Credit Card Fraud Transaction Detection Using Hybrid Random Forest And Logistic Regression Ensemble Machine Learning Approach

E.Nagaraju[1], K.Prem Kumar[2], M.Sai Krishna[3], Ms.S.Lavanya[4]
[1,2,3]*Department Of Artificial Intelligence And Data Science*
[4]*Assistant Professor, Department of Artificial Intelligence And Data Science*
[1,2,3,4]*Dhanalakshmi Srinivasan University Tamil Nadu,India*

***Abstract*—The recent surge in online and digital payments has resulted in a substantial increase in credit card frauds, making fraud detection a critical task for financial organizations. The task is complex as the number of fraudulent transactions is extremely low compared to legitimate transactions, resulting in most machine learning classifiers becoming biased and thus inefficient in detecting frauds. In this paper, a hybrid machine learning technique is presented using SMOTE to handle class imbalance, Random Forest to identify key features, and Logistic Regression for classification, making the detection process more efficient and reliable. The system also identifies and stores the fraudulent transactions in a separate CSV file, which can be used for further analysis and auditing, thus making the system useful for real-time banking and financial analysis applications.**

***Index Terms*—Credit Card Fraud Detection, Handling Class Imbalance, SMOTE Oversampling, Random Forest Feature Selection, Logistic Regression Classification.**

I. INTRODUCTION

The growth of digital payment systems and online shopping has brought a revolution in the way financial transactions are conducted worldwide. Credit cards have become one of the most favorite modes of payment as they are fast, convenient, and widely accepted. Although these benefits have made transactions easier for people, they have also opened doors to new opportunities for fraudulent acts. Credit card fraud has become a major concern for banks, merchants, and consumers because it results in financial losses and affects the credibility of digital payment systems. As the number of online transactions is increasing steadily, the need for efficient fraud detection systems has become more important than ever before.

Fraudulent transaction detection is a difficult process because fraud patterns are not constant and keep changing over time as the fraudsters come up with new patterns. The other significant problem is that the transaction data is highly imbalanced. In actual datasets, legitimate transactions make up the majority, and fraud transactions are very rare. In the actual dataset used for this project, only 492 transactions out of 284,807 are fraud transactions. This level of imbalance makes it difficult for most machine learning algorithms to learn the patterns of fraud transactions effectively because most algorithms tend to learn more about the legitimate transactions and less about the fraud patterns. This makes most fraud transactions go undetected, resulting in high false negative rates and system unreliability.This research fills the gap by proposing an end-to-end malnutrition detection system based on the ResNet deep Convolutional neural network, coupled with a large language model for crafting user-friendly health alerts.

The system is intended to be fully functional on standard computing hardware, with a straightforward web interface that accepts facial images captured from a webcam or mobile device. Once the image is uploaded, the ResNet model examines visual characteristics to determine whether the subject is healthy or malnourished. The result is then processed by a language model that transforms the numerical output into a concise, human-readable advisory with nutritional information. This two-model combination enables the system to be both intelligent and interpretable for non-technical users.

Decision Trees, Support Vector Machines, Neural Networks, and ensemble models have been investigated in previous studies as machine learning techniques for fraud detection. While these techniques demonstrate promising performance, they also have some limitations in practice. Some models are computationally intensive, while others are not interpretable. In most scenarios, models are considered black boxes that generate predictions without specifying which transactions are suspicious and why they are labeled as fraud. This makes them less useful in real-world banking applications, where explanation and traceability are required for auditing and investigation purposes.

To address these challenges, this project proposes a hybrid machine learning technique that integrates SMOTE, Random Forest, and Logistic Regression to efficiently detect credit card fraud. SMOTE is employed to handle the class imbalance problem in the dataset by creating synthetic samples of the minority class, which represents the fraud transactions. Random Forest is then utilized for feature selection to determine the most relevant features and eliminate redundant information. Finally, Logistic Regression is employed for the classification task, which offers interpretable results and easy decision boundaries.

Aside from the classification task, the proposed system has a unique capability to store the detected fraudulent transactions in a separate file. This capability is useful for real-time monitoring and further analysis by financial institutions. With the emphasis on both accuracy and usability, the proposed approach aims to offer a trustworthy and interpretable solution for today's credit card fraud detection systems.

II. RELATED WORK

Credit card fraud detection has received considerable attention from the research community because of the rapid growth of digital payment systems and the associated financial losses. With the growing number of transactions, manual verification has become unfeasible, and researchers have turned to machine learning for automated fraud detection. Over the years, different methods have been proposed, including conventional classifiers and hybrid models, each of which has dealt with different issues in fraud detection. Early research proved the relevance of supervised machine learning models to financial transaction data. Yee et al. [16] and Dornadula & Geetha [15] showed that models like Logistic Regression, Decision Trees, and Support Vector Machines could learn the transaction patterns and identify the fraudulent ones. These studies paved the way for further research by proving the feasibility of data-driven systems. Nevertheless, their results were greatly impacted by the presence of a large imbalance in real-world datasets, where fraudulent transactions made up only a small portion of the entire dataset, making it difficult to achieve high recall for fraud transactions.

To increase robustness and generalization capabilities, ensemble learning techniques were developed. Random Forest was one of the most popular classifiers because of its capability to combine the results of multiple decision trees and prevent overfitting. Thirunavukkarasu et al. [14] showed that Random Forest achieved higher accuracy than individual classifiers. Similar results were obtained by Panda [7] and Aburbeian & Ashqar [9], where ensemble models showed consistent performance on large-scale transaction data. The work of Khedkar & Kulkarni [3] further emphasized that Random Forest achieved high precision, while Logistic Regression was computationally efficient.

Class imbalance has been a persistent problem in fraud detection research. Various studies have tried to address this problem using sampling and optimization methods. Ileberi et al. [11] showed that a Genetic Algorithm-based feature selection approach, together with SMOTE preprocessing, could lead to optimized feature subsets that improve the detection of the minority class. Ileberi and Sun [2] furthered this research by examining cost-sensitive oversampling strategies and found that these approaches greatly improved the recall rate for fraudulent transactions. While these approaches improved the sensitivity of the model, they also increased the complexity of the system and sometimes required careful parameter tuning to prevent overfitting and high computational complexity.

Later, hybrid and multi-stage architectures were developed to combine the benefits of different learning approaches. Mniai et al. [5] developed a new architecture that used multiple processing stages to improve robustness and minimize false positives. Similarly, academic research by Kaundal and Jain [4] investigated hybrid models of learning to improve prediction reliability. While the hybrid models

performed better than individual classifiers, their increased complexity made them less interpretable and more difficult to implement in real-time banking applications.

Some researchers undertook extensive comparative analyses to assess machine learning approaches under varying scenarios. Afriyie et al. [6] developed a supervised learning approach for fraud prediction and stressed the need for predictable model performance across different datasets. Murkute et al. [8] analyzed different machine learning approaches and stressed the need for preprocessing and feature engineering to enhance detection accuracy. Upadhyay et al. [1] offered a comprehensive machine learning outlook by analyzing different classifiers and preprocessing techniques for fraud payment detection. These works offered important insights but mostly focused on performance analysis rather than applicability.

Recent works have also investigated the application of advanced machine learning and deep learning techniques. Alarfaj et al. [10] undertook an extensive comparison of traditional machine learning and deep learning approaches and demonstrated excellent detection accuracy using deep learning models. However, these models are computationally intensive, requiring substantial training time, and are not interpretable, which is a drawback in the context of a financial system where interpretability is paramount.

Project-based implementation works by AlEmad [12] and Ashik and Manmohan [13] proved the feasibility of end-to-end fraud detection systems using machine learning approaches. The above-mentioned works proved the feasibility of the system but did not provide much optimization technique and lacked the ability to support investigation after fraud detection.

The above-mentioned literature review indicates that there is constant improvement in the accuracy of fraud detection using ensemble, hybrid, and imbalance learning approaches. However, most of the existing works are biased towards prediction accuracy and lack interpretability and the ability to support investigation for transactions after fraud detection.

III. METHODOLOGY

This section presents the methodological approach used for designing the proposed credit card fraud detection system. The methodological approach is intended to provide a framework that is reproducible, transparent, and practical for financial applications.

A. Dataset Description

The proposed work uses the publicly available credit card transaction dataset downloaded from Kaggle. The dataset consists of 284,807 transactions with 31 features, of which 28 are anonymized numerical features (V1-V28), transaction amount, and a binary class label. The class label identifies whether the transaction is genuine (Class 0) or fraudulent (Class 1). Out of the total transactions, 284,315 (99.83%) are genuine, and only 492 (0.17%) are fraudulent. The class imbalance problem is quite prominent in this dataset, as it represents the actual transaction pattern. The class imbalance problem has a significant effect on the learning process of machine learning algorithms.

B. Environment and Equipment Specifications

The experimental setup is conducted using the Python programming environment. The experiments are conducted on a machine that has an Intel processor, 8 GB of RAM, and a Windows operating system. The experimental setup uses common machine learning libraries such as NumPy and Pandas for data processing, Scikit-learn for developing models, and Imbalanced-learn for oversampling.

Fixed random seeds are used during dataset splitting, oversampling, and model training to make the experiments reproducible.

C. Data Preprocessing and Normalization

Data preprocessing is done to ensure consistency and numerical stability during model training. Since the dataset does not have missing values, no imputation is needed. Feature normalization is done using standard scaling to convert the numerical attributes into comparable ranges.

The dataset is split into training and testing subsets, with the training subset being utilized for learning and the testing subset being held for unbiased testing. The preprocessing tasks are carried out only on the training subset to avoid data leakage.

D. Block Diagram of the Proposed System

The proposed system for fraud detection is represented through a block diagram, as shown in Fig. 1.

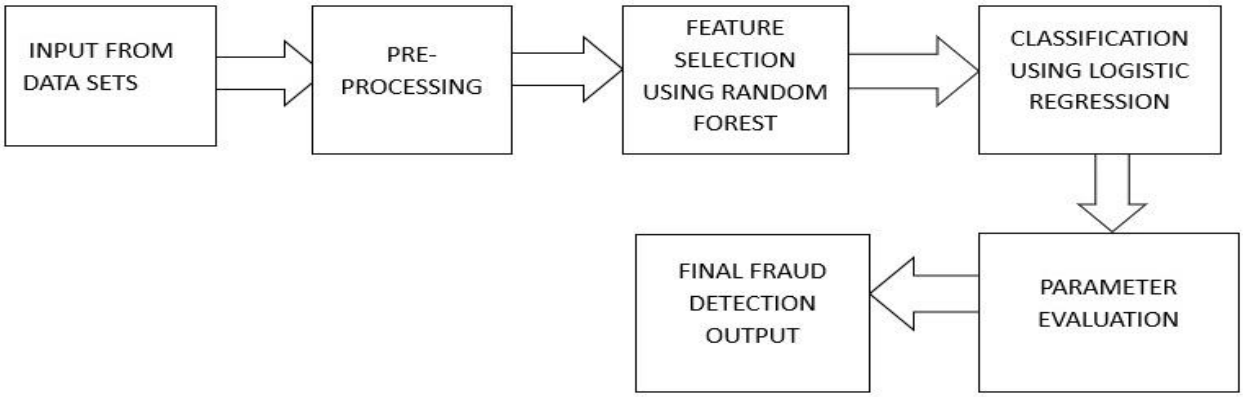

Fig. 1. Block diagram of the credit card fraud detection system.

The block diagram above illustrates the logical flow of data from various processing stages. The data from the transactions is first sent to the preprocessing module, where normalization and data partitioning are carried out. The balanced training data is then created using SMOTE. Random Forest is then used to determine the most important features of the transactions. The optimized feature set is then sent to the Logistic Regression classifier for fraud detection. Lastly, the fraudulent transactions are isolated and saved in a new CSV file for further processing.

The above block diagram is a systematic and organized way of illustrating the system, making it easier to understand and reproduce.

G. Class Imbalance Handling Using SMOTE

To counter the issue of class imbalance, the Synthetic Minority Oversampling Technique (SMOTE) is used on the training data. SMOTE creates new fraud instances by finding the midpoint between the existing instances of the minority class.

A synthetic sample is created using:

$$x_{new}=x_i+\delta(x_j-x_i)$$

where is a minority class instance, is one of its nearest neighbors, and ..

This method enhances the minority class while avoiding any replication of the original samples.

H. Feature Selection Using Random Forest

Random Forest is used for the selection of important transaction features. The method estimates the importance of features based on the reduction of impurity in decision trees.

The importance of a feature is measured as:

$$FI(f)=t=1\sum Tn\in t\sum \Delta Gini(n)$$

where is the number of trees, and is the reduction in Gini impurity at node .

Only those features that have high importance values are selected for classification.

I. Fraud Classification Using Logistic Regression

Logistic Regression is employed as the final classification model because of its interpretability and ability to provide probabilities. The probability of a transaction being fraudulent is computed using the sigmoid function:

$$P(y=1|x)=1/1+e-(\beta 0+\beta Tx)$$

A transaction is labeled as fraudulent if its predicted probability is above the specified decision boundary.

J. Statistical Evaluation Parameters

The performance of the system is measured using a set of statistical parameters that are derived from the confusion matrix, such as accuracy, precision, recall, F1-score, specificity, false positive rate, false negative rate, and AUC-ROC.

These parameters offer a complete evaluation in the presence of high class imbalance.

1. Accuracy

Accuracy is a measure of the total proportion of correctly predicted transactions.

While accuracy is a measure of overall correctness, it is not a reliable measure for fraud classification because of the presence of class imbalance.

2. Precision

Precision is the reliability of the fraud predictions, which is calculated by the number of predicted fraud transactions that are actually fraudulent.

$$\text{Precision} = \frac{TP}{TP + FP}$$

High precision means a low number of false positives, which is very important for avoiding unnecessary blocking of transactions.

3. Recall (Sensitivity)

Recall is the measure of the model's capacity to identify the fraudulent transactions correctly.

$$\text{Recall} = \frac{TP}{TP + FN}$$

High recall is very important in fraud detection, as it helps avoid undetected fraudulent transactions.

4. F1-Score

The F1-score is a balanced measure of precision and recall.

$$\text{F1-score} = \frac{2 \times Precision \times Recall}{Precision + Recall}$$

The F1-score is very important in the case of imbalanced datasets.

5. Area Under the ROC Curve (AUC-ROC)

AUC is the probability that the classifier will rank a randomly selected fraudulent transaction higher than a legitimate transaction.

$$\text{AUC} = \int_0^1 TPR(FPR)\, d(FPR)$$

The closer the AUC value to 1, the better the discriminatory power.

K. Fraud Transaction Extraction Module

After the classification process, the fraudulent transactions are extracted from the data set and saved in a new CSV file. This module allows for transaction-level analysis, which improves the usability of the proposed framework.

IV. RESULT

This section discusses the experimental results that were derived using the proposed credit card fraud detection system. The results were presented in an objective manner using quantitative assessment criteria, tables, and figures. All the experiments were performed on the testing dataset, which was not utilized during the training process of the proposed model.

A. Dataset Distribution

The total dataset had 284,807 transaction entries. For the experimental assessment, the dataset was split into training and testing datasets using stratified sampling.

Table I. Distribution of transactions in training and testing datasets

Dataset	Total Transactions	Legitimate	Fraudulent
Training set	199,364	199,019	345
Testing set	85,443	85,296	147
Total	284,807	284,315	492

B. Classification Performance Metrics

The performance metrics derived from the testing The performance metrics obtained from the testing dataset are presented in Table II. The performance metrics were computed using the confusion matrix obtained after the classification task.

Table II. Performance results of the proposed fraud detection system

Metric	Value (%)
Accuracy	99.93
Precision	80.00
Recall	81.63
F1-score	80.80
AUC-ROC	97.16

The performance metrics provided in the table are a summary of the classification results obtained during the evaluation process.

C. Confusion Matrix Results

The confusion matrix derived from the testing dataset is shown in Fig. 3.

$$\begin{bmatrix} 56844 & 20 \\ 18 & 80 \end{bmatrix}$$

Fig. 2. Confusion matrix of the proposed fraud detection model.

From the confusion matrix, it can be seen that 56,844 legitimate transactions were correctly identified, while 20 legitimate transactions were incorrectly identified as fraudulent. In addition, 80 fraudulent transactions were correctly identified, while 18 fraud transactions were incorrectly identified as legitimate.

D. ROC Curve Evaluation

The Receiver Operating Characteristic curve obtained during the evaluation is shown in Fig. 4.

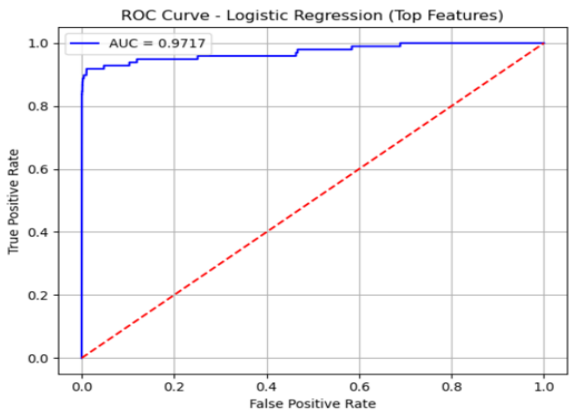

Fig. 3. ROC curve of the proposed fraud detection system.

The ROC curve shows the relationship between the true positive rate and the false positive rate for various levels of classification.

E. Fraud Transaction Extraction Output

The fraudulent transactions extracted from the testing dataset were stored in a separate comma-separated values (CSV) file.

A sample of the extracted fraudulent transactions is shown in Fig. 5.

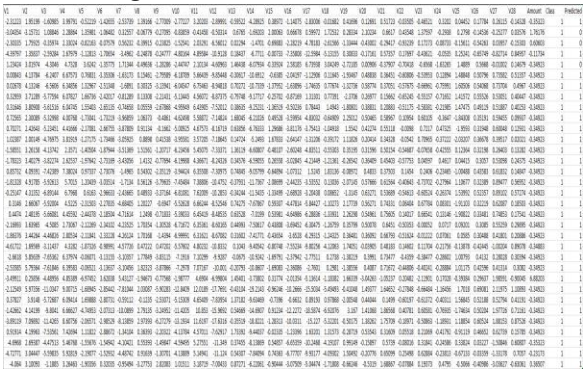

Fig. 4. Sample of detected fraudulent transactions stored in CSV format.

Only a few transactions were shown due to the naturally low rate of fraud events in the dataset.

F. Graphical Representation of Performance Metrics

A graphical representation of the key performance metrics is shown in Fig. 6.

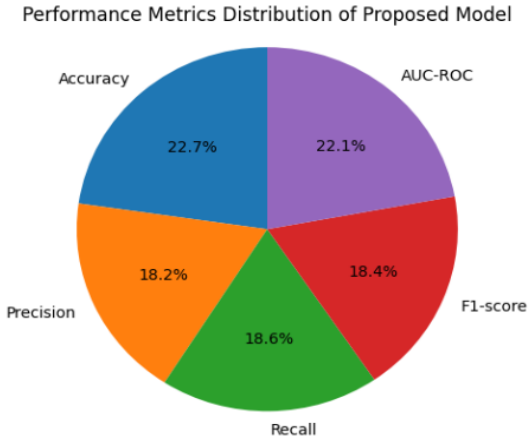

Fig. 5. Graphical representation of Performance Metrics

The graph offers a visual representation of the performance of the classification task achieved by the proposed model.

G. Result Summary

A summary of the experimental results is provided in Table III.

Table III. Summary of experimental results

Parameter	Description
Dataset	Kaggle credit card transaction dataset
Class imbalance	0.17% fraud transactions
Oversampling method	SMOTE
Feature selection	Random Forest
Classification model	Logistic Regression
Fraud output	Extracted and stored as CSV

V. DISCUSSION

The objective of this work was to design an accurate and interpretable credit card fraud detection model for imbalanced transaction datasets. The experimental results demonstrate that the proposed hybrid approach successfully addresses this challenge.

The key result is that the hybrid approach involving SMOTE, Random Forest-based feature selection, and Logistic Regression yields a trustworthy credit card fraud detection model. This is evident from the accuracy of 99.93% and AUC-ROC of 97.17% achieved, along with the successful detection of

fraudulent transactions as evident from the confusion matrix.

Table IV. Comparison of the proposed method with recent studies

Study	Year	Method Used	Accuracy (%)
Upadhyay et al.	2025	Multiple ML models	~99.4
Ileberi & Sun	2025	Cost-sensitive oversampling	~99.6
Khedkar & Kulkarni	2025	RF and LR with SMOTE	99.95
Ileberi et al.	2022	GA-based feature selection	~99.4
	2026	SMOTE + RF + LR	99.93

Although comparable accuracy has been reported in previous studies, most methods involve complex or less interpretable models. The proposed approach obtains competitive results with a simpler and more interpretable classifier. Moreover, the extraction of the identified fraudulent transactions offers useful assistance for investigation and auditing.

The proposed approach is only evaluated on a single public dataset with anonymized features, and further testing on real-time transaction data is needed.

In conclusion, the proposed framework illustrates a balanced and practical approach to credit card fraud detection.

VI. CONCLUSION

This paper has proposed a hybrid machine learning framework for credit card fraud detection to overcome the difficulties of extreme class imbalance, interpretability, and usability. The research question was whether an accurate and interpretable fraud detection model could be developed with a balanced and efficient approach. The experimental outcome has shown that the proposed framework effectively answers the research question, and it obtains high detection accuracy with 99.93% accuracy and 97.17% AUC-ROC value.

The novelty of this research work is in combining SMOTE for balancing the data, Random Forest for feature selection, and Logistic Regression for explainable classification in a single pipeline. Moreover, the detailed extraction of the fraudulent transactions identified adds to the applicability of the system. In summary, the proposed method provides an effective and explainable solution for credit card fraud detection and helps in the development of transparent machine learning models that can be applied to financial monitoring systems.

VII. FUTURE WORK

The proposed framework for fraud detection is a robust platform for further research, and there are many interesting extensions that can be pursued. Future research can be conducted to test the model using larger and more institution-specific transaction data to study its adaptability in different financial settings. These studies will help to evaluate the model's robustness in different transaction patterns and fraud patterns.

Another area of research can be the extension of the system for real-time transaction monitoring. Online learning methods can be incorporated into the system to enable the system to learn continuously from new transaction data as and when it is available. This will help the system to adapt dynamically to new fraud patterns.

Future research can also be conducted to study the application of cost-sensitive learning methods that take into account the financial cost of misclassification. Different costs for false positives and false negatives can be assigned to further improve decision-making in the system. The integration of deep learning or graph-based models can also be explored to further improve the detection of complex and coordinated fraud attacks. These extensions have the potential to make fraud detection systems more scalable, adaptable, and practical, leading to more robust financial security infrastructure.

REFERENCES

[1] Upadhyay, Y. S. Rathore, N. Bansal, S. Jhingran, G. Chaudhary, S. Maurya, R. Chaturvedi, and K. Soni, "Machine learning perspective: Fraud payment transaction detection," J. Mobile Multimedia, vol. 21, no. 3–4, pp. 577–598, 2025, doi: 10.13052/jmm1550-4646.213414.

[2] E. Ileberi and Y. Sun, "Performance analysis of cost-sensitive oversampling mechanisms for credit card fraud detection," IEEE Access, vol. 13,

pp. 202655–202670, 2025, doi: 10.1109/ACCESS.2025.3637132.

[3] D. S. Khedkar and R. Kulkarni, "Credit card fraud detection using machine learning," Int. J. Adv. Res. Sci. Commun. Technol. (IJARSCT), vol. 5, no. 6, Apr. 2025, doi: 10.48175/IJARSCT-25301.

[4] S. Kaundal and A. Jain, Credit Card Fraud Detection Using Machine Learning, B.Tech. major project report, Dept. Comput. Sci. Eng. & Inf. Technol., Jaypee Univ. Inf. Technol., Waknaghat, India, 2023–2024.

[5] A. Mniai, M. Tarik, and K. Jebari, "A novel framework for credit card fraud detection," IEEE Access, vol. 11, pp. 112776–112789, 2023, doi: 10.1109/ACCESS.2023.3323842.

[6] J. K. Afriyie et al., "A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions," Decision Analytics J., vol. 6, Art. no. 100163, 2023, doi: 10.1016/j.dajour.2023.100163.

[7] K. C. Panda, "Credit card fraud detection using machine learning," J. Sci. Eng. Res., vol. 10, no. 5, pp. 372–378, 2023.

[8] P. Murkute et al., "Credit card fraud detection using machine learning techniques," in Proc. Int. Conf. Adv. Electr., Electron. Comput. Intell. (ICAEECI), Tiruchengode, India, Oct. 2023, doi: 10.1109/ICAEECI58247.2023.10370832.

[9] A. H. M. Aburbeian and H. I. Ashqar, "Credit card fraud detection using enhanced random forest classifier for imbalanced data," Arab American Univ., Palestine, 2023.

[10] F. K. Alarfaj et al., "Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms," IEEE Access, vol. 10, pp. 39700–39715, 2022, doi: 10.1109/ACCESS.2022.3166891.

[11] E. Ileberi, Y. Sun, and Z. Wang, "A machine learning based credit card fraud detection using the GA algorithm for feature selection," J. Big Data, vol. 9, no. 24, 2022, doi: 10.1186/s40537-022-00573-8.

[12] M. AlEmad, Credit Card Fraud Detection Using Machine Learning, M.S. capstone project, Dept. Data Analytics, Rochester Inst. Technol., Dubai, UAE, 2022.

[13] M. Ashik and S. Manmohan, Credit Card Fraud Detection System, B.Tech. project report, Dept. Inf. Technol., Sathyabama Inst. Sci. Technol., Chennai, India, 2022.

[14] M. Thirunavukkarasu, A. Nimisha, and A. Jyothsna, "Credit card fraud detection using machine learning," Int. J. Comput. Sci. Mobile Comput. (IJCSMC), vol. 10, no. 4, pp. 71–79, Apr. 2021, doi: 10.47760/ijcsmc.2021.v10i04.011.

[15] V. N. Dornadula and G. S. Geetha, "Credit card fraud detection using machine learning algorithms," Procedia Comput. Sci., vol. 165, pp. 631–641, 2019, presented at Int. Conf. Recent Trends Adv. Comput. (ICRTAC 2019), Chennai, India, doi: 10.1109/ICCCI.2019.8821950.

[16] O. S. Yee, S. Sagadevan, and N. H. A. H. Malim, "Credit card fraud detection using machine learning as data mining technique," J. Telecommun. Electron. Comput. Eng., vol. 10, no. 1–4, pp. 23–27, 2018.