iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** I **Month of publication:** January 2025

DOI: https://doi.org/10.22214/ijraset.2025.66734

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue I Jan 2025- Available at www.ijraset.com

Exploring Machine and Deep Learning Approaches in Credit Card Fraud Prevention and Detection

Shayna Bano[1], Dr. Pharindara Kumar Sharma[2]
[1]*M.Tech Scholar,* [2]*Associate Professor, Dept. of Computer Science and Engineering, Shriram College of Engineering and Management, College in Bamor, Madhya Pradesh, 476444.*

Abstract: ***Establishing the foundation for the use of deep learning and artificial intelligence in the detection of credit card fraud is the primary objective of this study. A more accurate and improved fraud detection system is necessary to meet the primary goal of enhancing financial security. In order to facilitate this study, we collect a sizable dataset of credit card payment records that encompasses all relevant variables. Data pretreatment enhances analysis by normalising numerical values, eliminating superfluous characteristics, and verifying data consistency. Exploratory data analysis, or EDA, must be used to find connections and trends in the dataset before choosing a model. Random Forest, gradient boost, SVM, Logistic Regression, LSTM, and GRU are among the machine learning models that we combine. With a 90% F1 score, 90% recall, 90% specificity, and 90.3% accuracy, the Random Forest model outperforms all others. The deep learning model GRU outperforms LSTM by a small margin with an accuracy rate of 90.04% and strong recall and precision measures. Furthermore, compared to earlier models, the Artificial Neural Network's accuracy is 89%. The findings demonstrate the effectiveness of the suggested methods in detecting fraudulent transactions. The study's findings open the door for fascinating new consumer protection research and provide insight into the issue of credit card fraud.***

Keywords: Credit Card Fraud, Fraud Detection, Machine Learning .Data Analysis, Classification, Transaction

I. INTRODUCTION

Credit cards have quickly gained popularity in the e-commerce industry due to their adaptability and ease of usage. Due to the widespread use, credit card fraud has become a serious problem. Modern fraud detection systems respond to the changing nature of fraudulent activities, improving the safety of consumers and financial institutions. The complexity of scams and the large volume of transactions make traditional fraud detection techniques—which frequently rely on systems based on rules and manual evaluations—inadequate. Since scammers are always coming up with new ways to do things, it is essential to come up with original ways to detect and stop fraud in real time. Organisations may now evaluate enormous volumes of transaction data to find possible signs of fraud thanks to the recent development of machine learning (ML) approaches. Machine learning has many benefits over manual, conventional methods for detecting fraud. Its speed and accuracy in processing and analysing large datasets are advantages, since they allow it to spot outliers that people might overlook. Using a variety of methods, machine learning systems can adjust to emerging risks.

This class of algorithms includes ensemble, supervised, and unsupervised learning models. Over time, they increase the accuracy of their predictions by examining past data [1]–[4]. It is feasible to develop models for classification that can differentiate between authentic and bogus transactions by looking at historical trends using supervised learning methods like logistical regression, decision trees, and assist vector machines. However, even in the absence of labelled data, unsupervised learning methods, such as clustering algorithms, are effective in spotting emerging fraud tendencies. Machine learning techniques have the potential to improve gradually over time.

Retraining models with fresh data allows detection systems to adapt to the changing environment. Adaptability is crucial due to the increasing complexity of fraud campaigns that use strategies including account takeover, social engineering, and synthetic identity fraud [5], [6].

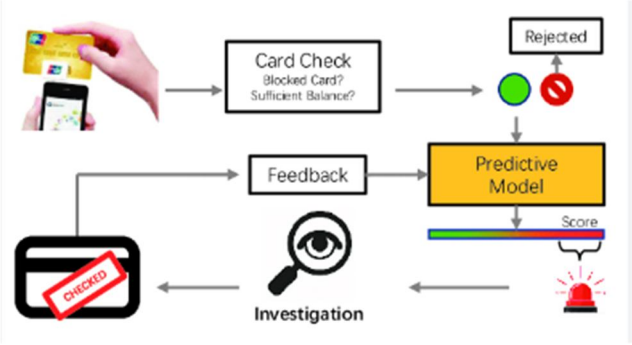


Fig. 1 Credit card fraud detection [7]

Financial institutions can enhance their fraud detection systems with advanced algorithms. These systems reduce false positives, which is great for both real clients and the institution's security. Credit card fraud detection using machine learning also encourages more cross-sector cooperation. By exchanging information and identifying trends, financial institutions can strengthen their collective fraud defences. Also, more advanced methods like deep learning and neural networks will likely appear when machine learning technology develops further. These will be able to examine transaction patterns in greater detail and spot complicated associations that simpler approaches could miss.
[8]–[11]. These developments give businesses the ability to prevent fraud by increasing detection rates and enabling predictive analytics. One important development in the fight against financial crime is the use of algorithms based on machine learning for credit card fraud detection. Businesses may create more reliable and efficient fraud detection systems by combining information-driven understanding with adaptive algorithms [12], [13]. Integrating machine learning is crucial for consumer protection and financial system integrity as the credit card transaction landscape evolves. In order to provide light on potential future fraud detection tactics, this study will examine several machine learning approaches and how well they fight credit card theft [14]–[16].

II. LITERATURE REVIEW

Azim 2024 et al. Soft voting is a method of ensemble learning that improves the detection of credit card fraud in datasets that are not balanced. We evaluate it by combining the suggested remedy for the class imbalance issue with advanced sampling strategies like hybrid, oversampling, or undersampling. Ensemble models are among the classifiers that either employ or do not use these sampling techniques. The results of the experiment show that the soft voting method is more accurate than individual classifiers at detecting fraud. False negative rate is 0.0306, recall is 0.9694, accuracy is 0.9870, the AUROC is 0.9936, and F1-score is 0.8764 [17].
Yılmaz 2024 et al. a technique that detects unauthorised transactions with credit cards using machine learning. Feature selection, classification, data standardisation, and information purification comprise the four primary components of the unique technique. Artificial neural networks employ naive Bayes, logistic regression, decision trees, and random forests for classification. They use particle swarm optimisation for feature selection. We evaluated the proposed methodology using a collection of European card data. The experimental results show that the proposed method outperforms previous machine learning strategies in detecting and classifying frauds [18].
Zhu 2024 et al. The study introduces a novel approach to improve detection efficiency by combining neural networks and the Artificial Minority The process of overs Technique (SMOTE). The study presents a novel idea that resolves the notable disparity in card data on transactions, enabling precise and efficient fraud detection. In terms of F1-score, recall, and precision, the experimental results show that the neural network and SMOTE combo performs better than traditional models. Based on the results, the method performs exceptionally well when dealing with often skewed data sets, which is a common situation when detecting credit card fraud [19].
Islam 2024 et al. The banking sector, governmental institutions, and the general population are all seriously threatened by financial fraud, which is why it is crucial to continuously develop novel fraud detection methods. Since criminals are always changing their tactics to evade detection, criminal activity continues. It is more difficult to discern between fraudulent and legitimate transactions due to the data's noticeable distortion. builds a rule-based system (RBM) that detects fraudulent transactions without the use of human sampling techniques.

The RBM's performance is evaluated using a number of metrics, including recall, specificity, accuracy, MCC, or ROC values. To assess the model, two benchmark datasets are utilised, and the model is compared with many contemporary machine learning techniques, including k-nearest neighbourhood (KNN), decision tree (DT), random- forest modelling (RF), naïve Bayes (NB), and logistic regression (LR). At 0.99 precision and accuracy, the proposed RBM performs better than competing methods [20].

Sani 2024 et al. Due to technology advancements, traditional payment methods have evolved, leading to an increased preference for online transactions. Regrettably, an increase in instances of online credit card fraud has accompanied this transition. The authors introduce a robust model for fraud detection in Python utilising machine learning methodologies. This work aims to identify fraudulent transactions by integrating logistic regression with Kaggle's credit card dataset. By employing distinct test data, one may assess the model's efficacy in identifying previously unreported fraudulent transactions with an impressive accuracy rate of 99.87%. The model's effectiveness with new data instances is substantiated by comprehensive research, which confirms this remarkable accuracy (equating to a rate of 99.8%). Data visualisations illustrate the enhancement of online transaction security through the method. This project aids in combating fraudulent activity by integrating Python programming with advanced machine learning techniques, benefiting both consumers and financial players [21].

TABLE 1 LITERATURE SUMMARY

Author/year	Model/method	Research gap	findings
Aghware/2024 [22]	RF with SMOTE enhances fraud detection.	Limited studies on combining algorithms for improved fraud detection accuracy.	RF and SMOTE significantly enhance credit card fraud detection accuracy.
Tank/2024 [23]	Random Forest excels in fraud detection.	Insufficient focus on real-time fraud detection methods in research.	Random Forest outperforms others; Isolation Forest effective for fraud detection.
Sruthi/2024 [1]	Light Gradient Boosting Machine enhances fraud detection.	Insufficient research on LightGBM's effectiveness in fraud detection applications.	Light Gradient Boosting Machine shows high precision and recall in detection.
Planinic/2024 [24]	CatBoost excels in credit card fraud detection.	Limited exploration of hyperparameter tuning in credit card fraud detection.	CatBoost outperforms Logistic Regression and Random Forest in detection.
Noviandy/2023 [25]	Digital transactions, fraud detection, machine learning.	Limited studies on advanced techniques for credit card fraud detection.	XGBoost improves accuracy in detecting credit card fraud effectively.

III. METHODOLOGY

This study employs a systematic approach to efficiently identify credit card theft with deep learning and machine learning models. The preliminary phase entails the collection of an extensive dataset of transaction records to acquire all pertinent transaction information. Preprocessing procedures ensure consistency, normalise numerical values, and eliminate extraneous features to ready the dataset for analysis. In the exploratory data analysis phase, you will identify patterns and relationships within the data. The subsequent phase in developing a resilient fraud detection system involves employing an array of deep learning and machine learning models, such as Random Forest, Gradient Boosting, LSTM, and GRU.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue I Jan 2025- Available at www.ijraset.com

Fig. 2 Flow chart

A. Data Collection

Each of the 23 columns and 1,296,675 elements in the dataset represents a credit card transaction's properties. While "trans_date_trans_time" logs transaction dates and "cc_num" displays credit card numbers, the "Unnamed: 0" column acts as an index. The "amt" column contains the transaction amount, while the "merchant" and "category" columns contain vendor information. All columns have non-null items, including customer details like "first," "last," "gender," "street," "city," "state," and "zip." The symbols "lat" and "long" stand for geographic data, and "city_pop" denotes the population of a city. "job," "dob," "trans_num," and "unix_time" are additional columns. To specify the merchant's position, use "merch_lat" and "merch_long." "is_fraud," the goal variable, detects fraudulent transactions. This dataset, which comes from Kaggle, is crucial for examining credit card activities and identifying fraud.

B. Data Preprocessing

Data preprocessing is essential for preparing the dataset for analysis and modeling. The process begins with detecting null or duplicate values to ensure data integrity. After confirming there are no missing or duplicate entries, we remove unnecessary columns that do not contribute to our analysis. Specifically, we drop the columns "Unnamed: 0," "cc_num," "trans_date_trans_time," "first," "last," "street," "city," "state," "job," "dob," and "trans_num," resulting in a more concise set of features. The remaining data is categorized into numerical and categorical columns for further processing. Numerical features are standardized to ensure variables with larger ranges do not disproportionately influence the model. To reduce dimensionality and extract relevant features, Principal Component Analysis (PCA) is applied with `n_components=10`, retaining variance while simplifying the model. After these steps, the refined dataset consists of 1,296,675 entries and 14 columns, including "category," "gender," "merchant," 10 principal components (PC1 to PC10), and the target variable "is_fraud," ready for analysis and model training.

C. EDA

This exploratory data analysis (EDA) utilises 'matplotlib' and 'seaborn' visualisations with a dark theme to examine the distribution of gender concerning fraud status. A 15x8-inch illustration featuring a dark background that accentuates two key visualizations—a pie chart depicting gender distribution and a count plot contrasting fraud and non-fraud instances by gender—facilitates clarity and comprehension. The pie chart employs a 'explode' effect to emphasise each group, facilitating a clearer comprehension of the gender distribution related to fraud incidences. The percentage labels are white to contrast with the dark background, and the black margins delineate each category. The second figure, a "seaborn" count plot, employs an alternative colour scheme and annotates bars with exact numbers to illustrate the distribution of fraud and non-fraud incidents by gender. The title "Distribution of Gender with Fraud Status" features a distinct legend that categorises several sorts of fraud status. This EDA offers valuable insights for future research by highlighting the similarities and variations in fraud incidents between genders.

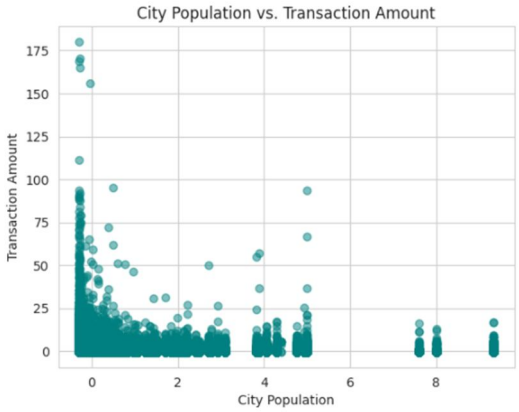


Fig. 3 Scatter Plot Showing Relationship between City Population and Transaction Amount

This scatter plot illustrates the correlation between the number of transactions and the population of cities. The relationship among urban populations & financial activity may be better understood with the help of this image, which plots city populations along the x-axis and total monetary transactions along the y-axis.

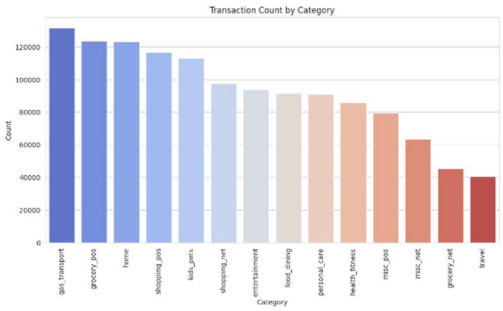


Fig. 4 Transaction Count by Category

This bar chart displays the transaction count across different categories, with each bar representing a distinct transaction category. The y-axis shows the number of transactions, providing insight into which categories experience higher or lower transaction volumes, revealing spending patterns and category popularity.

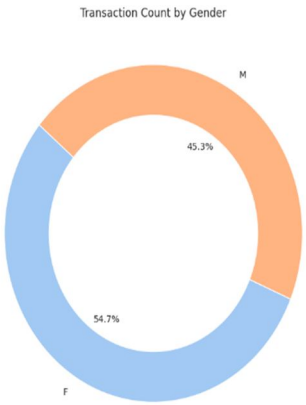


Fig. 5 Transaction Count by Gender

This bar chart illustrates the distribution of transaction counts by gender. Each bar represents one gender category, with the y-axis indicating the number of transactions. The figure highlights differences in transaction volumes between genders, offering insights into spending behaviors across gender demographics.

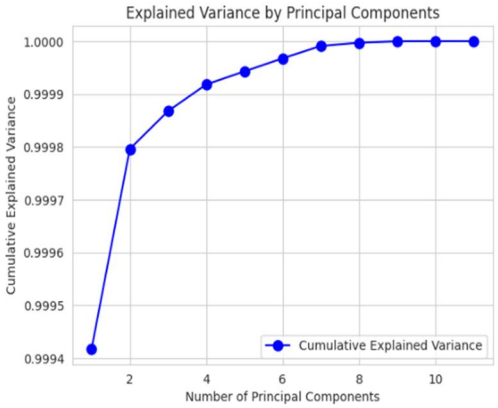


Fig. 6 Cumulative Explained Variance by Number of Principal Components

This line graph illustrates the cumulative explained variance in relation to the number of principal components in the variance analysis. The y-axis represents the total variance explained, whilst the x-axis indicates the number of principal components. The figure is essential in determining the number of components necessary to account for the majority of data variance.

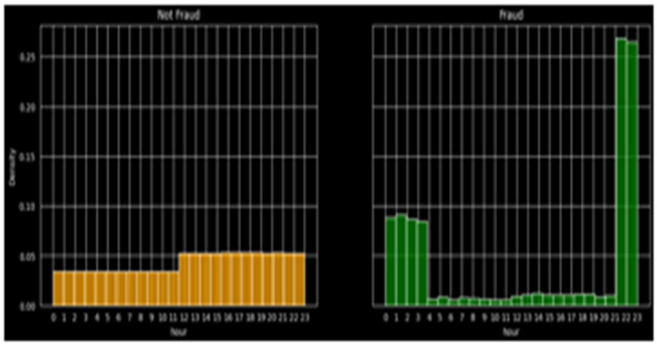


Fig. 7 Hourly Distribution of Fraudulent and Non-Fraudulent Transactions

The distribution of legitimate and fraudulent transactions by time of day is seen in this histogram. The number of transactions is shown on the y-axis, and the hours are shown on the x-axis. Hourly trends are shown in Figure 1, which also provides information on transactional behaviour and the frequency of fraudulent activity.

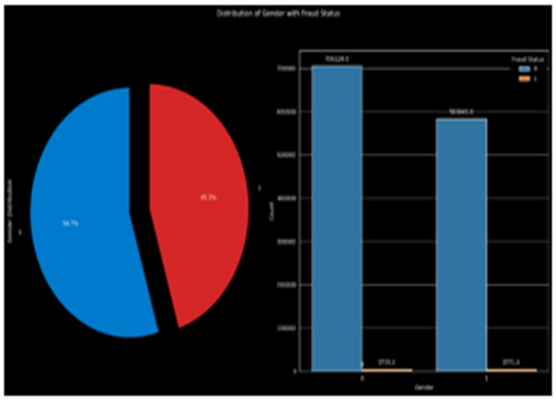


Fig. 8 Distribution of Gender with Fraud Status

You can see the breakdown of fraudulent and non-fraudulent transactions by gender in this bar chart. With gender categories shown on the x-axis and transaction counts broken down by fraud status on the y-axis, we can see the data visually. To better comprehend demographic fraud patterns, this visualisation shows possible gender disparities in fraud occurrence.

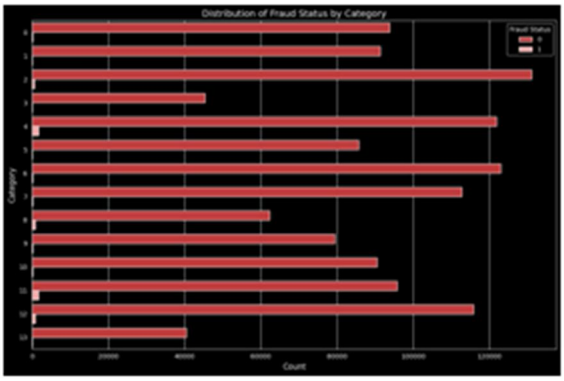


Fig. 9 Distribution of fraud Status by Category

This bar chart illustrates the distribution of fraudulent and non-fraudulent transactions by category. The x-axis represents different transaction kinds, and the y-axis indicates the total transaction count, categorised by fraudulent status. This picture illustrates the categories exhibiting the highest fraud rates, aiding in the comprehension of fraud trends within those categories.

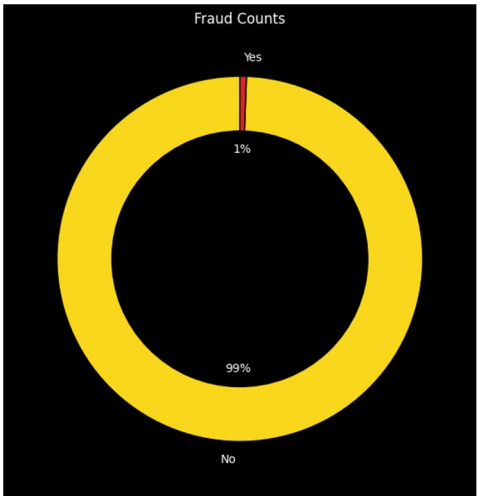


Fig. 10 Fraud Count

This bar chart illustrates the total count of fraudulent transactions. The y-axis represents the number of fraud occurrences, allowing for a quick assessment of the overall volume of detected fraudulent activities. This figure provides a summary view of fraud frequency within the dataset.

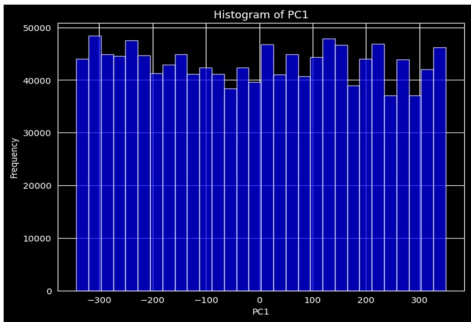


Fig. 11 Histogram of PC1

The data distribution for the dataset's first primary component (PC1) is depicted in this histogram. The range of PC1 values is shown on the x-axis, while the frequency of incidences is shown on the y-axis. This illustration highlights PC1's distribution and central tendency, which clarifies the main direction of data variance.

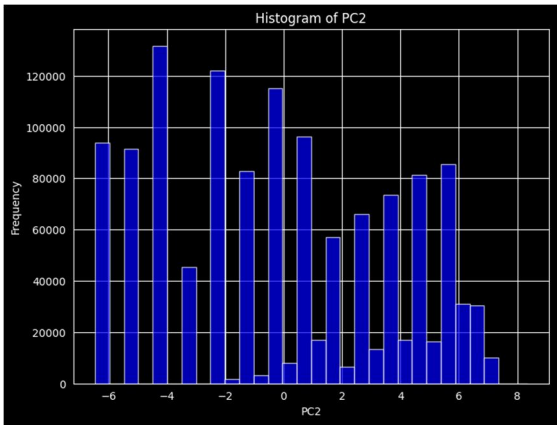


Fig. 12 Histogram of PC2

This histogram shows how the values for the second principal component (PC2) among all the dataset look like. On one side, we can see the frequency scale, and on the other, the range of PC2 values. This scatter plot shows the dispersion and distribution properties of the data along the second principle component, which sheds information on its variance.

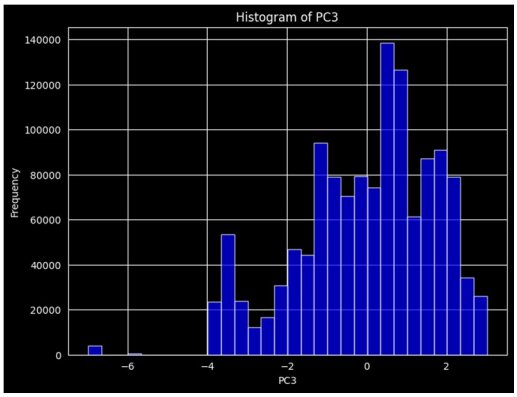


Fig. 13 Histogram of PC3

For the dataset's third principal component (PC3), this histogram shows the distribution of values. The x-axis displays the possible values of PC3, while the y-axis indicates how often each value occurs. The third principle component's spread and variance can be better understood with the help of this visualisation.

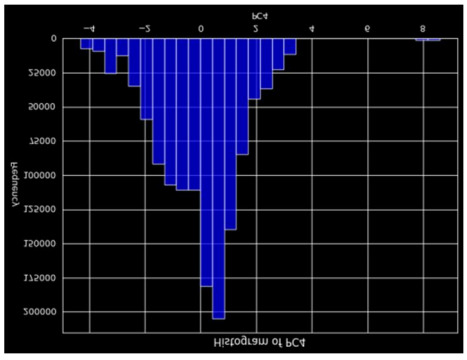


Figure 14 Histogram pf PC4

For the dataset's fourth major component (PC4), this histogram shows the data collection procedure. The y-axis indicates the frequency of occurrences, while the x-axis shows the range of PC4 values. This graphic provides insight into the data structure that this component contains and highlights the important function and major use of PC4.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue I Jan 2025- Available at www.ijraset.com

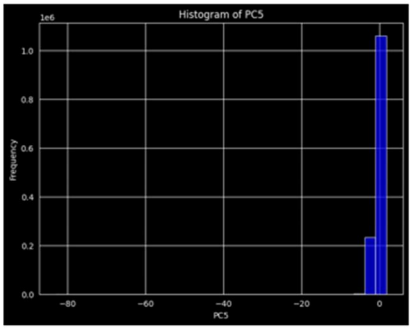


Figure 15 Histogram of PC5

This histogram can be found by looking at the fifth main component (PC5) distribution of the dataset. Possible PC5 values are plotted on the x-axis, and the frequency of each value is plotted on the y-axis. This graphic illustrates how PC5 captured variance, along with its distribution and characteristics within the sample.

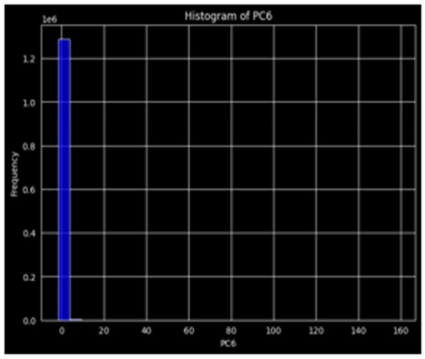


Figure 16 Histogram of PC6

The dataset's sixth principal component (PC6) distribution of values is seen in this histogram. The occurrence of each value is displayed on the y-axis, while the range of potential values for PC6 is displayed on the x-axis. The distribution and dispersal of PC6 are shown below, providing information about the variability of the study with regard to this variable.

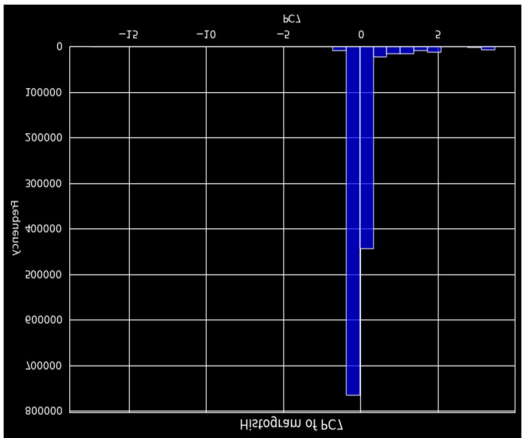


Fig. 17 Histogram of PC7

This histogram shows us the dataset's seventh main component (PC7) value distribution. The y-axis indicates the frequency of occurrence of each number, while the x-axis represents the range of potential PC7 values. The data visualisation helps to comprehend PC7's contribution to the overall variability of the dataset by giving a general overview of its presence and frequency.

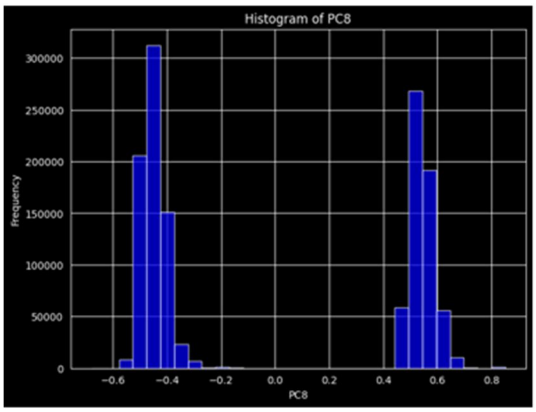


Fig. 18 Histogram of PC8

This histogram shows the dataset's eighth principal component's (PC8) range of values. The y-axis indicates the frequency of occurrences, and the x-axis shows the range of PC8 values. In order to better understand the variety that our study uncovered, this picture provides an illustration of the PC8 distribution.

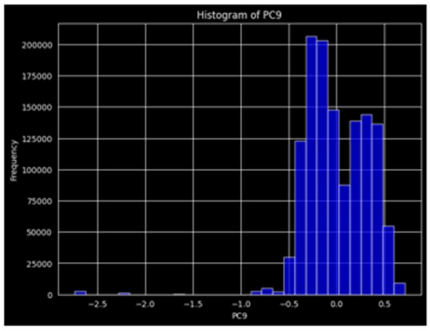


Fig. 19 Histogram PC9

Figure 18 uses the Principal Parts 9 (PC9) a histogram which shows the dataset's corrected feature distribution, to highlight trends and outliers relevant to fraud detection.

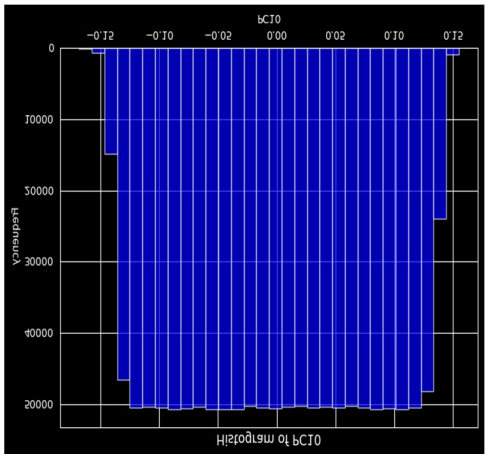


Fig. 20 Histogram of PC10

It shows the range of PC10 values in a histogram. The y-axis shows the average value of those values, while the x-axis displays the PC10 values.

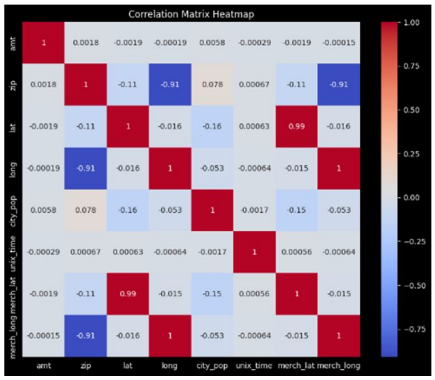


Fig. 21 Correlation Matrix Head map

This heatmap illustrates the dataset's correlation matrix, showing variable relationships. Color intensity indicates correlation strength, facilitating pattern identification and potential multicollinearity among features.

D. Machine Learning Models

1) Logistic Regression: One kind of binary classification model, logistic regression uses logistic functions to fit data and make predictions about future outcomes. For features with linear relationships to the target variable, it is effective due to its simplicity and interpretability.

2) Support Vector Machine (Svm): Search Vector Machines (SVMs) are very effective classification algorithms because they maximise the margin between classes by finding a hyperplane. Because it may use kernel tricks to transform the input space, it is useful when data is not linearly separable and works particularly well in high-dimensional spaces. On the other hand, big datasets could make it computationally intensive.

3) Gradient Boosting: To build decision trees sequentially, with each tree fixing the mistakes of its predecessor, gradient boosting uses an ensemble technique. It catches complex non-linear relationships by systematically minimising the loss function and focussing on misclassified instances; it achieves high accuracy but is prone to overfitting if not tuned properly.

4) Random Forest: An ensemble model, Random Forest builds a number of decision trees using randomly selected dataset subsets and then averages their predictions. It is more accurate and resilient than individual decision trees since it aggregates varied predictions to reduce overfitting. Random Forest shines when faced with massive datasets rich with features.

5) Ensemble: In order to boost performance, ensemble approaches integrate the predictions of numerous models. Bagging, boosting, and stacking are techniques that combine the capabilities of multiple algorithms to provide more accurate predictions with less bias and volatility. Through the integration of many prediction strengths, ensemble models are able to accomplish superior generalisation on unseen data.

E. Deep learning model:

1) Long Short-Term Memory (LSTM): LSTM, a type of a recurrent neural network (RNN), is perfect for time-series data, text, and other sequential data since it can learn from sequences. Long short-term recalls (LSTMs) may be able to handle the vanishing gradient problem more effectively than traditional recurrent neural networks (RNNs) and retain information for extended periods of time due to their memory cells or gating mechanisms. LSTMs thrive in a variety of domains, including as linguistic modelling, speech recognition, or anomaly detection, because to their capacity to comprehend long-term data correlations.

2) Gated Recurrent Unit (GRU): Because the GRU has fewer parameters and merges the input and forget gates into one update gate, it is a more efficient kind of RNN than LSTM. GRUs show faster training times and lower processing needs, even if LSTMs can identify long-term dependencies in data. Time-series forecasting & natural language processing are two examples of sequential jobs that frequently use GRUs because they emphasise computing efficiency. Although the decision between them may depend on the dataset's complexity and the available computing power, their performance is comparable to that of LSTMs.

IV. RESULTS & DISCUSSION

Machine learning algorithms demonstrate a high level of accuracy in differentiating between legitimate and fraudulent transactions when it comes to credit card fraud detection. In every instance, accuracy, recall, F1-score, and other crucial performance metrics yield dependable and consistent outcomes. These findings demonstrate the importance of appropriately sized training data sets and effective planning. In the future, a more effective technique for identifying credit card fraud may result from enhancing model generalisation with sophisticated algorithms and a bigger dataset.

A. Accuracy

A model's ability to differentiate between fraudulent and legitimate transactions may be assessed by looking at its accuracy, which is calculated as the ratio of actual positive and real negatives to the total number of cases. The prevalence of legal actions in cases of class disparity raises the possibility that they may not fairly represent performance in these circumstances.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

B. Loss

In machine learning, loss is a quantitative measure of the discrepancy between expected and observed values. Minimising loss is a sign of superior performance. By comparing the expected probabilities with the actual labels, binary cross-entropy guides parameter optimisation during training for credit card fraud detection models.

$$Loss = -\frac{1}{N}\sum_{i-1}^{N}[y_i \log(\hat{y_i}) + (1-y_i)\log(1-\hat{y_i})] \quad (2)$$

C. Precision

A positive predictive value, also known as precision, is the percentage of detected instances that were correct in identifying fraudulent transactions. In the financial sector, where incorrectly labelling lawful transactions can have serious consequences, a high precision score indicates accurate fraud detection.

$$Precision = \frac{TP}{TP+FP} \quad (3)$$

D. Recall

The sensitivity, or recall, of a model is defined as its ability to identify actual fraudulent transactions, represented as the ratio of true positives to all genuine positives. While a trade-off typically exists between precision and recall, elevated recall indicates superior detection and mitigates the risk of missing fraudulent activities.

$$Recall = \frac{TP}{TP+FN} \quad (4)$$

E. F1 Score

Particularly when dealing with unequal class distributions, the F1 score—which incorporates recall and precision into a single metric—reflects overall performance. An important metric for trustworthy fraud detection, it measures the ratio of false positives to negatives, which shows how well a model can identify and validate fraudulent transactions.

$$F1-score = \frac{2}{\frac{1}{precision}+\frac{1}{recall}} \quad (5)$$

TABLE 2.MACHINE LEARNING MODEL EVALUATION

Model	Accuracy	Precision	Recall	F1 Score
Logistic Regression	0.849	0.952	0.961	0.869
SVM	0.667	0.667	0.667	0.667
Gradient Boosting	0.873	0.873	0.873	0.873
Random Forest	0.903	0.903	0.903	0.903
Ensemble	0.880	0.880	0.880	0.880

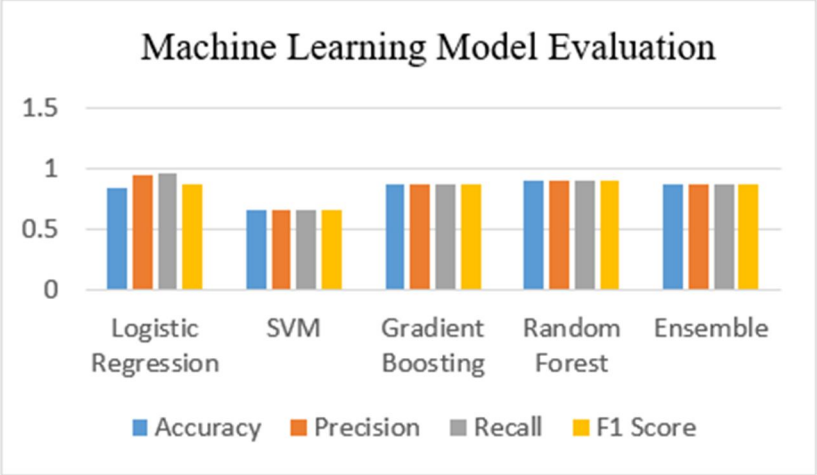


Fig. 22 Machine Learning Model

The models created using machine learning displayed a range of performance metrics. The accuracy, precision, and recall rates of Logistic Regression were 84.9%, 95.2%, and 96.1%, respectively. In terms of metrics, Gradient Boosting received an 87.3% score, while SVM received 66.7%. Random Forest emerged victorious with a total score of 90.3%, while the Group model achieved 88% in each category.

1) Confusion Matrix of Ml Model

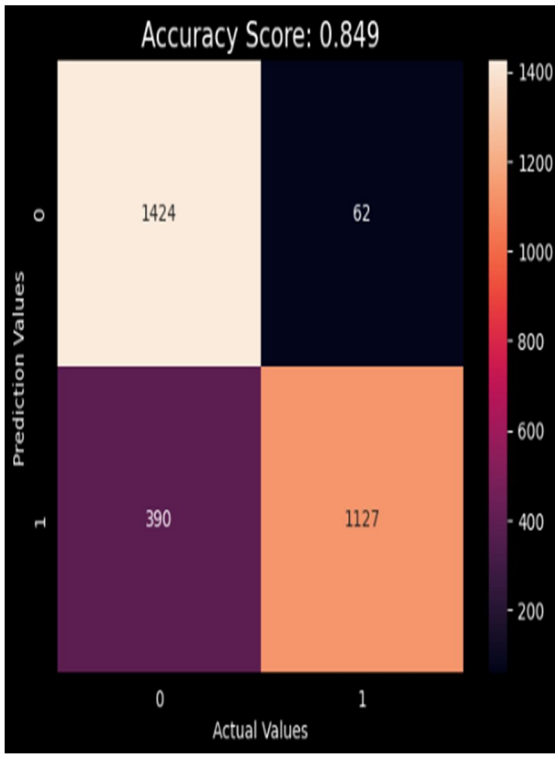


Fig. 23 Confusion Matrix of proposed Model

Examine the Model's Confusion Map to see how well the model created using machine learning categorises credit card transactions. The amount of false positives, false negatives, genuine positives, and genuine negatives shows the model's accuracy and error rates as well as the right and wrong classifications of authentic and fraudulent transactions.

2) SVM

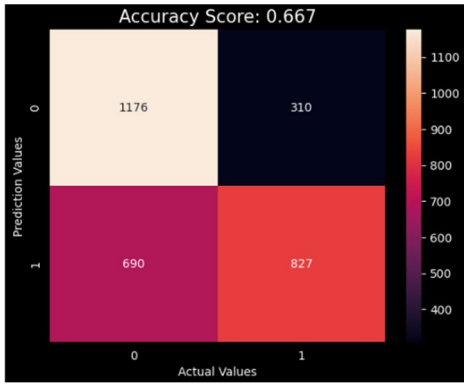


Fig. 24 Support Vector Machine

This chart illustrates the limits of the classes that the Support Vector Machine (SVM) model uses to categorise data points. The optimal hyperplane enhances classification accuracy by optimising the margin between classes; decision boundary establishment is heavily reliant on support vectors.

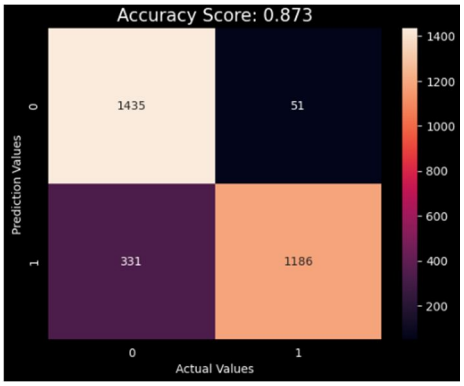


Fig. 25 Gradient boosting

To create a stronger prediction model, the Gradient Boosting technique combines several weak learners, such as decision trees. The trees improve accuracy and performance with each iteration by learning from the mistakes made by their predecessors and collecting increasingly intricate data patterns.

3) Random Forest

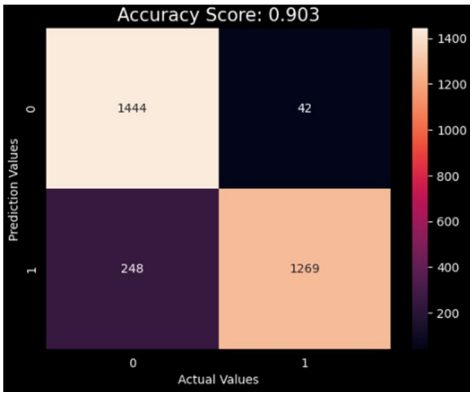


Fig. 26 Random Forest

As you can see in the image, the Random Forest model employs an ensemble technique to improve prediction accuracy, decrease overfitting, and strengthen resilience across different datasets. Using a combination of decision trees, the ensemble strategy

4) Ensemble

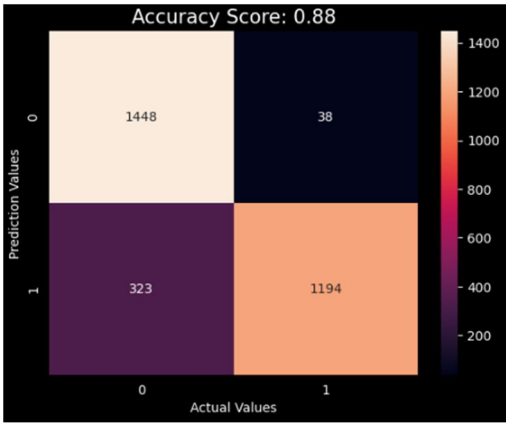


Fig. 27 Ensemble

This image illustrates how a combined model that incorporates multiple machine learning techniques can make predictions. When compared to individual models, ensemble methods—which include many models such as Random Forests, Vector Machines, & Gradient Boosting—show higher resilience and generalisability. This technique successfully reduces errors and improves model dependability.

TABLE 3. DEEP LEARNING MODELS EVALUATION

Model	Accuracy	Precision	Recall	F1 Score	Loss
LSTM	0.8978	0.91	0.90	0.90	0.2621
GRU	0.9004	0.91	0.90	0.90	0.2528

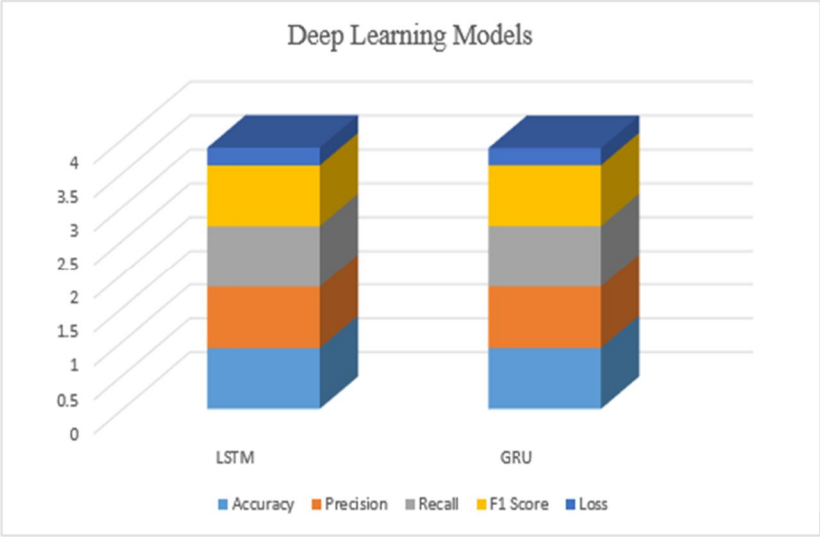


Fig. 28 Deep Learning Models

Metrics for the deep learning models' output look like this: The LSTM model achieved remarkable results, with a 90% recall, 90% F1 score, and an accuracy of 89.78%. Although both models had similar precision and recall scores, the GRU model managed a little better accuracy of 90.04% with a smaller loss of 0.2528 Graph for the Dl Model's Performance

5) LSTM

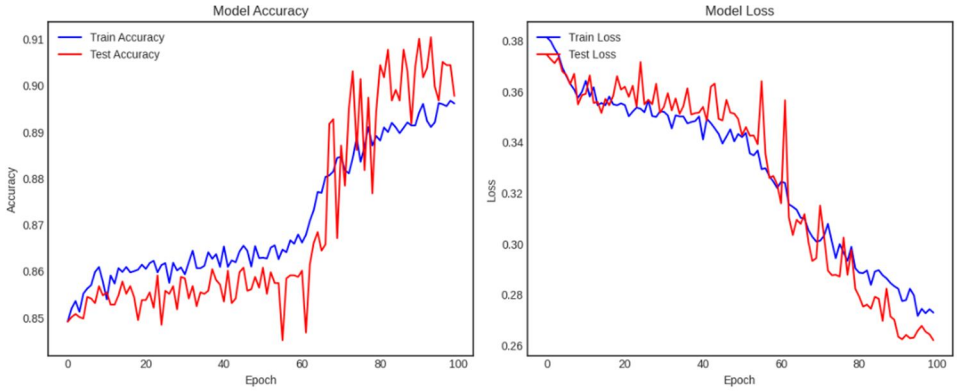


Fig. 29 LSTM Model Performance: Accuracy and Loss Curves

This graphic shows the accuracy and loss curves of the LSTM (Long Short-Term Memory) model over all the training epochs. The accuracy curve shows how the model's accuracy changes during training, while the loss curve shows how far the errors have come. Using these curves, you can identify model overfitting and underfitting, learning speed, and other difficulties.

6) GRU

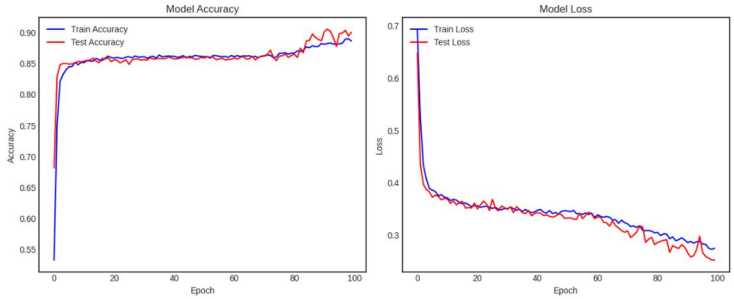


Fig. 30 GRU Model Performance: Accuracy and Loss Curves

This figure shows the accuracy and loss curves of the GRU (Gated Recurrent Unit) model over the training epochs. The accuracy curve displays the model's performance improvement over training, while the loss curve displays the reduction of the model's errors. When viewed collectively, these curves disclose details about the model's convergence, learning, and indications of overfitting or underfitting.

TABLE 4. MODEL PERFORMANCE COMPARISON

Model	Accuracy	References
RF	76%	[26]
ANN	89%	[27]
Proposed GRU	90	---

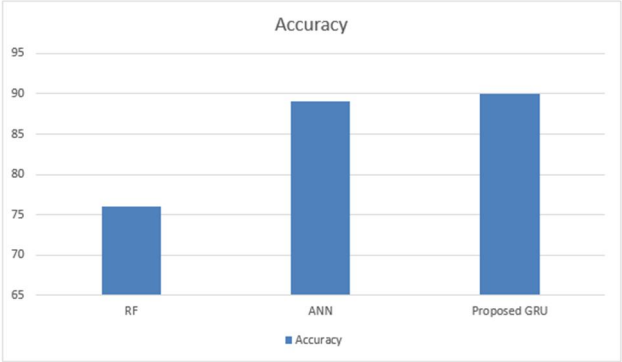


Fig. 31 Performance Comparison

The table shows the accuracy of various models: Random Forest (RF) with 76%, Artificial Neural Network (ANN) with 89%, and the proposed GRU model with 90%. The GRU model achieves the highest accuracy among the three.

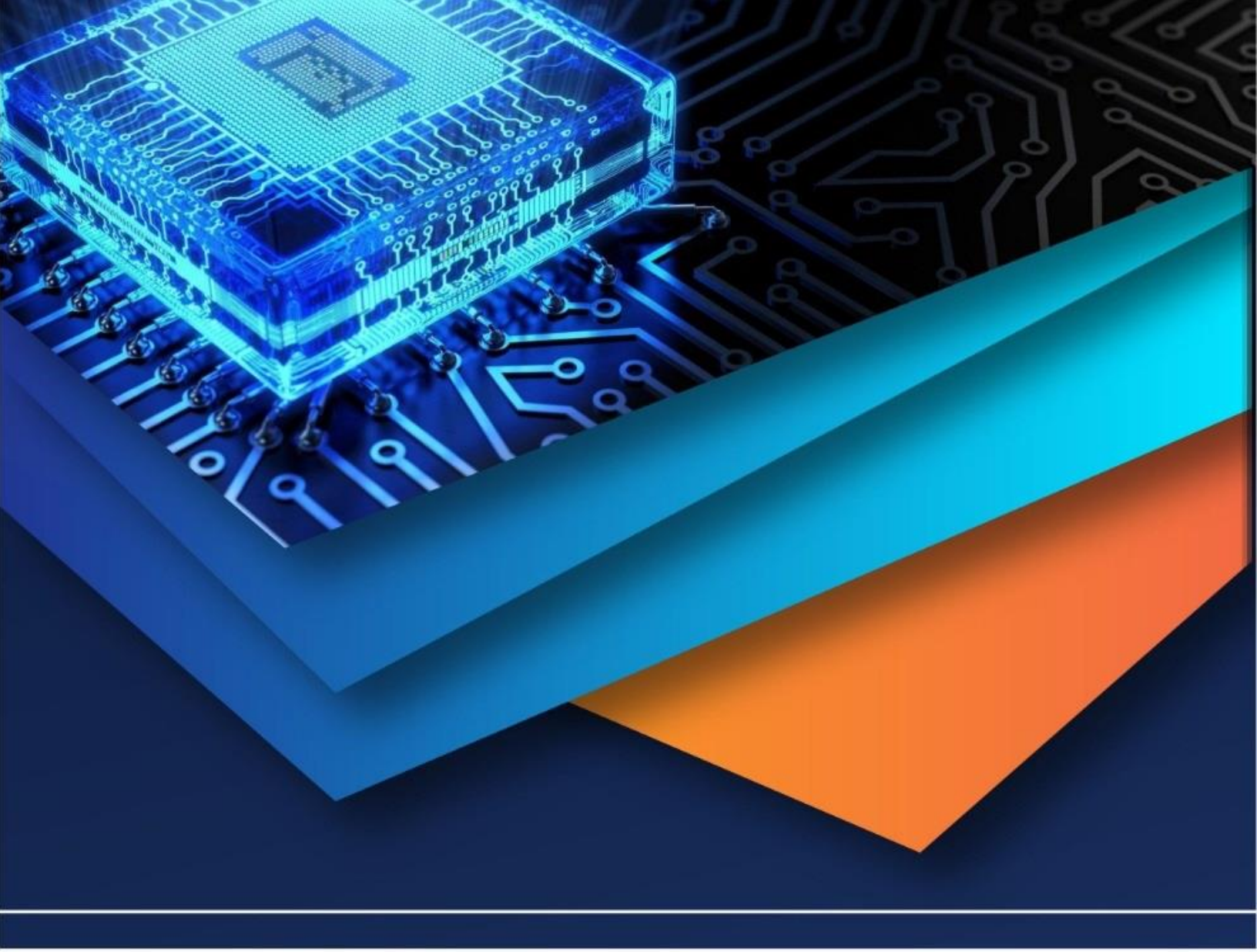
V. CONCLUSION

This study demonstrates the systematic application of state-of-the-art machine learning and deep learning algorithms for credit card fraud detection. With meticulous data collection, a comprehensive dataset containing all relevant transaction details was produced. Strict preprocessing procedures were employed to provide appropriate analytical circumstances and improve data integrity by eliminating superfluous features and standardising numerical values. The selection of the model was informed by the significant patterns and relationships discovered via the use of exploratory data analysis (EDA). Support Vector Machines, Random Forest, Logistic Regression, GRU, Gradient Boosting, and Long Short-Term Memory are some of the models that have demonstrated promise in detecting fraud. The most remarkable of all performance indicators, the Random Forest model's accuracy rate of 90.3%, was attained by aligning the recall, F1, and precision scores. GRU distinguished itself from the other deep learning models with an accuracy rate of 90.04% and above-average recall and precision. While LSTM demonstrated competence, it was not optimal. Additionally, its 89% accuracy was comparable to other well-known models, such as the ANN. By highlighting the use of realistic strategies to improve financial stability, this thorough investigation lays the foundation for future studies on credit card fraud detection. Systems for detecting fraud can be greatly enhanced by developments in machine and deep learning.

REFERENCES

[1] S. Sruthi, S. Emadaboina, and C. Jyotsna, “Enhancing Credit Card Fraud Detection with Light Gradient-Boosting Machine: An Advanced Machine Learning Approach,” 2024 Int. Conf. Knowl. Eng. Commun. Syst. ICKECS 2024, 2024, doi: 10.1109/ICKECS61492.2024.10616809.
[2] G. Airlangga, “Evaluating the Efficacy of Machine Learning Models in Credit Card Fraud Detection Journal of Computer Networks , Architecture and High Performance Computing,” J. Comput. Networks, Archit. High Perform. Comput., vol. 6, no. 2, pp. 829–837, 2024.
[3] X. Feng and S. K. Kim, “Novel Machine Learning Based Credit Card Fraud Detection Systems,” Mathematics, vol. 12, no. 12, 2024, doi: 10.3390/math12121869.
[4] D. Hove, O. Olugbara, and A. Singh, “Bibliometric Analysis of Recent Trends in Machine Learning for Online Credit Card Fraud Detection,” J. Scientometr. Res., vol. 13, no. 1, pp. 43–57, 2024, doi: 10.5530/jscires.13.1.4.
[5] C. G. Tekkali and K. Natarajan, “Assessing CNN’s Performance with Multiple Optimization Functions for Credit Card Fraud Detection,” Procedia Comput. Sci., vol. 235, pp. 2035–2042, 2024, doi: 10.1016/j.procs.2024.04.193.
[6] M. H. Chagahi, N. Delfan, S. M. Dashtaki, B. Moshiri, and M. J. Piran, “An Innovative Attention-based Ensemble System for Credit Card Fraud Detection,” pp. 1–9, 2024.
[7] M. Kanchana, V. Chadda, and H. Jain, “Credit card fraud detection,” Int. J. Adv. Sci. Technol., vol. 29, no. 6, pp. 2201–2215, 2020, doi: 10.55041/ijsrem35776.
[8] M. Kong et al., “CFTNet: a robust credit card fraud detection model enhanced by counterfactual data augmentation,” Neural Comput. Appl., vol. 36, no. 15, pp. 8607–8623, 2024, doi: 10.1007/s00521-024-09546-9.
[9] V. Chang, B. Ali, L. Golightly, M. A. Ganatra, and M. Mohamed, “Investigating Credit Card Payment Fraud with Detection Methods Using Advanced Machine Learning,” Inf., vol. 15, no. 8, pp. 1–20, 2024, doi: 10.3390/info15080478.
[10] I. D. Mienye, “A Hybrid Deep Learning Approach with Generative Adversarial Network for Credit Card Fraud Detection,” 2024.
[11] S. S. Sulaiman, I. Nadher, and S. M. Hameed, “Credit Card Fraud Detection Using Improved Deep Learning Models,” Comput. Mater. Contin., vol. 78, no. 1, pp. 1049–1069, 2024, doi: 10.32604/cmc.2023.046051.
[12] A. R. Jaiswal and A. Krishna, “Credit Shield Solutions : Credit Card Fraud Detection System Using Machine Learning Approach,” vol. 10, no. 5, pp. 2111–2115, 2024.

[13] K. Maithili et al., "Development of an efficient machine learning algorithm for reliable credit card fraud identification and protection systems," MATEC Web Conf., vol. 392, p. 01116, 2024, doi: 10.1051/matecconf/202439201116.
[14] D. P. Prabha and C. V. Priscilla, "A combined framework based on LSTM autoencoder and XGBoost with adaptive threshold classification for credit card fraud detection," Sci. Temper, vol. 15, no. 02, pp. 2216–2224, 2024, doi: 10.58414/scientifictemper.2024.15.2.34.
[15] O. G. Abdulateef, "Fraud Guard: A Comprehensive Comparative Analysis of Machine Learning Approaches to Enhance Credit Card Fraud Detection," J. Inf. Eng. Appl., vol. 14, no. 2, pp. 14–22, 2024, doi: 10.7176/jiea/14-2-02.
[16] S. Jhansi Ida, K. Balasubadra, R. R. Skandarsini, and T. Lakshmi Narayanaa, "Enhancing Credit Card Fraud Detection through LSTM-Based Sequential Analysis with Early Stopping," Proc. 2nd IEEE Int. Conf. Netw. Commun. 2024, ICNWC 2024, no. June, 2024, doi: 10.1109/ICNWC60771.2024.10537550.
[17] M. Azim Mim, N. Majadi, and P. Mazumder, "A soft voting ensemble learning approach for credit card fraud detection," Heliyon, vol. 10, no. 3, p. e25466, 2024, doi: 10.1016/j.heliyon.2024.e25466.
[18] A. A. Yılmaz, "A machine learning-based framework using the particle swarm optimization algorithm for credit card fraud detection," Commun. Fac. Sci. Univ. Ankara Ser. A2-A3 Phys. Sci. Eng., vol. 66, no. 1, pp. 82–94, 2024, doi: 10.33769/aupse.1361266.
[19] M. Zhu, Y. Zhang, Y. Gong, C. Xu, and Y. Xiang, "Enhancing Credit Card Fraud Detection: A Neural Network and SMOTE Integrated Approach," J. Theory Pract. Eng. Sci., vol. 4, no. 02, pp. 23–30, 2024, doi: 10.53469/jtpes.2024.04(02).04.
[20] S. Islam, M. M. Haque, and A. N. M. R. Karim, "A rule-based machine learning model for financial fraud detection," Int. J. Electr. Comput. Eng., vol. 14, no. 1, pp. 759–771, 2024, doi: 10.11591/ijece.v14i1.pp759-771.
[21] A. Sani, Z. L. Hassan, and A. T. Balarabe, "A Logistic Regression-based Model for Identifying Credit Card Fraudulent Transactions," Asian J. Res. Comput. Sci., vol. 17, no. 7, pp. 41–54, 2024, doi: 10.9734/ajrcos/2024/v17i7476.
[22] F. O. Aghware et al., "Enhancing the Random Forest Model via Synthetic Minority Oversampling Technique for Credit-Card Fraud Detection," J. Comput. Theor. Appl., vol. 1, no. 4, pp. 407–420, 2024, doi: 10.62411/jcta.10323.
[23] E. Tank and M. Das, "On Credit Card Fraud Detection Using Machine Learning Techniques," Lect. Notes Networks Syst., vol. 966 LNNS, no. September, pp. 293–303, 2024, doi: 10.1007/978-981-97-2004-0_21.
[24] D. Planinic and V. Popovic-Bugarin, "Credit Card Fraud Detection Using Supervised Learning Algorithms," 2024 28th Int. Conf. Inf. Technol. IT 2024, vol. 9, no. 10, pp. 2–5, 2024, doi: 10.1109/IT61232.2024.10475768.
[25] T. R. Noviandy, G. M. Idroes, A. Maulana, I. Hardi, E. S. Ringga, and R. Idroes, "Credit Card Fraud Detection for Contemporary Financial Management Using XGBoost-Driven Machine Learning and Data Augmentation Techniques," Indatu J. Manag. Account., vol. 1, no. 1, pp. 29–35, 2023, doi: 10.60084/ijma.v1i1.78.
[26] MD RASHED MOHAIMIN, Md Sumsuzoha, Md Amran Hossen Pabel, and Farhan Nasrullah, "Detecting Financial Fraud Using Anomaly Detection Techniques: A Comparative Study of Machine Learning Algorithms," J. Comput. Sci. Technol. Stud., vol. 6, no. 3, pp. 01–14, 2024, doi: 10.32996/jcsts.2024.6.3.1.
[27] M. A. Gill, M. Quresh, A. Rasool, and M. M. Hassan, "Detection of Credit Card Fraud Through Machine Learning In Banking Industry," vol. 05, no. 01, pp. 1–10, 2023.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY