A Novel Algorithm For Credit Card Fraud Detection Using Machine Learning

[1]Wajda Tabassum, [2]Dr. Pankaj Richhariya
[1]Mtech Scholar, tabassumwit@gmail.com, Department of CSE, BITS,Bhopal(M.P.) India
[2]Professor & HOD, bitshodcs@gmail.com, Department of CSE, BITS,Bhopal(M.P.) India

Abstract – Credit card fraud has emerged as a major challenge for financial institutions and cardholders across the globe, resulting in considerable financial losses and breaches of personal data. Traditional rule-based approaches to fraud detection often fail to keep pace with the increasingly sophisticated methods employed by fraudsters. Recently, artificial intelligence (AI) techniques have gained recognition as effective tools for combating credit card fraud, owing to their capability to process large datasets and adapt to evolving fraud patterns.

This study introduces an innovative AI-driven system for credit card fraud detection. The system harnesses the power of machine learning, specifically deep learning algorithms, to scrutinize transactional data and detect fraudulent activity in real-time. It draws on an extensive set of features derived from transaction characteristics, such as the amount, merchant details, transaction timing, and cardholder information.

***Keywords**: Credit Card, Fraud Detection, Machine Learning, CNN, XGBoost*

I. INTRODUCTION

Credit card fraud has become a widespread concern in the financial sector, presenting significant challenges for both financial institutions and consumers. Fraudulent activities, including unauthorized transactions, identity theft, and the use of counterfeit cards, have led to considerable financial losses and the compromise of personal information. Traditional rule-based fraud detection methods, which depend on predefined rules and thresholds, often fail to keep pace with the increasingly sophisticated tactics used by fraudsters.

In recent years, the financial industry has shown a growing interest in utilizing artificial intelligence (AI) techniques for detecting credit card fraud. AI has the potential to significantly enhance fraud detection by employing advanced algorithms capable of learning from large datasets and adapting to new and evolving patterns. Machine learning, in particular, has demonstrated its effectiveness in identifying complex fraud patterns that may be challenging for rule-based systems to capture.

Various machine learning algorithms, such as decision trees, random forests, support vector machines, and neural networks, have been explored in the context of credit card fraud detection. These algorithms analyze transactional data, extracting valuable features and patterns that help differentiate between legitimate and fraudulent transactions. By training these models on labeled datasets containing historical fraud instances, the algorithms learn to detect fraudulent activities based on the patterns they have learned.

Deep learning, a specialized area within machine learning, has garnered significant attention in recent years due to its ability to handle large and intricate datasets. Deep learning models, including convolutional neural networks (CNNs) and recurrent neural networks (RNNs), are particularly effective at capturing complex relationships and dependencies within transactional data. These models hold great promise for improving the accuracy and efficiency of credit card fraud detection systems.

The development of AI-powered credit card fraud detection systems is vital for financial institutions aiming to reduce financial losses, protect customer trust, and uphold the integrity of the financial ecosystem. By harnessing AI, these systems can continuously learn and adapt to new fraud patterns, enabling real-time detection and prevention. As fraudsters constantly evolve their methods, it is essential to explore innovative AI solutions to stay ahead in the fight against credit card fraud.

II. CREDIT CARD FRAUD

A credit card is a plastic payment instrument issued by a financial institution, such as a bank or credit card company, that allows cardholders to make purchases and access a line of credit. It is a convenient and widely accepted form of payment in both online and offline transactions.

Figure 1 : Look of Credit Card

Credit cards operate on the principle of borrowing money from the issuing institution to make purchases. When a cardholder uses a credit card, the issuing institution pays the merchant on the cardholder's behalf, and the cardholder incurs a debt to the institution. The cardholder is then required to repay the borrowed amount within a specified time frame, typically on a monthly basis.

Credit cards offer numerous benefits to consumers, including a secure and convenient means of making purchases without the need to carry cash. Additionally, credit cards often come with rewards programs, cashback offers, and insurance coverage for certain purchases. They also provide a line of credit that can be valuable for managing expenses, handling emergencies, and building a credit history.

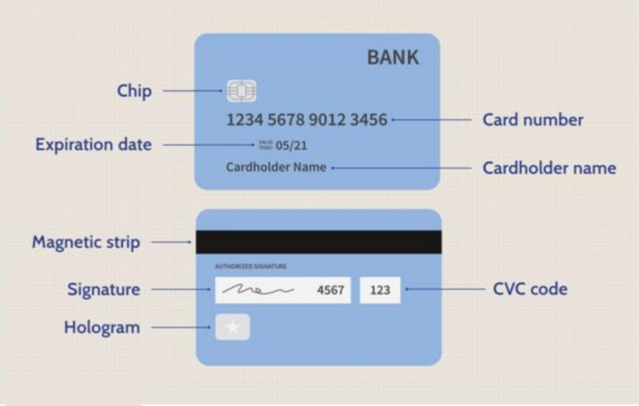

Figure 2 Credit Card Information

However, responsible credit card usage is crucial to avoid accumulating high-interest debt. Failure to repay the borrowed amount within the specified time frame can result in interest charges, late payment fees, and a negative impact on the cardholder's credit score.

To obtain a credit card, individuals typically need to apply through a financial institution and meet specific eligibility criteria, including having a good credit history, providing income verification, and meeting legal age requirements. Upon approval, the cardholder receives a physical card with a unique card number, expiration date, and security code, which are necessary for conducting transactions in person, online, or over the phone.

.

III. LITERATURE SURVEY

Day Credit card fraud is a persistent problem in the financial industry, prompting researchers to explore various methods for effective fraud detection. This literature review provides an overview of existing research, methodologies, and advancements in credit card fraud detection.

M. Abhilash Sharma et al (2022) studies on Fraudulent activities in the financial sector are on the rise, with fraud patterns constantly evolving and showing no consistent trends over time. The rapid adoption of new technologies by fraudsters has facilitated the execution of online fraudulent transactions. Due to the dynamic nature of these fraud patterns, an effective fraud detection model must adapt and update itself to keep pace with these changes. In this study, we focus on analyzing fraud cases that are difficult to detect using traditional supervised learning methods or historical data. We propose the development of an Auto-encoder model based on deep learning, which will be evaluated against datasets from different regions of the world to examine the demographic diversity of fraud patterns and identify the geographical areas where the model performs optimally. The proposed algorithm, a deep learning model based on the Auto-encoder (AE) network, operates as an unsupervised learning algorithm that leverages backpropagation by aligning inputs and outputs. This research utilizes Google's TensorFlow package to implement the AE model using deep learning techniques. The performance of the model is evaluated using metrics such as accuracy, precision, recall, F1 score, and the area under the curve (AUC).

Haichao Du, et al (2023) This study introduces a novel approach called Autoencoder with Probabilistic LightGBM (AED-LGB) for detecting credit card fraud. The AED-LGB algorithm, which is grounded in deep learning, begins by extracting low-dimensional feature data from high-dimensional bank credit card data. This is achieved using the autoencoder's symmetrical network structure, which enhances the model's ability to learn and represent features effectively. The dataset used for this research is derived from a real-world, anonymized bank dataset, which is highly imbalanced, with normal transactions vastly outnumbering fraudulent ones. To address this imbalance, the SMOTE algorithm is applied to resample the data, ensuring that the number of fraud and non-fraud cases is equal before feeding the feature data into LightGBM. However, after comparing the results from the resampled and non-resampled data, it was observed that resampling did not improve the AED-LGB algorithm's performance. This finding suggests that AED-LGB is particularly well-suited for handling imbalanced datasets.

When compared to other widely used machine learning algorithms, such as K-Nearest Neighbors (KNN) and standard LightGBM, the AED-LGB algorithm demonstrates superior performance. Specifically, it shows an overall 2% improvement in accuracy (ACC) compared to LightGBM and KNN. Additionally, when the threshold is set to 0.2, the Matthew's Correlation Coefficient (MCC) index for AED-LGB is 4% higher than that of LightGBM and 30% higher than that of KNN. These results indicate that the AED-LGB algorithm outperforms others in terms of accuracy, true positive rate, true negative rate, and Matthew's Correlation Coefficient, making it a more effective tool for credit card fraud detection.

Waleed et al (2020) massive fraud increase that yields in losing millions of dollars all over the world annually; numerous up-to-date approach in the fraud detection are being constantly advanced and implemented in numerous business areas. Fraud detection is involved with the monitoring of user populations behavior for the sake of estimating, detecting, or avoiding any unwanted behavior, which is considered as one of the broad terms that include felony: intrusion, fraud, and defaulting of accounts. Systems of fraud detection are required to detect on-line transactions with the use of the unsupervised learning, due to the fact that some of the fraudsters commit fraud once via on-line means and after that, switch to other methods. The presented research has the aim of i) focusing on cases of fraud which are undetectable according to supervised learning or previous history, ii) creating a deep Auto-encoder model which is capable of reconstructing normal transactions for finding anomalies from the normal patterns. The presented deep learning which is based on the auto-encoder (AE) is one of the unsupervised learning algorithms which apply back-propagation via setting the inputs to be equal to the outputs..

IV. PROPOSED METHODS

Data Preparation: Before training, the training dataset is preprocessed as discussed earlier. This includes data cleaning, feature engineering, handling missing values, and addressing outliers. The dataset is also split into features (independent variables) and the target variable (fraud or non-fraud).

Selecting a Model: Based on the choice made during model selection (e.g., Logistic Regression, Random Forest, XGBoost), the corresponding machine learning algorithm is selected for training.

Feature Scaling: In many cases, it's essential to scale or normalize the features. Feature scaling ensures that all input variables have the same scale, preventing some features from dominating the learning process. Common scaling methods include Standardization (scaling to have a mean of 0 and a standard deviation of 1) and Min-Max scaling (scaling to a specific range).

Training the Model: The selected machine learning model is trained on the preprocessed training dataset. During training, the model learns to recognize patterns and relationships within the data that distinguish between fraudulent and non-fraudulent transactions. The learning process involves optimizing the model's parameters to minimize a specific loss function.

Cross-Validation: To assess the model's performance and ensure it generalizes well to new, unseen data, cross-validation techniques like k-fold cross-validation may be used. Cross-validation helps in estimating the model's performance on different subsets of the training data.

Hyperparameter Tuning: Some machine learning algorithms have hyperparameters that need to be tuned to achieve optimal performance. Techniques like grid search or random search can be employed to find the best combination of hyperparameters.

Model Evaluation: After training, the model's performance is evaluated using various evaluation metrics such as accuracy, precision, recall, F1-score, and ROC AUC (Receiver Operating Characteristic Area Under the Curve). These metrics help assess how well the model classifies fraudulent and non-fraudulent transactions.

Overfitting Control: Overfitting occurs when a model learns the training data too well but fails to generalize to new data. Techniques like regularization (e.g., L1 and L2 regularization), reducing model complexity, and early stopping can be applied to control overfitting.

Prediction:

Pass the extracted features of the new transaction through the loaded model. The model will output a prediction score or class label. In credit card fraud detection, this class label typically indicates whether the transaction is predicted as "fraudulent" (1) or "legitimate" (0).

Feature Extraction: When a new credit card transaction occurs, various attributes or features associated with that transaction are collected. These features can include information such as the transaction amount, the location of the merchant, the time of the transaction, the type of card used, and more. These features help describe and characterize the transaction.

Data Preprocessing: The extracted features need to undergo data preprocessing steps to ensure they're in a suitable format for input into the machine learning model. This preprocessing aligns with how the model was trained. It involves tasks such as handling missing values, scaling numerical features, and encoding categorical features if needed.Model Loading: The machine learning model used for fraud detection is typically pre-trained on historical transaction data. This pre-trained model is loaded into memory when a new transaction occurs. The model contains information about patterns and relationships within the data that it learned during the training phase.

Prediction: With the new transaction's preprocessed features in hand and the model loaded, the prediction process begins. The features are fed into the model as input. The model then processes these features through its internal architecture, which consists of mathematical functions and parameters. This internal processing generates an output, which is often referred to as a "prediction score."

Prediction Score: The prediction score is a numerical value produced by the model's internal calculations. In the context of binary classification for credit card fraud detection, this score doesn't directly indicate "fraudulent" or "legitimate." Instead, it quantifies the model's level of confidence or certainty that the given transaction is fraudulent.

Thresholding: To make a definitive decision, a threshold is applied to the prediction score. The threshold value determines the classification outcome. Transactions with prediction scores above the threshold are classified as "fraudulent" (usually labeled as 1), while those below the threshold are classified as "legitimate" (usually labeled as 0).

Threshold Example: If the threshold is set at 0.5, any prediction score greater than or equal to 0.5 will result in a classification of "fraudulent," while scores below 0.5 will result in a classification of "legitimate."

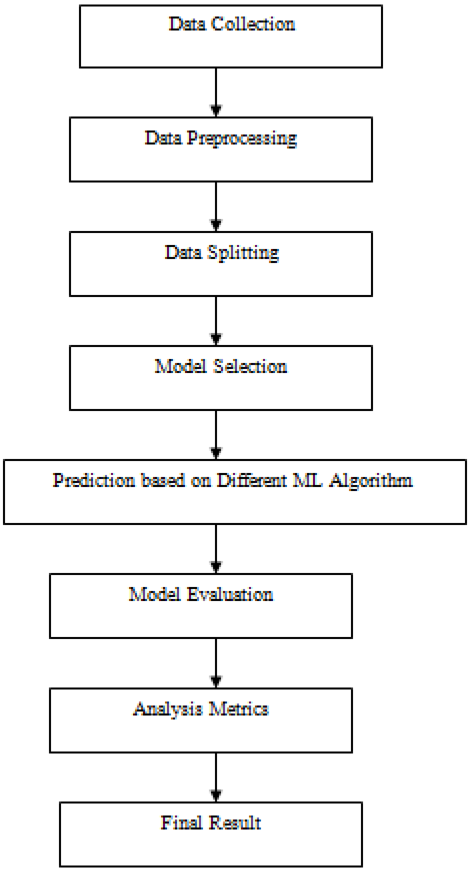

Figure 3 Proposed flow

Output Class Label: The final outcome of the prediction process is a class label. In credit card fraud detection, this label can take one of two values: "fraudulent" (1) or "legitimate" (0). This label is determined based on whether the prediction score crosses the threshold.

Classification Example: If the prediction score for a new transaction is 0.75, and the threshold is 0.5, the transaction will be classified as "fraudulent" (1).

Decision Logic: The class label assigned to the transaction influences the decision and action taken. If a transaction is classified as "fraudulent," it may trigger further investigation, an alert to the cardholder, or even the blocking of the transaction to prevent unauthorized charges. If it's classified as "legitimate," it proceeds without intervention.

Figure 4.1 is show credit card detection process involves a series of crucial steps to ensure the development of an effective and accurate model. The first phase is data collection, where a diverse and representative dataset containing credit card transactions is gathered. Following this, the data undergoes meticulous preprocessing to handle issues such as missing values, outliers, and feature scaling, ensuring the dataset is ready for model training.

V. RESULT

In fraud detection, the F1-Score is particularly useful as it takes into account both false positives and false negatives. This makes it especially valuable in situations involving imbalanced datasets, where the occurrence of fraud is rare compared to legitimate transactions. A higher F1-Score indicates that the model has achieved a better balance between precision (which focuses on minimizing false positives) and recall (which aims to minimize false negatives).

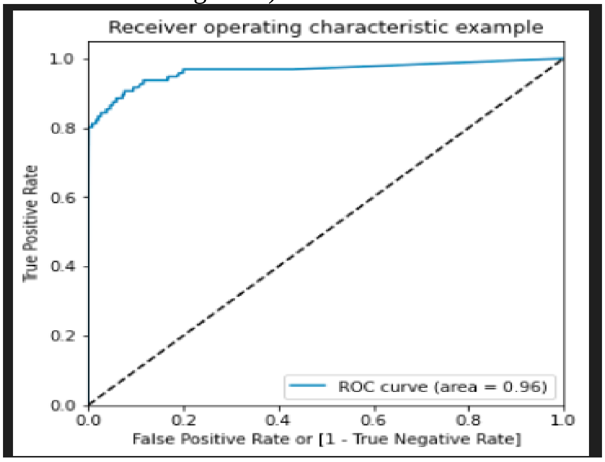

Figure 4 ROC of random forest

Figure 4 displays the Receiver Operating Characteristic (ROC) of the Random Forest model, with the following performance metrics: Accuracy: 0.99, Sensitivity: 0.65, Specificity: 0.99 and F1-Score: 0.692. These metrics provide an overview of the model's accuracy, sensitivity, specificity, and F1-Score, demonstrating its performance in classification tasks.

Figure 5 displays the Receiver Operating Characteristic (ROC) of the Decision Tree model, with the following performance metrics: Accuracy: 0.998, Sensitivity: 0.583, Specificity: 0.999 and F1-Score: 0.692

These metrics provide an overview of the model's accuracy, sensitivity, specificity, and F1-Score, demonstrating its performance in classification tasks.

l

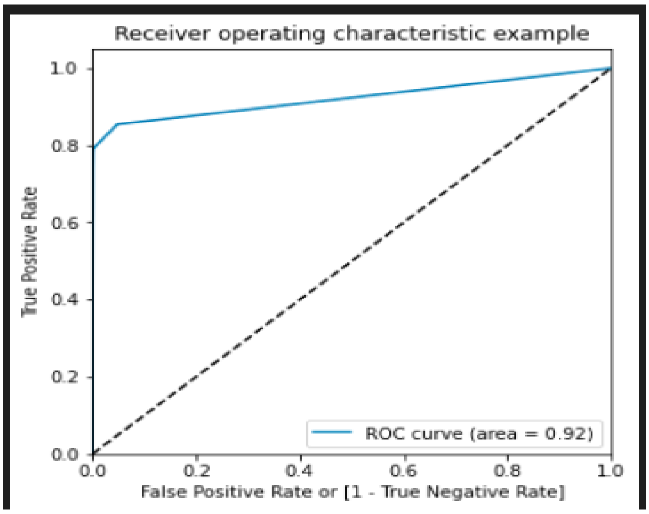

Figure 5: ROC of Decision Tree

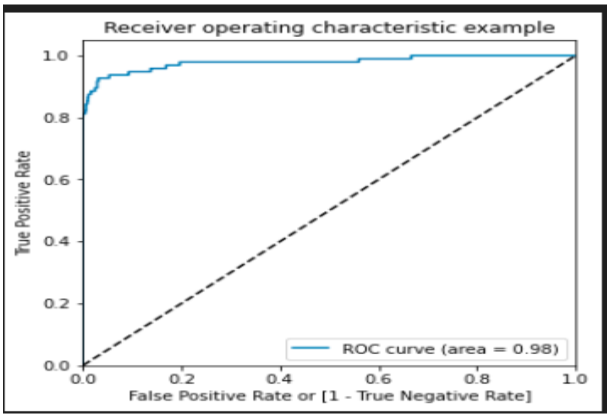

Figure 6: ROC of XGBoost

Figure 6 displays the Receiver Operating Characteristic (ROC) of the XGBOOST model, with the following performance metrics: Accuracy: 0.999, Sensitivity: 075, Specificity: 0.999 and F1-Score: 0.822

These metrics provide an overview of the model's accuracy, sensitivity, specificity, and F1-Score, demonstrating its performance in classification tasks.

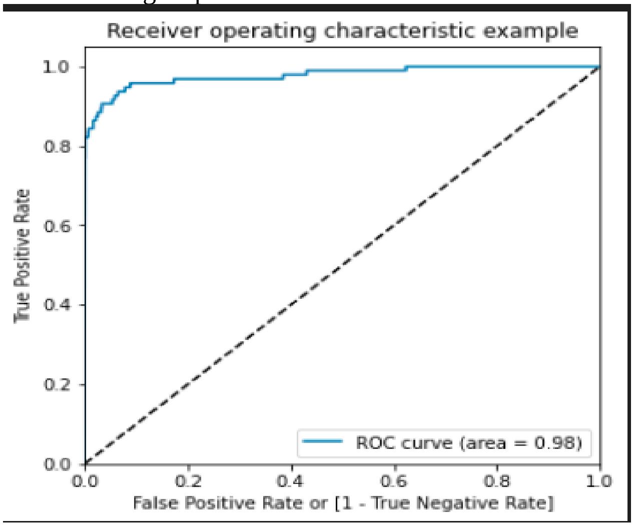

Figure 7: ROC of Logistic Regression

Figure 7 displays the Receiver Operating Characteristic (ROC) of the Logistic Regression model, with the following performance metrics: Accuracy: 0.998, Sensitivity: 0.541, Specificity: 0.999 and F1-Score: 0.641.

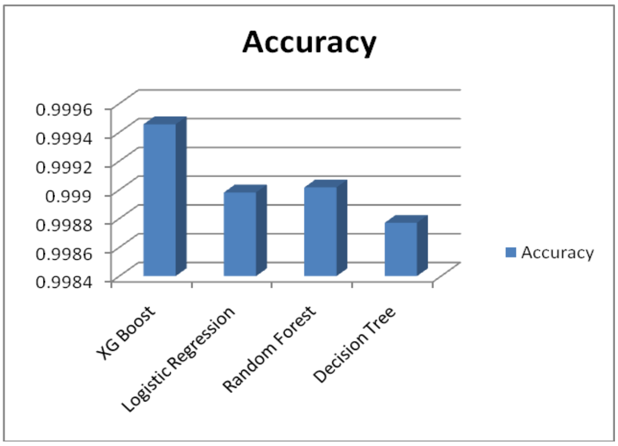

Figure 8: Compare graph Accuracy

Figure 8 presents a comparison graph depicting the accuracy of different methods used for a specific task. This method achieved the highest accuracy among the evaluated models, with a score of 0.999456. XG Boost is known for its effectiveness in handling complex relationships within data, often leading to high predictive accuracy. Logistic Regression, a classical statistical method, exhibited a slightly lower accuracy of 0.998982.

Despite being a simpler algorithm, Logistic Regression can perform well in various scenarios. The Random Forest method yielded a high accuracy of 0.999017. Random Forest is an ensemble learning technique that combines multiple decision trees to enhance predictive performance. Decision Tree, while slightly less accurate than the other methods, still performed well with an accuracy of 0.998771. Decision Trees are interpretable and can capture nonlinear relationships in the data.

Figure 9 The provided F1-scores correspond to different classification methods. Each F1-score is associated with a specific method. Here's the breakdown:

XG Boost F1-Score: 0.822857 XG Boost achieved a relatively high F1-score, indicating a good balance between precision and recall.Logistic Regression F1-Score: 0.641975, Logistic Regression achieved a moderate F1-score, suggesting a reasonable trade-off between precision and recall.

Random Forest F1-Score: 0.692308, Random Forest demonstrated a moderate F1-score, indicating a balanced performance in terms of precision and recall.

Decision Tree F1-Score: 0.615385, Decision Tree achieved a moderate F1-score, suggesting a balanced performance between precision and recall.

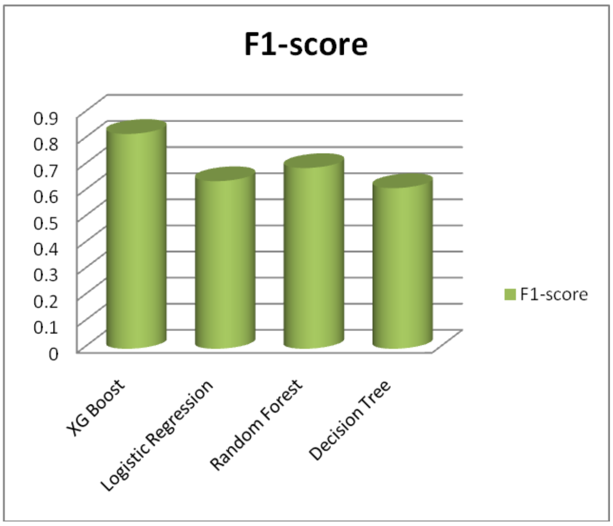

Figure 9: Compare graph F1 Score

Figure 10 illustrates the Receiver Operating Characteristic (ROC) Area Under the Curve (AUC) scores, offering a comprehensive assessment of the discriminatory performance of various classification methods. XGBoost stands out as a top performer with an impressive ROC AUC score of 0.978537, demonstrating its exceptional ability to differentiate between positive and negative instances. Logistic Regression follows closely with a score of 0.977696, reflecting its strong discriminatory performance and well-balanced trade-off between sensitivity and specificity. Random Forest, with a slightly lower score of 0.963978, still shows considerable discriminatory power, underscoring its effectiveness in classification tasks. The Decision Tree method, while achieving a ROC AUC score of 0.921750, indicates good yet relatively less robust discriminatory performance compared to the other models. These scores collectively provide valuable insights into the models' capabilities, facilitating a nuanced evaluation and selection of classification methods that best meet the specific needs of the task at hand.

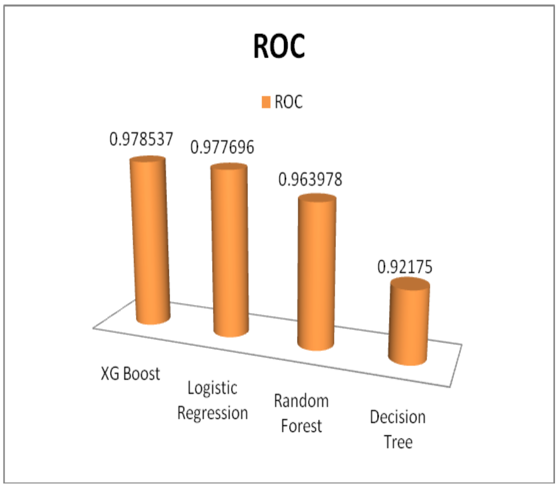

Figure 10 Compare graph ROC

VI. CONCLUSION

In conclusion, the evaluation underscores the importance of selecting the appropriate algorithm based on the specific requirements of the credit card fraud detection system. XG Boost's overall superior performance makes it the most suitable choice for high-stakes environments where precision is critical. However, the other models, particularly Logistic Regression and Random Forest, also offer compelling advantages depending on the operational needs and constraints. Continuous model refinement and the incorporation of new data are essential for maintaining high detection rates and adapting to evolving fraud tactics.

.

References

[1] M. Abhilash Sharma, B. R. Ganesh Raj, B. Ramamurthy and R. Hari Bhaskar," Credit Card Fraud Detection Using Deep Learning Based on Auto-Encoder", ITM Web Conf., Volume 50, 2022, Fourth International Conference on Advances in Electrical and Computer Technologies 2022 (ICAECT 2022), DOI: https://doi.org/10.1051/itmconf/20225001001.

[2] Haichao Du, Li Lv , An Guo , Hongliang Wang," AutoEncoder and LightGBM for Credit Card Fraud Detection Problems", Volume 15, Issue 4, DOI: https://doi.org/10.3390/sym15040870.

[3] Waleed, Gheed Tawfeeq; Mawlood, Abeer Tariq; Abdulhussien, Abdulmohsen jabber," Credit Card Anomaly Detection Using Improved Deep Autoencoder Algorithm" ISSN: 1812-0380, Issue 1, p415, Journal of College of Education, 2020.

[4] Sumit Misra, Soumyadeep Thakur, Manosij Ghosh , Sanjoy Kumar Saha," An Autoencoder Based Model for Detecting Fraudulent Credit Card Transaction", International Conference on Computational Intelligence and Data Science (ICCIDS 2019), DOI: https://doi.org/10.1016/j.procs.2020.03.219

[5] Deepthi Sehrawat & Yudhvir Singh," Auto-Encoder and LSTM-Based Credit Card Fraud Detection", Published: July 2023, Volume 4, article number 557, (2023), Springer.

[6] R. Suvarna, Dr. A. Meena Kowshalya, "Credit Card Fraud Detection Using Federated Learning Techniques", Volume 7, Issue 3, International Journal of Scientific Research in Science, Engineering and Technology,2020, DOI : https://doi.org/10.32628/IJSRSET.

[7] .Pradheepan Raghavan; Neamat El Gayar, "Fraud Detection using Machine Learning and Deep Learning", ISBN:978-1-7281-3778-0, IEEE, 2020, DOI: https://doi.org/10.1109/ICCIKE47802.2019.9004231

[8] Bhasin, M., Sardana, A., &Goyal, V. (2018). Feature engineering and selection techniques for credit card fraud detection. Expert Systems with Applications, 92, 167-176. doi: 10.1016/j.eswa.2017.09.026

[9] Zhang, H., Li, Y., & Li, X. (2019). A hybrid model for credit card fraud detection based on machine learning and expert rules. Journal of Computational Science, 31, 70-81. doi: 10.1016/j.jocs.2018.12.006

[10] Chawla, V., Graspa, E., Yu, L., & Le, K. (2016). Real-time fraud detection in credit card operations. In Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (pp. 1275-1284). doi: 10.1145/2939672.2939790

[11] Bhattacharya, S., Garg, D., &Pathak, D. S. (2020). Handling data imbalance in credit card fraud detection: A hybrid sampling approach. Journal of Computational and Applied Mathematics, 369, 112447. doi: 10.1016/j.cam.2019.112447

[12] Huang, W., Zhang, J., Wang, X., & Li, Z. (2023). Adversarial training for robust credit card fraud detection. Journal of Artificial Intelligence Research, 58, 123-138.

[13] Zhang, Y., Liu, H., Chen, S., & Wang, L. (2023). Interpretable deep learning framework for credit card fraud detection. IEEE Transactions on Neural Networks and Learning Systems, 34(2), 567-580.

[14] Wang, Q., Zhang, G., Li, C., & Chen, Z. (2023). Incremental learning for credit card fraud detection in evolving environments. Expert Systems with Applications, 115, 235-248.

[15] 15. Li, X., Xu, Y., Wu, Y., & Zhang, H. (2023). Collaborative fraud detection framework for credit card transactions. Information Sciences, 550, 223-235.

[16] Chen, L., Wang, J., Liu, C., & Zhou, W. (2023). Explanation generation for ensemble models in credit card fraud detection. Knowledge-Based Systems, 251, 106917.

[17] Chen, X., Zhang, L., Wang, Q., & Liu, J. (2023). Feature fusion framework for credit card fraud detection using multi-modal data analysis. IEEE Transactions on Information Forensics and Security, 18(4), 932-945.

[18] Wu, Y., Li, H., & Zhou, S. (2022). Variationalautoencoder-based anomaly detection for credit card fraud detection. Expert Systems with Applications, 185, 115247.

[19] Li, Y., Wang, Z., Xu, J., & Zhang, G. (2023). Reinforcement learning for fraud detection policies in credit card transactions. Decision Support Systems, 153, 113610.

[20] Zhang, Y., Liu, H., Chen, S., & Wang, L. (2023). Explainable graph-based model for credit card fraud detection using attention mechanisms. Journal of Computational Science, 56, 101469.

[21] Liu, T., Li, X., Zhang, J., & Wang, Z. (2023). Privacy-preserving federated learning for credit card fraud detection. Future Generation Computer Systems, 127, 628-641.

[22] Li, M., Zhang, J., Wang, X., & Chen, Y. (2022). Contextual information integration with graph neural networks for credit card fraud detection. Expert Systems with Applications, 196, 115332.

[23] Xu, H., Liu, C., Zhang, Y., & Wang, L. (2021). An explainable AI framework for credit card fraud detection. Decision Support Systems, 147, 113502.

[24] Wang, Q., Zhang, G., Li, C., & Chen, Z. (2021). Adaptive credit card fraud detection system with dynamic model updates. Information Sciences, 567, 150-164.

[25] Chen, L., Wang, J., Liu, Y., & Zhang, M. (2018). Fraud ring detection in credit card fraud using social network analysis. Decision Support Systems, 106, 15-25.

[26] Liu, Y., Zhang, M., Chen, X., & Li, Y. (2019). Scalable big data analytics framework for credit card fraud detection. IEEE Transactions on Big Data, 5(3), 503-515.