Dizhen Dizhi Journal (ISSN:0253-4967)

ENHANCING THE DETECTION OF FRAUD IN CREDIT CARD TRANSACTION USING ENSEMBLE STACKING

Naitik ST,Asst.Professor,
Dept. Computer Science And Engineering
Dayananda Sagar University
Bangalore, India
Email: naithikenator@gmail.com

Kushal Reddy HG
Dept. Computer Science And Engineering
Dayananda Sagar University
Bangalore, India
Email: eng20cs0169@dsu.edu.in

Nithin V
Dept. Computer Science and Engineering
Dayananda Sagar University
Bangalore, India
Email: eng20cs0234@dsu.edu.in

Manjunath M
Dept. Computer Science and Engineering
Dayananda Sagar University
Bangalore, India
Email: eng20cs0190@dsu.edu.in

Kumara
Dept. Computer Science and Engineering
Dayananda Sagar University
Bangalore, India
Email: eng20cs0166@dsu.edu.in

***Abstract*— Credit cards are a vital part of modern life, facilitating transactions for individuals, businesses, and global operations. While they offer convenience and financial advantages, the prevalence of electronic fund transfers has also attracted criminals who exploit credit cards for illicit gains. Despite efforts by financial institutions to improve fraud detection, criminals continue to develop sophisticated methods to bypass these systems. Card fraud not only jeopardizes personal security but also incurs significant financial losses. To mitigate these risks, advanced fraud detection solutions are needed. Machine learning techniques, which involve training computers to identify patterns in data, hold promise in enhancing fraud detection capabilities.**

***Keywords* :** Machine Learning , Decision Tree, Gaussian Naive Bayes, Random Forest, KNN

I. INTRODUCTION

Credit card usage is becoming increasingly common in underdeveloped nations. Users utilise it to make purchases, manage their tabs, and conduct online transactions. This solution offers numerous advantages, including Making it simpler to obtain goods and services, keeping track of loan repayments made by customers, Enhancing the security of purchases. The popularity of Visa cards and weak security measures make it easy for fraudsters to extort money from Mastercard, costing the company billions of dollars. Because credit card companies are typically hesitant to disclose such details, it is difficult to obtain a precise estimate of the losses. Nonetheless, information on the monetary losses caused by Visa misrepresentation is widely available. The usage of Visas without proper security results in billion-dollar financial losses. Global monetary losses due to Mastercard fraud were 16,82,60,69,40,000.00 Indian Rupees in 2017 and are expected to rise steadily by 2020, reaching 22,87,75,50,50,000.00 Indian Rupee.

In 2019, around 29 million Indians used credit cards. Despite the advancements in technology, the Indian town of Jamtara has become a notorious hub for cybercrime during the past five years. In 2019 alone, 107 individuals from Jamtara were apprehended due to their involvement in cybercrime.

Approximately 15,44,000 Indian Rupees and 163 credit cards were seized from the perpetrators. The unauthorized and fraudulent use of credit card data without the consent of the cardholder is referred to as "Mastercard extortion". Prediction analysis, outlier modelling, global profiling, and other critical components are necessary for an organization's fraud detection solutions. Outlier models are especially beneficial for detecting fraud in new company sectors when appropriate information to create projections is not yet available. An "outlier model" in predictive analytics identifies unusual card activity based on payment data. If a card is consistently used for purchases but suddenly shows a transaction for selling, the model will highlight it as suspicious. These models leverage vast amounts of credit card data and information about cardholders to predict potential fraud. Because of the variety of transactions conducted using credit cards, several nations are dealing with diverse and novel sorts of fraudulent activity. Their team is developing algorithms and working with both real-world and simulated data sets to find a solution. One of their current challenges is the lack of available data sets due to security concerns. Without human comprehension, all of the world's knowledge is meaningless. Many organisations are increasingly engaging fraud analysts to provide human assistance, technical explanations, and improved solutions.

Credit cards have become widely used for financial transactions in the digital era, providing ease and

efficiency. However, as the number of online transactions has increased, so has the chance of fraud. Credit card fraud can cause significant financial harm to individuals and businesses. Machine learning (ML) has emerged as a powerful tool to combat fraud by enhancing detection capabilities.

Credit card fraud refers to a wide range of fraudulent practices, including unauthorised purchases, identity theft, and account breach. Existing fraud detection systems based on fixed rules often struggle to keep pace with the evolving tactics of fraudulent individuals. Machine learning, however, allows the analysis of vast amounts of data, enabling the discovery of patterns and the continuous adaptation to novel and changing fraud strategies.

Our primary aim is to develop and utilize advanced machine learning models to enhance the detection of fraudulent credit card transactions. We aim to establish a reliable system capable of real-time identification of suspicious activities, minimizing false alerts. This system will offer proactive protection against fraudulent attempts.

II. RELATED WORK

Understanding recent developments in fraud detection techniques is crucial for identifying and preventing credit card fraud.

It [1] presents methods for pre-processing and improving detection accuracy. A logistic regression algorithm achieves an AUC value of about 0.946 by utilising strategies such as unbalanced learning and hyperparameter tweaking. Machine learning methods like random forest, k-nearest neighbors, and support vector machines are shown to be useful for identifying banking fraud in this study. The paper demonstrates their effectiveness in detecting fraudulent transactions by using artificial intelligence.

This study [2] proposes a novel approach for credit card fraud detection using sentiment analysis. By analysing the emotional content in textual data associated with transactions, the system aims to outperform traditional fraud detection methods. The approach involves data collection, text extraction, sentiment analysis using models like Text Blob and VADER, and subsequent fraud detection based on negative sentiment or suspicious remarks. Model effectiveness is evaluated in terms of accuracy, recall, and F1 score, outperforming conventional methods with an accuracy rate of 98%. The proposed technique offers an efficient way to identify fraudulent transactions in real-time applications, enhancing financial security and safeguarding a company's reputation.
A study [10] leverages machine learning algorithms like Naïve Bayes and K Nearest Neighbors to combat credit card fraud by examining datasets. Commercial banks use this approach to identify potential fraud by analysing cardholder behaviour. Data mining techniques have proven effective in detecting fraudulent Mastercard transactions online. Data preparation and cleansing pose significant challenges, with algorithms focusing on handling large datasets. However, solely relying on a single algorithm to detect fraud may not be optimal.

This study [9] evaluates the accuracy of a Random Forest algorithm in detecting credit card fraud. Using a dataset of 100,000 transactions from European cardholders, the researchers tested both raw and processed data. They measured accuracy, sensitivity, specificity, and precision. The proposed fraud detection system combines information from both current and past transactions, using a rule-based filter, Dempster-Shafer adder, transaction history database, and Bayesian learner. It calculates suspicion levels, classifies transactions as normal, abnormal, or suspicious, and adapts to evolving fraud patterns, making it effective against various types of fraud.

This study [8] uses the Random Forest Machine Learning technique to detect and forecast fraudulent transactions on a real-world dataset. The technique yields a remarkable prediction accuracy of 99.94%. The report emphasises the need of integrating machine learning models into real-world transactional systems to improve cyber security and safeguard consumers and enterprises. The dataset was collected from Kaggle, a reputable online community. The resilience of Random Forest, which employs decision trees, randomization, and categorical evaluations, demonstrates its effectiveness in delivering exact forecasts, making it a powerful tool in solving cybercrime and financial fraud challenges across several sectors.

This [7] examines the effectiveness of three machine learning models (logistic regression, decision trees, and random forest) at identifying fraudulent credit card transactions. Random forest has the greatest accuracy of 96% and an AUC value of 98.9%, making it the best model for fraud prediction. The data also shows that the majority of fraud incidents occur late at night (10 p.m. to 5 a.m.), emphasising the necessity for increased surveillance during these hours. Furthermore, persons over the age of 60 are frequent targets of fraud, implying that financial institutions should prioritise in-person services while strengthening security measures for online services at night.

It employs [5] machine learning models such as LightGBM, CatBoost, and XGBoost, together with deep learning for hyperparameter fine-tuning. Experiments on real-world data, which include recall-precision measurements as well as ROC-AUC, indicate considerable increases. LightGBM and XGBoost meet high standards, with deep learning yielding ROC-AUC = 0.94, accuracy = 0.80, recall = 0.82, F1 score = 0.81, and MCC = 0.81. This method surpasses previous approaches, increasing fraud detection performance by up to 50% and the F1-score by 20%. When it comes to dealing with data imbalance, hyperparameters outperform classic sampling strategies.

This study provides a comprehensive analysis of fraud detection methods utilizing machine learning techniques, following the guidelines established by Kitchenham.It examines 87 chosen papers and summarises prominent machine learning approaches (SVM and NN), common

fraud kinds (credit card fraud), and assessment criteria. The report addresses research gaps, specifically the underutilization of unsupervised learning and clustering, which might be useful for fraud detection in restricted circumstances. It implies that future research in financial fraud detection should focus on ensemble approaches and text-mining tools such as Word2Vec and BERT.

This research study [3] compares machine learning strategies for credit card fraud detection (CCFD) and data confidentiality, presenting a hybrid solution that employs an Artificial Neural Network (ANN) inside a federated learning framework. This technique improves CCFD accuracy while maintaining privacy. Real-time datasets are used in a privacy-preserving way, and the suggested hybrid technique represents a promising opportunity for the banking and financial industries. However, real-world implementation may be difficult because to the varied norms and regulations of banks and financial institutions, and winning their trust in implementing this technology is still a work in progress.

This [4] presents a unique machine learning technique, the cortex learning algorithm, for proactive credit card fraud detection. It combines object-oriented analysis and design while converting dense credit card data from the UCI Repository to a sparse representation. The model, written in Java and simulated in Matlab, detects fraudulent transactions with a remarkable accuracy of more than 91%, outperforming Neural Network models (89.6%). This paradigm employs recursive object-oriented development, which divides the system into subsystems and modules

III. METHODOLOGY

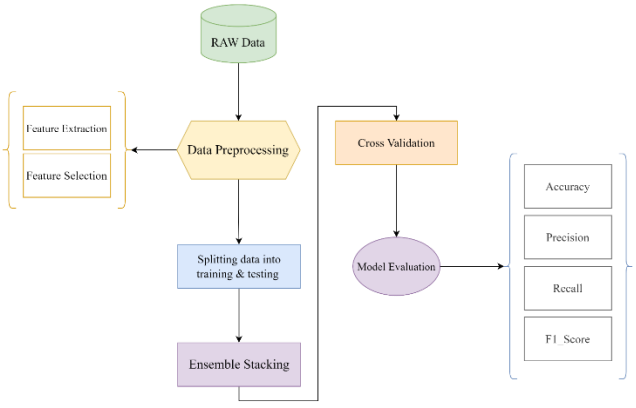


FIGURE 1 .CREDIT CARD FRAUD ARCHITECUTRE.

A . DATASET

The "creditcard" dataset includes 284,807 credit card transactions from September 2013. Within the dataset, 492 transactions were identified as fraudulent, representing approximately 0.172% of the total. The dataset exhibits a significant imbalance between regular transactions and fraudulent ones, presenting difficulties for machine learning models.

B. DATA PREPROCESSING

Identify the issue of class imbalance and suggest adjusting class weights as a remedy. Extract the "transaction hour" feature from the "time" feature to enhance data relevance. Employ the information gain (IG) method to select relevant features. Handle unbalanced data through class weight tuning, avoiding data loss or duplication techniques (under-sampling or over-sampling). Create a new "transaction hour" feature from the "time" feature to expand feature set.

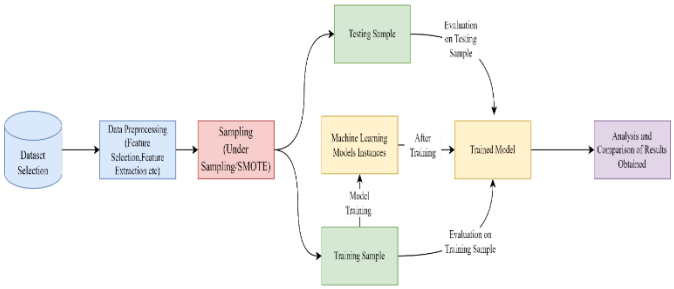


FIGURE 2 DATA FLOW DIAGRAM OF FRAUD DETECTION

C. DATA BALANCING

In credit card fraud detection, the available data is often unevenly distributed, with a much smaller proportion of fraudulent transactions compared to legitimate ones. This imbalance poses a challenge for machine learning algorithms, hindering their ability to accurately identify fraudulent activities. To overcome this issue, researchers frequently employ techniques to adjust the data balance. One approach is under sampling, which involves reducing the number of legitimate transactions. Another strategy is oversampling, which increases the number of fraudulent transactions. By creating a more balanced dataset, these techniques enhance the accuracy and dependability of fraud detection models.

In this the vast majority of transactions are legitimate, while fraudulent transactions are relatively rare. This creates a dataset with an uneven distribution, known as class imbalance. To address this, researchers often utilize a technique called Synthetic Minority Over-sampling Technique (SMOTE). SMOTE creates artificial samples of the minority class (fraudulent transactions) to make the dataset more balanced and improve the detection accuracy of fraud.

After SMOTE

Accuracy: 0.9996, Precision: 0.9118, F1: 0.8794, AUC: 0.9814

[Recall: 0.8493]

D. FEATURE SELECTION

We lack details about the features except for "Time" and "Amount." Feature selection seeks a subset of features that enhance fraud detection. The information gain (IG) method identifies crucial features for data reduction. IG extracts transaction similarities and assigns higher weights to more influential features based on transaction type (legitimate vs. fraudulent). IG is computationally efficient and has excellent precision, demonstrating its effectiveness in feature selection for credit card fraud detectio

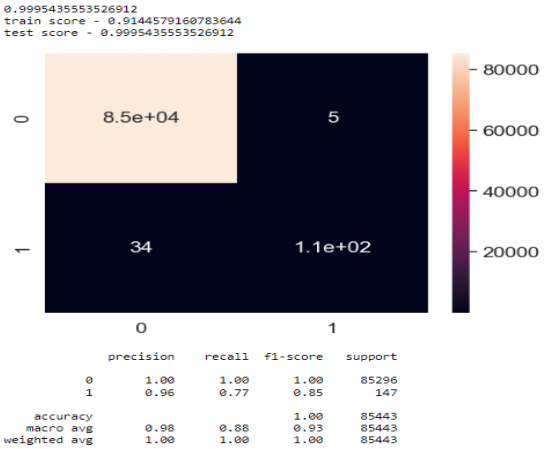
E. STACKING

Combining multiple base models through ensemble stacking boosts the accuracy of predictions. In identifying credit card fraud, ensemble stacking combines models like Decision Trees, Gaussian Naive Bayes, Random Forest, and KNN to enhance the effectiveness of fraud detection.
Develop and train four independent machine learning models (Decision Tree, Gaussian Naive Bayes, Random Forest, KNN) using a training data set.. and make predictions on a separate validation data set using each of the four trained models. Then create a new model, known as the "meta-learner". This meta-learner will combine the predictions from the four base models. Train the meta-learner using the predictions from the base models as input features and the actual values (labels) from the validation data set as the target variable. Then use the trained meta-learner to combine the predictions from the four base models, producing a final prediction. Choose a method for combining the predictions, such as simple averaging, weighted averaging, or stacking with the meta-learner. Finally Evaluate the performance of the ensemble model (created by stacking) on a held-out test dataset or the validation dataset.

FIGURE 4 USE CASE DIAGRAM

IV. RESULT ANALYSIS

Random Forest (RF) and ensemble methods like Voting and Stacking perform exceptionally well in detecting fraudulent transactions. These methods combine the strengths of different classifiers, boosting overall accuracy. Both K-nearest neighbors (KNN) and Decision Tree Classifier (DTC) algorithms have strong accuracy but are prone to changes in their datasets. To ensure their effectiveness, meticulous adjustments to their hyperparameters are essential. Gaussian Naive Bayes, though effective, has slightly lower accuracy than other models, possibly because it assumes features are independent, which may not always hold true in fraud detection.



	precision	recall	f1-score	support
0	1.00	1.00	1.00	85296
1	0.96	0.77	0.85	147
accuracy			1.00	85443
macro avg	0.98	0.88	0.93	85443
weighted avg	1.00	1.00	1.00	85443

FIGURE 5 ENSEMBLE STACKING EVALUATION

V. CONCLUSION

In summary, the ensemble stacking algorithm has demonstrated remarkable effectiveness in detecting credit card fraud, boasting an impressive accuracy rate of 99.95%, Precision of 0.96 , Recall Score of 0.77 and F1-Score of 0.85 .When stacked against conventional techniques like decision trees, Gaussian Naive Bayes, Random Forest, K-nearest neighbors (KNN), and majority voting, the stacking algorithm demonstrated superior performance. Its strength lies in its ability to combine the strengths of multiple models through ensemble learning, resulting in unparalleled precision in identifying fraudulent transactions. This advancement represents a significant milestone in combating credit card fraud, providing a powerful tool for enhancing security and maintaining trust in digital financial transactions. The banks have already modified the dataset for security reasons. It is also very unbalanced and not widely available in many implementations.

REFERENCES

[1] J. Nanduri, Y.-W. Liu, K. Yang, and Y. Jia, ``Ecommerce fraud detection through fraud islands and multi-layer machine learning model," in *Proc. Future Inf. Commun. Conf.*, in Advances in Information and Communication. San Francisco, CA, USA: Springer, 2022

[2] I. Matloob, S. A. Khan, R. Rukaiya, M. A. K. Khattak, and A. Munir, ``A sequence mining-based novel architecture for detecting fraudulent transactions in healthcare systems," *IEEE Access*,2022.

[3] E. F. Malik, K. W. Khaw, B. Belaton, W. P. Wong, and X. Chew, ``Credit card fraud detection using a new hybrid machine learning architecture," *Mathematics*, Apr. 2022.

[4] N. Kumaraswamy, M. K. Markey, T. Ekin, J. C. Barner, and K. Rascati, ``Healthcare fraud data mining methods: A look back and look ahead," *Perspectives Health Inf. Manag.*, 2022.

[5] H. Feng, ``Ensemble learning in credit card fraud detection using boosting methods," in *Proc. 2nd Int. Comput. Data Sci. (CDS)*, Jan. 2021.

[6] M. S. Delgosha, N. Hajiheydari, and S. M. Fahimi, ``Elucidation of big data analytics in banking: A four-stage delphi study," *J. Enterprise Inf. Manage.*, Nov. 2021.

[7] X. Kewei, B. Peng, Y. Jiang, and T. Lu, "A hybrid deep learning model for online fraud detection," in 2021 IEEE International Conference on Consumer Electronics and Computer Engineering (ICCECE), 2021.

[8] M. Puh and L. Brki¢, ``Detecting credit card fraud using selected machine learning algorithms," in *Proc. 42nd Int. Conv. Inf. Commun. Technol., Electron. Microelectron. (MIPRO)*, May 2019.

[9] K. Randhawa, C. K. Loo, M. Seera, C. P. Lim, and A. K. Nandi, ``Credit card fraud detection using AdaBoost and majority voting," *IEEE Access*, 2018.

[10] N. Shirodkar, P. Mandrekar, R. S. Mandrekar, R. Sakhalkar, K. M. Chaman Kumar, and S. Aswale, "Credit card fraud detection techniques – A survey," in 2020 International Conference on Emerging Trends in Information Technology and Engineering (icETITE),2020

[11] Suma, V., and Shavige Malleshwara Hills. " Data Mining based Prediction of Demand in Indian Market for Refurbished Electronics." Journal of Soft Computing Paradigm (JSCP) 2, no. 02 (2020).

[12] Kiran, Sai, et al. "Credit card fraud detection using Naïve Bayes model-based and KNN classifier." International Journal of Advanced Research, Ideas, and Innovations in Technology 4.3 ,2018.