2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI) | 979-8-3503-1590-5/23/$31.00 ©2023 IEEE | DOI: 10.1109/ACCAI58221.2023.10200905

A Comparative Analysis of Credit Card Fraud Detection with Machine Learning Algorithms and Convolutional Neural Network

Ms. E. Ajitha, Ms. S. Sneha, Ms. Shanmitha Makesh and Ms. K. Jaspin

Department of Computer Science and Engineering, St. Joseph's Institute of Technology, Chennai, India.

E-mail : ajithamano2129@gmail.com snehasrikanth18@gmail.com mshanmitha@gmail.com jaspinjose@gmail.com

Abstract- Credit cards offer an effective and user-friendly function, so people can use them for online transactions. Utilization of credit cards has increased, and with that, so has the potential for credit card fraud. Financial institutions as well as cardholders suffer considerable financial losses as a result of credit card theft. The major objective is to identify fraudulent credit card transactions with the help of machine learning and Deep Learning algorithms. The recent development of Deep learning algorithms has been the key area of concentration in this regard. To get effective results, a comparative study on Deep Learning and Machine Learning algorithms was conducted.

Keywords- KNN Classifier, Logistic Regression, XG Boost Classifier, Random Forest.

I. INTRODUCTION

Nearly every transaction that is made in the modern world is digital. Online transactions are carried out through a smooth system that incorporates the participation of many individuals and doesn't require the use of currency. Unless a security issue enters the picture, this is a very safe and secure form of cash flow. The time and effort required to complete any transaction globally are greatly reduced by internet transactions. [16] The use of a credit card for consumption is permitted when a fraud steals or defrauds the cardholder's details. Without special identity verification methods, anyone can fraudulently use another person's cards and e-wallets. Some people might be hesitant to use online payment methods due to these security worries. Additionally, weak authentication can jeopardize online payment systems. Moreover, there is a growing requirement for these systems to safeguard confidential financial data [17] from illegal access that is kept on company computers.

II. LITERATURE SURVEY

Kaithekuzhical Leena Kurien et al. [1], proposed that machine learning methods work well in detecting fraudulent transactions because they have high computing capacity and the ability to handle enormous datasets. With machine and deep learning, a number of real-world issues can be predicted, including email spam, fraud detection, and medical diagnostics. The fact that credit card passwords, CVV numbers, and other crucial data are always vulnerable due to the extensive use of e-commerce and online purchasing was one of the project's biggest setbacks.

Mr. S. Siva Prakash, et al. [2] proposed a way to deal with financial distress; hybrid models were created using clustering and classifier ensemble approaches. Here, classification was accomplished using LOR, MLP, and DT while clustering was accomplished using SOM and k-means methods. The project's two biggest flaws were the absence of secrecy and data protection.

According to a theory proposed by Bavadharani G, et al. [3], the bulk of papers addressing the credit card fraud detection problem makes the unreasonable assumption that the class of each transaction is immediately available for training the model. They intended to research classifiers trained on feedback and delayed supervised samples using adaptive and perhaps nonlinear aggregation approaches. To increase the warning precision even further, a learning-to-rank approach will likely replace the linear aggregation of posterior probabilities.

The random forest method will perform better with more training data, but speed during testing and

application will suffer, according to Devi Meenakshi. B, et al. [4]. They also said that employing more pre-processing methods would be beneficial. Although the results produced by SVM are outstanding, they could have been much better if the data had undergone further pre-processing. The unbalanced dataset issue plagued the SVM algorithm continually, and more preprocessing was required to improve performance.

Besenbruch, et al. [5] explored a number of techniques that could enhance classification accuracy when faced with unbalanced data. The emphasis is on deep learning, distance-based methodologies, and sampling strategies. It included figuring out how to handle data imbalances for each strategy. The most intriguing metrics and methodologies are applied to a fraud dataset in the second section of the paper. Although sampling is effective, the ideal sampling technique is not immediately apparent. Because of this, it is practically impossible to predict in advance which strategy will always be more effective than the other.

Muhammad Zeeshan Younas, et al. [6], paper was to identify and categorize a thorough grasp of the many machine learning approaches for the detection of fraud that are still occurring today in the current day. The accuracy of four machine learning algorithms—Logistic Regression, Multi-

Layer Perceptron, Naive Bayes, and Random Forest—is tested using the credit card fraud detection dataset. Machine learning techniques can help banks increase their performance and reputation in the market.

Stephen Coggeshall, [7], explored the use of statistical and machine learning models to data from linear and nonlinear credit card transactions. In order to identify the transactions that are most likely to be fraudulent, the models that were developed were supervised fraud models. It was shown that when enough trustworthy expert variables are produced, which occurs frequently in practice, the logistic regression model works brilliantly. With more data and variables, the model's performance may surely be improved (for instance, adding a point of sale data, time of day, or other cardholder or merchant information). Any of the models would gain from additional model parameter tuning.

Emmanuel Ileberi, et al. [8], In addition to the Random Forest, Decision tree, Naive bayes, Artificial neural network,and Linear regression, a genetic algorithm-based feature selection technique was also put out. The RF was used in the genetic algorithm's fitness function. Five ideal feature vectors were produced using the genetic algorithm after it was applied to the credit card transactions dataset from European cardholders. Results from this study were better than those from other studies using similar techniques. The use of a smaller amount of dataset was the main negative.

Using pre-processing techniques and algorithms such as support vector machines, KNN, logistic regression, naive bayes, random forests, backpropagation of errors, and gradient boosting, Kartik Madkaikar et al. offered a comparison of accuracy [9]. AdaBoost uses a high-weight observation point to identify its flaws, whereas gradient boosting accomplishes the same task by employing gradients in the loss function. The algorithm known as Gradient Boosting was determined to have the best accuracy.

The investigation and evaluation of Random Forest, AdaBoost, XGBoost, and LightGBM Classifier on skewed credit card fraud data was the main emphasis of Nishant Sharma's work [10]. The results demonstrate that XGBoost Classifier exhibits the highest precision and accuracy in credit card fraud detection using a dataset given by ULB machine learning, according to the results.

In order to identify fraud in the credit card system, Lakshmi S V S S Light, et al. [11] examined algorithms such as logistic regression, decision trees, and random forests. The performance of the suggested system is assessed using sensitivity, specificity, accuracy, and error rate. The decision tree and logistic regression were shown to be inferior to the random forest classifier when the three approaches were compared.

K. Ratna Sree Valli, et al. [12], It has been demonstrated that machine learning applications like Naive Bayes, Logistic Regression, and Random Forest with Boosting are accurate in identifying fraudulent data and reducing the number of false alarms. In terms of the application domain, supervised learning algorithms are provident in this literature. However, this study's limitations prevent us from employing the three aforementioned algorithms to identify the names of fraudulent and

legitimate credit card transactions for the provided dataset.

Pradheepan Raghavan, [13], This study performed an empirical analysis comparing several machine learning and deep learning models on various data sets in order to identify fraudulent transactions.The fact that this work exclusively addresses fraud detection in the context of supervised learning constitutes a drawback. Convolutional neural networks, k-nearest neighbours, and Random Forest have supervised learning techniques that, despite their attractiveness and success in static contexts, do not perform well in dynamic ones.

According to Sadgali, et al. [14], hybrid fraud detection approaches are the most popular since they integrate the advantages of a number of conventional detection techniques. It was shown that not all fraud kinds are suppressed by the research and that each type of fraud has unique limitations. Future work will concentrate on further research into credit card fraud to enhance existing algorithms and incorporate a hybrid model that can handle both the real-time problem and an unbalanced dataset in order to provide a more accurate response during the course of a financial transaction.

Abdulalem Ali, et al. [15] This study sought to uncover machine-learning-based fraud prevention methods used in financial transactions and to analyze research space to find an emerging trend. However, there are still some restrictions and dangers to the validity that can exist. Here, they presented a paper that conducted a thorough analysis and synthesis of the body of work on ML-based fraud detection. The Kitchenham approach was used in this work. To solve this issue, the simple linear regression (SLR) technique has been updated to make sure no crucial terms are omitted.

III.PROPOSED SYSTEM

The provided sign language is fairly distinct, and the pictures are uncluttered and background-free. Additionally, there are a sufficient number of photos, which strengthens our model. The disadvantage is that we would likely require additional data for various challenges in order to properly influence the parameters of our model. This study performed an empirical analysis comparing several machine learning and deep learning models on various data sets in order to identify fraudulent transactions. For example, gesture navigation can benefit from solving this specific classification challenge. The technique we'll use is convolutional neural networks powered by TensorFlow and Keras, deep learning. To avoid gestures, we provide a classification method based on deep learning for sign language. The LeNet convolutional neural network is the technique utilized in the study (CNN).

IV. ARCHITECTURE DESCRIPTION

The goal is to develop a deep learning model based on the convolutional neural network (CNN) method for identifying fraudulent and legitimate credit card transactions. The maximum level of classification accuracy is achieved with this technique.

The most popular neural network type used to solve image processing issues is the convolutional neural network. CNN views information as spatial. Rather than being coupled to every neuron in the layer above, neurons are only connected to those that are nearby and share the same weight. It has a number of layers, mostly for processing pictures.

The input layer, the hidden layer, and the output layer are the three basic layers of our suggested model.

Input Module

The CNN model's input layer accepts a CSV file as input. The dataset includes credit card transactions performed by European cardholders in September 2013. It includes of transactions that took place over the last two days, out of which 492 out of 284,807 transactions were fraudulent. Fraudulent transactions make for 0.172% of all transactions in the severely unbalanced dataset. Only numerical data that have undergone PCA (principal component analysis) processing are contained in it. A common technique for reducing the dimension of huge datasets is the PCA. The specifics of the qualities are kept secret because of concerns about confidentiality. The features V1, V2, ……V28 is the principal components obtained with PCA.The major components found by PCA are V28. Time and amount characteristics are not PCA converted, though. The response variable 'Class' is a feature that accepts 1 in cases of fraud and 0 in all other cases.

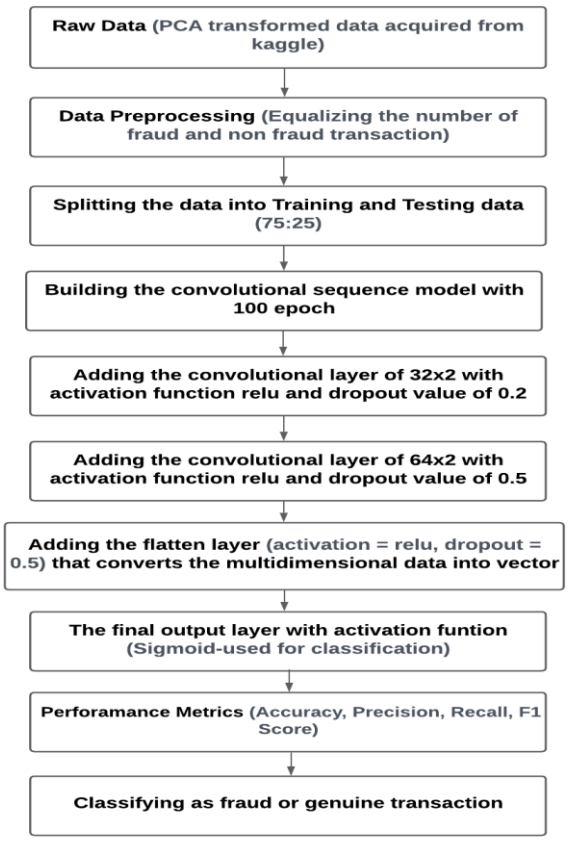

Fig. 1 Architecture Diagram for credit card fraud detection

CNN Module

The hidden layer consists of convolutional layers, an activation function, a dropout layer, and the flatten layer. The convolution layer is used to extract features from our input. It consists of filters (or kernels) that are smaller than the size of the actual image to be convoluted. The activation function used in this model is called Rectified Linear Unit (ReLU). It is one of the most popular linear functions that produces zero if any negative value and returns the same value as it is for positive input. ReLU activation function prevents exponential growth in computation as it does not allow activation of all the neurons at the same time. As for a negative input, it converts the value to zero and does not allow neurons to get activated.

A dropout layer is used to increase the neural network's performance by reducing overfitting problems. This is done by dropping out different neurons from the hidden layer at different rates. Now, the algorithm does not depend on one particular input as it might be dropped out at random. The neurons will not learn redundant details of input and thereby improve the performance of our algorithm. The flatten layer is used to convert our PCA-transformed 2-dimensional input into a single linear vector.

A dropout layer with a dropout rate of 0.2 is added after a convolutional layer with a kernel size of 32 x 2 and a ReLU activation function. Next, we add another convolutional layer with a kernel size of 64 x 2, a ReLUfunction, followed by a dropout layer with a dropout rate of 0.5. The last three layers are a dropout layer with a dropout size of 0.5, a ReLU activation layer, and a flatten layer with a size of 64 x 1.

Output Module

The dense output layer employs the sigmoid activation algorithm. The sigmoid activation function is typically employed in situations where the output provides a probability prediction.Since the outcome of the function ranges between 0 and 1, it can be used to classify if our transaction is fraudulent or genuine. After 100 epochs, the accuracy obtained is 97.15.

V. Machine Learning Module

The objective is to compare different machine learning algorithms and classify an online transaction as fraudulent or genuine. Detecting fake transactions manually is impractical due to the huge amount of data and its complexities. However, this can be done through machine learning models if adequate information is provided. The data collection and pre-processing is the same as the methods used for the convolutional neural network.

Modelling

The ratio of the train and test data is 70:30, with the train data being used to fit the machine learning model and the test data being used to assess the model's fit. We employ a variety of categorizations kinds of algorithms in our suggested model, including:

Decision Tree Classifier

It is a method of supervised machine learning that is applied to classification and regression issues. It comprises of a tree-like structure with a root node that branches out into other nodes to create the tree-like structure. It has leaf nodes, branches, and interior nodes. A dataset's properties are represented

by internal nodes, decisions are represented by branches, and results are represented by leaf nodes. According to Fig.2, the model has 135 true positives.

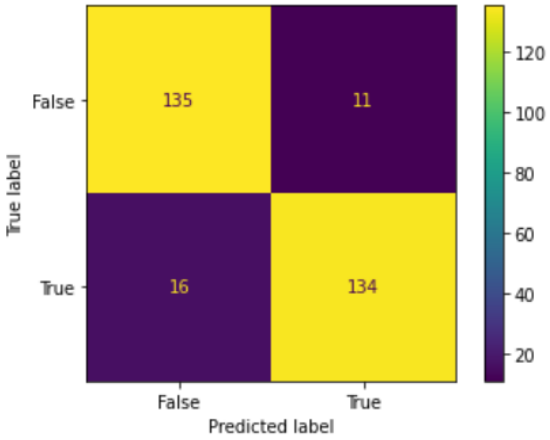

Fig. 2 Confusion matrix of Decision tree Classifier

KNN Classifier

It is a supervised machine learning approach that initially saves all the existing data and categorizes incoming data points based on how closely they resemble the existing data that is currently accessible. So, using the KNN algorithm[18], the new data is assigned to a class that is appropriate. Due to the fact that it does not learn from the current dataset, it is also known as the lazy learner algorithm. Rather, it keeps the dataset on hand until a fresh data point is available for categorization. There are 129 true positives in the model. Seven false positives were detected. Fig.3 describes the confusion matrix for the KNN Classifier.

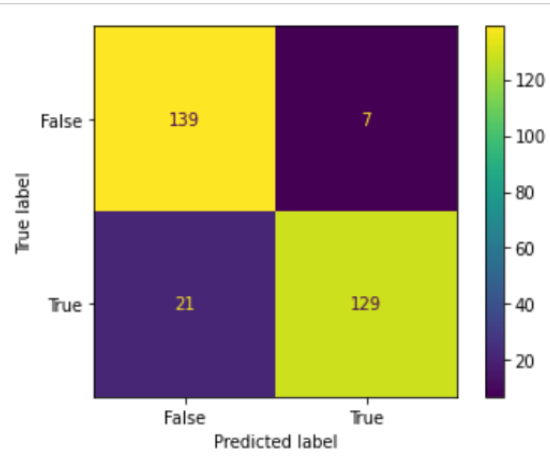

Fig. 3 Confusion matrix of KNN Classifier

Logistic Regression Classifier

To determine the likelihood of a binary event, supervised machine learning is utilized. It generates numbers that fall between 0 and 1 and is used to tackle classification-type challenges. Here, we employ an "S" shaped curve to estimate the probability values that predict two maximum values rather than a linear line (0 and 1). As seen by the confusion matrix in Fig.4, there were 135 genuine positives.

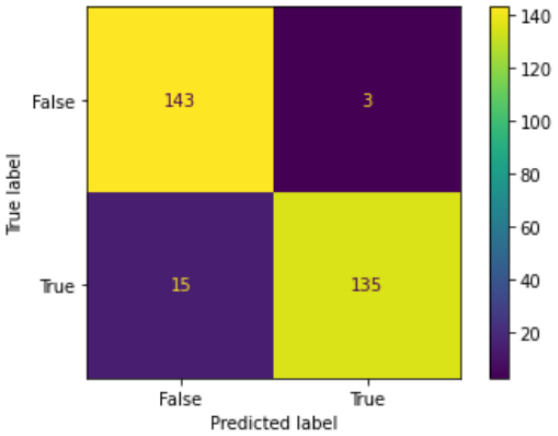

Fig. 4 Confusion matrix of Logistic Regression Classifier

Random Forest Classifier

Random forest is a prominent supervised machine learning technique that is used for handling both regression and classification sorts of problems. The entire dataset is broken up into batches of smaller datasets, and decision trees are then built for each of them. The technique divides the dataset using random sampling, thus the term "random forest." Each decision tree will offer a conclusion after receiving input, and the majority of all conclusions are taken into account before the random forest makes its ultimate judgement. As a result, it offers a high level of precision. Fig.5 describes the Confusion matrix of the Random Forest Classifier with 129 true positives.

Fig. 5 Confusion matrix of Random Forest Classifier

Support Vector Classifier

A well-liked machine learning approach for classification-related issues is the support vector classifier. The basic goal of this approach is to construct a best-fit line that serves as a decision boundary, classifying the data points so that we may later assign a new data point to the appropriate category. The term "Hyperplane" refers to the decision boundary dividing the classes. For the optimum outcome, the Hyperplane is positioned so that it maximizes the margin distance between the neighboring data points. Fig.6 describes the Support Vector Classifier's Confusion matrix.

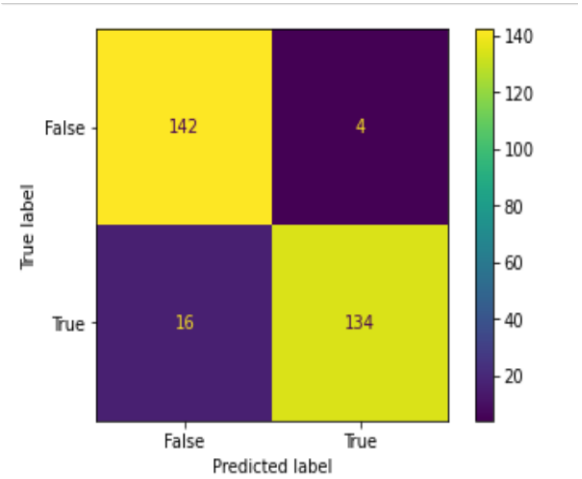

Fig. 6 Confusion matrix of Support Vector Classifier

XG Boost Classifier

Machine learning method XGBoost classifier is mostly used for structured and tabular data. Gradient-boosted decision trees are implemented using XGBoost, a fast and efficient method. Extreme gradient boost is the algorithm used. It is compatible with huge, intricate databases. The decision tree follows a sequential learning chain while boosting. Each split sub-part is taught by its predecessor, and any errors in the current component are fixed before the next sub-part is introduced. Fig.7 details the XG Boost Classifier's Confusion matrix.

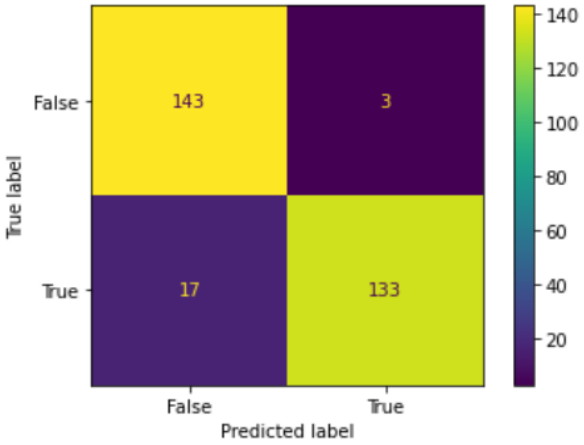

Fig. 7 Confusion matrix of XG Boost Classifier

Performance Analysis

The performance of different algorithms is measured using several performance metrics such as precision, accuracy, recall, and F1 score, and the following results were obtained:

Accuracy

The proportion of accurate forecasts to all other predictions in the model is known as accuracy. It specifies how closely these values resemble the measurement's real value. Fig.8 details the various models' accuracy. The suggested model has a 97.15% accuracy rate.

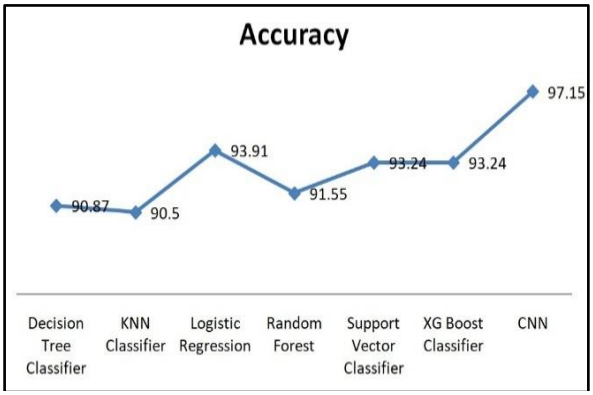

Fig. 8 Accuracy measure of various algorithms used

Recall

Recall is described as the proportion of properly detected genuine positive samples to both true positives and false negative samples. It assists in locating the model's sole pertinent data points. According to Fig.9, the model's recall score is 90.24%.

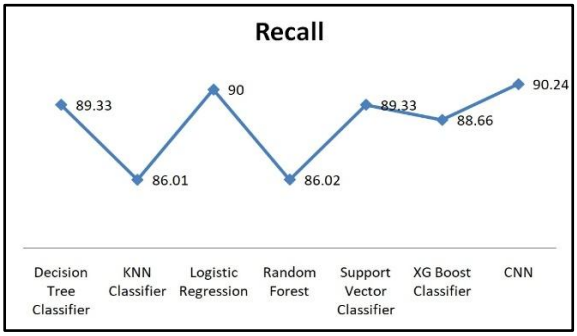

Fig. 9 Recall measure of various algorithms used

F1 Score

F1Score is a machine learning evaluation metric which combines the precision and recall score of the model. It is mainly used when False negatives and False positives are critical. The F1 score of the model is 94.46%.

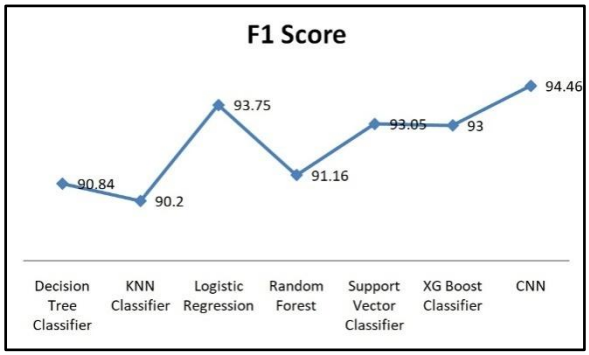

Fig. 10 F1 score of various algorithms used

Precision

It is used to assess how near the projected data points are one to another. It is calculated as the ratio of samples that were positively categorized to all positive samples, including both true positive and true negative samples. The suggested model's accuracy is 99.1%.

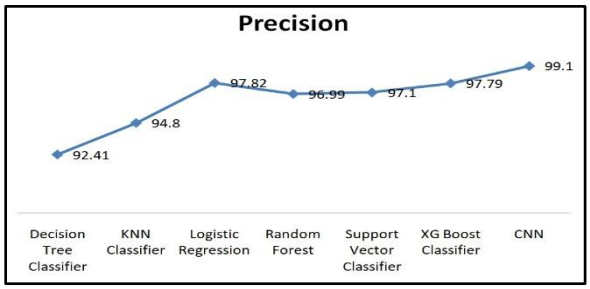

Fig. 11 Precision of various algorithms used

VI. Result

Out of all the machine learning algorithms, we find the convolutional neural network to have the highest accuracy and performance measure and hence is used for credit card fraud detection.

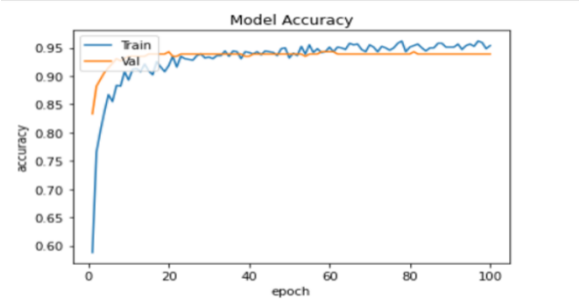

Fig.12 Model Accuracy Graph for CNN

This model uses CNN architecture. In this model, there are two convolutional layers with activation function relu, one flatten layer, and one fully-connected layer. Data is trained using training steps per epoch, total number of epochs, validation data, and validation steps. The model's accuracy in training and testing cases, is shown in Fig. 12. The model's data loss in both the training and testing case are shown in Fig. 13.

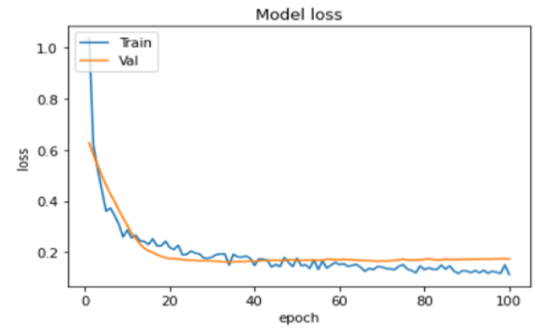

Fig. 13 Model Loss Graph for CNN

VII. Conclusion

The categorization of credit card fraud detection systems utilizing convolutional neural network models was concentrated on training the model with various features that account for the detectability of credit card fraud. This model helps in classifying whether the transaction made by the user is a fraud or not. We employed different techniques of machine learning and CNN and compared and contrasted their performance and saw that CNN makes the better classification among all. The future scope would be to employ different varieties and ranges of the dataset and also to classify the type of credit card fraud being made.

REFERENCES

[1] Kaithekuzhical Leena Kurien, Dr. Ajeet Chikkamannur- "Detection and prevention of credit card fraud transactions using machine learning", 2019.

[2] Mr. S. Siva Prakash, Ahubhakumar, S.Appash, J.Cibiragul- "Credit Card Fraud Detection using Adaboost and Majority Voting", 2019.

[3] Bavadharani. G, Deepika. B, Divya. K, Sathya. R- "Credit Card Fraud Detection using Novel Learning Strategy", 2018.

[4] Devi Meenakshi. B, Janani. B, Gayathri. S, Mrs. Indira. N- "Credit card fraud detection using random forest" 2019.

[5] Jurriaan Besenbruch- "Fraud Detection Using Machine Learning Techniques", 2018.

[6] Muhammad Zeeshan Younas- "Credit Card Fraud Detection using Machine Learning Algorithms", 2021.

[7] Stephen Coggeshall- "Predicting Credit Card Transaction Fraud Using Machine Learning Algorithms", 2019.

[8] Emmanuel Ileberi, Yanxia Sun and Zenghui Wang- "A machine learning based credit card fraud detection using the GA algorithm for feature selection", 2022.

[9] Kartik Madkaikar, Manthan Nagvekar, Preity Parab, Riya Raikar, Supriya Patil- "Credit Card Fraud Detection System", 2021.

[10] Nishant Sharma- "Credit card fraud detection predictive modeling", 2019.

[11] Lakshmi S V S S , Selvani Deepthi Kavila- "Machine Learning For Credit Card Fraud Detection System", 2018.

[12] Andhavarapu Bhanusri- "Credit card fraud detection using Machine learning algorithms", 2020.

[13] Pradheepan Raghavan, "Fraud Detection using Machine Learning and Deep Learning", 2019.

[14] I.Sadgeli , N.Sael , F.Benabbou- "Performance of machine learning techniques in the detection of financial frauds", 2019.

[15] Abdulalem Ali , Shukor Abd Razak , Siti Hajar Othman , Taiseer Abdalla Elfadil Eisa , Arafat Al-Dhaqm , Maged Nasser , Tusneem Elhassan , Hashim Elshafie and Abdu Saif- "Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review", 2022.

[16] Dahee Choi and Kyungho Lee,"An Artificial Intelligence Approach to Financial Fraud Detection under IoT Environment: A Survey and Implementation"(2018).

[17] Zohreh Darbandian, Alimohammad Latif , Sima Emadi "The discovery of the credit card transactions suspicious of fraud using unsupervised data-mining methods (single-link hierarchical clustering)"(2016) International Journal Of Humanities And Cultural Studies ISSN 2356-5926.

[18] E. Ajitha, B. Diwan and M. Roshini, "Lung Cancer Prediction using Extended KNNAlgorithm," 2022 6th International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2022, pp. 1665-1670, doi: 10.1109/ICCMC53470.2022.9753689.