IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Credit Card Fraud Detection System Using Machine Learning

[1] Ms. Kavita S. Pawar, [2]Mr. Dhaval Chudasama

[1]PG Student, [2]Assistant Professor,

[1]Dept. of Computer Engineering, [2]Dept. of Cyber Security,

[1]Gandhinagar University, Gandhinagar, Gujarat, India

Abstract: In this digital world, there are numerous credit card fraud detection systems. This research aims to explore the various approaches applied in Credit Card Fraud Detection, along with the selection or pre-processing of datasets for the purpose of constructing Machine Learning, Deep Learning, and Neural Network models. Many models, including decision trees, logistic regression, neural networks, Gaussian kernels, neural networks based on mining systems, self-organizing maps, generative adversarial networks, ensemble learning, AdaBoost, majority voting, deep convolution neural network model, adversarial learning, fuzzy clustering, optimized light gradient boosting, anti-k nearest neighbor, calibrated probabilities, bidirectional Long short-term memory (BiLSTM), and bidirectional Gated recurrent, will be covered.

Key Words - Credit Card Fraud Detection, Credit Card, Frauds, Machine Learning, Deep Learning, Detection, Methods, Classifiers.

Fig.1 Credit card fraud [12]

I. INTRODUCTION

Credit cards have become ubiquitous in modern life, offering unparalleled convenience and flexibility in managing finances. Credit cards facilitate a wide range of transactions, from routine purchases to online shopping and travel expenditures, ensuring a secure payment process. Furthermore, many credit cards offer rewards programs and additional benefits, encouraging their utilization. But with all the pros there comes cons as well, Credit card fraud remains a significant concern in today's digital age. Even with improvements in security protocols, criminals persist in discovering innovative methods to take advantage of weaknesses within the system. Frauds can occur through various methods, including Skimming, Phishing, Data breaches, Card-not-present transactions, Identity theft.

Fig.2 Uses of credit card [13]

1.1 MACHINE LEARNING AND DEEP LEARNING

1.1.1 **Machine Learning:**

Artificial Intelligence encompasses a specific subset and is a discipline within Computer Science that allows computers to acquire knowledge from data, enabling them to make predictions or decisions autonomously, without the need for explicit programming.

Types of machine learning techniques include:

1. Supervised learning involves training an algorithm on a dataset that is labeled, meaning the expected output
   is already known. This allows the algorithm to generate predictions or make decisions based on new, previously unseen data.
2. Unsupervised learning entails training an algorithm on a dataset that lacks labels, where the expected output is unknown. The primary objective is to identify patterns, structures, or relationships within the data, which may include clustering similar data points or reducing the dimensionality of the data while maintaining its essential structure.
3. Reinforcement learning operates on the principle of rewards and penalties when processing data. The algorithm learns from the feedback received after each action, enabling it to autonomously identify the most effective pathways to achieve desired outcomes.

1.1.2 **Deep Learning:**

Deep learning is a specialized area within machine learning and a division of computer science that employs artificial
neural networks with several layers, referred to as "deep." This approach enables computers to process information in
a way that mimics human cognitive functions. By recognizing patterns across various data types, including text, audio,
and images, deep learning models are capable of delivering accurate predictions and insights.

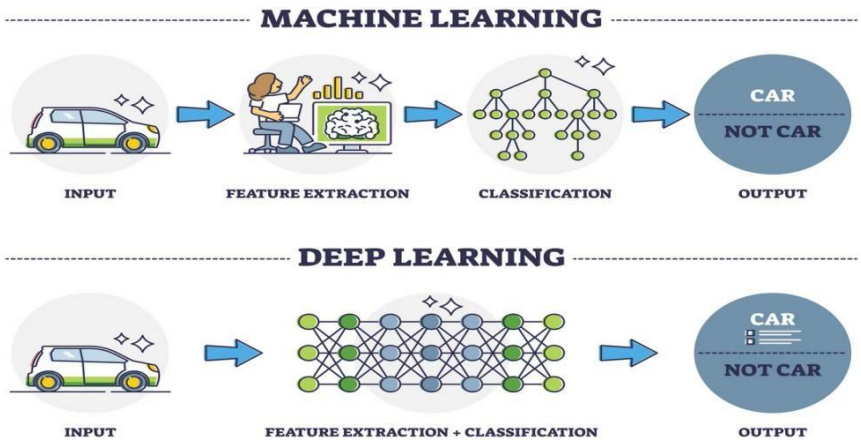

Fig.3 Machine learning and Deep learning [14]

II. LITERATURE SURVEY

In reference [1], the discussion centers on neural networks and their significant contribution to the detection of credit card fraud. This paper will explore conversational neural networks and their effectiveness in enhancing credit card fraud detection. Feature matrix also known as design matrix or feature set that is the structured representation of data is used to represent the abandoned transactions data. They started with giving a small description of CNN-based credit card fraud detection framework and then introduced us to the novel trading features and ended with the final step of problem solving of credit card fraud detection. First and second steps fall under offline training and the third step of prediction will be online. When the transaction arrives in the system it is categorized into legitimate or fraudulent in no time. Sequential steps that will be followed are feature selection, feature transformation and then classification. When we have a large set of data and over fitting of modules, CNN provides convenience. Image classification and speech signal processing are two prominent applications of convolutional neural networks. The original attributes of the transactions are used to generate a one-dimensional sequential data which is then further used to generate the feature matrix.

Random samples of legitimate and fraudster transactions are selected to generate the heat map. The sequential layers in CNN network are convolution, sampling layer and then again the convolution layer. The next three layers together are called fully connection layers as they contain all the connectivity information.

The data set chosen in this paper was from the traditional commercial bank. It contained 260 million transactions out of which 4000 transactions were fraudulent. Twelve months data from January to December was taken into consideration for training and 11 word records were taken for testing purposes. The output on CNN model was compared to other algorithms and it was found that CNN model has given more accurate results.

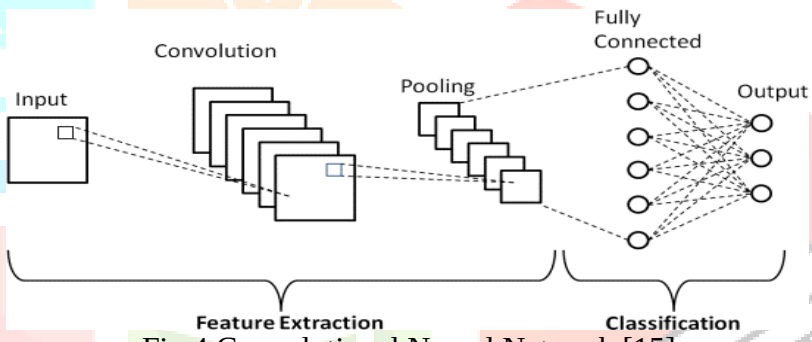

Fig.4 Convolutional Neural Network [15]

The paper [2] discussed the use of meta learning in fraud detection. They developed a system comprising two key elements: Local Fraud Detection Agents and a Meta Learning Agent.

Local fraud systems learn from the previous system and detect the intrusion of fraud agents. With the help of Meta learning we can learn, combine and integrate one or more classifiers or models. Multiple U.S banks contributed in creating a data set of around 500000 transaction records which had 30 fields each. Ten months data from January to October was used and labeled as fraud transaction and non-fraud transaction. This data set has 42000 records which were used for training purposes. November's data with 4000 records was used for validation and similarly December's data with same number transactions were taken into consideration for testing purposes. They used the ID3 and CART algorithm which uses a decision tree for learning. The procedure for obtaining a foundational classifier for Meta learning to utilize class-combiner was executed on two occasions, with each combination being processed 1,600 times. The data distribution comprised an equal split of 50% fraudulent transactions and 50% non-fraudulent transactions. The outcomes indicated a true positive rate of 80%, while the false positive rate remained below 16%. This distribution achieved an optimal fraud detection rate alongside a minimal alarm rate. The researchers concluded that they would implement the sliding window concept for data selection, which will be employed for training purposes to yield precise results.

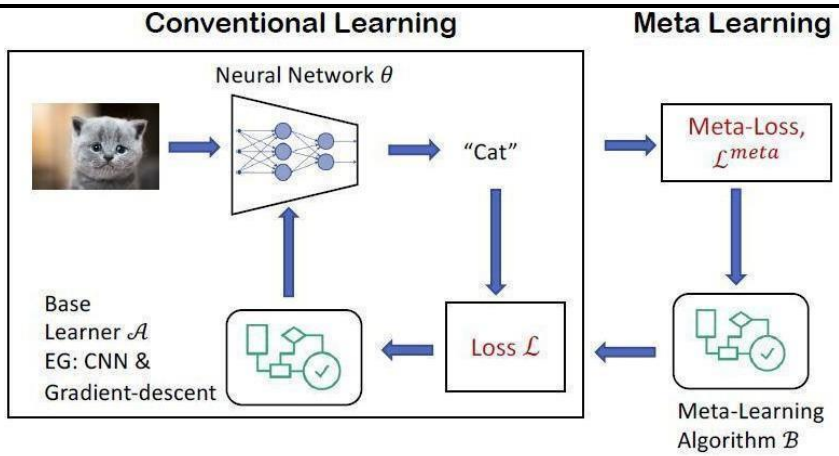

Fig.5 Meta Learning [16]

In [3], the discussion revolves around adversarial learning and its application in credit card fraud detection. The study outlines techniques to address algorithmic attacks and employs logistic regression to differentiate between fraudulent and legitimate transactions. The results indicate that adversary-aware classifiers outperform static models, achieving a higher area under the curve (AUC) score. To balance the class ratio, SMOTE is utilized for generating synthetic instances of fraudulent transactions through oversampling. The process allows the classifier to choose between strategies, either leveraging the same class or retraining. The ROC curve for adversarial learning demonstrates an improvement in the AUC, increasing from 0.78 to 0.84. Additionally, it is observed that the classifier's performance enhances progressively with each round.

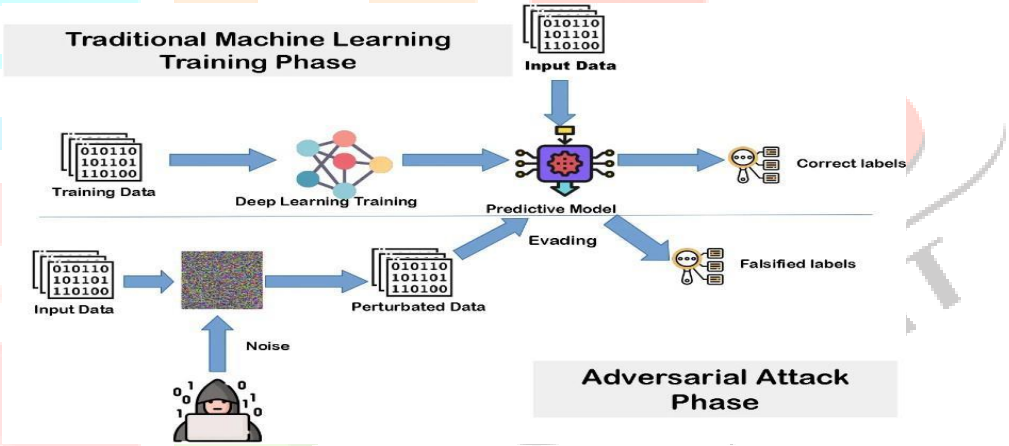

Fig.6 Adversarial Attack Phase [17]

Paper [4] discusses the application of a data mining system for credit card fraud detection, aiming to uncover implicit, interesting, and previously unknown patterns within datasets. It highlights that Visa and MasterCard users in the US collectively lose approximately $700 million annually due to fraud. The study introduces CARDWATCH, a fraud detection system implementing a feed-forward network architecture. The system comprises five key modules: the Global Constant Module (GCM), Core Graphical User Interface Module (GUIM), Database Interface Module (DBIM), Learning Algorithm Library (LAL), and Learning Algorithm Interface Module (LAIM).

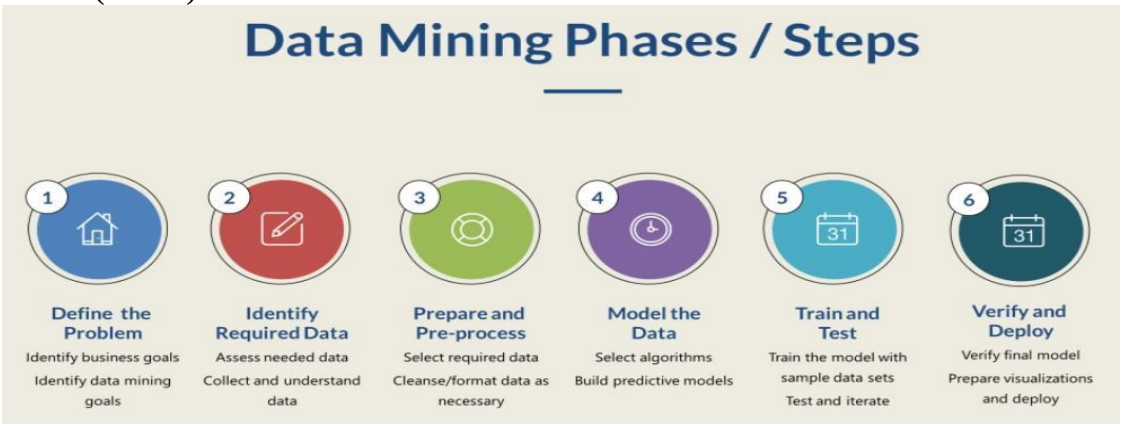

Fig.7 Data Mining Phases/ Steps [18]

CARDWATCH utilizes a three-layer neural network with an auto-associative network for training, designed to reproduce legal transaction patterns while identifying new ones. However, a limitation was its inability to reproduce fraud patterns and reliance on a single network for customer-specific restrictions. The study employed transaction generators to simulate 323 transactions across three purchase categories over a 365-day period, with 264 transactions used for training. Input data was structured in a 7-7-7 format, representing the three categories. RMS was used to evaluate whether transactions were fraudulent or legitimate. Testing results showed an 85% fraud detection rate and 100% accuracy in identifying legitimate transactions. The system's user-friendly GUI was a notable advantage. Future plans for CARDWATCH involve expanding its capabilities for general-purpose anomaly detection.

Research paper [5] presents a hybrid approach combining fuzzy clustering and neural networks for fraud detection. Fuzzy clustering refers to scenarios where a data point belongs to multiple clusters, overcoming the limitations of hard clustering, which struggles with overlapping cluster boundaries. The dataset, developed by Panigrahi due to the unavailability of real-life credit data, uses Gaussian distribution to generate synthetic transactions representing genuine and fraudulent user behavior.

The fraud detection system was implemented using MATLAB-2014, with the Fuzzy C-Mean algorithm module receiving input vectors. Each data point's suspicion score was calculated using Euclidean distance, and thresholds were set: 0.72 for the upper limit and 0.28 for the lower. Transactions with suspicion scores above the upper threshold were discarded, while those falling between the thresholds were recorded in a suspicion table. This table was then fed into the machine learning layer, where the SGC backpropagation algorithm processed it. The system utilized five hidden layers for training, with results improving as the number of layers increased, albeit at the cost of higher computation time.

The dataset was divided into 70% for training, 15% for validation, and 15% for testing. The algorithm achieved 93.9% correct classification and 6.1% misclassification of transactions. The study concluded with plans to explore experiments using different algorithms.

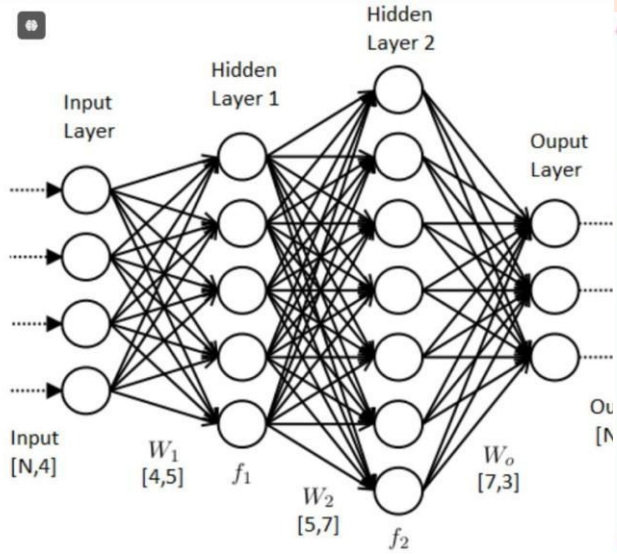

Fig.7 Neural Network [19]

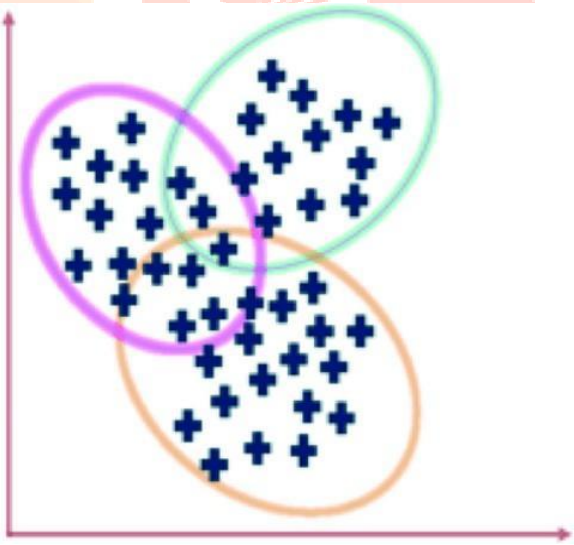

Fig.8 Fuzzy Clustering [20]

In paper [6], a hyperparameter optimization algorithm is employed to enhance the parameters of the Light Gradient Boosting Machine (LightGBM) system. Two real-world credit card transaction datasets were utilized for experimentation. The study's main contribution lies in optimizing LightGBM parameters. The experiments were conducted on a system with 8GB RAM and an Intel Core i7 processor. The first dataset comprised 284,807 credit card transactions, while the second dataset originated from the UCS-FICO data mining contest, containing e-commerce transactions. A five-fold cross-validation procedure was used for reliable comparison. The system achieved an AUC of 90.94% for dataset 1 and 92.90% for dataset 2. The recall scores were 40.50% and 28.30%, respectively. The Random Forest (RF) algorithm ranked second, with AUC scores of 90.9% and 92.8%, while the SVM algorithm achieved the lowest AUC scores of 47.8% and 70.90% for the two datasets.

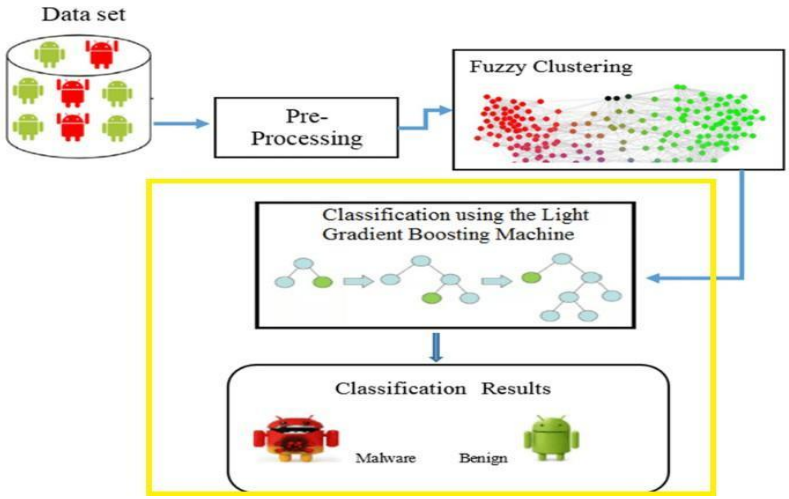

Fig.9 Light Gradient Boosting Machine [21]

In paper [7], two probability calibration methods were tested for credit card fraud detection, aiming to minimize real-world losses. The first method adjusted probabilities based on differences in bad rates between training and testing datasets, while the second calibrated probabilities by modifying the ROC curve. The dataset, provided by a major European company, covered transactions from January 2012 to June 2013. The system implemented a state-of-the-art fraud detection framework. The RF algorithm was trained using undersampling and base rate matching (BMR), enabling observation of various positive base rates. Scikit-learn was used for RF implementation, with tuned parameters to enhance estimate ranges. Logistic integration and decision trees were also applied. The BMR model showed improved fraud detection rates and precision, with savings of 41.7% and an increase of 5,820 euros. The LR-u-cal ROCCH-BMR model was identified as the best, with raw probabilities outperforming other methods in fraud detection.

Genetic algorithm is a new technology nowadays it's a means to obtain better solutions and eliminate fraud transactions. In [8], it is discussed how genetic algorithms can be used for fraud detection. Video Aar system is designed in a way that fraudulent rule sets are given to the system then a rule engine is applied in which data sets are given from that step then we move to the next step where field and priority are given then the process data is given to the genetic algorithm. This specific system is built in the applet viewer user interface module.

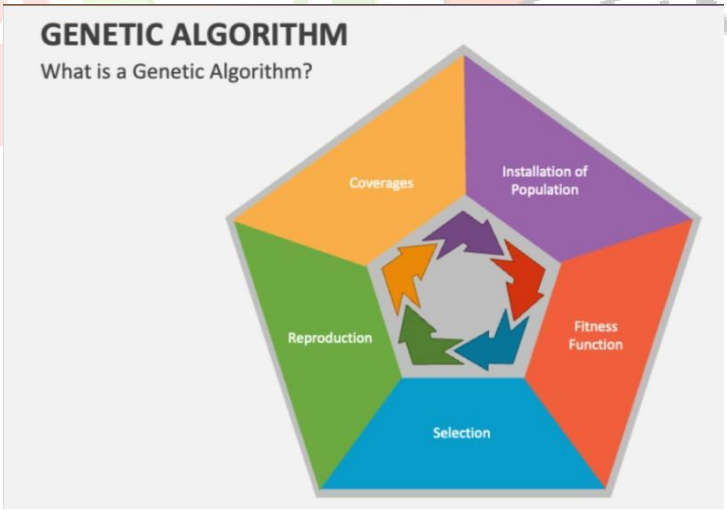

Fig.10 Genetic Algorithm [22]

In paper [9], the highly skewed nature of credit card transaction data, where fraudulent transactions are rare compared to normal ones, is addressed. The study reveals that Random Forest performs better in identifying normal transactions, while Neural Networks excel in detecting fraudulent ones. Currently, only a fraction (one-twelfth of one percent) of transactions can be identified in fraud detection systems. Fraud prevention and detection are two key strategies to combat credit card fraud, with measures like OTPs and security questions being commonly employed.

The experiment utilized a publicly accessible dataset containing numerical records. The approach combines the strengths of both algorithms to achieve higher accuracy. Training data consisted of 60% normal transactions and 60% fraudulent transactions. For cross-validation, 20% of normal and fraudulent transactions were used, while the same proportions were applied for testing.

The training process involved multiple steps:
1. Training a feed-forward neural network on the entire training dataset.
2. Training another feed-forward neural network using under sampled data with 60% fraudulent and 60% normal transactions.
3. Repeating the process with the same number of fraudulent transactions but half the normal transactions.
4. Training Random Forest models with 300 and 400 decision trees, respectively.

Cross-validation was applied to tune the parameters of these models. The outputs from the majority of classifiers were then used to test the dataset. The primary objective was to minimize the misclassification of fraudulent transactions, improving the system's accuracy and reliability.

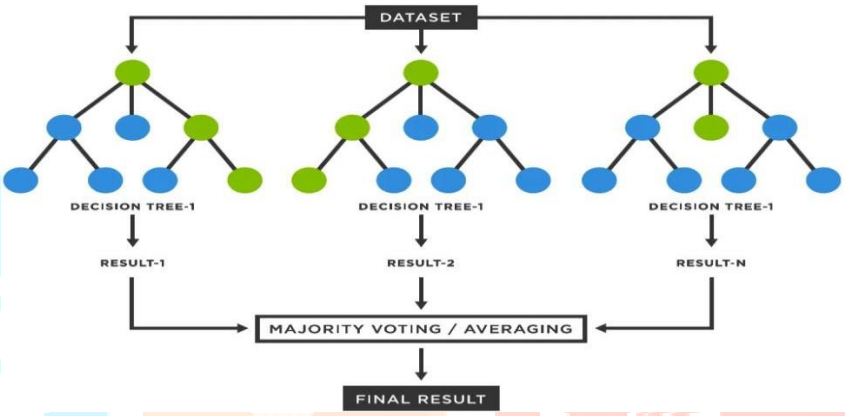

Fig.11 Random forest [23]

III. RESULT AND DISCUSSION

In the financial sector, detecting fraudulent transactions is an ongoing challenge. Traditional methods based on rule-based systems are often inefficient at handling large datasets and complex patterns. To address these challenges, machine learning (ML) models, especially Gradient Boosting Machines (GBM) such as XGBoost and Light Gradient Boosting Machine (LGBM), have proven to be highly effective in classifying transactions as either legitimate or fraudulent. Our proposed fraud detection model leverages
LGBM, which, according to studies [6] and [11], performs better than many other algorithms. The system also compares the performance of XGBoost and LightGBM to identify the more accurate model for fraud detection.

Step 1: Dataset Collection and Splitting

1. Comprehensive Data Collection: Collect datasets containing features such as transaction amounts, timestamps, transaction types, and user behavior data. These datasets often exhibit significant class imbalance, with fraudulent transactions being a small fraction of the total.
2. Dataset Splitting:
Training Set: Typically, 80% of the dataset, used for model training with labeled data.
Testing Set: The remaining 20%, used to evaluate the model's performance on unseen examples.

Step 2: Data Preprocessing

1. Feature Selection:
Retain relevant features using methods like correlation analysis or feature importance metrics.
Eliminate irrelevant features to improve efficiency and reduce overfitting risks.
2. Handling Imbalanced Data:
Apply techniques like SMOTE to balance the dataset by generating synthetic examples of fraudulent transactions.
3. Missing Data Imputation:

Address missing data by either removing incomplete rows or imputing missing values using statistical methods like mean, median, or mode imputation.

These steps ensure the dataset is prepared effectively for training machine learning models, optimizing their ability to detect fraudulent transactions.

Step 3: Normalization/Standardization

Purpose: To address differences in feature scales (e.g., transaction amount vs. time).

Normalization: Scales values to a [0, 1] range or [-1, 1] for certain algorithms.

Standardization: Centers features around zero with a standard deviation of one.

Importance: Ensures that no single feature dominates the model's decision-making, particularly for sensitive algorithms like gradient boosting.

Step 4: Categorical Encoding

Purpose: Convert categorical features into numerical formats compatible with machine learning models.

Techniques: One-Hot Encoding: Converts categories into binary columns (e.g., transaction type: online, POS → [1, 0] or [0, 1]).

Label Encoding: Assigns numeric values to categories (e.g., user IDs: User1 → 0, User2 → 1).

Selection Criteria: Depends on the nature of the feature and model requirements. One-Hot Encoding is preferred for nominal categories, while Label Encoding works well with ordinal data.

Step 5: Model Evaluation and Comparison

After training the XGBoost and LGBM models, it is crucial to evaluate their performance on the testing set using several key metrics:

Accuracy: Measures the percentage of correct predictions (both legitimate and fraudulent). However, accuracy may not be the best metric in imbalanced datasets, as high accuracy can be achieved by simply predicting the majority class (legitimate transactions).

Precision: Focuses on the fraudulent transactions predicted by the model. It measures the proportion of predicted fraudulent transactions that are truly fraudulent. Higher precision indicates fewer false positives (i.e., fewer legitimate transactions mistakenly classified as fraudulent).

Recall: Also known as Sensitivity, it measures the proportion of actual fraudulent transactions correctly identified by the model. Higher recall indicates fewer false negatives (i.e., fewer fraudulent transactions missed by the model).

Step 6: Other Evaluation Metrics

F1-Score: The harmonic means of precision and recall, giving a single metric to evaluate the trade-off between the two. A high F1-Score indicates a balanced model performance.

Area Under the Receiver Operating Characteristic (AUC-ROC) Curve: AUC is a more comprehensive measure of model performance. It evaluates the model's ability to distinguish between classes (fraudulent vs. legitimate) at various thresholds. A higher AUC indicates better model discrimination.

Confusion Matrix: Provides a detailed breakdown of true positives, true negatives, false positives, and false negatives, which helps further assess model performance in fraud detection.

Step 7: Model Comparison

After evaluating both XGBoost and LGBM, the next step is to compare their performance based on key metrics:

F1-Score: This metric balances precision and recall, offering a combined measure of the model's ability to correctly identify fraudulent transactions. A higher F1-Score indicates better performance, especially in handling both false positives and false negatives.

AUC-ROC: The Area Under the Receiver Operating Characteristic Curve provides insights into how well

the model distinguishes between fraudulent and legitimate transactions at different classification thresholds. A higher AUC value indicates that the model is better at separating the two classes.

Comparison Criteria

If both models exhibit similar performance, consider factors like:

Training Time: Choose the model that trains faster, especially if real-time processing is required.

Resource Efficiency: Select the model that uses fewer computational resources, which is essential for deployment in production environments with limited infrastructure.

Ease of Deployment: If one model has easier integration or requires less fine-tuning post-training, it could
be the better option for a smooth production rollout.

Conclusion and Model Selection

The model comparison process highlights the strengths of both XGBoost and LGBM in detecting fraudulent transactions. After evaluating both models using metrics like F1-Score, AUC-ROC, accuracy, precision, and recall, the best-performing model will be selected based on its ability to balance false positives and false negatives.

In cases where both models perform similarly, factors such as training time, resource efficiency, and ease of deployment should influence the final choice. For example, if one model is faster or requires fewer resources, it could be more suitable for real-time fraud detection systems in financial environments. Once the best model is selected, further fine-tuning and optimization can be done to ensure that it performs efficiently in production environments. This step will help minimize computational overhead while
maintaining high accuracy and performance.

Future Outlook

While traditional machine learning models like XGBoost and LGBM are highly effective in fraud detection, the evolving nature of fraud techniques and data complexity points towards the potential of deep learning models. Neural networks, with their ability to handle large and unstructured datasets and detect intricate patterns, could improve fraud detection systems significantly. Deep learning approaches could be particularly advantageous in identifying emerging fraud trends that may not be captured by traditional models. As fraud detection systems advance, incorporating deep learning techniques will provide a more robust and scalable solution for safeguarding financial transactions, representing the next frontier in financial security.

REFERENCES

[1] Fu, K., Cheng, D., Tu, Y., & Zhang, L. (2016, October). Credit card fraud detection using convolutional neural networks. In International conference on neural information processing (pp. 483-490). Springer, Cham.K. Elissa, "Title of paper if known," unpublished.

[2] Stolfo, S., Fan, D. W., Lee, W., Prodromidis, A., & Chan, P. (1997, July). Credit card fraud detection using metalearning: Issues and initial results. In AAAI-97 Workshop on Fraud Detection and Risk Management (pp. 83-90).M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[3] Aleskerov, E., Freisleben, B., & Rao, B. (1997, March). Cardwatch: A neural network based database mining system for credit card fraud detection. In Proceedings of the IEEE/IAFE 1997 computational intelligence for financial engineering (CIFEr) (pp. 220-226). IEEE.

[4] Zeager, M. F., Sridhar, A., Fogal, N., Adams, S., Brown, D. E., & Beling, P. A. (2017, April). Adversarial learning in credit card fraud detection. In 2017 Systems and Information Engineering Design Symposium (SIEDS) (pp. 112-116). IEEE.

[5] Behera, T. K., & Panigrahi, S. (2015, May). Credit card fraud detection: a hybrid approach using fuzzy clustering & neural network. In 2015 second international conference on advances in computing and communication engineering (pp. 494-499). IEEE.

[6] Taha, A. A., & Malebary, S. J. (2020). An intelligent approach to credit card fraud detection using an optimized light gradient boosting machine. IEEE Access, 8, 25579-25587.

[7] Bahnsen, A. C., Stojanovic, A., Aouada, D., & Ottersten, B. (2014, April). Improving credit card fraud detection with calibrated probabilities. In Proceedings of the 2014 SIAM international conference on data mining (pp. 677- 685). Society for Industrial and Applied Mathematics.

[8] RamaKalyani, K., & UmaDevi, D. (2012). Fraud detection of credit card payment system by genetic algorithm. International Journal of Scientific & Engineering Research, 3(7), 1-6.

[9] Sohony, I., Pratap, R., & Nambiar, U. (2018, January). Ensemble learning for credit card fraud detection. In Proceedings of the ACM India Joint International Conference on Data Science and Management of Data (pp. 289-294).

[10] Sisodia, D. S., Reddy, N. K., & Bhandari, S. (2017, September). Performance evaluation of class balancing techniques for credit card fraud detection. In 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI) (pp. 2747-2752). IEEE.

[11] Apapan Pumsirirat, Tongji University Shanghai (2018). Credit Card Fraud Detection using Deep Learning based on Auto-Encoder and Restricted Boltzmann Machine. International Journal of Advanced Computer Science and Applications (ijacsa), Volume 9 Issue 1, 2018.

[12] https://medium.com/analytics-vidhya/credit-card-fraud-detection-fd634f70327d - Last access date 13 Dec 2024

[13] https://www.incardtech.com/- Last access date 13 Dec 2024

[14] https://www.turing.com/kb/ultimate-battle-between-deep-learning-and-machine-learning - Last access date 13 Dec 2024

[15] https://d14b9ctw0m6fid.cloudfront.net/ugblog/wp-content/uploads/2020/12/1-4.png - Last access date 13 Dec 2024

[16] https://research.samsung.com/blog/Meta-Learning-in-Neural-Networks - Last access date 13 Dec 2024

[17] https://towardsdatascience.com/adversarial-machine-learning-mitigation-adversarial-learning-9ae04133c137 - Last access date 13 Dec 2024

[18] https://digitaltransformationpro.com/data-mining-steps/ - Last access date 13 Dec 2024

[19] https://www.datasciencecentral.com/the-artificial-neural-networks-handbook-part-1/ - Last access date 13 Dec 2024

[20] https://www.researchgate.net/figure/Hard-and-soft-fuzzy-clustering_fig5_351817295 - Last access date 13 Dec 2024

[21]https://www.researchgate.net/figure/The-proposed-approach-for-Android-malware-classification_fig1_345040132-
Last access date 13 Dec 2024

[22] https://www.collidu.com/presentation-genetic-algorithm - Last access date 13 Dec 2024

[23] https://medium.com/@denizgunay/random-forest-af5bde5d7e1e - Last access date 13 Dec 2024

[24] Najadat, H., Altiti, O., Aqouleh, A. A., & Younes, M. (2020, April). Credit card fraud detection based on machine and deep learning. In 2020 11th International Conference on Information and Communication Systems (ICICS) (pp. 204-208). IEEE

[25] Abhishek Shah, Dhaval Chudasama. Investigating Various Approaches and Ways to Detect Cybercrime. Journal of Network Security. 2021; 9(2): 12–20p.

[26] Makwana Utkarsh, Rathod Gopal, Dhaval Chudasama. How to Take Care During Covid 19 Situation Phishing Emails Scams. International Journal of Information Security and Software Engineering. 2021; 7(2): 24–30p.