An Improved Fraud Detection System Using the LDX Ensemble Machine Learning Technique

M. Mansab[1], M. F. Mushtaq[2], T. B. Tariq[3], U. Akram[4]

[1,2,3,4] *Department of Artificial Intelligence, The Islamia University of Bahawalpur, 63100, Bahawalpur, Pakistan*

[2] faheem.mushtaq@iub.edu.pk

Abstract- Credit cards are widely used for fast and convenient cashless transactions. However, the incidence of fraud is increasing due to usage growth. Detecting fraudulent credit card transactions presents a significant challenge for the financial industry. One of the main obstacles is the imbalance between fraudulent and legitimate transactions, as fraud cases are relatively rare, making it difficult for models to identify them accurately. This research proposes a trustworthy fraud detection system using the LDX ensemble machine learning technique based on Logistics Regression, Decision Tree, and XGBoost models. For that purpose, the credit card fraud dataset from Kaggle was examined. The SMOTE and Weight of Evidence encoding approach was used to preprocess the data to improve feature representations and change categorical variables. After that downsampling methods were used to rectify the class imbalance and ensure a balanced dataset. The following machine learning models were used and assessed: Logistic Regression (LR), Random Forest, Gaussian Naïve Base, Decision Tree (DT), Support Vector Machine (SVM). Hyperparameter tuning was applied to each model to enhance performance. The ensemble LDX model's maximum accuracy is roughly 95%, and the outcome is assessed using metrics like precision, recall, and F1 score. This AI-driven approach demonstrates an effective solution for detecting credit card fraud, contributing to enhanced cybersecurity in economic transactions and minimizing business financial risks.

Keywords- Artificial Intelligence, Ensemble Learning, Credit Card Fraud Detection, Cybersecurity, AI-driven Solutions.

I. INTRODUCTION

Credit cards have become a popular payment option in recent years, replacing cash in many daily transactions. Credit Cards provide convenience, flexibility and a secure way for users to manage their money [1]. The rapid progress of digital technology has dramatically changed the way financial transactions are carried out. Today, credit cards have emerged as one of the most preferred techniques for cashless transactions [2]. Their simplicity, quickness, and general acceptance make them the favored alternative for individuals and businesses around the world. However, the growing use of credit cards has increased fraudulent activity, creating significant challenges for the financial industry. Fraudulent credit card transactions not only cause significant economic losses but also undermine customer trust and confidence [3]. This critical issue requires the development of robust and effective fraud detection technologies. The growing popularity of online facilities is all the more reason for credit card use [2]. Digital transactions have become that much more important to businesses and institutions as technology seeps into every corner of society. A large part of hotel reservations, online shopping, and subscription services are paid using credit cards. They generally increase convenience, but users are exposed to such risks as credit card scam.

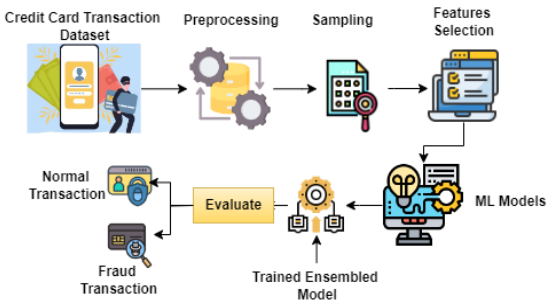

Fig. 1. The Abstract Level Model of Credit Card Fraud Detection System

Fraud detection is a bigger area of study in cybersecurity. Detecting fraudulent behaviors in financial transactions is hard, given several factors. One of such major points is the imbalance of genuine and fraudulent transactions [4]. Fraud cases comprise a small percentage of total credit

card transactions thus, it is hard for detection systems to distinguish genuine activity from questionable ones. In addition, fraudsters are constantly changing and developing new ways to exploit vulnerabilities, so detection systems must constantly upgrade and improve [5].

A fraud detection system's main goal is to accurately identify fraudulent transactions while keeping false positive rates to a minimum. False positives are those instances in which a transaction legitimately performed is wrongfully identified as fraudulent and may obstruct consumers or financial institutions [6]. In contrast, failure to detect genuine fraudulent transactions can lead to considerable financial loss and damage to reputation. Therefore, a perfect fraud detection system should weigh between sensitivity and specificity while maintaining a high degree of accuracy and reliability. Traditional ways, for example, rule-based systems, apply existing templates to recognize suspicious transactions [7]. Nonetheless, those algorithms are generally ineffective in detecting novel schemes that look like legitimate behaviors. As fraudulent ones become closer in appearance to legitimate transactions, the detection becomes all the more difficult.

Machine learning has become a potent instrument for tackling fraud detection issues. By analyzing historical transaction data, machine learning models can pick out patterns and anomalies that indicate fraud [5]. Such models have the capability to learn and adapt over time, making them suitable for dynamic and evolving fraud situations. However, elements like feature engineering, model selection, and data preparation are critical to the effectiveness of machine learning-based fraud detection systems [8].

The research is dedicated to developing an improved fraud detection system using the ensemble machine learning technique LDX by combining Logistic Regression [9], Decision Tree [10], and XGBoost models [4]. Ensemble learning methods leverage the strengths of numerous models to outperform any single model on its own. This study's LDX model seeks to increase the accuracy and robustness of fraud detection systems in comparison to existing systems. In this research, the authors used a Kaggle dataset of credit card transactions composed of authentic and fraudulent transactions. Multiple preprocessing steps were applied for data quality improvement and class distribution, i.e. changing all categorical variables to numerical variables through the Weight of Evidence encoding method [11]. The downsampling method addressed class imbalance and provided each machine-learning model with relatively balanced training data. Several machine learning algorithms were implemented and evaluated, such as Gaussian Naïve Bayes, XGBoost, logistic regression, support vector machines, decision trees, and random forests [12]. Hyperparameter tuning was used to optimize the algorithms' performance. The evaluation metrics used to assess the models' ability to accurately distinguish fraudulent transactions included F1 score precision, recall, and precision. The LDX ensemble model achieved better results, with 95% accuracy as the maximum. The LDX model gathers intricate patterns and associations in the data thanks to the interplay of benefits from Logistic Regression, Decision Tree and XGBoost as it strives for accuracy in detecting fraud. The findings of the study have significant consequences for enhancing cybersecurity in financial transactions, lowering financial risk to organizations, and advancing the overall consumer experience. This study provides a strong solution to the problem of credit card fraud detection by addressing important challenges of class imbalance and using current machine learning methodologies. This research contributes to the field of fraud detection through the following:

- To propose a reliable and efficient machine learning-based fraud detection system using the LDX ensemble technique.
- To develop an innovative approach by addressing class imbalance and leveraging advanced techniques such as Weight of Evidence (WoE) encoding and ensemble learning.
- To implement and estimate multiple machine learning models, demonstrating the effectiveness of the LDX ensemble model in achieving high accuracy and reliability.
- The performance evaluation is conducted using the evaluation parameters such as accuracy, precision, recall, f1-score.

The lasting sections of this study are organized as follows: Section 2 presents a detailed analysis of related studies on the subject of fraud detection, emphasizing the strengths and margins of current approaches. Section 3 explains the approach for this study, which includes data pretreatment, model selection, and evaluation measures. Section 4 summarizes the findings and analysis of the proposed LDX ensemble model, comparing it to existing machine learning models. Finally, Section 5 concludes this study and discusses prospective areas for future research.

II. Related Work

The employment of ensemble machine-learning models to detect fraudulent transactions has been the subject of numerous investigations. To improve fraud detection systems' precision and dependability, these studies have looked into a variety of ensemble procedures and data-balancing techniques. Additionally, several artificial

intelligence and neural network-based methods are being developed and used to better anticipate credit card fraud. The distribution of the datasets used to identify fraud is quite uneven. Methods for under-sampling and over-sampling are therefore being developed to get relatively balanced data to get around this problem. Data mining techniques are also being used to construct a more efficient fraud detection system [12]. Nevertheless, the article did not fully analyze the computational complexity and resource requirements of the suggested approach.

This study investigates the use of machine learning methods to detect credit card fraud in highly imbalanced datasets. It reveals that unsupervised methods handle skewness effectively, achieving better classification results. However, the approach depends on the availability of quality datasets [13]. Furthermore, a novel feature set is proposed that examines customer purchasing patterns [14]. When detecting credit card fraud, the attributes are helpful. However, this model can take too long to classify a new transaction by calculating the characteristics.

Another research that employed six classifiers with a dataset both earlier and later in the pre-processing stage, demonstrates a notable development when the dataset is under-sampled [15]. Specifically, 492 of the 284,807 transactions in the dataset used are fraudulent transactions. After using the random under-sampling technique, they changed the ratio to 1:1, showing that the number of fraudulent transactions is equal to the number of valid transactions. Using both datasets, they assessed the classifiers' precision and recall and found that using the undersampled dataset significantly improved the precision of every classifier. However, applying random under-sampling can result in the loss of crucial information from legitimate transactions, which may reduce the model's capability to perform effectively on real-world, imbalanced datasets.

Table-1 Performance Comparison Proposed LDX Model

Ref.	Years	Methods	Dataset	Acc.
[16]	2020	Random Forest, Adaboost	European credit card company	89
[17]	2020	Random Forest Naïve Baiyes Logistic Regression, SVM, KNN, DT	European credit card company	91
[18]	2021	SVM,KNN,ANN	European bank	91
[19]	2022	AllKNN-CatBoost, GBM, DT	European cardholders	93
[20]	2024	SVM, KNN, RF	European credit card holders	94
[21]	2024	RF,LR,DT,KNN, NB	European cardholder	94.5

Using a variety of datasets, such as credit cards, NSL-KDD, and UNSW, an ensemble stacking approach was suggested for detecting cyberattacks in the Internet of Things (IoT) and shown that their stacked ensemble classifier beat each of the ensemble classifiers [22]. The inventive model attained an astounding 93.49% accuracy rate, which augurs well for counteracting credit card fraud and cyber-attacks. A new transaction's pattern was compared to pre-existing patterns using a matching algorithm to determine whether it is more likely to fit the fraud pattern or the legal pattern created for each customer [23]. To uncover both trends, each customer's transactions had to be dissected. Then, the fraud and lawful transactions for each customer had to be separated and used as input to the Apriori algorithm for each customer's set of fraud and legal transactions. For every client transaction, the largest frequent itemset was selected for both legal and fraudulent patterns from the set of frequent itemsets generated by the apriori algorithm. Since each client has both fraud and lawful patterns, any new transaction from any client will be compared with both patterns, making it simpler to determine if the transaction is legitimate or fraudulent. However, separate fraud and legal patterns must be created and maintained for every customer, which takes a lot of computational resources and could not scale well for big datasets with many customers.

It has been found that the skewness of the available datasets, which are often unequal, affects the performance of all machine learning models. The imbalanced datasets must be swapped out for balanced ones in order to resolve this issue. There are two primary approaches to do this: the intrinsic approach and the network-based approach. While the network-based features approach makes use of the user and card merchant network, the intrinsic feature methodology looks for patterns in the customer's activity. These methods could greatly enhance some models' performance as they operate on more balanced datasets [24]. Moreover, the intrinsic feature approach could find it challenging to identify intricate, non-linear behavioral patterns, whereas the network-based approach depends on the availability of thorough user and merchant network data, which isn't always available.

The values of the parameters are chosen by cross-validation, applying Grid search in the proposed model, which uses a Support Vector Machine (SVM) with RBF kernel task. The RBF function is the most adaptable function to use with SVM applications. A traditional feature that is pertinent to customer performance including Transaction Amount, Date, Time, Frequency of card usage, Place, Customer ID, and Usual amount of transactions per month, were chosen for training because the amount of features affects the SVM's performance and produces good results when a small number of features are chosen. These features are converted into numerical data and are later used. The accuracy of this model was over 80%,

based on the results [25]. However, the SVM's performance with an RBF kernel is largely dependent on meticulous feature selection and parameter adjustment, which can be laborious and may not translate well to datasets with different properties.

III. Research Methodology

By using past data on equally fraudulent and non-fraudulent transactions, machine learning may identify fraud. Machine learning algorithms are excellent at spotting irregularities in transactions before they become uncontrollable problems. Choosing a dataset with records of together authentic and fraudulent transactions is the first step in the procedure. Predictive outcomes built based on a number of evidence-set features will possibly give inaccurate results due to unordered, rare, misplaced, or duplicate examples in the dataset. Specific sampling methodologies that can be useful are for addressing data imbalance. The sorted and sampled dataset is cutoff into training and test samples. The training sample is used to create an updated version of machine learning algorithms, and evaluation of the trained models is conducted on both samples. When prediction results are obtained referring to certain evaluation metrics for example accuracy, precision, recall, confusion matrix values-performance analysis and comparison are made. This methodological framework used in this study depended upon an experimental design developed and executed to realize a real-world experiment for credit card fraud detection shown in Fig.2.

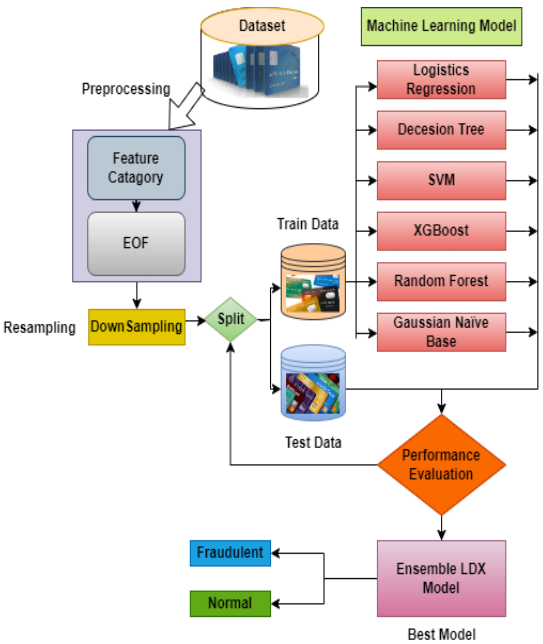

Fig. 2. The Architecture of the Proposed Credit Card Fraud Detection Model

A. Dataset Description

The Credit Card Transactions Fraud Detection Dataset is openly accessible on Kaggle. It contains 556,000 credit card transaction simulation entries in the test file and 1.3 million records in the train dataset file. It was carried out from January 1, 2019, until December 31, 2020. It includes transaction data from 800 distinct businesses and 1,000 credit cardholders that made transactions. The 46 columns in the dataset capture a range of characteristics associated with both legitimate and fraudulent transactions. Of the transactions, 45% are male and 55% are female shown as in Fig. 3.

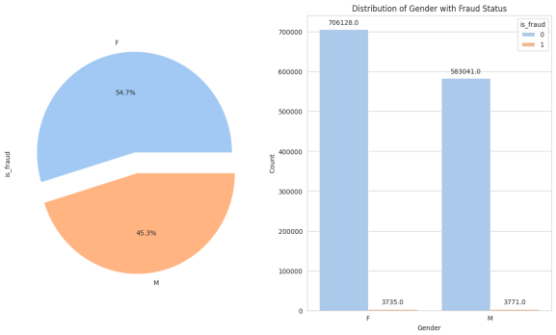

Fig. 3. The Distribution of Gender with Fraud Status in Dataset

B. Dataset Preprocessing

Following dataset selection, the first step is preprocessing the data to get it ready for model training and testing. The following methods of processing information were used in this step. Locating any null values and adding or deleting them. Making the "Amount" column standardized to facilitate analysis. Since, the "Time" column was not making a significant contribution to training or evaluation, it was removed from the dataset. The dataset is examining and eliminating duplicate items. There were no null or missing values in the dataset that was used in the method. Machine learning uses WOEEncoder [13], a kind of categorical encoding approach, especially when dealing with categorical data in predictive modeling tasks like classification. This well-known encoding method is applied to fraud detection and credit rating. WOE encoding provides more meaningful representations for categorical variables in some modeling contexts, particularly those where the predictive power of categorical variables is critical, whereas label encoding merely assigns numerical labels to categories. WOE encoding computes numerical values based on the relationship between each category and the target variable [14]. Please take note that deliberate measures to lessen the impact of outliers were excluded. In order to improve the model's capacity to manage the dynamic and distinct character of credit card transactions, this study avoided the use of explicit outlier-handling techniques. This

method improved the model's flexibility and suitability for practical situations.

C. Data Sampling

This study uses the resampling techniques to rectify the skewed dataset. In particular, employed the downsampling strategy, which entails lowering the majority class's sample size to equal the minority classes [15]. This method improves the model's ability to discover patterns in the minority class and helps limit its propensity towards the majority class. SMOTE is a numerical method that can be used to proportionately increase the number of minority class instances in the dataset [16]. The component produced new instances from previously existing minority cases. The fraud class was then oversampled for SMOTE so that it had an equal amount of entries with the legitimate class and also trained the models as efficiently as possible. After the component was applied to both classes, they were combined into one dataset, similar to under-sampling.

D. Algorithms for Fraud Detection

The machine learning algorithms used to trains a computer to carry out a particular activity without the need for explicit programming instructions. These models includes Naïve Bayes, Decision trees, XGboost, Logistic Regression, Random Forest, and Gaussian Naïve Bayes have demonstrated their effectiveness in obtaining high scores and are frequently engaged in the detection of credit card fraud.

With the aid of the Random Forest Classifier (RFC), the decision tree is a tool that can handle both classification and regression problems with similar effectiveness. By essentially dividing the feature space recursively based on informative traits, it creates a tree-like structure that facilitates decision-making. Its robustness and interpretability make it a popular choice in many applications. It decreases overfitting and produces a more accurate and dependable model by combining the outcomes of several trees' predictions of the target variable. RFC is useful for tasks like feature selection, regression, and classification in a variety of industries, including marketing, banking, and healthcare. The Gradient Boosting Classifier (GBC), another ensemble learning method, iteratively creates a sequence of decision trees, each of which is trained to correct the mistakes of the one before it. The GBC creates a very successful prediction method by utilizing the benefits of each tree. GBC is frequently utilized in applications like customer churn prediction, click-through rate prediction, and web search ranking due to its excellent accuracy results. XGBoost is a gradient-boosting technique optimized for speed and performance [17]. To prevent overfitting and improve generalization, it uses a regularization term in the objective function. Personalized recommendation systems, time series forecasting, and credit risk modeling are just a few of the many uses for XGBoosts great adaptability. Several machine learning classifier methods were used in this experiment to detect credit card fraud and the best parameters to improve model performance were found.

E. Ensemble LDX Model

Ensemble approaches combine several models to produce a model that is more reliable and accurate than a single model. Machine learning models known as voting classifiers predict an output class by calculating the probability that the selected class will be the result. A sizable ensemble of models is used to teach them. The output class is merely projected based on the class with the highest votes once the results of all the classifiers that have been submitted to the voting classifier have been added together. This study creates a single model that trains on three different models and guesses output based on their combined popularity of soft voting for each output class, rather than creating distinct, specialized models and assessing their correctness as shown in Fig. 4.

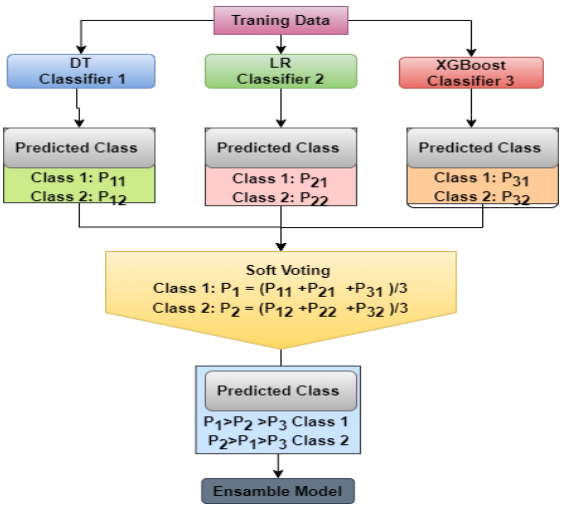

Fig. 4. The Architecture of the Proposed Ensemble LDX Model

F. Model Evaluation Metrics

This study use a variety of performance criteria to evaluate the effectiveness of the suggested approach, guaranteeing a thorough analysis. These measurements include confusion matrix, Area Under the Curve (AUC) score, F1-score, recall, accuracy, and precision.

A number of metrics were used to assess the classifier's performance, includes accuracy, which may be defined as the ratio of all input samples to all accurate predictions [18]. The classification rate is another name for it.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} * 100 \quad (1)$$

By taking the sum of the true positives and false positives and dividing it by the total number of true positives, the accuracy is determined. The number of positive predictions divided by the total number of expected positive class values is one way to describe it [19].

$$\Pr ecision = \frac{TP}{TP+FP} * 100 \quad (2)$$

Recall is calculated by dividing the total number of false negatives by the total amount of true positives. It can be expressed as the ratio of the amount of positive class values in the test data to the number of positive forecasts [20]. It is sometimes mentioned to as the True Positive Rate or Sensitivity.

$$\Re call = \frac{TP}{TP+FN} * 100 \quad (3)$$

Precision incursions a balance between recall and F1-Score precision [19]. It can be computed in this way:

$$F1-score = 2 * \frac{\Pr ecision * \Re call}{\Pr ecision + \Re call} \quad (4)$$

IV. Result and Discussion

In order to detect fraudulent transactions, this study introduces a novel integrated ensemble machine learning model. This section provides a brief overview of the experimental design, performance measures, preliminary analysis of the results, and a discussion that follows.

G. Machine Learning Algorithms

Fraud detection is a very critical task with machine learning models being able to identify suspicious transactions. Different models were tested, each with varying combinations of strengths and weaknesses. For this purpose, the logistic regression model was selected with C=0.0001, undertaking strong regularization to prevent overfitting. Though it sometimes leads to underfitting, which in turn affects the performance, it could only train for a maximum of 5 iterations with max_iter=5. Logistic Regression scored moderate accuracy at 73%, with 79% precision and 73% recall, implying it could classify a good number of fraudulent cases but also missed some classes due to low recall.

Support Vector Machine scored rather higher on this task, yielding an overall accuracy of 90.5%, of which 88% precision and 91% recall. It happens to be one of the most appreciated models in fraud detection. For the Linear SVC, set C=100 which regulates the compromise between decreasing classification mistakes and optimizing the margin., by controlling regularization. A larger value of C corresponds to less regularization and thus more flexibility in the model. It also had max_iter=600, which allowed the model to converge in around 600 iterations, and random_state=42 ensured consistent outputs.

Table-II Performance Comparison Proposed LDX Model

Models	Accuracy	Precision	Recall	F1-Score
Decision Tree	89.5	89	90	89
Logistics Regression	73	79	73	76
Random Forest	88.5	87	89	88
XGBoost	92	91	92	91
Gaussian Nave Bayes	54	82	54	63
SVM	90.5	88	91	88
Ensemble LDX	95.5	96	95	95

The Random Forest gave a slight edge on accuracy, reaching 88.5%. A better balance of precision 87% and recall (89%) made it a more stable choice. However, XGBoost surpassed most of the models with an accuracy of 92% and also had 91% precision and 92% recall. Thus, XGBoost proves to be a powerful algorithm for detecting fraud. On the other hand, the Gaussian Naïve Bayes fared poorly, with a mere accuracy of 54%, despite a high score on precision, of 82%. With a recall at 54%, the model failed miserably at identifying a large number of fraud cases. The Decision Tree Classifier achieved a balanced F1-score of 89% and demonstrated good performance with an accuracy of 89.5%. Nevertheless, decision trees may be more likely to overfit, which reduces its dependability for unknown data.

The LDX model, a hybrid of XGBoost, SVM, and Decision Tree, gave the highest accuracy 95.5% and indeed achieved precision and recall of 96% and 95% respectively. A good compromise of detecting fraudulent cases while keeping false positives and false negatives at a minimum. The ensemble LDX approach proved very effective because it took leverage from strengths of multiple models, and performed far superior to each of the available classifiers as shown in Fig. 5.

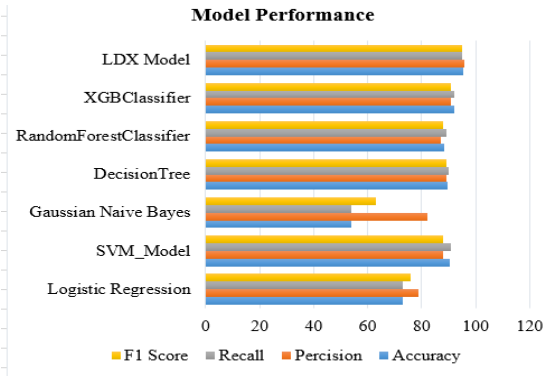

Fig. 5. Models Performance Measurement Graph of Different Evaluation Matrices

H. Proposed Ensemble LDX Model

The suggested LDX model kinds use of a soft voting ensemble model in which linearSVC, logistic regression, and decision tree classifier are put to use to enhance fraud detection performance. In this approach, all individual models produce estimates of the probability, each contributing further according to their estimate in obtaining the final class label prediction of more balanced and accurate classifications. With C=100, the LinearSVC model incorporates sufficient relaxation in fitting the data. For sufficient, max_iter=600 guarantees enough iterations to allow convergence. The logistic regression models C is set to 0.0001, driving down overfitting with strong regularization; max_iter=5 means it has only been trained for a few passes. Using the max_depth=1, the decision tree classifier is a really simple model, catching only basic patterns and avoiding complexity.

On integrating these models, along with XGBoost, SVM, and decision tree, the LDX Model attained the highest accuracy of 95.5%. It also gave a precision of 96% and a recall of 95%, aptly identifying fraud cases while minimizing errors occurring as shown in Fig. 6. Due to unifying different classifiers, the ensemble method enhances overall performance making it more robust than its individual models. It has been duly demonstrated to be effective for fraud detection purposes by standardizing accuracy, precision, and recall for reliable results.

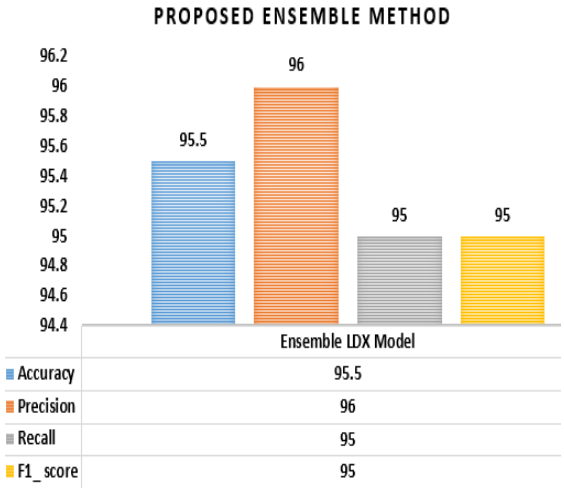

Fig. 6. Ensemble LDX Models Performance Measurement Evaluation Matrices

I. Performance Comparison Proposed LDX Model

The learning vector quantization LDX model outperformed the others in fraud detection, with a 95.5% accuracy, 96% precision, and 95% recall. This was followed by the XGBoost Classifier, which reached up to 92% accuracy with 91% precision and 92% recall. The SVM Model also had good performance with 90.5% accuracy but slightly lower precision 88% and recall 91%.

The Decision Tree and Random Forest classifiers were quite like with 89.5% and 88.5% accuracy, respectively, and fairly balanced precision and recall values hovered around 87-90%. However, Logistic Regression and Gaussian Naïve Bayes lagged far behind with just 73% accuracy and 54%, respectively. Although Gaussian Naïve Bayes was operating on high precision at 82%, low recall of 54% made it completely ineffective for fraud detection. The superior nature of LDX Model can be qualified to its ensemble learning capability and an amalgam of strengths seen in XGBoost, SVM, and Decision Tree, leading to great accuracy, excellent fraud detection, and reduced false positive and negative detection, when put in comparison with individual models.

V. CONCLUSIONS

This LDX ensemble model decreases detection difficulties in credit card fraud using XGBoost, Decision Trees, and Logistic Regression. Majorly one of the problems in fraud detection is dealing with the imbalance between the number of fraudulent and legitimate transactions that negatively impact the performance of a model in its overall process. The imbalanced sample is solved with the synthetic minority over-sampling technique SMOTE and weight of evidence encoding for a good representation of the data in comparisons between credit card transactions. Different algorithms utilized and tested for their performance are Gaussian Naïve Bayes, logistic regression, SVM, decision trees, random forests, and Boost according to F1 score, precision, and recall. The LDX model correctly identifies 95% of fraudulent transactions while decreasing false-positive and false-negative predictions. The paper emphasizes ensemble learning as an effective way to run fraud detection, whose common aim remains security maximization over financial transactions and risk mitigation for businesses.

This research can be further extended by employing the more complicated ensemble learning strategies using deep learning models with recurrent neural networks and transformer-based architectures towards better feature extraction. In addition, systems are developed for real-time detection of fraud, which must be incorporated in banks and other financial institutions for monitoring transactions immediately. Finally, adaptive learning techniques could be put forward, where the model continuously updates itself based on emerging fraud patterns.

REFERENCES

[1] S. Mittal and S. Tyagi, "Performance evaluation of machine learning algorithms for credit card fraud detection," in *Proc. 2019 9th Int. Conf. Cloud Comput., Data Sci. & Eng. (Confluence)*, 2019, pp. 288–293.

[2] W. Hussain, M. Shamsi, M. M. Fraz, M. K. Rafique, A. Iqbal, and S. Aslam, "Ensemble genetic and CNN model-based image classification by enhancing hyperparameter tuning," *Scientific Reports*, vol. 15, no. 1, p. 1003, 2025.

[3] A. Roy, J. Sun, R. Mahoney, L. Alonzi, S. Adams, and P. Beling, "Deep learning detecting fraud in credit card transactions," in *Proc. 2018 Syst. Inf. Eng. Des. Symp. (SIEDS)*, 2018, pp. 129–134.

[4] R. Soleymanzadeh, "Cyberattack and fraud detection using ensemble stacking," *AI*, vol. 3, no. 1, pp. 22–36, 2022.

[5] A. Karim, A. Akbar, M. R. F. Mahmod, A. M. Kibria, and M. A. Rahman, "Anticipating impression using textual sentiment based on ensemble LRD model," *Expert Systems with Applications*, vol. 263, p. 125717, 2025.

[6] S. Dhankhad, E. Mohammed, and B. Far, "Supervised machine learning algorithms for credit card fraudulent transaction detection: A comparative study," in *Proc. 2018 IEEE Int. Conf. Inf. Reuse Integr. (IRI)*, 2018, pp. 122–129.

[7] Z. Guo, Y. Chen, L. Wang, F. Xiao, and Z. Lin, "Detecting advanced persistent threats via causal graph neural network," in *Proc. 4th Int. Conf. Netw. Commun. Inf. Secur. (ICNCIS 2024)*, 2025, pp. 89–95.

[8] A. Rawal, K. Naik, V. Gupta, M. Kumar, and P. Arora, "Causality for trustworthy artificial intelligence: Status, challenges and perspectives," *ACM Comput. Surv.*, 2024.

[9] J. Gaspar, J. O. Farias, H. S. Oliveira, M. E. Fernandes, and D. R. da Silva, "Smart substation communications and cybersecurity: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, 2023.

[10] M. A. Talukder, M. Khalid, and M. A. Uddin, "An integrated multistage ensemble machine learning model for fraudulent transaction detection," *J. Big Data*, vol. 11, no. 1, p. 168, 2024.

[11] R. Chhabra, S. Goswami, and R. K. Ranjan, "A voting ensemble machine learning based credit card fraud detection using highly imbalance data," *Multimedia Tools Appl.*, vol. 83, no. 18, pp. 54729–54753, 2024.

[12] D. H. de Souza and C. J. Bordin Jr., "Ensemble and mixed learning techniques for credit card fraud detection," *arXiv preprint arXiv:2112.02627*, 2021.

[13] A. Menshchikov, K. Ivanov, A. Prokhorov, and D. Pavlov, "Comparative analysis of machine learning methods application for financial fraud detection," in *Proc. 32nd Conf. Open Innov. Assoc. (FRUCT)*, 2022, pp. 272–279.

[14] U. Detthamrong, S. Sattayatham, T. Laohakosol, and K. Phoomvuthisarn, "Enhancing fraud detection in banking using advanced machine learning techniques," *Int. J. Econ. Financial Issues*, vol. 14, no. 5, pp. 177–184, 2024.

[15] R. Majeed, M. Arif, M. A. Sattar, A. A. Sheikh, A. Khan, and F. Ahmad, "Intelligent cyber-security system for IoT-aided drones using voting classifier," *Electronics*, vol. 10, no. 23, p. 2926, 2021.

[16] M. A. Abid, S. Ullah, M. A. Siddique, M. F. Mushtaq, W. Aljedaani, and F. Rustam, "Spam SMS filtering based on text features and supervised machine learning techniques," *Multimedia Tools Appl.*, vol. 81, no. 28, pp. 39853–39871, 2022.

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

[18] M. Ali, F. R. Siddiqui, M. Rafiq, H. Ahmad, A. Rehman, and M. Z. Khan, "Hybrid machine learning model for efficient botnet attack detection in IoT environment," *IEEE Access*, 2024.

[19] S. Dhankhad, E. Mohammed, and B. Far, "Supervised machine learning algorithms for credit card fraudulent transaction detection: A comparative study," in *Proc. 2018 IEEE Int. Conf. Inf. Reuse Integr. (IRI)*, 2018, pp. 122–129.

[20] S. Mittal and S. Tyagi, "Performance evaluation of machine learning algorithms for credit card fraud detection," in *Proc. 2019 9th Int. Conf. Cloud Comput., Data Sci. & Eng. (Confluence)*, 2019, pp. 288–293.

[21] M. A. Abid, A. Nasir, S. Jamil, H. Khalid, and R. A. Khan, "Comparative analysis of TF-IDF and loglikelihood method for keywords extraction of Twitter data," *Mehran Univ. Res. J. Eng. Technol.*, vol. 42, no. 1, pp. 88–94, 2023.

[22] Amna, M. N. Khan, and H. Rehman, "The comparative performance analysis of

clustering algorithms," in *Proc. Int. Conf. Soft Comput. Data Min.*, Cham, Springer Int. Publ., 2022, pp. 354–362.

[23] A. Roy, J. Sun, R. Mahoney, L. Alonzi, S. Adams, and P. Beling, "Deep learning detecting fraud in credit card transactions," in *Proc. 2018 Syst. Inf. Eng. Des. Symp. (SIEDS)*, 2018, pp. 129–134.

[24] U. Farooq, M. M. Qureshi, M. Ali, S. Khalid, and N. Kamal, "Time series analysis of solar power generation based on machine learning for efficient monitoring," *Engineering Reports*, vol. 7, no. 2, p. e70023, 2025.

[25] M. Abdul Salam, M. Z. Malik, A. F. Rehman, A. Ali, M. A. Khan, and M. Shahbaz, "Federated learning model for credit card fraud detection with data balancing techniques," *Neural Comput. Appl.*, vol. 36, no. 11, pp. 6231–6256, 2024.

[26] R. Majeed, M. Arif, M. A. Sattar, A. A. Sheikh, A. Khan, and F. Ahmad, "Intelligent cyber-security system for IoT-aided drones using voting classifier," *Electronics*, vol. 10, no. 23, p. 2926, 2021.