ISSN : 2455-9679
SJIF Impact Factor : 6.190

IJRTSM
INTERNATIONAL JOURNAL OF RECENT TECHNOLOGY SCIENCE & MANAGEMENT

"MACHINE LEARNING-BASED FRAUD DETECTION FRAMEWORK FOR SECURE DIGITAL BANKING TRANSACTIONS USING CLASS IMBALANCE HANDLING"

Nisha Golkar [1], Dr. Sanmati Kumar Jain [2]

[1] M.Tech. Scholar, Department of Computer Science and Engineering, Vikrant Institute of Technology and Management, Indore, M.P. India

[2] Associate Professor & HOD, Department of Computer Science and Engineering, Vikrant Institute of Technology and Management, Indore, M.P. India

ABSTRACT

Digital banking has improved the speed, accessibility, and convenience of financial services, but it has also increased the risk of fraudulent transactions through unauthorized access, stolen credentials, phishing, malware, and abnormal transaction behaviour. Traditional rule-based fraud detection systems are limited because they depend on predefined rules and may fail to identify new or hidden fraud patterns. Therefore, this paper presents a machine learning-based fraud detection framework for secure digital banking transactions. The study uses the Credit Card Fraud Detection Dataset, which contains 284,807 transactions, including 284,315 genuine transactions and 492 fraudulent transactions. Since fraudulent transactions represent only 0.172% of the dataset, the problem is highly imbalanced and requires careful preprocessing. The methodology includes dataset analysis, missing value checking, duplicate record checking, feature separation, scaling of numerical features, stratified train-test splitting, and class balancing using SMOTE. An 80:20 stratified split is used to preserve the original class ratio in both training and testing sets. SMOTE is applied only to the training data to improve minority-class representation while keeping the testing data unchanged for realistic evaluation. The analysis confirms that class imbalance is a major challenge in digital banking fraud detection and that preprocessing and balancing are essential for developing reliable machine learning models. The proposed framework provides a systematic foundation for fraud detection by improving the learning capability of models toward rare fraudulent transactions while supporting secure digital banking operations.

Keywords: *Digital banking; fraud detection; machine learning; credit card fraud; class imbalance; SMOTE; secure transactions; financial security; transaction classification.*

I. INTRODUCTION

Digital banking has transformed the traditional banking system by allowing customers to perform financial transactions through internet banking, mobile banking, debit cards, credit cards, automated teller machines, digital wallets, and other electronic payment channels. These services provide speed, convenience, accessibility, and flexibility to customers. However, the rapid growth of digital banking has also increased the risk of fraudulent activities. Fraudsters continuously attempt to exploit weaknesses in digital banking systems by using stolen credentials, fake identities, unauthorized access, phishing links, malware, social engineering, and abnormal transaction behavior. Therefore, fraud detection has become an essential component of secure digital banking.

Fraud detection in digital banking refers to the process of identifying suspicious or unauthorized transactions before

ISSN : 2455-9679
SJIF Impact Factor : 6.190

they cause financial loss to customers, banks, or financial institutions. In earlier banking systems, fraud detection was mainly performed through manual inspection and fixed rule-based systems. These systems used predefined rules such as transaction amount limits, unusual location checks, repeated failed login attempts, and abnormal transaction

frequency. Although such traditional systems are useful to some extent, they are not sufficient for modern digital banking because fraudulent behavior changes continuously. A fixed rule may detect known fraud patterns but may fail to identify new or hidden fraud patterns [1], [2].

Machine learning provides a powerful approach for fraud detection because it can learn from historical transaction data and identify patterns that may not be easily detected through manual rules. A machine learning model can be trained on previous genuine and fraudulent transactions and then used to classify new transactions as legitimate or fraudulent. This makes machine learning suitable for large-scale banking systems where millions of transactions are generated every day.

In a machine learning-based fraud detection system, transaction data is collected from digital banking platforms and processed through different stages such as data cleaning, feature selection, data normalization, model training, model testing, and final fraud prediction. The system learns the behavioral difference between genuine and fraudulent transactions and generates a decision based on learned patterns. In this thesis, the topic “Machine Learning-Based Fraud Detection System for Secure Digital Banking Transactions” focuses on developing a data-driven fraud detection system that can improve the security of digital banking transactions by identifying suspicious transaction behavior.

The importance of this research lies in the fact that fraud detection is not only a technical problem but also a financial and social concern. A successful fraud detection system can reduce financial loss, improve customer trust, support secure banking operations, and help financial institutions respond quickly to suspicious activities. Since digital banking is continuously expanding, an intelligent and efficient fraud detection mechanism is required to protect users and banking systems from modern fraud threats [3], [4].

Digital banking is the use of electronic platforms and information technology to deliver banking services without requiring the customer to visit a physical bank branch. It includes internet banking, mobile banking, card-based transactions, electronic fund transfer, digital wallets, unified payment systems, and other online financial services. Through digital banking, customers can transfer funds, pay bills, check account balances, apply for services, manage cards, and perform financial operations at any time and from any location. This has made banking faster, more accessible, and more customer-oriented [5-7].

The development of digital banking has changed the structure of financial services. Earlier, banking activities were mostly branch-based and required physical verification, paper records, and direct interaction between the customer and bank staff. With the introduction of automated teller machines, online banking, mobile applications, and real-time payment systems, financial services became faster and more automated. Digital banking has also helped banks reduce operational cost, improve service delivery, and provide 24-hour access to customers. However, the same digital infrastructure that provides convenience also creates new opportunities for cybercriminals and financial fraudsters.

II. METHODOLOGY

2.1 Dataset Description

Dataset selection is one of the most important steps in a machine learning-based fraud detection study. A machine learning model learns patterns from data, and therefore the reliability of the model depends strongly on the quality and relevance of the dataset. In real banking systems, transaction data is highly confidential because it contains sensitive financial and customer-related information. For academic research, publicly available anonymized datasets are commonly used to avoid privacy and security issues.

In the present thesis, the Credit Card Fraud Detection dataset is used for developing and evaluating the proposed fraud detection system. This dataset contains real anonymized credit card transactions and is widely used in fraud detection research. It contains both genuine and fraudulent transactions. The dataset is suitable for this thesis because it represents a realistic imbalanced fraud detection problem, where the number of genuine transactions is much higher

ISSN : 2455-9679
SJIF Impact Factor : 6.190

than the number of fraudulent transactions [8-11].

The dataset contains 284,807 transactions. Out of these, 284,315 transactions are genuine, while 492 transactions are fraudulent. The fraudulent transactions represent only 0.172% of the complete dataset. This shows that the dataset is highly imbalanced. Such imbalance is common in real digital banking systems because fraudulent transactions are rare compared with normal banking activity. This makes the dataset suitable for evaluating machine learning models under realistic fraud detection conditions.

The selected dataset contains 31 columns. Out of these, 30 columns are input features and one column is the target variable. The input features include Time, Amount, and anonymized features V1 to V28. The target variable is Class. In the Class column, value 0 represents a genuine transaction, while value 1 represents a fraudulent transaction. Due to confidentiality reasons, the original meanings of V1 to V28 are not provided. These features are principal component transformed variables generated from the original transaction attributes. The dataset used in the study is described in Table 1.

Table 1: Description of the dataset used in the study

Parameter	Description
Dataset Name	Credit Card Fraud Detection Dataset
Domain	Digital banking and financial transaction security
Transaction Type	Credit card transaction data
Total Number of Records	284,807 transactions
Number of Genuine Transactions	284,315 transactions
Number of Fraudulent Transactions	492 transactions
Number of Input Features	30 input features
Target Variable	Class
Genuine Class Label	0
Fraud Class Label	1
Nature of Dataset	Highly imbalanced binary classification dataset
Main Purpose	Fraud detection using machine learning algorithms

Table 2 shows the main details of the dataset. The table confirms that the dataset is a binary classification dataset because the target variable contains two classes. It also confirms that the dataset is highly imbalanced because the number of fraud cases is extremely small compared with genuine transactions. This imbalance is a major methodological concern and must be handled carefully during model development. The feature structure of the dataset is shown in Fig. 1.

ISSN : 2455-9679
SJIF Impact Factor : 6.190

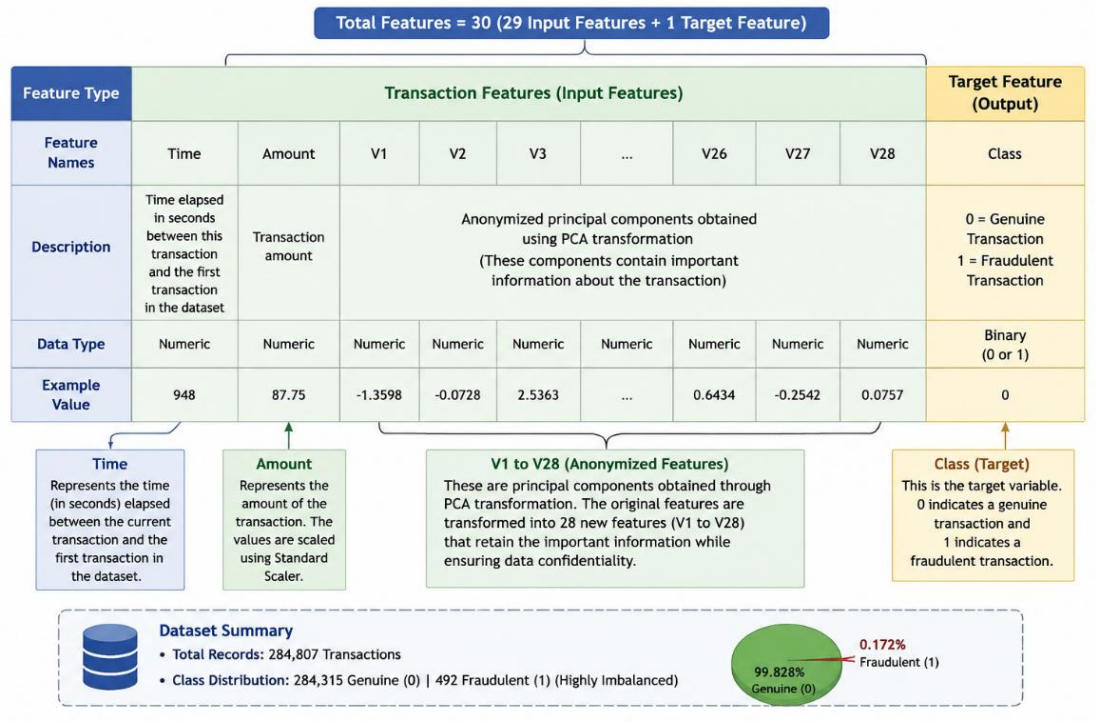

Fig.1. Feature structure of the credit card fraud detection dataset

III. Results and Discussion

The dataset is highly imbalanced because the number of genuine transactions is much larger than the number of fraudulent transactions. This imbalance reflects real digital banking conditions, where most transactions are genuine and fraud cases occur rarely. However, from a machine learning perspective, this creates a serious challenge. A model trained directly on such imbalanced data may classify most transactions as genuine and still show high accuracy. Therefore, class distribution analysis is necessary before training and evaluating the models. The dataset description and original class distribution are presented in Table 3.

Table 3: Dataset description and original class distribution

Parameter	Value
Total number of transactions	284,807
Number of input features	30
Target variable	Class
Genuine transaction label	0
Fraudulent transaction label	1
Number of genuine transactions	284,315
Number of fraudulent transactions	492
Percentage of genuine transactions	99.828%

Parameter	Value
Percentage of fraudulent transactions	0.172%
Nature of problem	Highly imbalanced binary classification

Table 3 shows that fraudulent transactions are extremely low in comparison with genuine transactions. Only 492 transactions are fraudulent out of 284,807 total transactions. This means that fraud cases represent less than 1% of the total dataset. Such class imbalance confirms that the fraud detection problem cannot be evaluated properly using accuracy alone. More meaningful metrics such as recall, precision, F1-score, PR-AUC, and confusion matrix are required. The original class distribution of the dataset is shown in Fig. 2.

Figure 4.2 visually shows the imbalance between genuine and fraudulent transactions. The bar representing genuine transactions is much higher than the bar representing fraudulent transactions. This difference indicates that the machine learning models may receive far more examples of genuine transactions than fraud transactions during training. If this imbalance is not handled, the model may fail to learn the minority fraud class effectively.

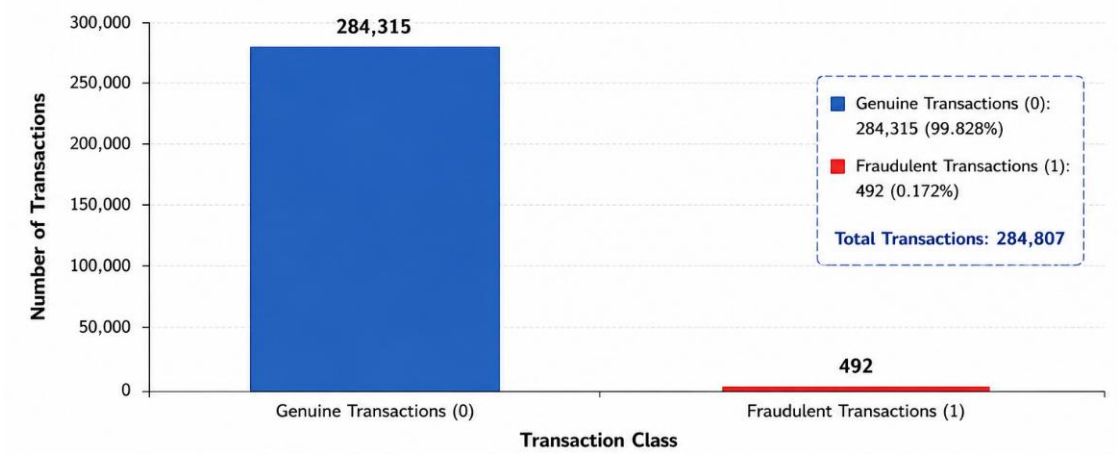

Fig. 2. Original class distribution of genuine and fraudulent transactions before balancing

The dataset analysis confirms that the selected dataset is suitable for fraud detection research because it represents a realistic and difficult classification condition. The dataset contains enough total records for model training, but the fraud class is very small. Therefore, preprocessing, stratified splitting, and class imbalance handling become necessary steps before model evaluation.

Before model training, the dataset was preprocessed to improve data quality and prepare it for machine learning algorithms. The preprocessing process included checking missing values, checking duplicate records, separating input features and target variable, scaling numerical features, splitting the dataset into training and testing sets, and handling class imbalance.

The dataset contains numerical features only. Therefore, categorical encoding was not required. However, the Time and Amount features were scaled because these features are not transformed in the same way as V1 to V28. Feature scaling is important because some machine learning algorithms, such as Logistic Regression, Support Vector Machine, and K-Nearest Neighbour, are sensitive to numerical ranges. Scaling ensures that no feature dominates the learning process only because of a larger numerical scale.

The dataset was divided into training and testing sets using an 80:20 stratified split. Stratified splitting was used so that the proportion of genuine and fraudulent transactions remained similar in both training and testing sets. This is important because the fraud class is very small. If fraud samples are not properly represented in the training or testing set, model learning and evaluation may become unreliable. The training and testing distribution, along with the balancing result, is presented in Table 4.

ISSN : 2455-9679
SJIF Impact Factor : 6.190

Table 4: Train-test split and class balancing summary

Dataset Stage	Genuine Transactions	Fraudulent Transactions	Total Transactions	Purpose
Complete dataset	284,315	492	284,807	Total data used in the study
Training set before balancing	227,451	394	227,845	Used for model training
Testing set	56,864	98	56,962	Used for model evaluation
Training set after SMOTE	227,451	227,451	454,902	Balanced training data

Table 4 shows that the training set initially contained 227,451 genuine transactions and only 394 fraudulent transactions. This imbalance could make the model biased toward the genuine class. Therefore, SMOTE was applied only to the training dataset. After applying SMOTE, the number of fraudulent samples in the training set increased to 227,451, making the training data balanced. The testing set was kept unchanged so that model performance could be evaluated under realistic imbalanced conditions. The class distribution after applying SMOTE to the training data is shown in Fig. 3.

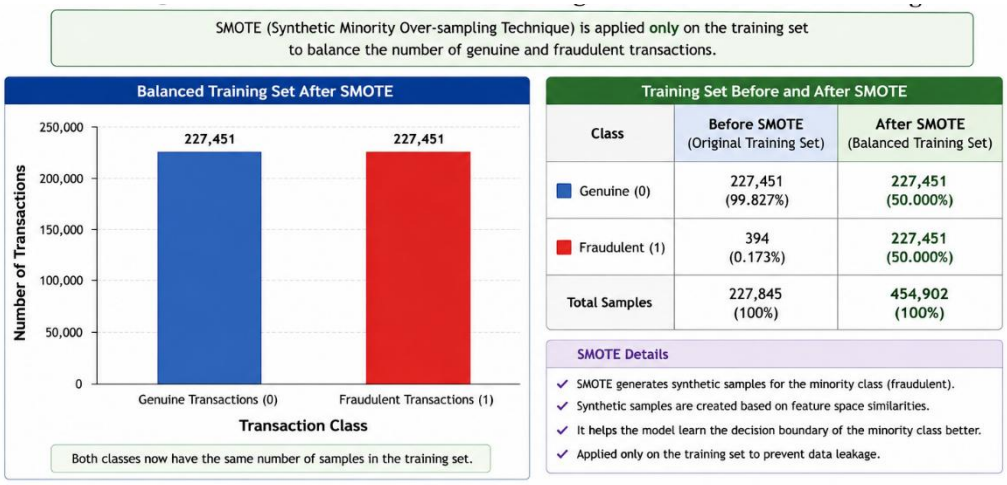

Fig. 3. Class distribution of training data after SMOTE balancing

Figure 3 shows that after class balancing, the training dataset contains equal numbers of genuine and fraudulent transactions. This balanced training data allows the machine learning models to learn both classes more effectively. The figure also confirms that SMOTE was applied only to the training data, not the testing data. This is important because balancing the testing data would create unrealistic evaluation conditions.

The preprocessing and balancing results show that the dataset was prepared in a systematic manner before model training. Missing value checking ensured that incomplete records did not affect the model. Feature scaling improved model readiness. Stratified train-test splitting preserved class proportions. SMOTE improved minority class representation in the training data. These steps collectively improved the reliability of the experimental analysis.

ISSN : 2455-9679
SJIF Impact Factor : 6.190

V. CONCLUSIONS

This paper presented a machine learning-based fraud detection framework for secure digital banking transactions. The study focused on the Credit Card Fraud Detection Dataset, which represents a realistic fraud detection problem due to its highly imbalanced class distribution. Out of 284,807 transactions, only 492 transactions were fraudulent, showing that fraud cases are rare compared with genuine banking activity. This imbalance makes fraud detection challenging because a model may achieve high accuracy by predicting most transactions as genuine while still failing to detect fraudulent cases.

The preprocessing stage played an important role in preparing the dataset for machine learning analysis. The dataset was checked for missing values and duplicate records, input features and target labels were separated, and numerical features such as Time and Amount were scaled. Since the dataset contained only numerical values, categorical encoding was not required. Stratified train-test splitting was used to divide the dataset into 80% training data and 20% testing data while maintaining the fraud and genuine transaction ratio in both sets.

To handle class imbalance, SMOTE was applied only to the training dataset. Before balancing, the training set contained 227,451 genuine transactions and only 394 fraudulent transactions. After applying SMOTE, the training data contained 227,451 genuine and 227,451 fraudulent samples, resulting in a balanced training dataset. The testing set was kept unchanged to ensure that model evaluation could be performed under realistic imbalanced conditions. This approach helps machine learning models learn the minority fraud class more effectively without creating unrealistic testing conditions.

The study concludes that effective fraud detection in digital banking requires more than simple accuracy-based classification. Proper preprocessing, stratified data splitting, and class imbalance handling are essential for developing reliable fraud detection systems. The proposed framework provides a strong basis for applying machine learning algorithms to identify suspicious transactions and improve the security of digital banking systems. In future work, different classification algorithms such as Logistic Regression, Random Forest, Support Vector Machine, Decision Tree, K-Nearest Neighbour, and ensemble learning models can be trained and compared using performance metrics such as precision, recall, F1-score, ROC-AUC, PR-AUC, and confusion matrix.

REFERENCES

[1] C. Bahnsen, D. Aouada, A. Stojanovic, and B. Ottersten, “Feature engineering strategies for credit card fraud detection,” Expert Systems with Applications, vol. 51, pp. 134–142, Jun. 2016.

[2] A. Abdallah, M. A. Maarof, and A. Zainal, “Fraud detection system: A survey,” Journal of Network and Computer Applications, vol. 68, pp. 90–113, Jun. 2016.

[3] J. West and M. Bhattacharya, “Intelligent financial fraud detection: A comprehensive review,” Computers & Security, vol. 57, pp. 47–66, Mar. 2016.

[4] T. Chen and C. Guestrin, “XGBoost: A scalable tree boosting system,” in Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, San Francisco, CA, USA, 2016, pp. 785–794.

[5] G. Lemaître, F. Nogueira, and C. K. Aridas, “Imbalanced-learn: A Python toolbox to tackle the curse of imbalanced datasets in machine learning,” Journal of Machine Learning Research, vol. 18, no. 17, pp. 1–5, 2017.

[6] R. F. Lima and A. Pereira, “Feature selection approaches to fraud detection in e-payment systems,” in E-Commerce and Web Technologies, vol. 278, Cham, Switzerland: Springer, 2017, pp. 111–126.

[7] A. Pouramirarsalani, M. Khalilian, and A. Nikravanshalmani, “Fraud detection in E-banking by using the

ISSN : 2455-9679
SJIF Impact Factor : 6.190

hybrid feature selection and evolutionary algorithms," International Journal of Computer Science and Network Security, vol. 17, no. 8, pp. 271–279, Aug. 2017.

[8] F. Carcillo, A. Dal Pozzolo, Y. Le Borgne, O. Caelen, Y. Mazzer, and G. Bontempi, "SCARFF: A scalable framework for streaming credit card fraud detection with Spark," Information Fusion, vol. 41, pp. 182–194, May 2018.

[9] A. Dal Pozzolo, G. Boracchi, O. Caelen, C. Alippi, and G. Bontempi, "Credit card fraud detection: A realistic modeling and a novel learning strategy," IEEE Transactions on Neural Networks and Learning Systems, vol. 29, no. 8, pp. 3784–3797, Aug. 2018.

[10] A. Salazar, G. Safont, and L. Vergara, "Semi-supervised learning for imbalanced classification of credit card transaction," in Proceedings of the International Joint Conference on Neural Networks, Rio de Janeiro, Brazil, 2018, pp. 1–7.

[11] 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, vol. 6, pp. 14277–14284, 2018.