IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Integrating Unsupervised Techniques with Supervised Techniques for CCF Detection

LOKESWARI.G[1]
Department of Computer Science and Engineering,
Srinivasa Ramanujan Institute of Technology (AUTONOMOUS),
B.K. Samudram, Anantapur, Andhra Pradesh, INDIA.
.

ABSTRACT As the usage of credit cards for online transactions has increased, so has the potential for credit card misuse and fraud, which can result in significant financial losses for both cardholders and financial institutions. This research study aims to detect credit card fraud, taking into account the challenges posed by publicly available data, imbalanced datasets, evolving fraud tactics, and high rates of false alarms. The literature review highlights various machine learning-based approaches for credit card fraud detection, including Extreme Learning Method, Decision Tree, Random Forest, Support Vector Machine, Logistic Regression, and XG Boost. An empirical analysis is conducted using the European card benchmark dataset to assess the effectiveness of these approaches. The machine learning algorithm is applied to the dataset, resulting in improved fraud detection accuracy. Further experiments are conducted by varying the number of hidden layers, epochs, and using the latest models, resulting in improved accuracy, f1-score, precision, and AUC curves with optimized values of 99.9%, 85.71%, 93%, and 98%, respectively. The proposed model outperforms advanced machine learning models for credit card fraud detection, even when applied to imbalanced datasets. The proposed approaches can be implemented effectively for real-world credit card fraud detection, including balancing the data to improve detection accuracy.

INDEXTERMS Fraud detection, machine learning, online fraud, credit card frauds, transaction data analysis.

I. INTRODUCTION

Credit card fraud (CCF) refers to the unauthorized use of credit card or account details by someone other than the card owner, resulting in financial losses. CCF can occur when a credit card is lost, stolen, or counterfeited. Card-not-present fraud is also a prevalent form of CCF, particularly with the rise of online shopping.

The expansion of e-banking and online payment systems has resulted in a significant increase in CCF and other types of fraud, leading to annual losses of billions of dollars. Detecting and preventing CCF has become a crucial goal in the digital age of payments.

As a business owner, it is essential to recognize that the future is moving towards a cashless society, where traditional payment methods will no longer suffice. Customers increasingly expect the convenience of debit and credit card payments, and businesses must adapt to meet this demand. In the coming years, the need to accept all forms of payments, including credit cards, will only become more critical [1].

In 2020, around 1.4 million cases of identity theft were reported, out of which 393,207 cases were related to CCF [4]. CCF is currently the second most common type of identity theft, following government documents and benefits fraud [5]. New credit card accounts were used in 365,597 fraud cases in 2020 [10]. The number of reported identity theft cases has increased by 113% from 2019 to 2020, with CCF reports increasing by 44.6% [11]. Payment card theft caused a global loss of $24.26 billion last year, with the United States being the most vulnerable country to credit theft, accounting for 38.6% of reported card fraud losses in 2018.

Therefore, it is crucial for financial institutions to prioritize implementing an automated system for detecting credit card fraud. The objective of supervised CCF detection is to develop a machine learning (ML) model using historical transactional credit card payment data. The model should be able to distinguish between fraudulent and non-fraudulent transactions and use this information to determine whether a new transaction is fraudulent or not. This task involves several critical issues, such as the system's response time, cost-effectiveness, and feature pre-processing. ML is an artificial intelligence field that utilizes computer algorithms to make predictions based on previous data patterns [1].

Machine learning models have been utilized in various studies to address a range of challenges. We investigate the real-world implementation of machine learning. In the case of data categorization problems, the support vector machine (SVM) is a supervised machine learning technique that can be used. It is applied in numerous domains, such as image recognition [13], credit assessment [5], and public safety [12]. SVM is capable of handling both linear and nonlinear binary classification issues, and it identifies a hyperplane that separates the input data in the support vector, making it superior to other classifiers.

This research paper aims to utilize ML algorithms for the detection of fraudulent credit card transactions, making the following significant contributions:

- Use of feature selection algorithms to rank the top features from the CCF transaction dataset to enhance class label predictions.
- Employment of performance evaluation measures such as accuracy, precision, and recall to assess the classifiers' efficiency. The latest credit card dataset is used for experiments.

The paper is organized as follows: Section 2 examines related works. Section 3 provides a detailed description of the proposed model and its methodology. Section 4 describes the dataset and evaluation measures used, along with the analysis and outcomes of tests on a real dataset. Finally, Section 5 concludes the paper.

II. RELATEDWORK

In the domain of CCF detection, various research studies have been conducted. This section highlights different research studies related to CCF detection. Furthermore, we place particular emphasis on research that has addressed fraud detection in the context of class imbalance. Several techniques are employed for CCF detection. Therefore, to examine the most relevant work in this area, the primary approaches can be classified into ML, CCF detection, ensemble and feature ranking, and user authentication approaches [1], [3].

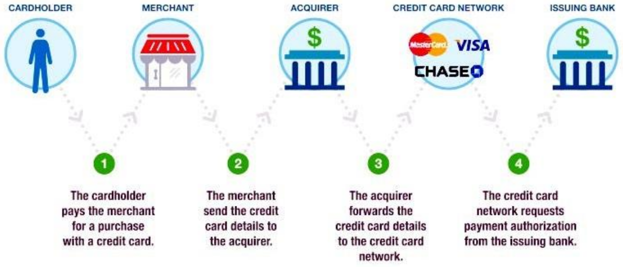

CARDHOLDER
MERCHANT
ACQUIRER
CREDIT CARD NETWORK
ISSUING BANK
MasterCard
VISA
CHASE
1
The cardholder pays the merchant for a purchase with a credit card.
2
The merchant send the credit card details to the acquirer.
3
The acquirer forwards the credit card details to the credit card network.
4
The credit card network requests payment authorization from the issuing bank.

FIGURE1.Paymentcardauthorizationprocess.

Figure 1 illustrates the typical payment card authorization process used for credit card verification. Authentication can be achieved through two methods, namely password-based authentication and biometric-based authentication. Biometric-based authentication can be classified into three categories: physiological authentication, behavioral authentication, and combined authentication [4], [5].

TABLE1.Algorithms of machine learning and their accuracy.

Sr. #			(%)	Reference
1.	The bankcard enrolment records			
2.	Commercial banks in China	SVM		
3.	Records of credit card transactions	Light Gradient Boosting Machine		
4.	Data are collected in the law enforcement department in China			

A. SUPERVISEDMACHINELEARNINGAPPROACHES

Machine learning (ML) has various subfields, each designed to address specific learning tasks. However, there are different types of ML frameworks. For instance, the random forest (RF) approach is commonly used for CCF detection. RF is an ensemble of decision trees [3]. Many researchers use this approach, and it can be combined with network analysis to form the APATE method [1]. CCF detection can be performed using various ML techniques, including supervised and unsupervised learning. Commonly used algorithms for CCF detection include logistic regression (LR), artificial neural networks (ANN), decision trees (DT), support vector machines (SVM), and Naive Bayes (NB). By combining these techniques with ensemble techniques, researchers can build robust detection classifiers [3]. Artificial neural networks involve linking multiple neurons and nodes.

A feed-forward perceptron multilayer contains several layers, including an input layer, an output layer, and one or more hidden layers. The first layer contains input nodes for representing the exploratory variables. The input layers are multiplied with precise weights, and each hidden layer node is transferred with a certain bias, which is added together. An activation function is then applied to create the output of each neuron, which is transferred to the next layer. Finally, the output layer provides the algorithm's response. The weights are adjusted using algorithms such as backpropagation [2], [6]. Bayesian belief networks are graphical models for contingency relationships between a set of variables. Nodes represent variable quantities, and dependencies of conditions between variables are shown as arcs between nodes. Each node's conditional probability table is linked, making the node's variable possibilities conditional on the parent's node values [7], [8]. The bilateral-branch network (BBN) computational system involves finding a construction for the network, which is raised by human experts, and may be conditional on specific algorithms using the data. Once the network topology is determined, the network is fit using antique data in naive Bayes so that the constant variables are also discretized and supposedly distributed normally. In BBN, each node is assumed to be independent of its non-offspring, assuming its maternities in the graph. This is known as the Markov condition [3], [9].

Support vector machines (SVM) are linear classification models used for regression problems. According to the SVM algorithm, the points closest to the line from both classes are found, and these points are called support vectors [10], [11]. This paper focuses on *integrating unsupervised techniques with supervised techniques for CCF detection*. Table 1 provides a summary of machine learning algorithms.

III. RESEARCHMETHODOLOGY

Research is considered systematic, and research methodology is determined by the applied research approach. Applied research is conducted to solve problems. Before conducting real-world experiments, research covers all basics by following these steps:

A. *LIST OF FEATURES OF CREDIT CARD TRANSACTION DATA*

Sr No.	Name of Feature	Description
1	Account number	Related with account number
2	Open to buy	The availability of balance
3	Credit Limit	The maximum amount of credit of the associated account
4	Card number	Number of Credit card
5	Transaction Amount	The transaction amount submitted by the merchant
6	Transaction Time	Time of the transaction
7	Transaction Date	Date of the transaction
8	Transaction Type	Types of Transaction, such as a cash withdrawal and purchase
9	Currency Code	The currency code
10	Merchant Category Code	The Merchant business type code
11	Merchant Number	The merchant reference number
12	Transaction Country	The country where the transaction takes place
13	Transaction City	The city where the transaction takes place
14	Approval Code	The response to the authorisation request, it means approve or reject.

1) EXPERIMENTALSTEP-UP

The experimental setup is a crucial aspect of any research study as it directly influences the accuracy and reliability of the results obtained. A well-designed experimental setup ensures that the study is conducted in a systematic and objective manner, minimizing the potential for errors or bias. In this section, we will review the dataset and performance evaluation metrics that will be used in this study.

a: DESCRIPTION OFDATASET

The dataset used in this study contains transaction data from credit cardholders, and it is obtained from a publicly available source. The dataset consists of a total of 284,807 transactions, out of which 492 are fraudulent transactions. The dataset is highly imbalanced, with only 0.17% of the transactions being fraudulent. Each transaction in the dataset contains 30 numerical input variables that are anonymized, and the only available features are related to time and amount. Therefore, it is challenging to identify the features that are most important in predicting fraudulent transactions.

The dataset is divided into two parts: training data and test data. The training data contains 70% of the total transactions, and the test data contains the remaining 30% of the transactions. The training data is used to train the ML models, and the test data is used to evaluate the performance of the models.

To evaluate the performance of the ML models, several evaluation metrics are used, such as accuracy, precision, recall, F1-score, and area under the receiver operating characteristic curve (AUC-ROC). These metrics are used because of the imbalanced nature of the dataset, and they provide a better understanding of the performance of the models.

Since revealing a consumer's transaction details can pose a confidentiality issue, the majority of the dataset's features are subjected to principal component analysis (PCA), which is a widely used technique in the literature for dimensionality reduction, making the data more interpretable while minimizing information loss [2], [4], [19]. PCA creates new uncorrelated variables that maximize variance, reducing the dataset's complexity. Table 4 displays the dataset's 31 columns, including time, V1, V2, V3, and V28 as features that underwent PCA, the amount, and the class labels.

TABLE4. Characteristicsofthe dataset.

S. No	Feature	Description
1.	Time	Time in seconds to require the lapses between the current transaction and the first transaction
2.	V1, V2, V3……V28 attributes	These 28 columnsshow result of dimensionality reduction to protect user identities and sensitive features.
3.	Amount	Amount of transaction
4.	Class label	Binary class labels 1 and 0for nonfraudulent and fraudulent

b: APPLIED MACHINE LEARNING & ENSEMBLE LEARNING TECHNIQUES

We will implement and utilize the following machine learning and ensemble learning algorithms.

i)Random Feature Method

The Random Feature Method (RFM) is a type of neural network used for various purposes such as classification, clustering, regression, and feature learning. It can have one or multiple layers of hidden nodes, with their parameters being tuned during training. The weights of the output are learned in a single step, which is the minimum required for learning a linear model. For a single hidden layer of ELM, the output function of the j^th node is assumed to be: h(z) = G (p, q, z), where p and q are the parameters of the jth node. The output function satisfies the following equation: Σ αiyi = 0; 0 ≤ α ≤ C, where the sum is over all training examples, y_i is the label of the i^th example, and α is the weight of the jth node.

$$f(z) = \sum_{n} \gamma\, h(z) \quad (1)$$

$$h(z)=\left|^{L} Gh_i(z), \ldots\ldots, {}_{j=1}^{ii} hL(z)\right| \quad (2)$$

ii)DECISIONTREE

A decision tree is a supervised learning algorithm that is mostly used for classification and regression problems. It works by recursively dividing the input data into subsets based on the values of the features. Each internal node in the tree corresponds to a feature, and each leaf node corresponds to a class label. The algorithm selects the best feature to split the data at each internal node based on certain criteria, such as Gini index or entropy. Decision trees can be easily interpreted and visualized, which makes them useful for explaining the reasoning behind classification or regression decisions. They can also handle both categorical and numerical data, and can be combined with ensemble learning techniques to improve their performance. However, decision trees are prone to overfitting, especially when the tree becomes too deep, which can lead to poor generalization on new data.

Consequently, we utilized the decision tree classifier to construct the model, commencing with the decision tree. The parameter for 'max depth' was set to '4' in the algorithm, indicating that the tree could be divided up to four times, and 'entropy' was selected as the 'criterion,' which determines when to halt splitting the tree similar to 'max depth.' Consequently, all necessary installations and storage have been completed.

iii)K-NEARESTNEIGHBOURS(KNN)

Supervised learning refers to a type of machine learning where the desired output or outcome in the training data is known as the target or dependent variable. Moving on to the K-Nearest Neighbors (KNN) algorithm, we create a model using the 'K Neighbors Classifier' model and set the value of k (representing the a PCA nearest neighbors) to '5'. The value of 'neighbors' is chosen arbitrarily, but can be chosen optimally by iterating through a range of values and evaluating the predicted values, which are stored in the 'knn-yhat' variable.

iv)RANDOMFOREST(RF)

Random Forest (RF) is a popular ensemble learning technique that can be used for classification and regression tasks. It involves building multiple decision trees and combining their predictions to improve accuracy and reduce overfitting. RF is particularly effective at learning complex, non-linear relationships in data.

To build an RF model, we start by selecting a random subset of the training data and a random subset of the features for each tree in the forest. This process is called bagging, and it helps to reduce variance and prevent overfitting. Each tree is grown to the maximum depth allowed, and the prediction for a new data point is based on the average prediction of all the trees in the forest.

The RF algorithm can be summarized as follows: given a training dataset with inputs (p = p1, ..., pn) and corresponding outputs (Q = q1, ..., qn), and a bagging parameter X, the following steps are performed for each tree in the forest:

1. Randomly select a subset of the input features.
2. Randomly select a subset of the training data with replacement.
3. Grow a decision tree using the selected features and data subset.
4. Repeat steps 1-3 for X trees.
5. To predict the output for a new data point, take the average prediction of all X trees.

v)SUPPORTVECTORMACHINE(SVM)

The SVM algorithm performs well in text classification. It separates positive and negative instances using high margins and has been shown to produce better results than naive Bayes in previous studies on fraud detection. The SVM uses a decision surface to divide training points into two categories based on support vectors. The optimization is computed as follows:

vi)LOGISTICREGRESSION

Logistic regression is a simple algorithm that estimates the relationship between a dependent binary variable and independent variables, calculating the probability of an event occurrence. The regularization parameter 'C' balances the trade-off between increasing complexity (overfitting) and maintaining a simple model (underfitting). A high value of 'C' reduces the power of regularization, increasing the model complexity and causing overfitting. 'C' is tuned using Randomized Search CV () for different datasets: the original, standardized, and feature-selected datasets. Once 'C' is defined, the logistic regression model is initialized and fitted to the training data, as described in the methodology. The logistic regression hypothesis function is defined as hθ (x) = g (θ T x) (6), where the function g(z) is the sigmoid function. The logistic regression hypothesis function can be written as h (x :) = 1 / (1 + e^-θTx), where θ (theta) is a vector of parameters that the model calculates to fit the classifier.

vii)XGBOOST

The ensemble ML technique based on decision trees is known as XG Boost, which utilizes a gradient boosting framework. Hence, when dealing with unstructured data in prediction problems such as text, artificial neural networks generally outperform all other frameworks or algorithms. The XG Boost model for classification is referred to as the XGB Classifier, which can be fitted to our training dataset. The model is fitted using the sci-kit-learn API and the model's fit() function, and parameters for training the model can be provided to the model in the constructor. We are currently using default parameters. →vj, →vk

d: BENCHMARKING METRICS

Conventional techniques for evaluating ML classifiers involve using confusion matrices to assess the dissimilarity between the actual ground truth of the dataset and the model's forecast. Here, TP (true positive), TN (true negative), FP (false-positive), and FN (false-negative) are employed to represent the different outcomes.

i) ACCURACY

Precision is used to evaluate the performance of the data recovery and processing in the evidence domain. It represents the fraction of the correctly classified positive instances out of all the instances classified as positive. It can be calculated using equation (9) as follows:

$$Accuracy = \frac{TP+TN}{TP+FP+TN+FN}$$

Precision is a performance assessment that measures the ratio of correctly identified positives and the total number

$$Precision = \frac{TP}{TP+FP}$$

iii) F-MEASURE/F1-SCORE

The f-measure considers both the precision and the recall. The f-measure may be assumed to be the average weight of all values, which can be seen as follows:

B.TOP 10 ALGORITHMS IN MACHINE LEARNING FOR FRAUDDETECTION

In the study [3], the top ten ML algorithms are incorporated for the detection of credit card frauds. The list of these algorithms is given below:

a. LinearRegression
b. LogisticRegression
c. DecisionTree
d. SVM
e. Naïve Bayes
f. CNN
g. K-Means
h. Random Forest
i. DimensionalityReductionAlgorithms
j. GradientBoostingAlgorithms

Thesealgorithmscanalsoencompassassociationanalysis,

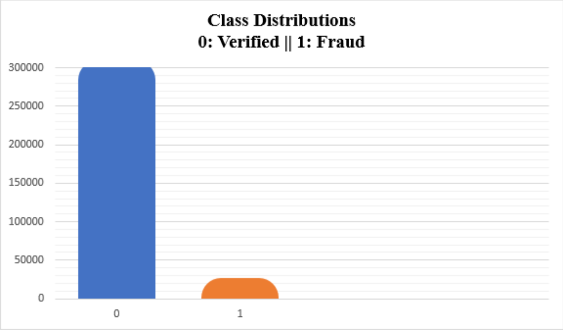


FIGURE5. Classdistributionoffraudulentandnonfraudtransactions.

Another observation regarding the data is that it does not contain any null or missing values, and therefore there is no requirement to impute them.

ii) PRECISIO(N9)

of identified positives. This can be seen as follows:

(10)

iv) RECALL

$$F = 2X\ precision \times Recall\ precision + Recall$$

(11)

ML research and development cover various crucial topics such as clustering, classification, statistical learning, and link analysis.

The recall is also known as sensitivity, representing the proportion of relevant instances retrieved over the total number of instances that are actually relevant and can be defined as follows:

THE CONFUSION METRICS FOR MODELS

A visualization for evaluating a classification model is a confusion matrix that illustrates how well the model is expected to perform based on the predicted results compared to the actual results.

$$\text{Recall} = \frac{\text{TP}}{\quad}$$

IV

A.

(1

T

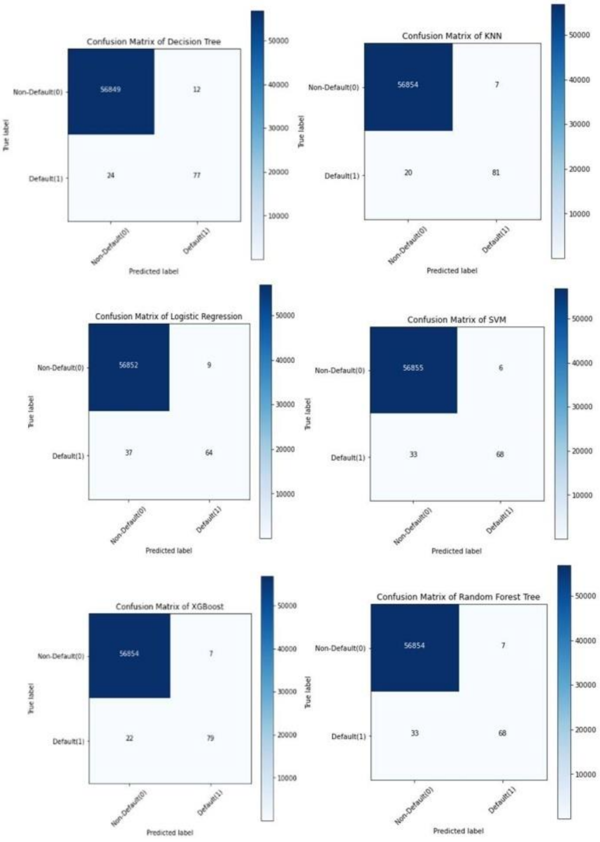


FIGURE6. Confusion metrics of machine learning algorithms.

Often, the expected results are stored in a variable, which is then transformed into a contingency table. Using the contingency table in the form of a heatmap, the performance metrics can be visualized. While there are several built-in methods for visualizing performance metrics, we can define and visualize them based on the threshold to allow for better comparison. Figure 6 illustrates the performance metrics of machine learning algorithms. The dataset consists of credit card transactions made by European cardholders in October 2018. The dataset covers transactions that occurred in two days, and it includes 492 instances of fraud out of 284,807 transactions. It includes only numerical input variables, which are the result of a PCA transformation. Due to privacy issues, we cannot provide the original dataset's details and additional information on the data. The feature 'Time' represents the number of seconds elapsed between the first transaction in the dataset and each transaction. Figure 5 depicts the distribution of the CCF dataset into fraudulent and non-fraudulent transactions.

1) THE ACCURACY OF MACHINE LEARNING ALGORITHMS

In this stage, we construct six different types of classification models. While there are other models available to address classification problems, these are the most commonly used ones. All of these models can be implemented effectively using algorithms provided by the sci-kit-learn library. Table 5 presents the outcomes of the ML algorithms applied.

TABLE5. TheaccuracyandF1-socreofmachinelearningalgorithms.

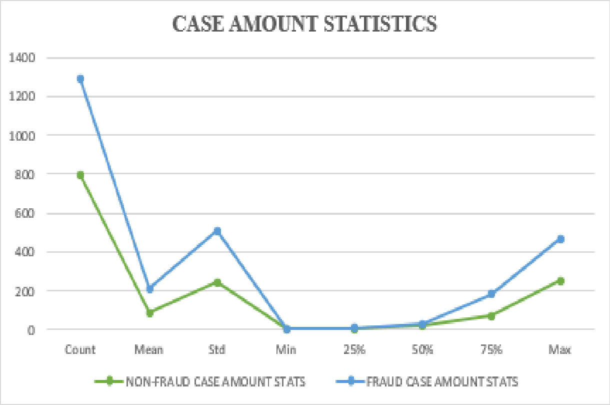
Sr No	Algorithm Name	Accuracy Score (%)	F1 Score (%)
1.	Decision tree algorithm	99.93	81.05
2.	KNN algorithm	99.95	85.71
3.		99.91	73.56
4.		99.93	77.71
5.	Random forest tree algorithm	99.92	77.27
6.	XG Boost	99.94	84.49

2) RESULT OF THE CASE AMOUNT STATISTICS OF THE DATASET

As illustrated in Figure 7, the number of cases, the values of the 'Amount' feature show significant variation compared to the rest of the features. To mitigate the impact of this disparity, we can normalize the values using the "Standard Scaler" method in Python.

3) THE COMPARATIVE ANALYSIS OF MACHINE LEARNING ALGORITHMS

Figure 8 displays a comparative analysis of the machine learning algorithms applied to the CCF dataset, using accuracy and F1 score as evaluation metrics.



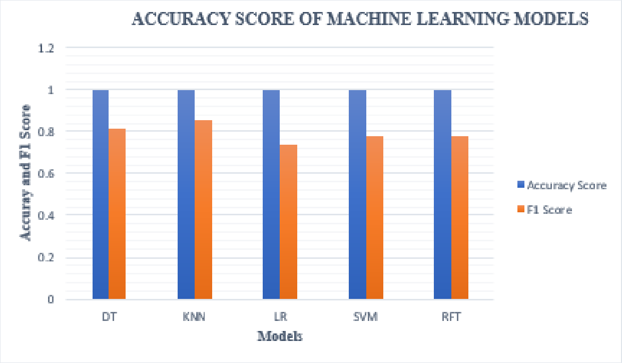


FIGURE7. The case count statistics for fraud and non-fraud transactions.

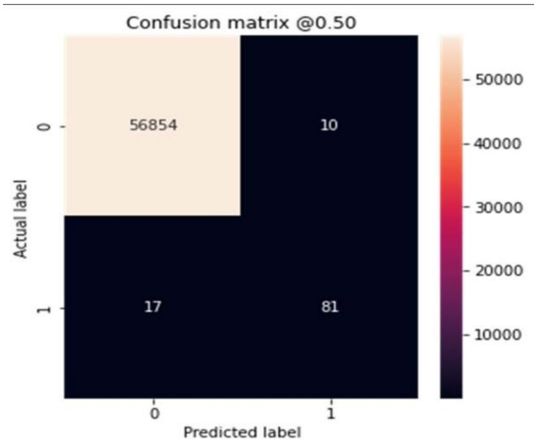
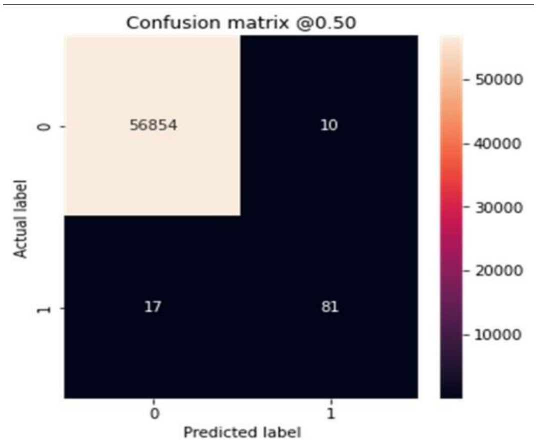


FIGURE8. Comparative analysis of machine learning algorithms.



V. CONCLUSION

Credit card fraud (CCF) is a growing concern for financial organizations, as fraudsters continue to devise new methods to deceive the system. To effectively combat CCF, a robust classifier that can adapt to evolving fraud techniques is crucial. The top priority for a fraud detection system is accurately identifying fraudulent cases while minimizing false positives. The effectiveness of various ML methods varies depending on the specific business case. The performance of a model is largely influenced by the type and amount of input data, such as the number of features, transactions, and correlations between features.

REFERENCES

[1] Y. Abakarim, M. Lahby, and A. Attioui, ‘‘An efficient real time modelforcreditcardfrauddetectionbasedondeeplearning,’’in*Proc.12thInt. Conf. Intell. Systems: Theories Appl.*, Oct. 2018, pp. 1–7, doi:10.1145/3289402.3289530.

[2] H.AbdiandL.J.Williams,‘‘Principalcomponentanalysis,’’*WileyInter-discipl. Rev., Comput. Statist.*, vol. 2, no. 4, pp.433–459, Jul. 2010, doi:10.1002/wics.101.

[3] V. Arora, R. S. Leekha, K. Lee, and A. Kataria, ‘‘Facilitating userauthorization from imbalanced data logs of credit cards using artificialintelligence,’’ *Mobile Inf. Syst.*, vol. 2020, pp.1–13, Oct. 2020, doi:10.1155/2020/8885269.

[4] A.O.Balogun,S.Basri,S.J.Abdulkadir,andA.S.Hashim,‘‘Performanceanalysis of feature selection methods in software defect prediction: Asearch method approach,’’ *Appl. Sci.*, vol. 9, no. 13, p.2764, Jul. 2019,doi:10.3390/app9132764.

[5] B. Bandaranayake, ‘‘Fraud and corruption control at education systemlevel: A case study of the Victorian department of education and earlychildhooddevelopmentinAustralia,’’*J.CasesEduc. Leadership*,vol.17,no. 4, pp. 34–53, Dec. 2014, doi: 10.1177/1555458914549669.

[6] J.Błaszczyński,A.T.deAlmeidaFilho,A.Matuszyk,M.Szelg,,and R.Słowiński,‘‘Autoloanfrauddetectionusingdominance-basedroughsetapproachversusmachinelearningmethods,’’*ExpertSyst.Appl.*,vol.163,Jan. 2021, Art. no. 113740, doi: 10.1016/j.eswa.2020.113740.

[7] B.Branco,P.Abreu, A.S.Gomes,M.S.C.Almeida,J.T.Ascensão,andP.Bizarro,‘‘InterleavedsequenceRNNsforfrauddetection,’’in*Proc.26thACMSIGKDDInt.Conf.Knowl.DiscoveryDataMining*,2020, pp.3101–3109,doi:10.1145/3394486.3403361.

[8] F.Cartella,O.Anunciacao,Y.Funabiki,D.Yamaguchi,T.Akishita,and O. Elshocht, ‘‘Adversarial attacks for tabular data: Application to frauddetection and imbalanced data,’’ 2021, *arXiv:2101.08030*.

[9] S. S. Lad, I. Dept. of CSERajarambapu Institute of TechnologyRa-jaramnagarSangliMaharashtra, and A. C. Adamuthe, ‘‘Malware classificationwithimprovedconvolutionalneuralnetworkmodel,’’*Int. J.Comput.Netw.Inf.Secur.*,vol.12,no.6,pp.30–43,Dec.2021,doi:10.5815/ijcnis.2020.06.03.

[10] V. N. Dornadula and S. Geetha, ‘‘Credit card fraud detection using machinelearning algorithms,’’ *Proc. Comput. Sci.*, vol. 165, pp.631–641, Jan. 2019,doi:10.1016/j.procs.2020.01.057.

[11] K. He, X. Zhang, S. Ren, and J. Sun, ‘‘Deep residual learning for imagerecognition,’’ 2015, *arXiv:1512.03385*.

[11] X. Hu, H. Chen, and R. Zhang, ‘‘Short paper: Credit card fraud detectionusingLightGBMwithasymmetricerrorcontrol,’’in*Proc. 2ndInt. Conf. Artif. Intell. for Industries (AII)*, Sep. 2019, pp. 91–94, doi:10.1109/AI4I46381.2019.00030.

[12] J.Kim,H.-Kim,andH.Kim,‘‘Frauddetectionforjobplacementusing hierarchicalclusters-baseddeepneuralnetworks,’’*Int. J. SpeechTechnol.*,vol.49,no.8,pp.2842–2861,Aug.2019,doi:10.1007/s10489-019-01419-2.

[13] M.-J. Kim and T.-S. Kim, ‘‘A neural classifier with fraud density map foreffectivecreditcardfrauddetection,’’in*IntelligentData EngineeringandAutomatedLearning*,vol.2412,H.Yin,N. Allinson,R.Freeman,J.Keane,and S. Hubbard, Eds. Berlin, Germany: Springer, 2002, pp. 378–383, doi:10.1007/3-540-45675-9_56.

[14] R.F.LimaandA.Pereira,‘‘Featureselectionapproachesto frauddetectionin e-payment systems,’’ in *E-Commerce and Web Technologies*, vol. 278, D. Bridge and H. Stuckenschmidt, Eds. Springer, 2017, pp. 111–126, doi:10.1007/978-3-319-53676-7_9.

[15] H.Najadat,O.Altiti,A.A.Aqouleh,andM.Younes,‘‘Creditcardfrauddetectionbasedonmachineanddeeplearning,’’in*Proc.11thInt. Conf. Inf. Commun. Syst. (ICICS)*, Apr. 2020, pp.204–208, doi:10.1109/ICICS49469.2020.239524.