International Journal of Management Technology
Vol.11, No 3, pp.42-63, 2024
Print ISSN: ISSN 2055-0847(Print)
Online ISSN: ISSN 2055-0855(Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Secure and Efficient Federated Learning Framework for Advanced Credit Card Fraud Detection with Optimization

Venkatesh Popuri
Master's Degree in Information Systems Engineering and Management
Harrisburg University of Science and Technology, PA

doi: https://doi.org/10.37745/ijmt.2013/vol11n34263 Published August 10, 2024

Citation: Popuri V (2024) Secure and Efficient Federated Learning Framework for Advanced Credit Card Fraud Detection with Optimization, *International Journal of Management Technology*, Vol.11, No 3, pp.42-63

Abstract: *In recent years, credit card fraud has cost banks and customers a great deal of money. A strong Fraud Detection System (FDS) is therefore necessary to reduce losses for consumers and banks. Our analysis shows that the dataset of credit card transactions is extremely biased, with many fewer examples of fraudulent purchases than of genuine ones. In addition, banks are typically prohibited from sharing their transaction statistics because of concerns about data security and privacy. These issues make it challenging for FDS to identify fraud tendencies and to identify them. In this investigation, we offer a framework in which we label FFD (Federated learning for Fraud Detection) to train a fraud detection model utilizing behavior features with federated learning and convolutional neural networks (CNN) with Greylag Goose Optimization. In contrast to the conventional FDS trained on cloud-centralized data, FFD allows banks to use training data from their local databases to create fraud detection models. Subsequently, a shared fraud detection model is created by combining locally computed updates. Banks can profit collectively from a shared model without exchanging datasets to safeguard the cardholders' sensitive information. In addition, an oversampling strategy is employed to counterbalance the skewed dataset. We use an extensive set of actual credit card transactions to assess the effectiveness of our credit card FDS system. The findings demonstrate the great accuracy with which each algorithm may be applied to the detection of credit card fraud.*

Keywords: Federated Learning, Credit Card Fraud Detection, CNN, Graylag Goose Optimization, Security, Efficiency

INTRODUCTION

Globally, the number of newly established businesses is rising [1]. All of those businesses strive to give their clients the highest caliber of service possible. Businesses analyze a lot of data every day in order to be successful in that. These data are available in various formats and are sourced from a multitude of sources. Furthermore, some of the most important components of the business's future are contained in this data. For

this reason, businesses need to handle, store, and most importantly keep the data secure. Many pieces of data can be misused by other businesses or, worse yet, stolen if security isn't maintained. Financial information is typically stolen, which can be detrimental to an individual or the entire firm. Frauds come in a variety of forms [2]. When someone forges a check or pays with one realizing there isn't enough money, it's known as fraud with checks. Online fraud involves the sale of phony or fraudulent goods and the collection of money without the delivery of the promised goods. There are a few more, including theft of identities, credit card fraud, debt reduction, fraudulent insurance policies, and fraud involving charities. Since electronic payments are becoming more and more ubiquitous, credit card fraud is one of the most prevalent types of fraud. When a credit card is used for fraudulent purposes without its proprietor's knowledge, it is referred to as credit card fraud. Fraudulent activities utilizing credit cards obtained from all across the world [3]. Despite a sharp rise in credit card activity, the number of frauds has either remained constant or declined as a result of advanced fraud detection systems. Still, Information theft is an ongoing endeavor for scammers, as evidenced in [4-5]. Considering the advancement of contemporary computer technology and worldwide connectivity, credit card transactions have become more commonplace. Fraud is also sharply rising at the same period. The European Central Bank research [6-8] states that credit card fraud costs Europe billions of euros annually. Due to the low risk of obtaining a substantial quantity of money quickly, credit cards are seen to be a desirable target for fraud [9]. Fraud involving credit cards may be committed in a variety of ways, including online, offline, and counterfeit card fraud, as well as application fraud [10]. Application fraud is a common and dangerous kind of fraud where thieves obtain credit cards by providing fraudulent personal information or the data of another person, intending to never pay back the purchases [11]. When a credit card is used remotely, only the credit card details are required, which leads to imitation fraud [12]. While online fraud is conducted through phone, computer, or cardholder not-present buying, offline fraud occurs when thieves steal a credit card and use it in stores as the real owner [13].

The two most popular tools for preventing and detecting fraud are fraud recognition and avoidance. The first line of defense against fraud is to filter transactions that are high-risk and prevent them from happening in the first place. Many authorization strategies, including signatures [14], credit card numbers, identifying numbers, cardholder addresses expiration dates, etc., are available to avoid credit card fraud. Nevertheless, these approaches are cumbersome for the clients and insufficient to reduce credit card fraud cases. The adoption of fraud detection techniques that examine data to identify and eradicate fraudulent use of credit cards is urgently needed [15].

LITERATURE REVIEW

The topic of identifying fraudulent transactions in the credit card industry is an issue that is frequently addressed and given a lot of attention, there aren't many publications that are available to the community [16]. One of the causes is that credit card companies guard against customer privacy being revealed through the sharing of data sources. The two types of data mining technologies used to generate credit card FDS mentioned in the detection of credit card theft research are supervised and unsupervised methods. Supervised learning methods are dependent on the data sets labeled as "fraud" and "normal". This is the method of fraud detection that is most commonly used. A dynamic model for detecting credit card fraud has been suggested recently

[17], combining contextual bandits with decision trees. Adaptive learning techniques can modify a fraud detection model for continuously changing streams of data to adjust to and record shifts in the patterns of fraud over time [18]. In [19], data level-adjusted approaches like Easy Ensemble, SMOTE, and the below sampling methodology are used to determine the most effective mechanism for credit card fraud detection. A collective approach under supervision [20] was created by fusing the concepts of boosting and bagging. To cut down on time spent training, an FDS built with the scalability method BOAT (Boostrapped Positive method for Tree Construction) enables multiple tree levels in a single scan across the training collection [21]. In fraud, Bayes [20], artificial neural networks (ANN) [21, 22], and support vector machines [23, 24] are further supervised learning techniques. There isn't a class label for building fraud detection models in unsupervised learning. Similar to [25], it proposed unsupervised techniques that don't need the precise identification of illegal activities, but rather spot alterations in behavior or anomalous occurrences. An unsupervised learning approach called K-means clustering groups data according to how similar they are to each other characteristics [26] that is used to identify credit card fraud.
In recognition of the significant losses caused by fraudulent activity, academics are working to develop a method for identifying and stopping scams. Numerous approaches have previously been put out and examined. A quick summary of a few of them is given below. Traditional methods that have shown useful include Gradient Boosting (GB), Support Vector Machines (SVM), Decision Trees (DT), LR, and RF. GB, LR, RD, SVM, and various combinations of specific classifiers were employed in the study [27], which produced a high recall of more than 91% on a European dataset. Only after the dataset was balanced by underestimating the data were high precision and recall attained. A comparison of models based on LR, DT, and RF was conducted in the publication [29], which also used a European database. Through a 95.5% accuracy rate, RF outperformed the other two models, DT came in second with 94.3% accuracy, and LR came in third with 90% accuracy.

k-Nearest neighbors (KNN) and [30] state that techniques for identifying outliers can be effective in detecting fraud. Their utility in reducing false alarms has been demonstrated rates as well as an increased rate of fraud detection. The authors tested and compared the KNN method with other traditional algorithms in an experiment for their publication [31], and it worked well. Three sets of information were utilized in investigation [32] to compare the Auto-encoder and Restricted Boltzmann Machine techniques. The results showed that MLP algorithms can be useful for detecting credit card fraud.

Deep neural network fraud detection has been the subject of numerous articles. These models work better on larger datasets, but they are computationally expensive [33]. As several studies have shown, this strategy can produce excellent outcomes. But what if it is possible to produce even greater results with fewer assets? Our main objective is to demonstrate how various machine learning algorithms, with the right preprocessing, may produce respectable results. The majority of the aforementioned papers' authors employed under sampling techniques, which served as justification for adopting an alternative strategy: oversampling techniques.

International Journal of Management Technology
Vol.11, No 3, pp.42-63, 2024
Print ISSN: ISSN 2055-0847(Print)
Online ISSN: ISSN 2055-0855(Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

RESEARCH METHODOLOGY

Data Collection

The Credit Card Fraud Detection dataset, available for download from Kaggle [34], was used in this study. This dataset includes two-day transactions performed in September 2013 by cardholders across Europe. There are 31 numerical features in the dataset. To maintain the anonymity of the data, the PCA transformation of the input variables was carried out because some of them contained financial information. Three of the available features were changed. The "Time" feature displays the interval of time between the first and each subsequent transaction in the collection. Characteristic The term "Amount" refers to the total amount of credit card transactions. The feature "Class" denotes the label and has just two possible values: 1 in the event of a fraudulent transaction and 0 in all other cases. 283,253 transactions total in the dataset; 473 of those were fraudulent, and the remaining transactions were legitimate.

Looking at the numbers, we can observe that just 0.173% of the transactions in this dataset are classified as fraudulent, indicating a significant imbalance. Preprocessing the data is vital since the distribution ratio of classes affects the accuracy and precision of the model.

Pre-processing

The process of converting unprocessed data into a comprehensible format is known as data preparation. The first, and most important, stage in preparing the data for use is data preprocessing. The dataset has a large number of data points, so it is necessary to filter out uncertainties like missing values, null values, and irrelevant data. Remove the uncertainties from the dataset because they will negatively affect the accuracy of the consequences.

A basic method for choosing the variables that are most important in a given dataset is feature selection. Reducing overfitting, increasing accuracy, and shortening training time can all be achieved by carefully selecting the right features and eliminating the less crucial ones. In such process, visualization tools can be useful.

CNN Model Development for Fraud Detection

The neural network that makes up biology is analogous to the convolutional neural network. The way neuron is arranged in a network is modeled after the human minds and visual cortex-influenced processing mechanism. It is composed of an output layer, fully linked layers, pooling layers, and a convolution layer. The fundamental architecture is shown in fig. 1 below.

International Journal of Management Technology
Vol.11, No 3, pp.42-63, 2024
Print ISSN: ISSN 2055-0847(Print)
Online ISSN: ISSN 2055-0855(Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

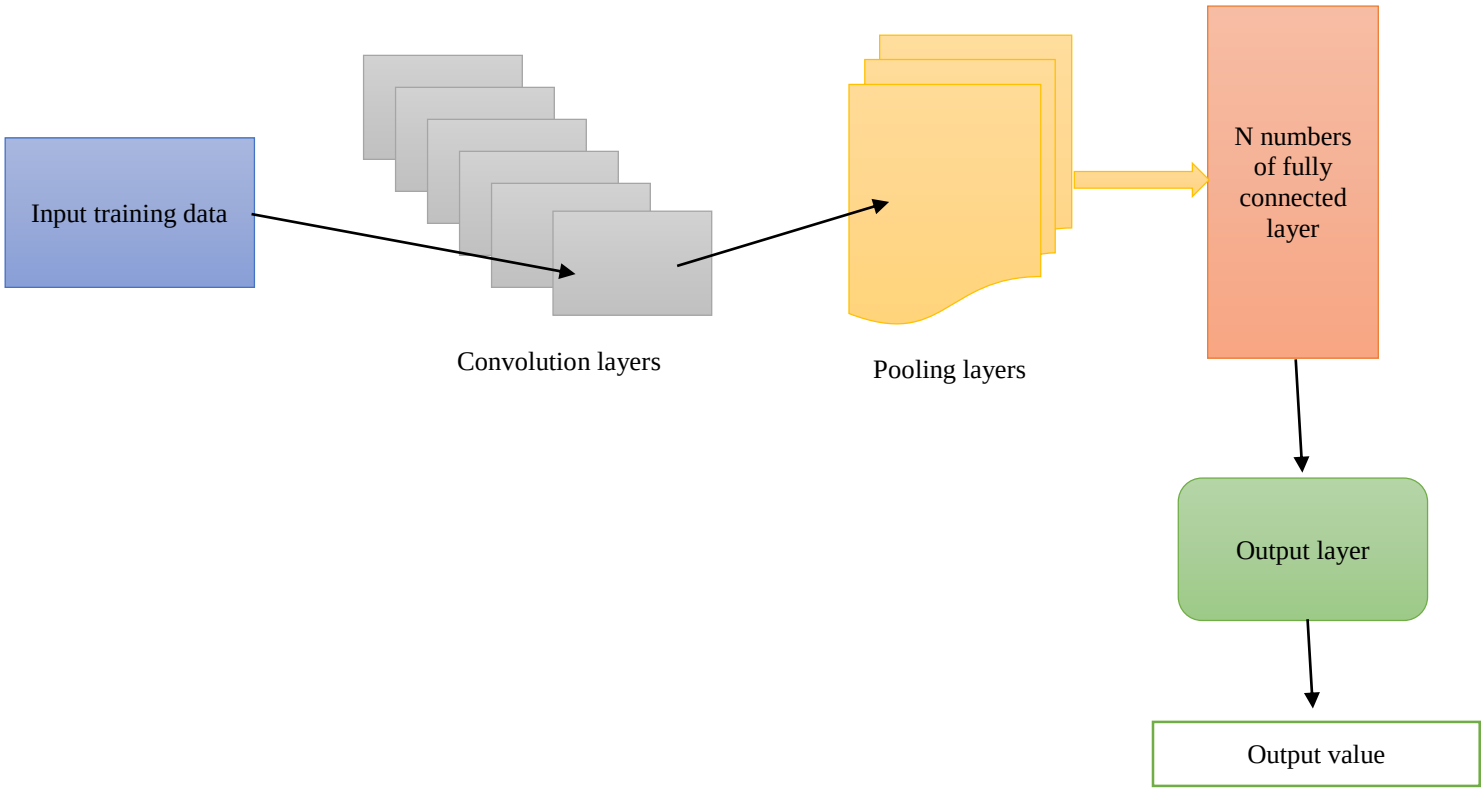


Figure. 1. CNN Basic Architecture

The convolution layer receives input in the form of training data. The features are extracted from the provided training data by the convolution layer. Subsequently, the convolution layer outputs are reduced in size to fit the appropriate pooling layer size. After that, pooling layers are flattened to provide a vector, which serves as the input for dense or completely linked layers. The final output layer receives the output that the dense layers have learned.
Equation 1 provides Z for the training data X, the filter f, and the convolution.

$$Z = X * f \qquad 1$$

where f is the filter and X is the data input matrix. This is an elementwise multiplication.
In the event when X is (n, n) in size and the filter is (f, f) in size. Z will therefore have the following size: ((n-f+1), (n-f+1))
Z is the pooling layer's output. The process of flattening the pooling result involves converting the ((n-f+1), (n-f+1)) dimensional values into a single dimensional array.
The denser layer modifies things based on the information. Dense layers carry out two kinds of transformations. Both linear and non-linear modifications are involved.

Similar to other neurons, the weights (a matrix of randomly assigned values), W, and the bias constant, denoted by b, carry out linear transformations in accordance with equation 2.

$$Z = W^T.X + b \qquad 2$$

W^T is the matrix W transposed. The intricate computations of features are beyond the scope of linear transformation. Therefore, activation functions a type of non-linear component are included in order to use non-linear transformations. With the exception of the output layer, all layers in this model have rectifier linear units (relu) as their activation function. The following equation 3 defies the relu function.

$$relu = f(x) = x^+ = (0, x) \qquad 3$$

This only uses the positive value of the output since the other dense layer may find it difficult to learn from the negative results of one layer, and learning time will be reduced by avoiding negative results.

Since there are no more hidden layers, we can also take negative values into consideration when choosing an activation function for the output layer, which is the sigmoid function.

The following equation 4 defines the sigmoid function.

$$S(x) = \frac{1}{1+e^{-x}} = \frac{e^x}{1+e^x} \qquad 4$$

Consequently, the following actions can be used to summarize the forward propagation's output: Accept this input: X Convolution layer application: $C_n = X * f$ Use the activation function of relu: $A_n = relu(C_n)$For every layer of density, use a linear transformation: $Z_n = W^T * A_{n-1} + b$ The input for the following dense layer is the output of each dense layer. Iteratively working up to the final layer are the steps from a to d. This is the stage of learning. Put the output layer's sigmoid function to use.

$$Z_n = S(Z_{n-1}) \qquad 5$$

Federated Learning Implementation

A fixed set of C banks, or financial institutions, are involved; each bank has a fixed private dataset, $D_i = \{x_i^c, y_i^c\}$ (c = 1, 2, 3,..., C). The amount of the dataset linked to participant bank c is denoted by nc, the feature vector is represented by x_i^c, and the corresponding label is y_i^c. The skewness of credit card transaction data fraudulent transactions makes up a very small portion of the total dataset could make it difficult for credit card FDS to operate effectively. For data rebalancing at Di, the data level approach SMOTE [35] is chosen. SMOTE creates artificial minority examples close to observed ones, oversampling the minority class. The objective of our federated learning fraud detection solution is to enable several banks to share datasets to develop an efficient fraud detection model without disclosing the privacy of each bank's clientele. All banks will first agree on a common fraud detection model (including the model's architecture, the activation function in each hidden layer, the loss function, etc.) before engaging in the model's training. The goal for a neural network model that is non-convex is:

$$min_{\omega \epsilon \mathbb{R}^d}\ l(x, y; w) \quad where \quad l(x, y; w) def = \frac{1}{n}\sum_{i=1}^{n} l(x_i, y_i; w) \qquad 6$$

With a fixed dataset $|D_i| = n_c$, C banks participate in the federated fraud detection model. We use n to represent all the data samples included in the entire FDS. As a result, $n = \sum_{I=1}^{C}|D_i| = \sum_{c=1}^{C} n_c$. The goal (6) can be rewritten as

$$l(x, y; w) = \quad where \quad L_c(x_c, y_c; w) = \frac{1}{n_c}\sum_{i\epsilon D_i} l(x_i^c, y_i^c; w) \qquad 7$$

The parameters of the fraud detection model will be initialized by the server. Every communication round (t=1, 2, ...) will see the selection of a random proportion F of banks. The server and these banks will speak with each other directly. Download the global model parameters from the server in the first instance. Next, using a fixed learning rate η, each bank computes the average gradient of the loss fc on its own private dataset at the current fraud detection model parameters w_t, where fc = $\Delta L_c(x_c, y_c; w)$. These banks communicate updates to the fraud detection model to the server in a synchronous manner.

By combining these updates, the server enhances the shared mode.

$$w_{t+1} \leftarrow w_t - \eta \nabla l(x, y; w) \qquad 8$$

$$w_{t+1} \leftarrow w_t - \eta \sum_{C=1}^{C} \frac{n_c}{n} \nabla L_c(x_c, y_c; w) \qquad 9$$

$$w_{t+1} \leftarrow w_t - \eta \frac{n_c}{n} f_c \qquad 10$$

$$w_{t+1} \leftarrow w_t - \sum_{C=1}^{C} \frac{n_c}{n} w_{t+1}^c \qquad 11$$

We employ the combination of data size and detection model performance α_{t+1}^con each bank as the weight of parameter vector, taking into account the effect of skewed data on model performance. It may be expressed as

$$w_{t+1} \leftarrow w_t - \sum_{C=1}^{C} \frac{n_c}{n} \alpha_{t+1}^c w_{t+1}^c \qquad 12$$

To create a better global shared model, strong classifiers should be given greater weight and consideration. Every bank uses its own credit card transactions to evaluate on a fraud detection model in a step-by-step fashion. After that, the server applies them to all participating banks by calculating a weighted average. There will be T iterations in total in this process.

Data exchange is restricted and made more difficult by the growing concern about data privacy, which also makes it challenging to organize extensive joint efforts to build a trustworthy FDS. A federated learning-based credit card fraud detection system is suggested, which allows any bank to train a fraud detection model using data that is spread across several banks. It not only aids in improving credit card FDS learning patterns of fraud and authentic transactions while also maintaining the confidentiality and privacy of the datasets. One of the biggest obstacles to federated optimization is communication cost. Banks should, on the one hand, retrieve the initial fraud detection model parameters obtained from the server. Banks should publish the updated model to the server at the same time. Thus, the cost of communication in FDS is symmetric. Although upload bandwidth has an impact, there are three important factors in our FDS that are related to communication cost: F is the percentage of banks that will be chosen to compute for

each round; B is the size of the minibatch that is utilized to update banks. E is the quantity of local epochs. By adjusting these three parameters, we may control the cost of communication by adding computation through increased parallelism through the use of more banks or by doing more computation on each bank in between communication rounds.

Optimization using Greylag Goose Algorithm

Inspired by the foraging habits of the greylag goose, the Greylag Goose Optimization (GGO) method is a metaheuristic optimization technique. In 2018, Ramalingam et al. made the proposal. The system replicates the exploration, exploitation, and flocking behaviors of a greylag geese during its foraging excursion.

Inspiration and Mechanism: The patterns of migration of the Greylag Goose provide inspiration for the GGO Algorithm. The grin flocking of birds, in which the lead goose guides the others, is created using this algorithm. The birds then modify their placements to arrive at the best option. This algorithm determines if a feature is meaningful by comparing lists of features that are represented as 1s and 0s.

Key Features: To fully explore and exploit the search space, GGO uses position-updating operations and the leader-follower technique. To find the ideal final feature combination, it provides a half-against-half option (search for new features versus refine recognized good features).

Training and Evaluation Strategies

Training: Each bank begins with the downloaded global model and uses its local data to train its local learning model. Based on its local dataset, the local model modifies its parameters during train. After several training cycles, the global model reaches a state where data security and privacy are maintained while knowledge from all local models (fog nodes) is gathered. After the training phase is finished, the final global model is put into use, but each bank keeps its local data private and does not share it with the cloud service.

Evaluation Strategies; In order to choose the ideal settings for a credit card fraud detection system, it is imperative to measure the machine learning algorithm's performance [32]. Accuracy alone is insufficient to assess the effectiveness of FDS when the dataset exhibits substantial imbalances. Even if the FDS predicts all occurrences of lawful transactions incorrectly, accuracy will still have a high value. Because of this, we also take into account additional metrics like precision, recall, and F1, where Positive metrics relate to samples that were fraudulent and Negative metrics relate to genuine samples. Accuracy shows that FDS has correctly identified all experimental records. The precision rate indicates the FDS's dependability, whereas the recall rate gauges how well the FDS finds all fraudulent transactions. The harmonic mean of recall and precision is denoted as F1. Researchers use accuracy, precision, recall, F1-score, computation time, and average loss as performance indicators to assess our predictive classifier models. The true positive (TP), true negative (TN), false positive (FP), and false negative (FN) parameters are used to evaluate these measures. When the anticipated result comes to pass, it's a true positive. On the other hand, a

situation is called a true negative if the expected outcome turns out to be false. When an output is projected to be true but is false, this is known as a false positive. On the other hand, it is referred to as a false negative if the expected outcome is true but untrue. The following are each metric's definitions and equations.
The ratio of accurate predictions to total predictions is known as accuracy.

$$\text{Accuracy}=\frac{(TP+TN)}{(TP+FP+TN+FN)} \quad 13$$

The ratio of true positives to all positive predictions true positives plus false positives is known as precision.

$$\text{Precision}=\frac{TP}{(TP+FP)} \quad 14$$

Accuracy for positive instances (class 1) of fraudulent transactions is provided by recall (sensitivity).

$$\text{Recall}=\frac{TP}{(TP+FN)} \quad 15$$

The ratio of true positives to all positives (true positive and false negative) is known as the F1-Score.

$$\text{F1-score}=2\times\frac{(precision\times Recall)}{(precision+Recall)} \quad 16$$

Simulation Results

Performance Evaluation:
A variety of standards for algorithm comparison have been used to evaluate which algorithm is best suited for the task of detecting fraudulent transactions. The metrics accuracy, recall, and precision are most frequently used to assess the performance of machine learning systems. A confusion matrix can be used to compute each of the metrics listed above. These measures were used to assess a model's performance. Testing the models on both the original and processed data revealed the importance that sampling essential.

Logistic Regression
One of the most often used classification algorithms in machine learning is logistic regression. Relationships between continuous, binary, and categorical predictors are described by the logistic regression model. One type of dependent variable is binary. We forecast whether something will occur or not based on a few factors. For a given collection of predictors, we calculate the likelihood of falling into each group.

Classification reports show different metrics for each class in the classification issue, including precision, recall, and F1 score. The accuracy can be defined as the ratio of actual positive results to all expected positive results. It gauges how well the model predicts the favorable outcomes. The recall can be defined as the proportion of genuine positives to all actual positives. It assesses how well the model can recognize

positive samples. The F1 score offers a fair assessment of the model's performance and is calculated as the harmonic mean of precision and recall. The function can be used to construct the classification report using two arguments: the predicted labels produced by the model and the true labels of the test data. The categorization report can be a helpful resource for pinpointing potential weak points in your model and implementing fixes to increase accuracy. One may improve your model's accuracy and effectiveness in classifying fresh samples by utilizing the report's information to refine model.

Table: 1 Classification report of Logistic Regression

	Precision	**Recall**	**F1_score**	**Support**
0	0.95	0.99	0.97	11245
1	0.98	0.90	0.93	5750
Accuracy			0.96	16995
Macro avg	0.96	0.94	0.95	16995
Weighted avg	0.96	0.96	0.96	16995

Confusion matrix:

This system is supported by the ML group execution framework. Calculating the chaotic grid will help us better comprehend the average illustration's correctness and the kinds of duties it creates. The correctness of the representation is assessed in a similar manner to how true and prescient markers are grouped. They graphically depict the classifier and its representation. Figure 2 in the LR's confusion matrix. Our model's metric is shown in the attached graphic. The confusion matrix indicates how many distinct and projected brands there are for a certain process. Both the total number of real marks and the names intended for arrangement are addressed by the disorganized dot matrix. These realistic and anticipated names include a range of false positives, true negatives, false negatives, and true positives.

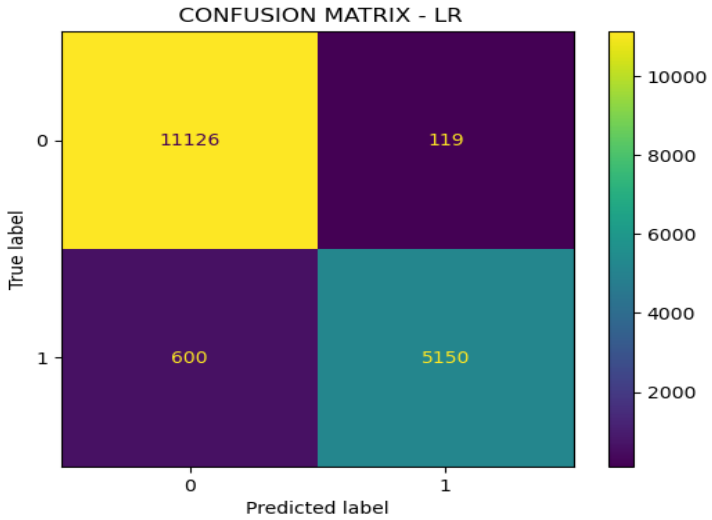


Figure 2. Confusion matrix of LR

International Journal of Management Technology
Vol.11, No 3, pp.42-63, 2024
Print ISSN: ISSN 2055-0847(Print)
Online ISSN: ISSN 2055-0855(Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Simple Neural network

Although the results are not flawless, it is clear from examining the obtained data that accuracy is very high. 99.7% accuracy is desirable; nonetheless, it should be understood in conjunction with other criteria. The presented results demonstrate that a basic neural network can produce outcomes comparable to those of a traditional method such as logistic regression. In this section we chart the variations in metrics such as accuracy and loss during training and validation. Figure 3. Graphical representation on loss and accuracy in each epoch.

Table: 2 Classification report of Simple Neural network

	Precision	**Recall**	**F1_score**	**Support**
0	1.00	1.00	1.00	11245
1	0.99	1.00	1.00	5750
Accuracy			1.00	16995
Macro avg	1.00	1.00	1.00	16995
Weighted avg	-1.00	1.00	1.00	16995

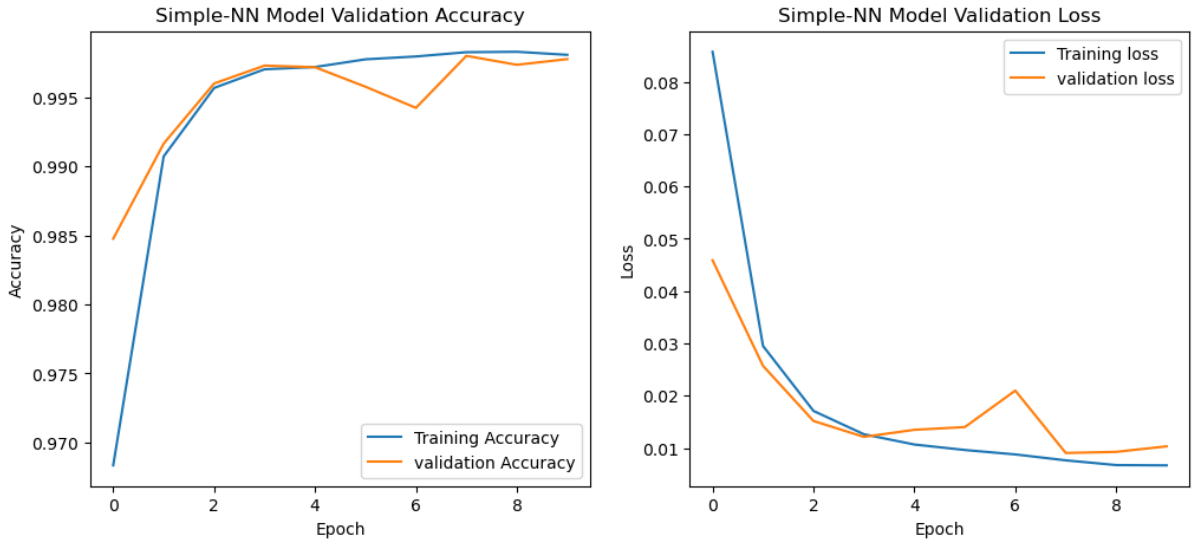


Figure 3. Graphical representation on loss and accuracy in each epoch

The ML group implementation plan uses this strategy. We can have a deeper understanding of the illustration approaches accuracy and the sorts of flaws it generates by computing the chaotic grid. In the same way as true and prophetic markers are set up, it is used to evaluate the accuracy of the depiction. To visually represent the classifier and its illustration, they employ visuals. Figure 4: SNN confusion matrix

The offered figure shows the measure in our model. The total number of actual and anticipated labels is shown in the confusion matrix for a particular algorithm. There are several different types of false positives, true positives, false negatives, and false positives.

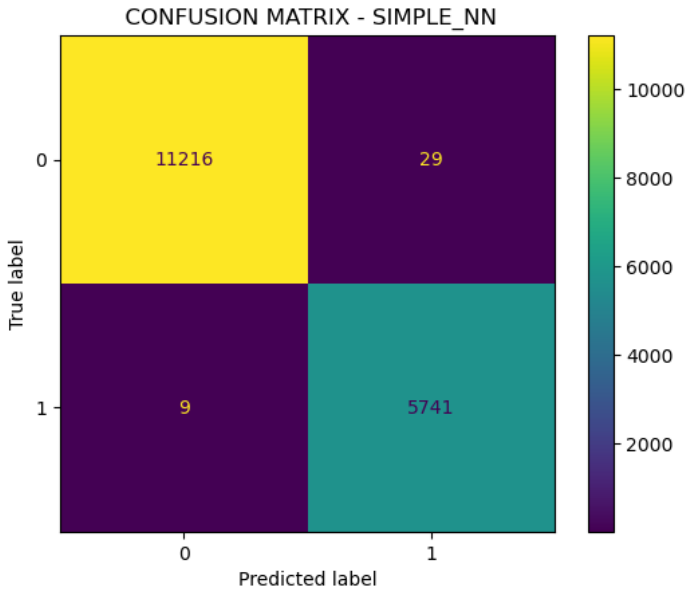


Figure 4. Confusion matrix of simple neural network model

CNN based federated learning

In terms of fraud transactions, the more effective fraud detection system outperformed the others. When the data is more balanced, FDS is able to identify patterns of fraud and genuine transactions more effectively. First line of Table 3 shows that performance increased while the number of communication rounds needed to obtain the desired AUC dropped when more Banks participated in parallel computing improved the CNN-based FDS. Because CNN-FDS must be able to manage limited time resources, time efficiency is also crucial.

Federated learning (FL) is a distributed machine learning technique in which local data samples are stored on numerous decentralized devices or servers, and a global model is trained across them without transferring the actual data. This strategy is very helpful for protecting data privacy and cutting down on data transport expenses. Assessment of the global and client models: (C) 99.6%, (G) 99.8% accuracy. (Fig 5)

International Journal of Management Technology
Vol.11, No 3, pp.42-63, 2024
Print ISSN: ISSN 2055-0847(Print)
Online ISSN: ISSN 2055-0855(Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

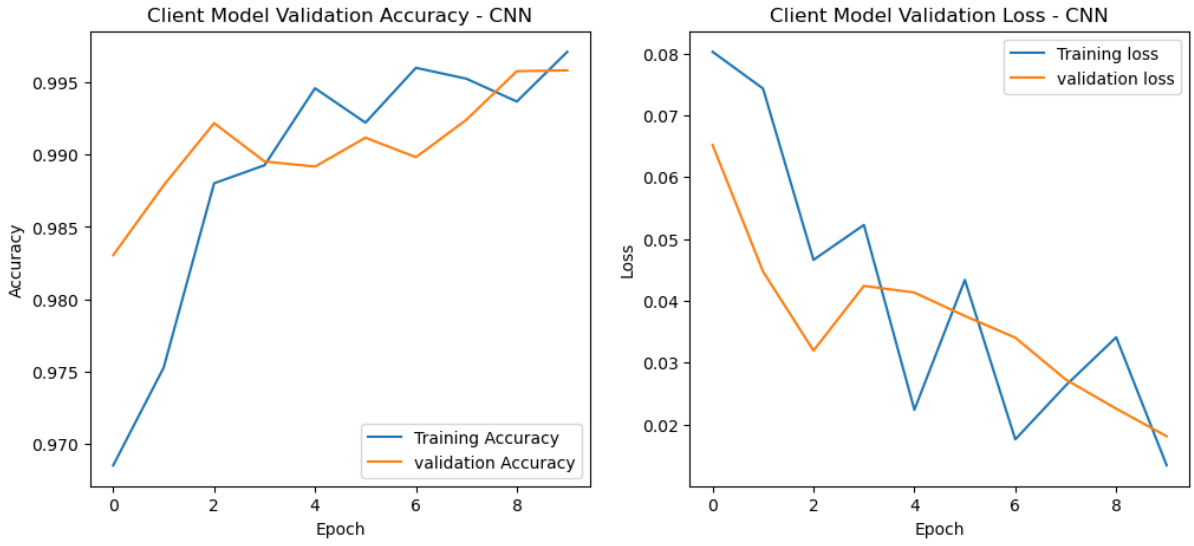
Table: 3 Classification report of Client model & Global model

Client model

	Precision	**Recall**	**F1_score**	**Support**
0	1.00	0.99	1.00	11245
1	0.99	1.00	0.99	5750
Accuracy			1.00	16995
Macro avg	0.99	1.00	1.00	16995
Weighted avg	1.00	1.00	1.00	16995

Global model

	Precision	**Recall**	**F1_score**	**Support**
0	-1.00	1.00	1.00	11245
1	1.00	1.00	1.00	5750
Accuracy			1.00	16995
Macro avg	1.00	1.00	1.00	16995
Weighted avg	1.00	1.00	1.00	16995



International Journal of Management Technology
Vol.11, No 3, pp.42-63, 2024
Print ISSN: ISSN 2055-0847(Print)
Online ISSN: ISSN 2055-0855(Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

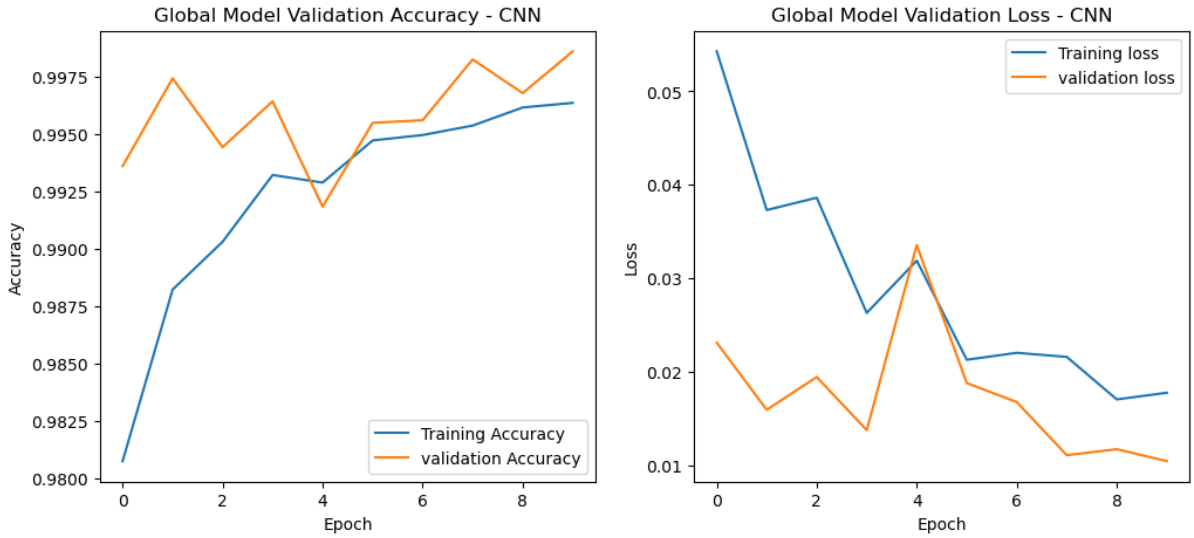


Figure 5. Graphical representation of CNN Client & Global model

The ML group's execution plan uses this secondhand tactic. We can have a deeper understanding of the illustration approach accuracy and the sorts of flaws it generates by computing the chaotic grid. It is used to evaluate the accuracy of the depiction, similar to the arrangement of true and prescient markers. They describe the classifier and its representation directly. Figure 6 shows CNN's client and global model confusion matrix. The metric of our model is shown in the following diagram. The total number of forecast and real components for a certain method is represented by the confusion matrix. The disordered dot matrix considers the total number of marks as well as the names that will be used for arranging. There are various types of false positives, false negatives, real positives, and false negatives.

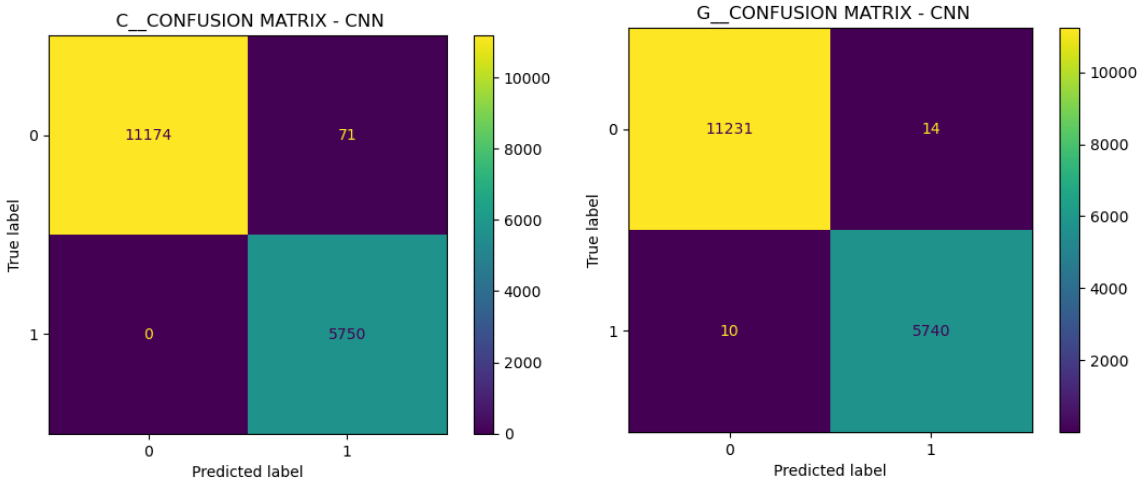


Figure 6. Confusion matrix of CNN – Client model & Global model

Enhanced CNN based federated learning

The more successful fraud detection system performed better than the others in terms of fraud transactions. More balanced data makes it easier for FDS to spot trends of fraud and legitimate transactions. The Enhanced CNN-based FDS was enhanced when more Banks engaged in parallel computation, as seen by the first line of Table 4, which also demonstrates that performance rose and fewer communication rounds were required to attain the necessary AUC. Time efficiency is also critical since Enhanced CNN-FDS needs to be able to handle limited time resources.

Federated learning, or FL for short, is a distributed machine learning technique where a global model is trained across multiple decentralized devices or servers using local data samples stored there without sending the real data. This approach is highly beneficial for reducing data transit costs and safeguarding privacy. Evaluation of the client and global models: accuracy of (C) 99.2% and (G) 99.8% (Fig 7).

Table: 4 Classification report of CNN Enhanced model for client model & global model

	Precision	**Recall**	**F1_score**	**Support**
0	1.00	0.99	0.99	11245
1	0.98	1.00	0.99	5750
Accuracy			0.99	16995
Macro avg	0.99	0.99	0.99	16995
Weighted avg	0.99	0.99	0.99	16995

	Precision	**Recall**	**F1_score**	**Support**
0	1.00	1.00	1.00	11245
1	0.99	1.00	1.00	5750
Accuracy			1.00	16995
Macro avg	1.00	1.00	1.00	16995
Weighted avg	1.00	1.00	1.00	16995

International Journal of Management Technology
Vol.11, No 3, pp.42-63, 2024
Print ISSN: ISSN 2055-0847(Print)
Online ISSN: ISSN 2055-0855(Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

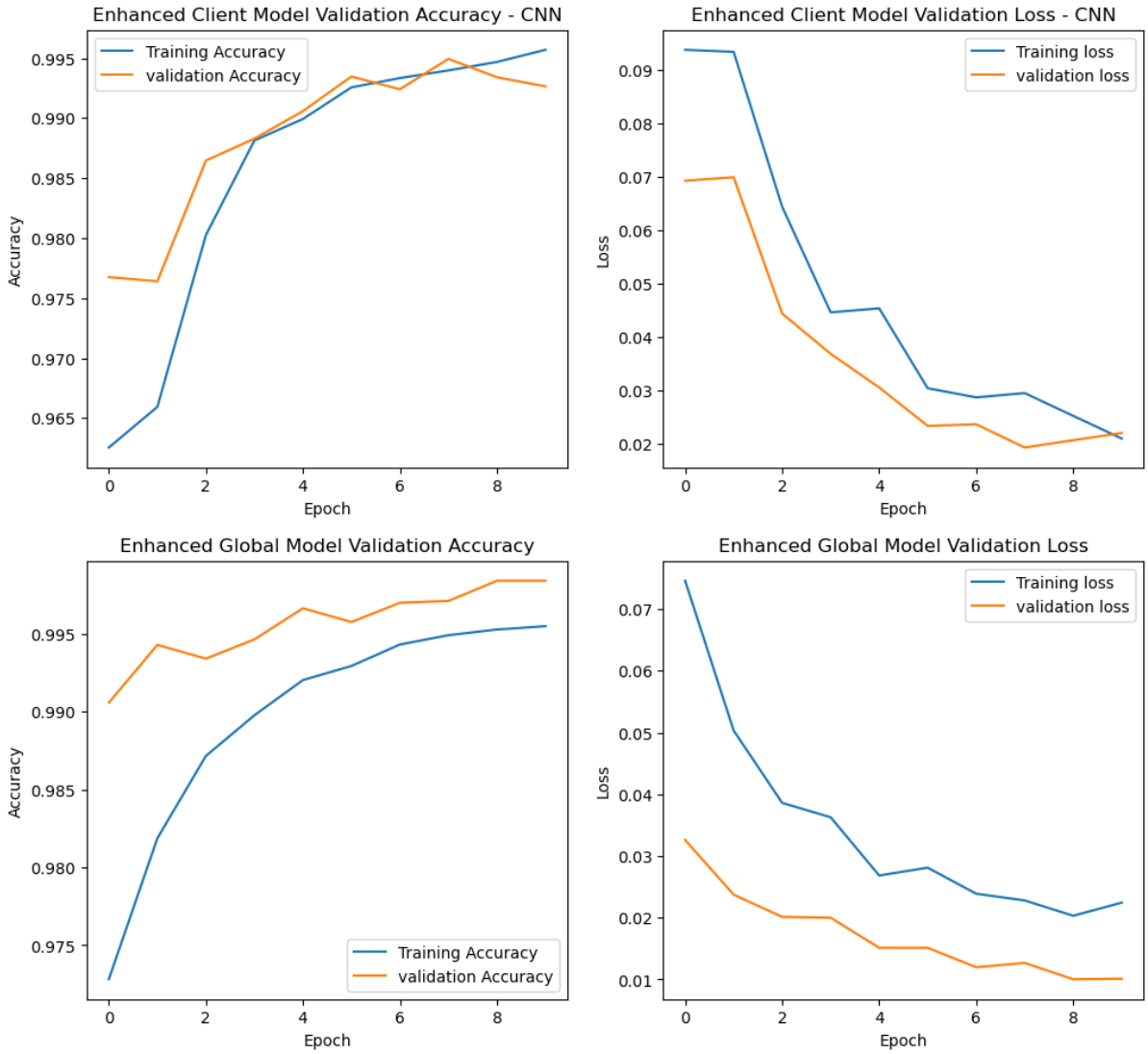


Figure 7. Graphical representation of enhanced CNN model

The ML group's execution plan uses this secondhand tactic. We can have a deeper understanding of the illustration approach accuracy and the sorts of flaws it generates by computing the chaotic grid. It is used to evaluate the accuracy of the depiction, similar to the arrangement of true and prescient markers. They describe the classifier and its representation directly. Figure 8: Client and global model confusion matrix for the Enhanced CNN. The metric of our model is shown in the following diagram. The total number of forecast and real components for a certain method is represented by the confusion matrix. The disordered dot matrix considers the total number of marks as well as the names that will be used for arranging. There are several types of false positives and false negatives that can occur.

International Journal of Management Technology
Vol.11, No 3, pp.42-63, 2024
Print ISSN: ISSN 2055-0847(Print)
Online ISSN: ISSN 2055-0855(Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

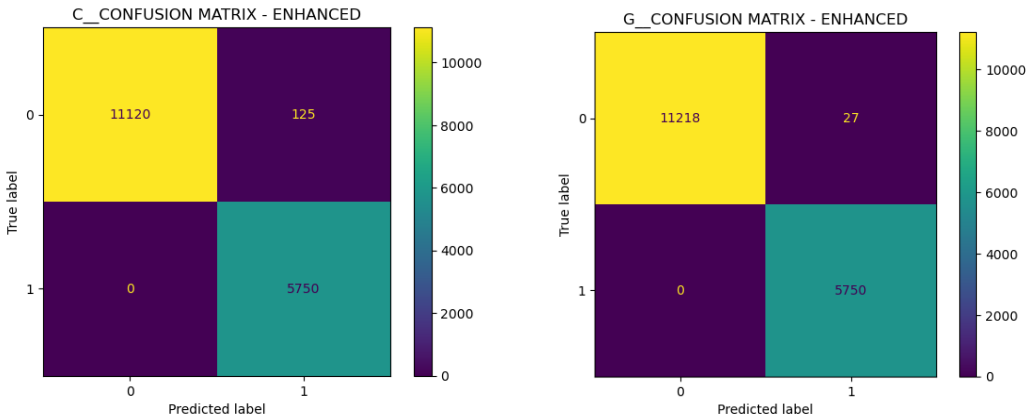


Figure 8. Enhanced Confusion matrix

Performance Comparison:

The proposed framework has an approximate accuracy increase rate of 10% over the current model, according to the section comparing the current and indicated models. This was found across all four algorithms: CNN-Federating Learning, Enhanced CNN-Federating Learning, Simple Neural Network, and Logistic Regression. After further analysis, we discovered that DT, out of the three algorithms in the suggested model, has the highest increased accuracy rate roughly 98%. Credit Card Fraud Detection for CNN-Federating Learning outperforms all other algorithms in the suggested model, as shown by the comparison table and graph above. To ensure the reliability of the suggested framework, we tested it on a different dataset. Our conclusion that the DT model's implementation algorithm was concise and produced an accurate result was validated by the data we discovered table 5 shows the comparison analysis.

Performance metrics (accuracy, precision, recall, F1-score) for all models are calculated and compared. Credit Card Fraud Detection (bar chart) of the performance metrics for different models is plotted (Fig 9).

Table: 5 Comparison and performance evaluation:

	Logistic Regression	**Simple Neural Network**	**CNN-Federating Learning**	**Enhanced CNN-Federating Learning**
Accuracy	0.9577	0.9978	0.9986	0.9984
precision	0.9631	0.9971	0.9983	0.9977
Recall	0.9425	0.9979	0.9985	0.9988
F1-Score	0.9517	0.9975	0.9984	0.9982

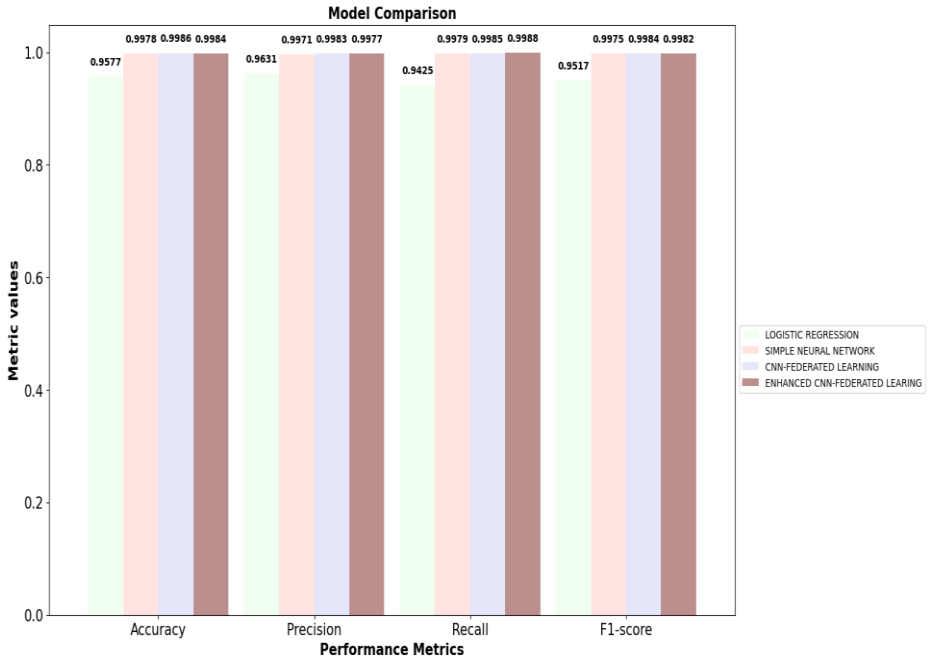


Figure 9. performance Metrics

DISCUSSION

The credit card FDS with federated detection was built in this paper. Our trials' outcomes demonstrate the considerable improvement of federated learning for credit card detection systems. Banks may train a fraud detection system using a federated fraud detection framework without having to transfer their confidential data to a data center. In this paper, a blockchain-federated learning credit card fraud detection system that combines federated learning (FL). Our technology ensures better privacy, better data protection, and reduced risk of data breaches by integrating FL and blockchain techniques. infractions. Further guarantees of maintained privacy, data safety, decentralized storage, safe payment networks, and automated tasks are provided by the integration of FL in credit card services. The efficiency and efficacy of systems and frameworks developed in academic and industrial domains are adversely affected by a number of obstacles and limits. More attention must be paid to resolving these limitations, which include problems with feature engineering, adversarial attacks, imbalanced data, real-time detection, false positive costs, and data privacy. One major problem influencing prediction accuracy because of class is data imbalance differences in distribution. Fraud is a constantly evolving crime that uses various techniques and assaults to trick systems and avoid being discovered fraudulent dealings. Adversarial assaults, such as data poisoning, evasion attempts, and input data modification, are employed by fraudsters to trick the model. Furthermore, data security and privacy are important issues that demand further focus. However, these worries make it difficult for developers of credit card fraud detection systems to find publicly available data for analysis.

CONCLUSION

In this investigation, a federated detection credit card FDS was built. Our trials' outcomes demonstrate the notable improvement of federated learning for credit card detection systems. Banks can train a fraud detection system using a federated fraud detection framework without having to transfer their confidential data to a data center. This decentralized data approach can mitigate the impact of partially unavailable datasets and safeguard the confidentiality and sensitivity of the dataset. Privacy issues persist in the federated fraud detection system. The approach we use reduces the danger of data breaches, improves privacy, and protects data better by integrating blockchain technology with FL. Furthermore, decentralized storage, automated assignments, secure payment networks, privacy preservation, and data protection are all guaranteed by the integration of FL and blockchain in credit card services. Three strategies for optimization are used in addition to CNN, the machine learning methods: Greylag Goose Optimization technique is used for hyperparameter tuning Prior to model training, the dataset is balanced using the SMOTE oversampling technique. It has been demonstrated that the proposed structure improves prediction accuracy and performance in classification.

Future research will focus more on preserving data security and privacy by putting defensive mechanisms in place against possible threats. Our goal is to significantly enhance data security and privacy by implementing a defensive system that can instantly identify and stop possible fraud or attack attempts. In our upcoming project, we'll be putting into practice an online credit card fraud detection system that mimics different types of fraud and attacks, and then we'll assess how well it works. We will use attack patterns to determine its capacity to stop, identify, and lessen fraudulent transactions.

Reference

1. Abdul Salam, M., Fouad, K. M., Elbably, D. L., Hamdy, M., & Farag, A. (2024). Federated learning model for credit card fraud detection with data balancing techniques. Neural Computing and Applications, 36(7), 6231–6256.
2. Awosika, T., Shukla, R. M., & Pranggono, B. (2024). Transparency and privacy: The role of explainable AI and federated learning in financial fraud detection. IEEE Access, 12, 64551–64560.
3. Pushpita Chatterjee , Debashis Das , Danda Rawat . Securing Financial Transactions: Exploring the Role of Federated Learning and Blockchain in Credit Card Fraud Detection. TechRxiv. April 28, 2023.
4. Mniai, A., Tarik, M., & Jebari, K. (2023). A novel framework for credit card fraud detection. IEEE Access, 11, 112776–112786.
5. Zhang, S., Tay, J., & Baiz, P. (2024). The effects of data imbalance under a federated learning approach for credit risk forecasting. arXiv.
6. Ferreira, L., Silva, L., Morais, F. et al. International revenue share fraud prediction on the 5G edge using federated learning. Computing 105, 1907–1932 (2023).

7. Prabhakaran, N., & Nedunchelian, R. (2023). Oppositional cat swarm optimization-based feature selection approach for credit card fraud detection. Computational Intelligence and Neuroscience, 1, 1–13.
8. Karthikeyan, T., Govindarajan, M., & Vijayakumar, V. (2023). An effective fraud detection using competitive swarm optimization-based deep neural network. Measurement: Sensors, 27, 100793.
9. Zhang, Y.-F., Lu, H.-L., Lin, H.-F., Qiao, X.-C., & Zheng, H. (2022). The optimized anomaly detection models based on an approach of dealing with imbalanced dataset for credit card fraud detection. Mobile Information Systems, 1, 1-10.
10. Jovanovic, D., Antonijevic, M., Stankovic, M., Zivkovic, M., Tanaskovic, M., & Bacanin, N. (2022). Tuning machine learning models using a group search firefly algorithm for credit card fraud detection. Mathematics, 10(13), 2272.
11. Padhi, B. K., Chakravarty, S., Naik, B., Pattanayak, R. M., & Das, H. (2022). RHSOFS: Feature selection using the rock hyrax swarm optimization algorithm for credit card fraud detection system. Sensors, 22(23), 9321.
12. Geetha, N., & Dheepa, G. (2022). A hybrid deep learning and modified butterfly optimization based feature selection for transaction credit card fraud detection. Journal of Positive School Psychology, 6(7), 5328–5345.
13. Alarfaj, F. K., Malik, I., Khan, H. U., Almusallam, N., Ramzan, M., & Ahmed, M. (2022). Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms. IEEE Access, 10, 39700–39715.
14. Ganji, V. R., Chaparala, A., & Sajja, R. (2023). Shuffled shepherd political optimization-based deep learning method for credit card fraud detection. Concurrency and Computation: Practice and Experience, 35(10), 1–13.
15. Ning, W., Chen, S., Qiang, F., Tang, H., & Jie, S. (2023). A credit card fraud model prediction method based on penalty factor optimization AWTadaboost. Computers, Materials & Continua, 74(3), 5952–5965.
16. Soemers, D., Brys, T., Driessens, K., Winands, M., & Nowé, A. (2018, April). Adapting to concept drift in credit card transaction data streams using contextual bandits and decision trees. In *Proceedings of the AAAI Conference on Artificial Intelligence* (Vol. 32, No. 1).
17. Žliobaitė, I. (2010). Learning under concept drift: an overview. *arXiv preprint arXiv:1010.4784*.
18. Chen, R. C., Chen, T. S., & Lin, C. C. (2006). A new binary support vector system for increasing detection rate of credit card fraud. *International Journal of Pattern Recognition and Artificial Intelligence*, *20*(02), 227-239.
19. Dal Pozzolo, A., Caelen, O., Le Borgne, Y. A., Waterschoot, S., & Bontempi, G. (2014). Learned lessons in credit card fraud detection from a practitioner perspective. *Expert systems with applications*, *41*(10), 4915-4928.
20. Bian, Y., Cheng, M., Yang, C., Yuan, Y., Li, Q., Zhao, J. L., & Liang, L. (2016). Financial fraud detection: a new ensemble learning approach for imbalanced data.

21. Bahnsen, A. C., Stojanovic, A., Aouada, D., & Ottersten, B. (2013, December). Cost sensitive credit card fraud detection using Bayes minimum risk. In *2013 12th international conference on machine learning and applications* (Vol. 1, pp. 333-338). IEEE.
22. Patidar, R., & Sharma, L. (2011). Credit card fraud detection using neural network. *International Journal of Soft Computing and Engineering (IJSCE)*, *1*(32-38).
23. Syeda, M., Zhang, Y. Q., & Pan, Y. (2002, May). Parallel granular neural networks for fast credit card fraud detection. In *2002 IEEE World Congress on Computational Intelligence. 2002 IEEE International Conference on Fuzzy Systems. FUZZ-IEEE'02. Proceedings (Cat. No. 02CH37291)* (Vol. 1, pp. 572-577). IEEE.
24. Lu, Q., & Ju, C. (2011). Research on credit card fraud detection model based on class weighted support vector machine. *Journal of Convergence Information Technology*, *6*(1).
25. Wu, C. H., Tzeng, G. H., Goo, Y. J., & Fang, W. C. (2007). A real-valued genetic algorithm to optimize the parameters of support vector machine for predicting bankruptcy. *Expert systems with applications*, *32*(2), 397-408.
26. Bolton, R. J., & Hand, D. J. (2001). Unsupervised profiling methods for fraud detection. *Credit scoring and credit control VII*, 235-255.
27. Srivastava, A., Kundu, A., Sural, S., & Majumdar, A. (2008). Credit card fraud detection using hidden Markov model. *IEEE Transactions on dependable and secure computing*, *5*(1), 37-48.
28. Mishra, A., & Ghorpade, C. (2018, February). Credit card fraud detection on the skewed data using various classification and ensemble techniques. In *2018 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS)* (pp. 1-5). IEEE.
29. Lakshmi, S. V. S. S., & Kavilla, S. D. (2018). Machine learning for credit card fraud detection system. *International Journal of Applied Engineering Research*, *13*(24), 16819-16824.
30. KRISHNAN, S. Credit Card Nearest Neighbor Based Outlier Detection Techniques.
31. Awoyemi, J. O., Adetunmbi, A. O., & Oluwadare, S. A. (2017, October). Credit card fraud detection using machine learning techniques: A comparative analysis. In *2017 international conference on computing networking and informatics (ICCNI)* (pp. 1-9). IEEE.
32. Pumsirirat, A., & Liu, Y. (2018). Credit card fraud detection using deep learning based on auto-encoder and restricted boltzmann machine. *International Journal of advanced computer science and applications*, *9*(1).
33. Learning – Towards Data Science. [online] Available at: https://towardsdatascience.com/deep-learning-vs-classical-machinele arning-9a42c6d48aa [Accessed 19 Jan. 20
34. Kaggle.com. (2019). Credit Card Fraud Detection. [online] Available at: https://www.kaggle.com/mlg-ulb/creditcardfraud [Accessed 10 Jan. 2019].

35. Chawla, N. V., Bowyer, K. W., Hall, L. O., & Kegelmeyer, W. P. (2002). SMOTE: synthetic minority over-sampling technique. Journal of artificial intelligence research, 16, 321-357.