO and HHO for the detection and controlling the financial frauds during the money transferring process. This work aims to detect the frauds and manage the optimal transaction performance of banking sectors. The presented framework was modelled in MATLAB software version R2020a, running in 64-bit Windows Operating System. The developed framework utilizes the BankSim dataset and performances of the presented method are assessed as accuracy, recall, precision, and f-measure.

5.1 Dataset description

The dataset is produced by the BankSim simulator, which replicates realistic transaction behaviours without compromising actual customer data. It includes various attributes such as transaction amounts, types, timestamps, and customer identifiers, facilitating comprehensive analysis. Primarily used for research in fraud detection, the dataset allows for the development and testing of machine learning models aimed at identifying fraudulent activities. The BankSim dataset serves as a valuable resource for developing and evaluating fraud detection methodologies in financial transactions.

5.2 Simulation outcomes

In the simulation, initially take 50 epochs which demonstrates that the developed GB-WHOB model significantly rise in both the training and testing performance accuracy. From this evaluation suggesting the proposed model has higher learning efficiency. Moreover, the training accuracy keeps increasing over the 200 epochs and after 150 epochs, the testing accuracy reaches a high, which indicates that the developed GB-WHOB model is start to overfit and perform too well on training data as well as losing generalization ability. During the training phase, the difference among testing and training accuracy has slightly grows based on the new overfitting value which may be occurring within few epochs. Overall, the fig.5 indicates that the model is learning and attained better performance, but there is a chance that overfit in the end because the testing accuracy reaches a high while the training accuracy preserves increasing. Strong performance and generalization are indicated when both the performance are simultaneously at a high level.

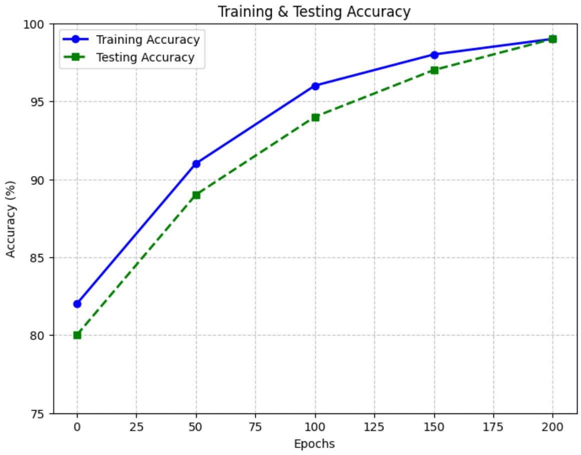


Figure.5 Accuracy in terms of training and testing

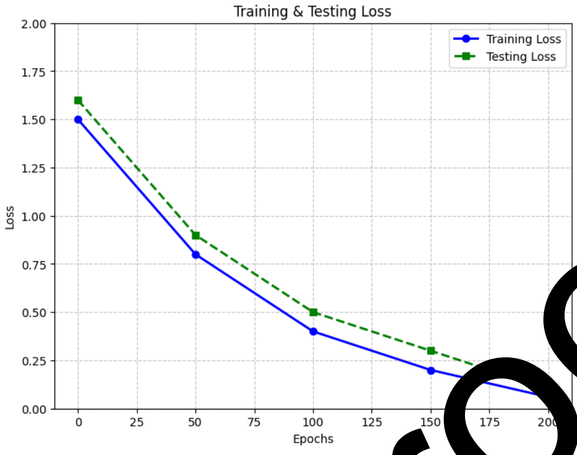


Figure.6 Loss in terms of training and testing

In the first 50 epochs, both training and testing loss is significantly reduced. In addition, 200 epochs the training loss again decreasing steadily, indicating that the model is still learning and getting better at fitting the training data. After 100 epochs, the testing loss begins to smooth out after initially decreasing as well. Consequently, Performance on unknown data may not significantly increase with additional training after this point. As training goes on, the difference between the testing loss and the training loss grows. In the early phases of training, the graph shows that the model is learning efficiently in fig.6. The testing loss plateau and the growing difference between training and testing loss point to the possibility of overfitting. The model's performance on fresh, untested data may actually begin to deteriorate if this pattern persists.

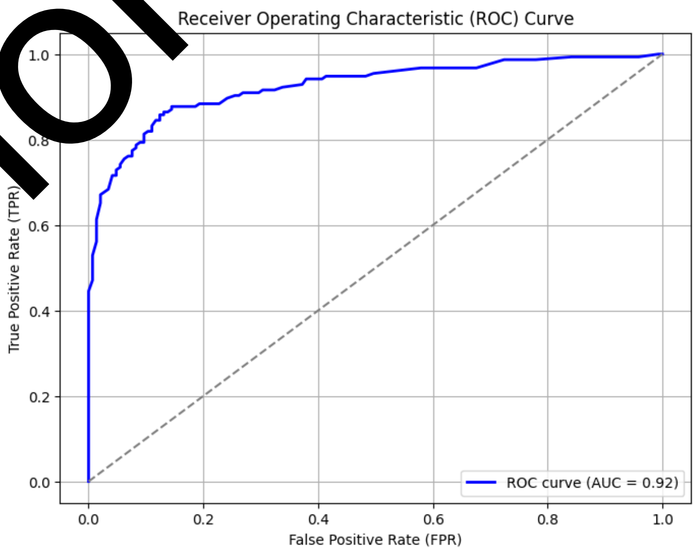
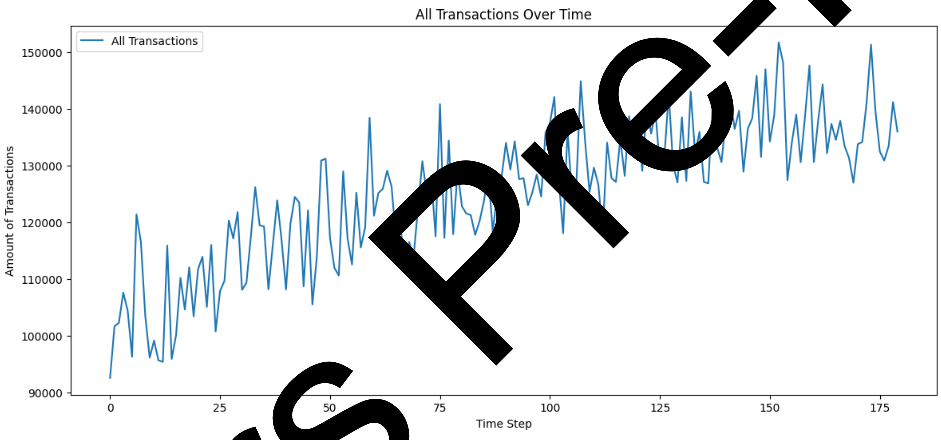
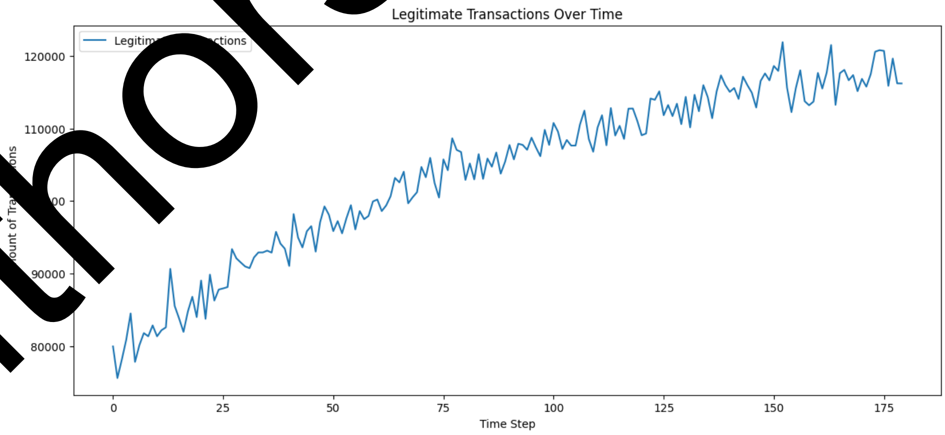


Fig.7 ROC curve of the overall performance

A high sensitivity indicates that the majority of transaction with online modes are appropriately identified by the frauds. When a transaction has a poor specificity, it frequently fails to identify fraudsters individuals as having the specific condition. Also, Fig. 7 shows that the two things are balanced by looking at the ROC curve. A curve that is high and to the left, with a high AUC, indicates that the test is both sensitive and specific. The model does a better performance at achieving this balance in this instance, as indicated by the AUC of 0.92. Furthermore, the sensitivity value between 0.8 and 0.9 (80–90%) if it proceeds down the curve to a point where the FPR is 0.1 (10%). This indicates that just 10% of transaction without online modes are mistakenly flagged by the model, but 80–90% of those with the normal transaction are appropriately identified. To sum up, the ROC curve and its AUC offer a useful method for evaluating a binary classifier's performance. The high AUC of 0.92 in this graph suggests a model that does a good performance of differentiating between the two groups.





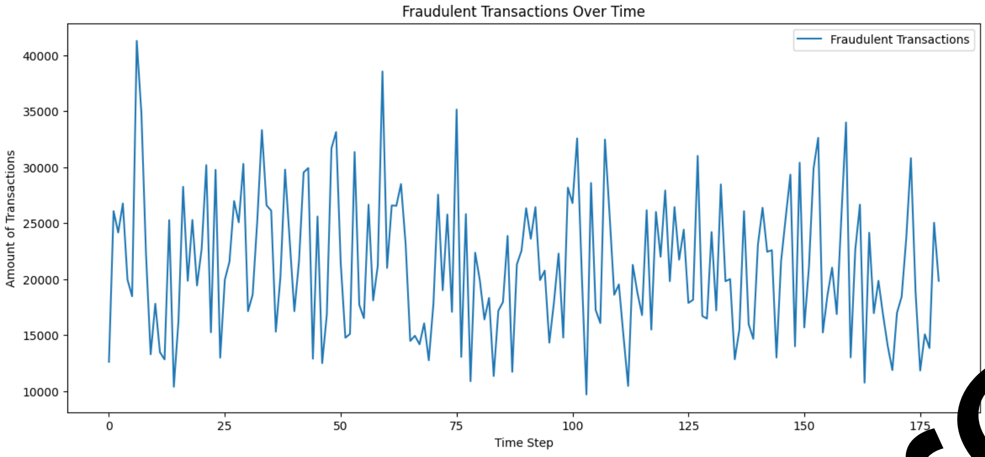


Fig.8 Transaction overtime with various conditions

The entire number of financial transactions at each time step is shown by the fig.8. All transactions over time indicates a general rise in transactions with notable alternations, suggesting that activity levels varied throughout time. There, legitimate transactions over time separates the transactions that are not fraudulent actions. Here, most of the transactions in the dataset appear to be authentic and follow a natural growth trajectory over the time periods. Only fraudulent activity is the subject of fraudulent transactions over time displays transactions, suggesting that fraudulent transactions happen sporadically rather than steadily. The adaptive behavior of fraudsters in trying to evade detection systems may be reflected in this variability.

5.3 Performance estimation

5.3.1 Accuracy

accuracy is one of the essential performance metrics used to analyse the efficiency a developed GB-WHOB model. The ratio of accurately predicted transaction such as true positives and true negatives to all transaction in the dataset. Moreover, accuracy in fraud detection refers to how well the model differentiates between transactions that are fraudulent and those that are valid. Reduced financial losses and increased confidence in financial systems can result from high fraud detection accuracy. Moreover, the accuracy is mentioned in eqn. (14),

$$A'y = \frac{T_{ps} + T_{ns}}{T_{ps} + T_{ns} + F_{ps} + F_{ns}} \tag{14}$$

True Positive (T_{ps}) This is occurs when the expected transaction and actual transaction of a data point are both 1. True Negative (T_{ns}): A data point is considered to have this property when its anticipated transaction and actual transaction are both 0. False Positive (F_{ps}): This happens when a data point has a predicted transaction of 1 but a real transaction of 0. False Negative (F_{ns}): To put it simply, this happens when a data point has a real transaction of 1 but an estimated transaction of 0.

5.3.2 Precision

Out of entire positive prediction transaction the model makes true positives and false positives, it calculates the percentage of true positive predictions from fraudulent transactions that are successfully identified is referred as precision, which is mentioned in eqn. (15).

$$\mathrm{P'r} = \frac{T_{ps}}{T_{ps} + T_{ps}} \tag{15}$$

5.3.3 Recall

Recall, is referred to as sensitivity or the true positive rate, measures the percentage of real positive cases that is, fraudulent transactions that the model properly detected. When assessing machine learning models for fraud detection, recall is an essential parameter. It highlights how the model can detect all relevant fraud transaction, reducing false negatives and enhancing the overall efficacy of fraud protection tactics. Consequently, recall is calculated using eqn. (16),

$$R'c = \frac{T_{ps}}{T_{ps} + T_{ns}} \tag{16}$$

5.3.4 F-measure

The harmonic mean of recall and precision is termed as F-measure. These two conditions are used to create a single score that sums up the proposed GB-WHOB model’s overall performance. Datasets used in fraud detection are frequently unbalanced, with a disproportionately high number of valid transactions compared to fraudulent ones. Compared to accuracy alone, the F-measure offers a more realistic assessment of performance, which is calculated using eqn. (17),

$$F'(m) = 2\left(\frac{R'c \times \mathrm{P'r}}{R'c + \mathrm{P'r}}\right) \tag{17}$$

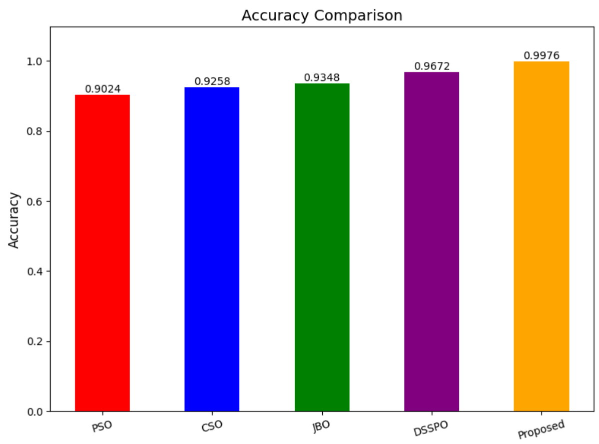
5.3.5 Error rate

The number of inaccurate transactions from of all predictions is measured by the error rate. Error rate is the important parameter for evaluating the calibre of machine learning models and data analysis utilized in fraud detection.

5.4 Comparative analysis in terms of optimization models

In this section we discussed the comparative analysis of optimization algorithms to assess the performance of developed GB-WHOB algorithm in terms of various performance metrices. The comparative optimization algorithm are Particle Swarm Optimization (PSO) [26], Cuckoo Search Optimization (CSO) [27], Jellyfish Beetle Optimization (JBO) [28], Dwarf Shuffled Shepherd Political optimization (DSSPO) [29].

From the comparison of accuracy measure we take four optimization algorithms such as PSO, CSO, JBO and finally DSSPO which are recently used in fraudulent behaviour identification performance. This algorithm has provided better results for fraud prediction. However, the developed GB-WHOB frameworks offered highest value which nearly 7% to 8% enhancement. First of all, accuracy of the PSO algorithm is 0.9024% which is lower than the other three comparative models such as CSO, JBO and DSSPO. Then, CSO algorithm has 0.9258% of accuracy which is higher than the PSO model and lower than the JBO and DSSPO. After that, take the JBO algorithm which has attained 0.9348% lower than the DSSPO replica and higher than the CSO and PSO algorithm. Finally, DSSPO model has achieved 0.9672% of accuracy which has higher than the PSO, CSO and JBO algorithms. While comparing this with our developed model, the GB-WHOB model has gained better results as 0.9976% accuracy. This performance has demonstrated the better prediction behaviour of financial transactions and also identify the fraudsters with higher accuracy, which is mentioned in fig.9.



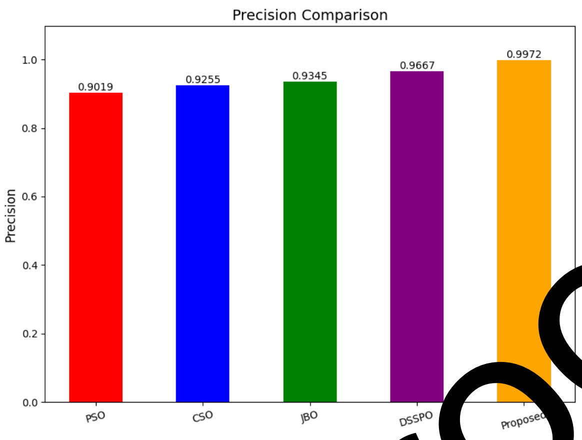


Figure.9 Comparison of accuracy with proposed GB-WHOB model

Figure.10 Comparison of precision with proposed GB-WHOB model

Moreover, precision measure we take four optimization algorithms such as PSO, CSO, JBO and finally DSSPO which are recently used in fraudulent behaviour identification performance. This algorithm has provided better results for fraud prediction. However, the developed GB-WHOB frameworks offered highest precision measure which nearly 7% to 8% enhancement. First of all, precision of the PSO algorithm is 0.9019%, while comparing the other three models PSO has less precision measure. Furthermore, CSO algorithm has 0.9255% of precision measure and JBO algorithm which has attained 0.9345% of precision. These two algorithms have nearly 1% to 2% of increment of precision while comparing the DSSPO replica. After that, DSSPO model has achieved 0.9667% of precision which has higher than the PSO, CSO and JBO algorithms. While comparing this with our developed model, the GB-WHOB model has gained better results as 0.9972% precision. The improvement of precision in the proposed GB-WHOB analyses that the integration of optimization and classifiers to provide the finest outcomes. Moreover, the comparative assessment of developed model with existing model in terms of precision performance metrics are demonstrated in figure.10.

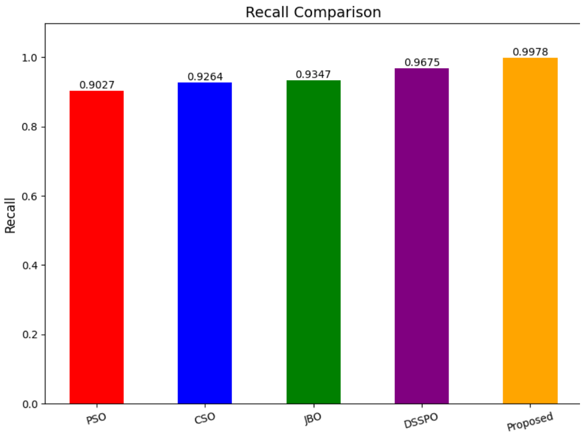


Figure.11 Comparison of recall with proposed GB-WHOB model

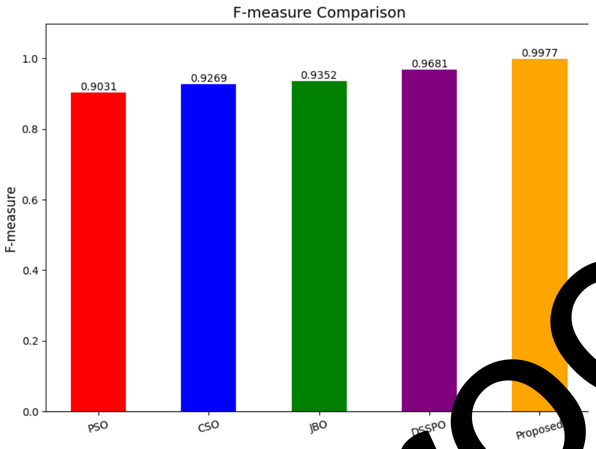


Figure.12 Comparison of F-measure with proposed GB-WHOB model

For the comparative analysis of recall measurement, we take optimization algorithms such as PSO, CSO, JBO and finally DSSPO which are recently used in fraudulent behaviour identification performance. This algorithm has provided better results for fraud prediction performance towards the financial transactions. First of all, recall of the PSO algorithm is 0.9027% which is lower than the other three comparative models such as CSO, JBO and DSSPO. Then, CSO algorithm has 0.9264% of recall which is higher than the PSO model and lower than the JBO and DSSPO. After that, take the JBO algorithm which has attained 0.9347% lower than the DSSPO replica and higher than the CSO and PSO algorithm. Finally, DSSPO model has achieved 0.9675% of recall which has higher than the PSO, CSO and JBO algorithms. While comparing this with our developed model, the GB-WHOB model has gained better results as 0.9978% recall. Here, the developed GB-WHOB frameworks offered highest value which nearly 7% to 8% enhancement. The enhancement of recall measure demonstrates efficiency and accurate prediction performance of the positive classes and reducing the false negative and positive classes, which is demonstrated in fig. 11.

In addition, F-measure rate of the PSO algorithm is 0.9031%, while comparing the other three models PSO has less F-measure rate. Furthermore, CSO algorithm has 0.9629% of F-measure rate and JBO algorithm which has attained 0.9352% of F-measure rate. These two algorithms have nearly 1 to 2% of increment of F-measure rate while comparing the DSSPO replica. After that, DSSPO model has achieved 0.9681% of F-measure rate which has higher than the PSO, CSO and JBO algorithms. While comparing this with our developed model, the GB-WHOB model has gained better results as 0.9977% F-measure rate. The improvement of F-measure rate in the proposed GB-WHOB analyses that the integration of optimization and classifiers to provide the finest outcomes, which is demonstrated in fig. 12.

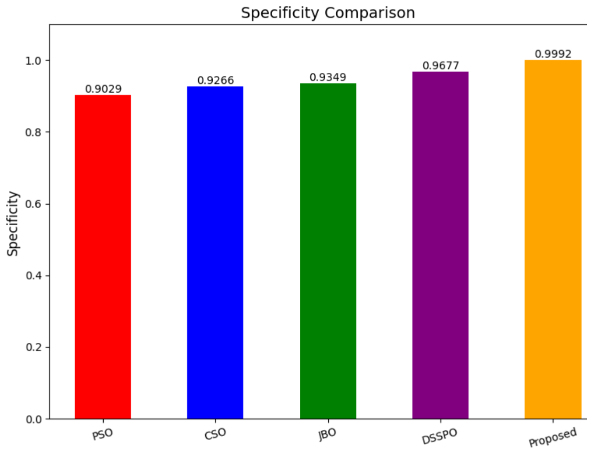


Figure.13 Comparison of specificity with proposed GB-WHOB model

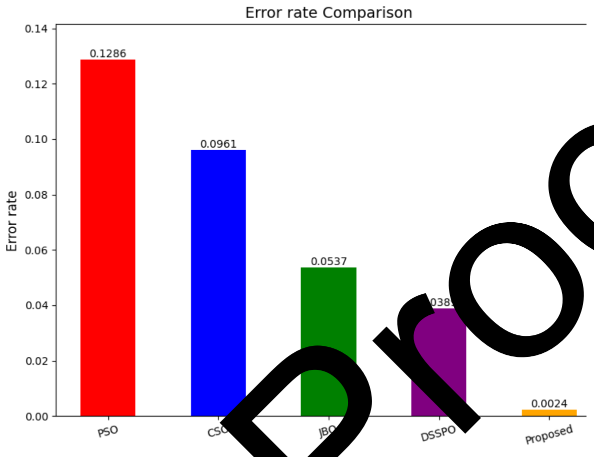
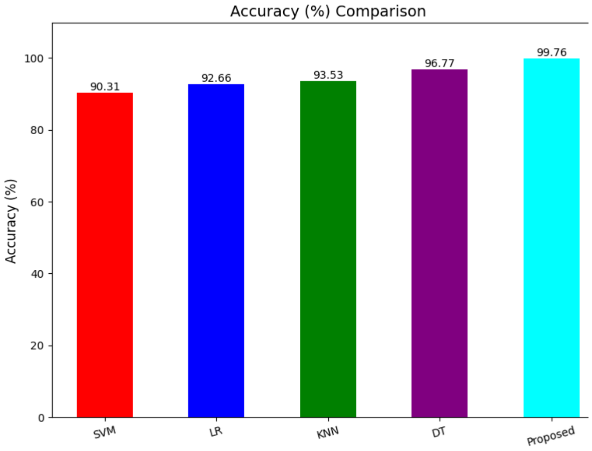


Figure.14 Comparison of Error rate with proposed GB-WHOB model

Consequently, specificity and error rate comparative analysis we take optimization algorithms such as PSO, CSO, JBO and finally DSSPO which are recently used in fraudulent behaviour identification performance. This algorithm has provided better results for fraud prediction performance towards the financial transactions. From the comparison, the specificity value of the as PSO, CSO, JBO and DSSPO has 0.9029%, 0.9266%, 09349% and 0.9677% respectively. Similarly, the attained error rate of the existing models such as 0.1286%, 0.0961%, 0,0537 and 0.0389% respectively. But the developed GB-WHOB model gas gained 0.9992% specificity measure, which is demonstrated in fig. 13. This improvement has ensured the effectiveness of the accurately detect the fraudulent behaviour based on that predicted feature. Then, the error rate of the proposed GB-WHOB model has got 0.0024% error which is very low while comparing the existing models, which is demonstrated in fig. 14.

5.5 Comparative analysis in terms of classifiers models

In this section we discussed the comparative analysis of ML classifier to assess the performance of developed GB-WHOB algorithm in terms of various performance metrices. The comparative classifiers are Support Vector Classifier (SVM) [30], Logistic Regression (LR) [31], K-Nearest Neighbour (KNN) [32], and Decision Tress (DT) [33].



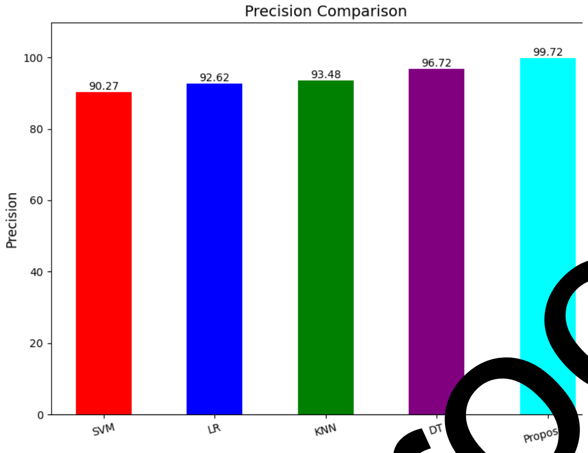
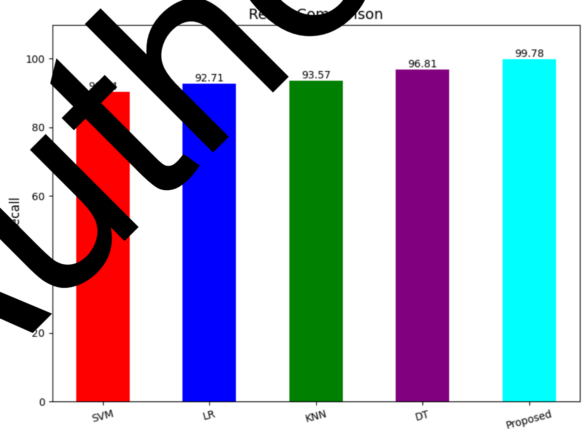


Figure.15 Comparison of accuracy with proposed GB-WHOB model

Figure.16 Comparison of precision with proposed GB-WHOB model

Accuracy is referred as overall exactness level of the model for identifying the fraudulent behavior based on the extracted features. Moreover, accuracy of the proposed algorithm with the traditional classifiers like SVM, LR, KNN and DT. These existing classifiers and the developed GD-WHOB model has achieved an accuracy value of 0.9031, 0.9266, 0.9353, 0.9677 and 0.9976, respectively. Similarly, precision rate is 0.9027, 0.9 262, 0.9348, 0.9672 and 0.9972. Based on the analysis, the developed GD-WHOB algorithm has gained higher accuracy and better precision measures while comparing the convention classifier models, which is demonstrated in fig. 15. Also, the developed algorithm has validated the BO and GB model for better prediction results. This performance has highlighted the effectiveness of reliability of the fraud detection for enhancing the financial transaction. Furthermore, comparative analysis of accuracy as well as precision with existing classifiers models are illustrated in figure.16.



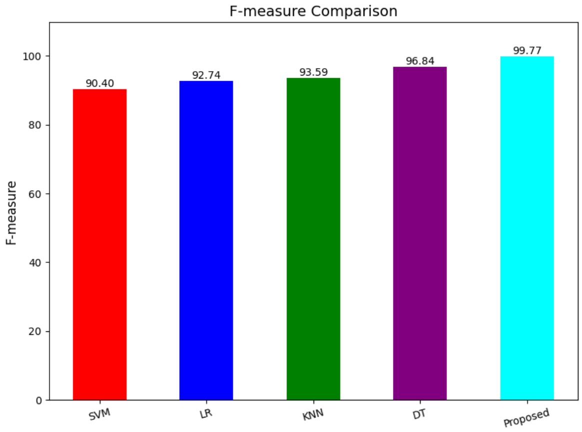
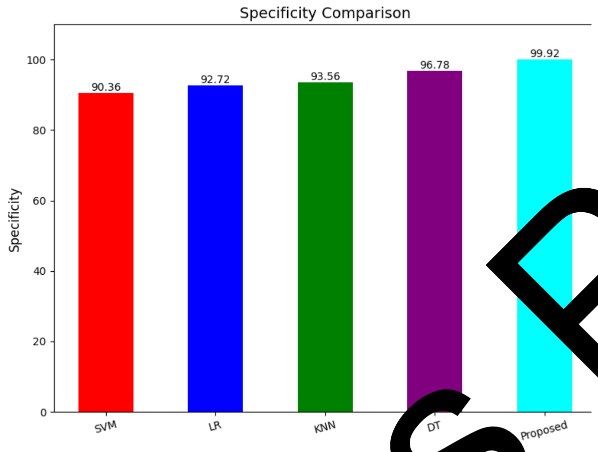


Figure.17 Comparison of recall with proposed GB-WHOB model

Figure.18 Comparison of F-measure with proposed GB-WHOB model

Consequently, recall is referred as correctly predicted actual positive classes for avoiding the negative classes. For the comparative analysis we take four classifiers such as SVM, LR, KNN and DT for validating the effectiveness of the developed model. Moreover, the attained values are 0.9034, 0.9271, 0.9357 and 0.96781 respectively. Similarly, f-measure values are 0.9040, 0.9274, 0.9359 and 0.9684 respectively. SVM model has lower performance while comparing the other three classifiers. Also, LR model processed rationally better that the conventional models. Consequently, DT and KNN has achieved well performance but its significantly poor for validating the developed GB-WHOB framework, which is demonstrated in fig. 17. Here, our developed model has gained 0.9978, which are better ability to accurate prediction performance. Also, the F-measure is 0.9977 which is better compared to conventional models, which is demonstrated in fig. 18.



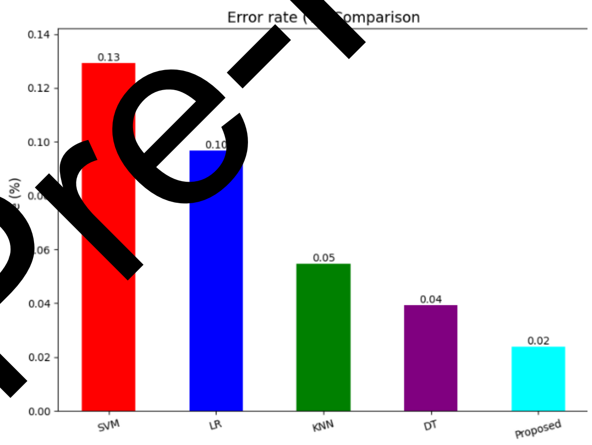


Figure.19 Comparison of specificity with proposed GB-WHOB model

Figure.20 Comparison of error rate with proposed GB-WHOB model

Consequently, recall is referred as correctly predicted actual positive classes for avoiding the negative classes. For the comparative analysis we take four classifiers such as SVM, LR, KNN and DT for validating the effectiveness of the developed model. Moreover, the attained values of specificity are 0.9036, 0.9272, 0.9356 and 0.96780 respectively. Similarly, error rates are 0. 1254, 0.0968, 0.0547 and 0.0394 respectively. SVM model has lower performance while comparing the other three classifiers. Also, LR model processed rationally better that the conventional models. Consequently, DT and KNN has achieved well performance but its significantly poor for validating the developed GB-WHOB framework, which is demonstrated in fig. 19. Here, our developed model has gained specificity is 0.9992, which are better ability to accurate prediction performance. Also, the error rate is 0.0024 which is better compared to conventional models, which is demonstrated in fig. 20.

5.5 Discussion

For comparative evaluation, the proposed model's performance was assessed against baseline methods including Particle Swarm Optimization (PSO), Cuckoo Search Optimization (CSO), Jellyfish Bloom Optimization (JBO), and Dynamic Self-Adaptive Particle Swarm Optimization (DSSPO). These benchmarks were selected to highlight the performance gains achieved through our hybrid optimization–enhanced GBT approach. The findings are clearly demonstrating that the suggested GB-WHOB approach is successful in the given categorization challenge. Its accuracy and robustness are demonstrated by the nearly flawless results on entire parameter. However, the crucial task to take into account both the particular issue being treated and the context of the data. Additional investigation, including cross-validation and testing on data, which would confirm the effectiveness of the proposed GB-WHOB approach. Understanding each method's computing cost and complexity is also essential. Even though the developed GB-WHOB approach performs the best performance in this case, and more computationally costly than a traditional less precise approach.

Table.2 overall performance and comparative analysis

Parameters	**Accuracy**	**Precision**	**Recall**	**F-measure**	**Specificity**	**Error rate**
Optimization techniques						
PSO	0.9024	0.9019	0.9027	0.9031	0.9029	0.1286
CSO	0.9258	0.9255	0.9264	0.9269	0.9266	0.0961
JBO	0.9348	0.9345	0.9347	0.9352	0.9349	0.0537
DSSPO	0.9672	0.9667	0.9675	0.9681	0.9677	0.0389
Proposed	0.9976	0.9972	0.9978	0.9977	0.9992	0.0024
Classifiers						
SVM	0.9031	0.9027	0.9034	0.9040	0.9036	0.1291
LR	0.9266	0.9262	0.9271	0.9274	0.9272	0.0968
KNN	0.9353	0.9348	0.9357	0.9359	0.9356	0.0547
DT	0.9677	0.9672	0.96781	0.9684	0.96780	0.0394
Proposed	0.9976	0.9972	0.9978	0.9977	0.9992	0.0024

6 Conclusion

In this research, we proposed a finest strategy for fraudsters detection and optimization methods using the combined model of ML and optimization algorithms. The GB-WHOB is named as proposed method is responsible for identifying the frauds in financial transaction. Consequently, the hybrid optimization algorithm and tuning the parameters can analyse the accurate prediction results. identified fault. Finincial transaction analysis is the main motive of this research into ML methods for financial fraud detection. Moreover, proposed GB-WHOB efficacy in differentiating between genuine and fraudulent transactions was proved via the application of classification models such as BO and GBT. The developed model for fraud detection performance, which had the greatest performance among the models with accuracy (99.76), precision (99.72), and recall (99.77), f0measure (99.92) and error rate (0.0024. The proposed GB-WHOB framework offers substantial practical value for real-world banking systems by delivering highly accurate, scalable, and adaptive fraud detection capabilities. Its integration of residual-enhanced Gradient Boosting with Whale Optimization, Harris Hawks Optimization, and Bayesian hyperparameter tuning enables the model to adapt to evolving fraud strategies, detect complex behavioral anomalies in real time, and minimize false positives. This ensures faster, more reliable decision-making for high-volume transaction streams, reducing financial losses, enhancing customer trust, and supporting compliance with regulatory requirements—making it a robust and future-ready solution for modern digital banking ecosystems.

Compliance with Ethical Standards

Conflict of interest

The authors declare that they have no conflict of interest.

Human and Animal Rights

This article does not contain any studies with human or animal subjects performed by any of the authors.

Informed Consent

Informed consent does not apply as this was a retrospective review with no identifying patient information.

Funding: Not applicable

Conflicts of interest Statement: Not applicable

Consent to participate: Not applicable

Consent for publication: Not applicable

Availability of data and material:

Data sharing is not applicable to this article as no new data were created or analyzed in this study.
Code availability: Not applicable

Reference

[1] N. F. Ryman-Tubb, P. Krause, and W. Garn, “How Artificial Intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark,” Engineering Applications of Artificial Intelligence, 2018, doi: 10.1016/j.engappai.2018.07.008.

[2] M. R. Kishore Mullangi, Vamsi Krishna Yarlagadda, Hirenkumar Dhameliya, “Integrating AI and Reciprocal Symmetry in Financial Management: A Pathway to Enhanced Decision-Making,” Int. J. Reciprocal Symmetry Theor. Phys., vol. 5, no. 1, pp. 42–52, 2018.

[3] S. K. R. A. Sai Charan Reddy Vennapusa, Takudzwa Fadziso, Dipakkumar Kanubhai Sachani, Vamsi Krishna Yarlagadda, “Cryptocurrency-Based Loyalty Programs for Enhanced Customer Engagement,” Technol. Manag. Rev., vol. 3, no. 1, pp. 46–62, 2018.

[4] H. Zhou et al., “A distributed approach of big data mining for financial fraud detection in a supply chain,” Comput. Mater. Contin., 2020, doi: 10.32604/CMC.2020.09834.

[5] K. Rai and R. K. Dwivedi, “Fraud Detection in Credit Card Data using Unsupervised Machine Learning Based Scheme,” in Proceedings of the International Conference on Electronics and Sustainable Communication Systems, ICESC 2020, 2020. doi: 10.1109/ICESC48915.2020.9155615.

[6] H. Ghaneei, A. Keramati, S. M. Mirmohammadi, "Developing a prediction model for customer churn from electronic banking services using data mining", Financial Innovation, Vol. 2, No. 1, 2016, pp. 1-13.

[7] [illegible] Huang, W. Wang, Y. Wei, Y. Sun, "A two-route CNN model for bank account classification with heterogeneous data", PlosOne, Vol. 14, No. 8, 2019, p.e0220631.

[8] Smeureanu, G. Ruxanda, L. M. Badea, "Customer segmentation in private banking sector using machine learning techniques", Journal of Business Economics and Management, Vol. 14, No. 5, 2013, pp. 923-939.

[9] F. N. Ogwueleka, S. Misra, R. Colomo, L. Fernandez, "Neural network and classification approach in identifying customer behavior in the banking sector: A case study of an international bank", Human factors and ergonomics in manufacturing & service industries, Vol. 25, No. 1, 2015, pp. 28-42.

[10] Ismail, Mustafa Mohamed, and Mohd Anul Haq. "Enhancing Enterprise Financial Fraud Detection using Machine Learning." *Engineering, Technology & Applied Science Research* 14.4 (2024): 14854-14861.

[11] Pillai, Retheesh P., and D. Ponmary Pushpa Latha. "Study on Application of Artificial Intelligence and Machine Learning in the Banking Sector for Fraud Detection and Prevention." *Machine Learning for Environmental Monitoring in Wireless Sensor Networks*. IGI Global, 2025. 359-382.

[12] Usman, Abdullahi Ubale, et al. "Financial Fraud Detection Using Value-at-Risk with Machine Learning in Skewed Data." *IEEE Access* (2024).

[13] Damanik, Nurafni, and Chuan-Ming Liu. "Advanced Fraud Detection: Leveraging K-SMOTEENN and Stacking Ensemble to Tackle Data Imbalance and Extract Insights." *IEEE Access* (2024).

[14] Sabareesh, R., et al. "AI-Driven Fraud Detection in Banking: Enhancing Transaction Security."

[15] Vashistha, Astha, and Anoop Kumar Tiwari. "Building Resilience in Banking Against Fraud with Hyper Ensemble Machine Learning and Anomaly Detection Strategies." *SN Computer Science* 5.5 (2024): 1-14.

[16] Sharma, Renuka, Kiran Mehta, and Poonam Sharma. "Role of Artificial Intelligence and Machine Learning in Fraud Detection and Prevention." *Risks and Challenges of AI-Driven Finance: Bias, Ethics, and Security*. IGI Global, 2024. 90-120.

[17] Kamble, Vitthal B., et al. "Enhancing UPI Fraud Detection: A Machine Learning Approach Using Stacked Generalization." *International Journal of Multidisciplinary on Science and Management* 2.1 (2025): 69-83.

[18] Zheng, Xiangling. "Suspicious Transaction Recognition Based on KNN Model for Credit Card Fraud Prevention." *International Conference on Computational Finance and Business Analytics*. Cham: Springer Nature Switzerland, 2024.

[19] Udeh, Ezekiel Onyekachukwu, et al. "The role of big data in detecting and preventing financial fraud in digital transactions." *World Journal of Advanced Research and Reviews* 22.2 (2024): 1746-1760.

[20] Nhien, Cao Thi, Dang Ngoc Hung, and Vu Thi Thanh Bình. "Using random forest and artificial neural network to detect fraudulent financial reporting: Data from listed companies in Vietnam." *Calitatea* 25.202 (2024): 160-173.

[21] Hou, Xuechen. "Financial Abnormal Data Detection System Based on Reinforcement Learning." *Mobile Information Systems* 2022.1 (2022): 7358383.

[22] Hajek, Petr, Mohammad Zoynul Abedin, and Uthayasankar Sivarajah. "Fraud detection in mobile payment systems using an XGBoost-based framework." *Information Systems Frontiers* 25.5 (2023): 1985-2003.

[23] Arfeen, A. Asad, and B. Muhammad Asim Khan. "Empirical analysis of machine learning algorithms on detection of fraudulent electronic fund transfer transactions." *IETE Journal of Research* 69.11 (2023): 7920-7932.

[24] Vashistha, Astha, et al. "A Robust Framework for fraud Detection in Banking using ML and NN." *Proceedings of the National Academy of Sciences, India Section A: Physical Sciences* 94.2 (2024): 201-212.

[25] Shdefat, Ahmed Younes, et al. "Comparative Analysis of Machine Learning Models in Online Payment Fraud Prediction." *2024 Intelligent Methods, Systems, and Applications (IMSA)*. IEEE, 2024.

[26] Al-dahasi, Ezaz Mohammed, et al. "Optimizing fraud detection in financial transactions with machine learning and imbalance mitigation." *Expert Systems* 42.2 (2025): e13682.

[27] Sorour, Shaymaa E., et al. "Credit card fraud detection using the brown bear optimization algorithm." *Alexandria Engineering Journal* 104 (2024): 171-192.

[28] Yu, Gui, and Zhenlin Luo. "Financial fraud detection using a hybrid deep belief network and quantum optimization approach." *Discover Applied Sciences* 7.5 (2025): 454.

[29] Talukder, Md Alamin, Majdi Khalid, and Md Ashraf Uddin. "An integrated multistage ensemble machine learning model for fraudulent transaction detection." *Journal of Big Data* 11.1 (2024): 168.

[30] Usman, Abdullahi Ubale, et al. "Financial Fraud Detection Using Value-at-Risk with Machine Learning in Skewed Data." *IEEE Access* (2024).

[31] Esmail, Fahd Sabry, Fahad Kamal Alsheref, and Amal Elsayed Aboutabl. "Review of loan fraud detection process in the banking sector using data mining techniques." *International journal of electrical and computer engineering systems* 14.2 (2023): 229-239.

[32] Ashtiani, Matin N., and Bijan Raahemi. "Intelligent fraud detection in financial statements using machine learning and data mining: a systematic literature review." *Ieee Access* 10 (2021): 72504-72525.

[33] Nalini, M., et al. "Enhancing anomaly detection Efficiency: Introducing grid searchbased multi-population particle Swarm optimization algorithm based optimized Regional based Convolutional neural network for robust and scalable solutions in High-Dimensional data." *Biomedical Signal Processing and Control* 96 (2024): 106651.