Human-Centric Intelligent Systems (2022) 2:55–68
https://doi.org/10.1007/s44230-022-00004-0

REVIEW ARTICLE

Review of Machine Learning Approach on Credit Card Fraud Detection

Rejwan Bin Sulaiman[1] · **Vitaly Schetinin**[1] · **Paul Sant**[1]

Received: 25 November 2021 / Accepted: 28 March 2022 / Published online: 5 May 2022

Abstract
Massive usage of credit cards has caused an escalation of fraud. Usage of credit cards has resulted in the growth of online business advancement and ease of the e-payment system. The use of machine learning (methods) are adapted on a larger scale to detect and prevent fraud. ML algorithms play an essential role in analysing customer data. In this research article, we have conducted a comparative analysis of the literature review considering the ML techniques for credit card fraud detection (CCFD) and data confidentiality. In the end, we have proposed a hybrid solution, using the neural network (ANN) in a federated learning framework. It has been observed as an effective solution for achieving higher accuracy in CCFD while ensuring privacy.

Keywords Artificial neural network (ANN) · Credit card fraud · Federated learning · Random forest (RF) method · Support vector machine (SVM) · Privacy-preserving · Blockchain

1 Introduction

In the twenty-first century, most financial institutions have increasingly made business facilities available for the public through internet banking. E-payment methods play an imperative role in today's competitive financial society. They have made purchasing goods and services very convenient. Financial institutions often provide customers with cards that make their lives convenient as they go shopping without carrying cash. Other than debit cards the credit cards are also beneficial to consumers because it protects them against purchased goods that might be damaged, lost or even stolen. Customers are required to verify the transaction with the merchant before carrying out any transaction using their credit card.

According to statistics, Visa [50] and Mastercard [51] issued 2287 million total credit cards during 2020 (4th quarter) worldwide (Figs. 1 and 2).

✉ Rejwan Bin Sulaiman
rejwan.binsulaiman@study.beds.ac.uk

Vitaly Schetinin
vitaly.schetinin@beds.ac.uk

Paul Sant
paul.sant@beds.ac.uk

[1] University of Bedfordshire, Luton, UK

Visa issued 1131 million, whereas master card issued 1156 million cards worldwide. These statistics show how the usage of card-based transactions became easy and famous to the end-users. Fraudsters pave their way to manipulate this group of people due to the massive portion of global transactions falling in this category. And perhaps sometimes it is easy to social engineer humans easily.

Despite the several benefits that credit cards provide to consumers, they are also associated with problems such as security and fraud. Credit card fraud is considered a challenge which banks and financial institutions are facing. It occurs when unapproved individuals use credit cards for gaining money or property using fraudulent means. Credit card information is sensitive to be stolen via online platforms and web pages that are unsecured. They can also be obtained from identity theft schemes. Fraudsters can access the credit and debit card numbers of users illegitimately without their consent and knowledge.

According to "U.K. finance" [27], fraudulent activities associated with credit and debit cards have proven to be one of the major causes of financial losses in the finance industry. Due to the advancement of technology, it is big threat that leads to massive loss of finances globally. Therefore, it is imperative to carry out credit card fraud detection to reduce financial losses.

Machine learning is effective in determining which transactions are fraudulent and those that are legitimate. One of the main challenges associated with detection techniques is

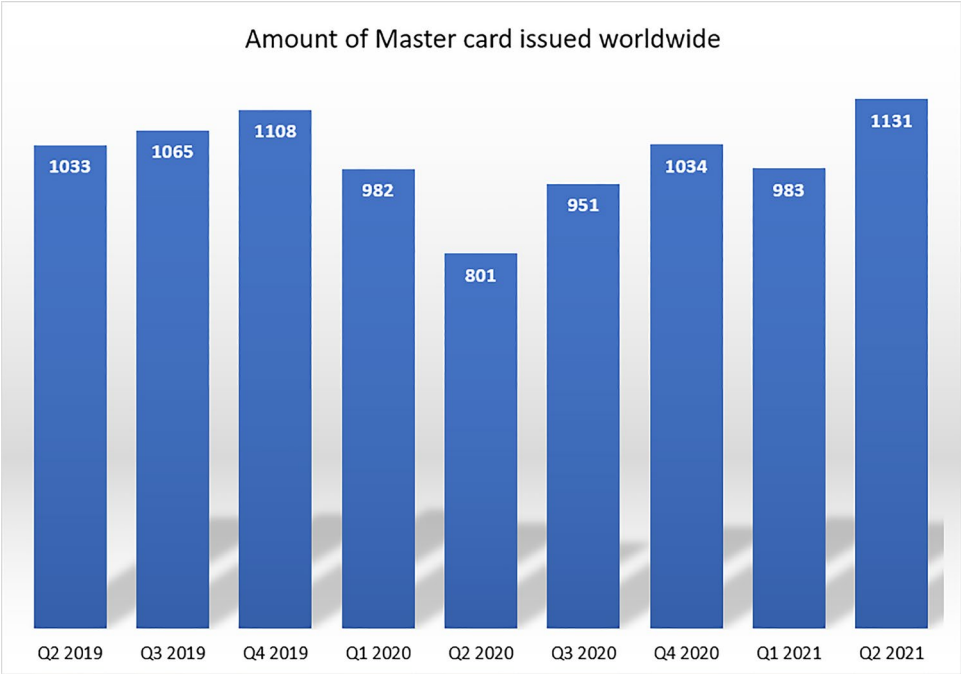

Fig. 1 Amount of Master credit card issued worldwide [51]

Fig. 2 Amount of Visa credit issued worldwide [50]

the barrier to exchanging ideas related to fraud detection. According to a study by "U.K. finance", the number of credit and debit fraud cases reported in the U.K. worth £574.2 million in 2020 [27].

In recent years, fraud detection in credit card has increased tremendously, drawing the attention of most scholars and researchers [22]. This research paper seeks to review and evaluate various aspects of credit and debit fraud detection. The paper examines various techniques used to detect fraudulent credit card transactions and finally proposes a better technique for credit card fraud. Researchers are trying to solve some methodological barriers that pose a limitation in ML real-time application. Various research has been done in different domains such as abnormal patterns detection [28–35], biometric identification [36, 37], Diabetes Prediction [38, 39], Happiness prediction [40], Water quality prediction [41], accident prevention at Heathrow [42], timely diagnosis of bone

diseases [43], Predicting informational efficiency using deep Neural Network [49]. Despite these limitations, researchers are working to gain the ML power to detect frauds.

1.1 Motivation

CCFD involves quite complex procedures and techniques for developing an effective detection system. Following are some of the problems in CCFD that I have analyzed from the literature review, and it has motivated me to propose an effective solution to the problems.

Credit card transactions are substantial in number and are heterogeneous. The users use the credit cards for various purposes based on geographical locations and currencies, which shows that the fraudulent transactions are widely diverse [10]. This problem has motivated me to devise a solution that can potentially help to detect the fraudulent transaction irrespective of geographical location. Fraud detection is also a multi-objective task. Banks and financial institutions need to give their users a good experience and service at all times. Therefore, it is challenging to use the customer datasets for experimental purposes while ensuring service availability and privacy. To compensate this challenge, my motivation leads to introduce the framework of federated learning for data privacy assurance.

Fraudulent transaction diversity and imbalanced datasets is also a big challenge in CCFD [22]. Getting real-time datasets of credit card transactions is quite challenging. Banks and financial sectors do not expose their customer's data due to GDPR. Therefore, it creates a challenge for the researchers to gather the datasets for credit card fraud detection. My motivation leads to helping research communities and data scientist who work in the financial sector to devise a system to fulfil the challenges of getting big data for an effective machine learning model.

2 Literature Review

It is imperative for any banking or financial institution that issues credit and debit cards to put in place an effective measure to detect any cases of fraudulent transactions. Some of the notable methods identified to help detect fraud in credit card that includes RF, ANN, SVM, k-nearest neighbors and other techniques that have a hybrid and privacy-preserving approach for data privacy.

We will discuss in brief all the approaches mentioned above.

2.1 Random Forest (R.F.)

Random forest is an algorithm based on ML which is constructed from a decision tree (DT) algorithm, commonly used to resolve various regression and classification problems. It helps in predicting output with high accuracy in large datasets. The Random Forest technique combines several classifiers to provide a solution to different intricate issues. The random forest helps in predicting the average mean of output from other trees. An increase in the number of trees tends to increase the precision of the outcome. The random forest method helps in eradicating various limitations of a decision tree algorithm [8]. It also minimizes the lifting of datasets and thus increasing precision. Several decision trees exist in a forest whereby a individual tree act as weak-learner; however, they together form strong learner. The RF technique is high-speed and effective in handling large volumes of datasets and unbalanced ones. However, the random forest has limitations in training the range of datasets, especially in the regression problems.

The various traditional algorithm was used, such as Logistic regression (L.R.), C4,5, and R.F. Logistic regression (L.R.) describes and explains the association between the dependent binary variable and independent variable. The C4.5 is commonly considered for data mining as DT classifiers in generating decisions based on various sets of data provided. Traditionally, the algorithm combined Threshold optimization (T) as well as Baye's Minimum Risk Classifiers (M.R.) were used in fraudulent grouping transactions by altering the prospect of the limit. T and M.R. improve predictions' accuracy and reduce the overall cost involved [11]. However, logistic regression performs well in the regression problem, as it tolerates the model overfitting, unlike the decision tree. Also, there is a significantly less real-time scenario of having linear problems. When considering the CCFD, the real-time datasets are nonlinear. Therefore, the use of logistic regression is not suitable to be considered.

Olena et al. have proposed a hybrid approach for credit card fraud detection using random forest and isolation forest, which is used to identify anomaly-based transactions [15].The proposed model of the author is based on two primary sub-systems. One of them is concerned about anomaly detection that works based on unsupervised learning. The second one is an interpretation that incorporates the anomalies type. It is based on supervised learning. The proposed work's primary concern is the data speed that works effectively when considered with the hybrid model on the real-time data [15, 16]. The system was evaluated for identifying the users' geolocation while performing transactions for detection purpose. This hybrid model is not based on the anomaly level. However, the anomaly type determines it. The system of anomaly-based transactions detects fraud,

based on geolocation. However, preserving privacy and confidentiality is a lack of finding in this research work, as the real-time data is involved in detecting the fraudulent transaction. The researcher did not mention any hashing, or encrypted methods followed to keep user's data from being exposed. Therefore, to comply with this challenge, there is a need to ensure data confidentiality for the credit card users for the research purpose. The researcher also did not mention how to tackle geolocation spoofing techniques to prevent fraud. Our contribution will be focused on considering the geolocation and time features for detecting frauds combining ANN and federated learning approach to ensure data confidentiality.

Although the random forest algorithms are quite effective in predicting the class of regression problems, they constitute various limitations when it comes to the CCFD in real-time. It can perform well on lab-based datasets where limited data is available. The random forest algorithms are slower in performance in real-time scenarios. The training process is slower, and it takes a longer time to make predictions. Therefore, for effective CCFD in real-life datasets, we need a large volume of data, and random forest algorithms lack the capability of training the datasets effectively and making predictions.

2.2 Artificial Neural Network (ANN) Method

ANN is a ML algorithm which functions similarly to the human brain. Typically, ANN is based on two types of methods: supervised method and unsupervised method. The Unsupervised Neural Network is widely used in detecting fraud cases since it has an accuracy rate of 95%[4]. The unsupervised neural network attempts to find similar patterns between the credit cardholders present and those found in earlier transactions. Suppose the details found in the current transactions are correlated with the previous transactions. Then, a fraud case is likely to be detected [4]. ANN methods are highly fault tolerant. For instance, the generation of output is sustained even with the corruption in single or multiple cells. Due to its high speed and effective processing capabilities, ANN can be considered an effective solution for the CCFD.

The author used three stages in detecting fraud; verifying the user, fuzzy clustering algorithm, and ANN classification phase to differentiate between legitimate and suspicious transactions. This technique helped generate an accuracy rate of 93.90 and 6.10% in classifying transactions incorrectly [7]. Although ANN, along with the clustering, performs well in detecting fraudulent transactions, the author failed to consider the appropriate structure of ANN that requires progressive trials and errors.

An artificial neural network that is trained using a simulated annealing algorithm is effective in identifying various fraudulent credit card transactions. The stimulation annealing algorithm optimizes the performance by finding out the best suitable configuration weight in the neural network [10].

Saurabh et al. have proposed a model based on the artificial neural network (ANN) [17] and backpropagation for credit card fraud detection [17, 18]. The procedure is followed by taking the customers' dataset, i.e., name, transaction ID and time. With 80% of data for training, the author experimented, 20% of the data is taken for testing and validation purpose. The proposed model has given a significant outcome for the detection of fraudulent transactions in real-time data. For the evaluation purpose, authors have used confusion matrix, recall, accuracy, and precision. By performing this experiment, the achieved accuracy is 99.96% which is enhanced compared to the previous model while considering the real-time data. Although it has produced good results; however, for training and researching, this research work lacks the potential solution of data threat by the researcher or even by an individual bank employee. Therefore, it is required to have a solution that can potentially fulfil all the criteria for data confidentiality and integrity of the bank credit card transactions. The authors have not mentioned anything about data confidentiality while using it for training like name, age and gender. Therefore, our proposed work will use a federated learning model to ensure data privacy to train it for credit card fraud detection.

Data mining techniques such as the DT, MLP, and CFLANN are widely considered to determine patterns from the previous transaction. These models often use two types of datasets in comparing the performance. The Multiple-layer perception (MLP) model has an accuracy of 88.95% in the Australian-credit card dataset [Class Distribution: CLASS 2: +: 307 (44.5%), CLASS 1 383 (55.5%)] and 78.50% in the German-credit card dataset [24]. which gives the indication that the MLP perform differently in a different dataset. The use of MLP could not be very effective in CCFD as reason been having a larger number of parameters, and it causes the highly dense structure that ultimately results in redundancy and performance inefficiency. The author did not highlight this concern which is essential to consider to use the MLP process in real-time.

ANN is an effective algorithm that can be used in CCFD [4, 7, 10]. It can be seen from the literature; it has produced good performance when used in congestion with various functions and algorithms. Those functions have their individual lacking. However, the use of ANN in CCFD is proven to be promising due to its capability

to accommodate a larger volume of data and distributed memory structure.

2.3 Support Vector Machine (SVM)

SVM is considered for classification and carry out regression analysis for various problem. In this approach, researchers often analyze the patterns in which customers use credit cards. The paying patterns of the customers were collected from the datasets. The support vector machine technique is used in classifying consumer patterns into either fraudulent or non-fraudulent transactions. The SVM method is effective, and it provides accurate results when fewer features have been used from the dataset [5]. However, the problem exists when a larger volume of datasets (at least over 100,000) is used. While considering the use of SVM in CCFD, it is ineffective when used in real-time as the size of datasets are large.

Rtayli et al. have proposed a method for credit card fraud risk (CCR) for the higher dimensionality data by using the classification technique of random forest classifier (RFC) [27] and SVM [26, 27], in a hybrid approach. The idea was inspired by the feature selection of fraudulent transactions in the big imbalanced dataset. The fraud transactions are minimal in number and become difficult for detection. To evaluate the model, the author has used evaluation metrics that comprise accuracy, recall and area under the curve.

Based on SVM while using RFC suggested that it has produced the accuracy of 95%, false-positive transactions are decreased by improving the sensitively to 87% which has caused the better fraud detection in the massive dataset and imbalanced data [26, 27]. This model has also improved the classification performance. Although the method produced efficient corresponding output for fraud detection while using classification features, this model limits the transaction's privacy in term of performing the evaluation metrics of accuracy and recall. Therefore, to fix privacy concern, we are using a federated learning model that trains data locally. We are also combining it with artificial neural network. RFC performs slow when dealing with large datasets.

2.4 K-Nearest Neighbour (KNN)

KNN is type of supervised ML method helpful in classifying and performing regression analysis on problems. It is an effective method in supervised learning. It helps in improving the detection and decreasing false-alarm rate. It uses a supervised technique in establishing the presence of fraudulent activity in credit card transactions [14]. The KNN fraud detection technique requires two estimates: correlation of transaction and distance between the occurrence of transaction in data. The KNN technique is suitable for detecting fraudulent activity during transaction time. By performing over-sampling and separating data, it can be possibly used to determine the anomalies in the targets. Therefore, it can be considered for CCFD in memory limitations. It can assist in CCFD while utilizing low memory and less computation power. It is a faster approach for any number of datasets. While comparing with other anomaly-based techniques, KNN results higher in accuracy and efficiency [12].

It is widely used in identifying a similar pattern in previous transactions carried out by the cardholder. The commonly used machine learning algorithms include LR, Naïve Bayes and KNN. The KNN has an accuracy rate of 97.69% when it comes to the detection of fraudulent transactions in Credit card [13]. It has produced optimum performance KNN is proven to be efficient in performance with respect to all metrics been used, as it didn't record any false-positive while classifying. Another study was performed using KNN, where 72% accuracy was achieved for CCFD [12].

Although the authors conducted progressive tests while utilizing KNN, it is critical to note the algorithm's limitations. KNN is a memory-intensive algorithm that scales up non-essential data characteristics. It likewise falls short in the experiments cited above. When the algorithm is fed a large amount of data, the performance of the KNN algorithm degrades. As a result, these constraints have an effect on the accuracy and recall matrix in the CCFD process.

2.5 Hybrid Approach

The procedures for CCFD are now replaced by the ML techniques that have resulted in higher efficiency. One of the research teams has proposed a method that involves loan fraud detection while using the ML in credit card transactions [44]. The process was experimented with by using the Extreme Gradient Boosting (XGBoost) algorithm with other data mining procedures that have produced optimal results in CCFD. The research work was followed by keeping the valuable information without having knowledge about it.

To achieve the research targets, the authors have used a hybrid technique of supervised and unsupervised ML algorithms. In this procedure, PK-XGBoost and XGBoost were used. While observing the performance, PK-XGBoost has performed better in comparison with simple XGBoost [45, 46]. The performance metric keeps the higher efficiency in detecting fraud while ensuring user privacy. Due to the higher number of transactions in credit cards, this approach possesses limitations in terms of privacy assurance. Also, XGBoost overfits the dataset in some cases to avoid these various parameters need to be tuned and act together to attain adequate accuracy.

The researchers have used the hybrid method for CCFD using the random forest as well as isolation forest that is used for identification of anomaly transaction [47]. This method is comprised of two categories. The first one is involved in

anomaly-based detection while using unsupervised learning, and the other one is used for interpretations of anomaly detection, and it works on the basis of supervised learning. The proposed method is considered by using high-speed data when the method is used on real-life datasets [15, 16]. The evaluation of the proposed system was evaluated for the identification of the user geolocation. This technique is not cantered on the anomaly level; instead, it is the anomaly-type that defines it. Although it helped to detect the fraudulent transaction on the basis of geolocation, however, data confidentiality and privacy could be compromised. While considering the author work, the model should be evaluated while ensuring the confidentiality of the data. Therefore, it is required to have a model that provides data confidentiality while achieving higher accuracy in CCFD of more extensive datasets.

2.6 Privacy-Preserving Techniques

In the ML approach, dataset training is essential, and for practical training, ML algorithms should be provided with a large volume of data. There has been various research done by using Credit card data in a privacy-preserving manner. One of the experiments was done using the supervised ML approach with blockchain technology. It was used on Ethereum, and it was performed on 300 thousand accounts. The results achieved showed that the alteration of parameters changes the value of precision and recall. Also, it was observed that the use of blockchain could be a threat on the basis of the fact that it is decentralised technology [53]. However, blockchain technology is one of the effective ways of ensuring data privacy due to its decentralised nature. However, considering the use of decentralized technology in the Real World for CCFD, it possesses various limitations that include scalability issues, maintaining data in the wallets. It is also processor-intensive, consuming higher energy, Hence it is expensive, and standardisation is not globally adapted. Therefore, considering the blockchain in banks and financial institutions for CCFD could not be the right choice.

The use of data for experimental purposes should be followed by the GDPR. The research was done by using the techniques of gossip learning and federated learning. It was observed that the gossip learning techniques are ineffective because of not having a central control system. While on the other hand, F.L. has performed better as of its semi decentralised nature [52, 54].

Credit card data is imbalanced and skewed. Finance institutions are not allowed to share their credit card data due to privacy concerns and GDPR. Therefore, while considering this issue, experiments were done by using the techniques of federated learning. In this method, the data was trained locally on the participants, i.e., banks and financial institutes. The result showed that the use of F.L. could fulfil the privacy issue where the data is not shared to the central aggregated server; instead, only the trained model is shared [55]. This is an ideal situation where the data is secured in terms of privacy and confidentiality. F.L. is a cyclic process where the information is trained locally at the client's devices, and the mean average of the model from the individual client is aggregated together. And by this way, anomaly-based fraudulent transactions are learnt from the respective clients, and thus an effective ML model is trained.

2.7 Blockchain Technology

There are various applications based on blockchain technology that has achieved good public attention. It is based on the fact that; it goes beyond the limits of central servers like banks and other institutions. Instead, it provides the decentralised approach where the user behaviour depends on the nature of the Blockchain technology. There is malicious software that can cause fraud in blockchain transactions. Michal et al. (2019) have proposed a supervised machine learning approach in blockchain technology [56]. The authors have used this technique on Ethereum blockchain. The experiment was performed on 300 thousand accounts, and the results were compared with random forest, SVM and XGBoost [57]. They have concluded in the experiment that the various transaction parameters alter the value of precision and recall. They have also suggested that Blockchain is self-maintained technology. This reliance on this could be a potential threat, especially in the finance sector. Therefore, our research is based on a more practical approach with federated learning which is semi-decentralised that ensures efficiency and privacy at the same time.

2.7.1 Why Not Blockchain?

Machine learning approaches are life-changing and continuously evolving in our daily life to make things more comfortable around us. The main hurdle in ML constitutes the diversified and complex training data. Crowdsourcing is one technique used for data collection for the central server, but it possesses limitations concerning data privacy [53]. Blockchain is one of the emerging technologies for making the possibility of providing the decentralised platform that could result in providing enhanced security to the data [57]. Therefore, it could be considered the medium of data collection for CCFD in how data is exchanged among banks and financial institutions securely. However, there are several drawback and limitation that make this technology less efficient to use for exchanging data. Furthermore, due to GDPR exchanging data constitutes privacy concerns. Following are some of the disadvantages of blockchain technology while considering CCFD:

- The process slows down if there are too many users in a network.
- Due to the consensus method used in Blockchain, it is harder to scale the data.
- It requires higher energy usage.
- Blockchain sometime show inefficiency in its operation.
- User must maintain its data in wallets.
- The technology is costly.
- It is not standardised.

The issues mentioned above in blockchain technology discourage researchers and academic institutions from adopting this technology for CCFD. Our proposed research will fix this issue using the semi-decentralised technique of federated learning. It would provide higher efficiency where the participants will train their model locally (preserve security), resulting in faster processing capability than blockchain technology and higher data scalability (Table 1).

3 Classification Imbalance Problem

In credit cards, fraud detection data imbalance is one of the challenging parts that the researchers tried to study. While training the machine learning algorithm could lead to misclassification because of the ratio of genuine transactions towards the fraud transactions (Fig. 3).

Pre-processing the data is one of the techniques to handle imbalanced data, where the oversampling of fraud transactions and under-sampling the legit transaction is performed. That increases the fraud class and decrease the legit transaction class in the original dataset. The performance of the ML algorithm increased after over-sampling where synthetic minority oversampling technique (SMOTE) is considered [10] for imbalanced data. Balanced classification-rate (BCR) and Matthews correlation-coefficient (MCC) are two metrics for handling class imbalances, and it was observed that the fraud miner is better at achieving higher accuracy. Even though there are various drawbacks of using the SMOTE that includes the noise and probability of overlapping between the class that results in overfitting the model, In the experiment [19], SMOTE is found to have achieved 2–4% better accuracy as compared to other classification methods. Although adaptive synthetic (ADASYN) and Ranked Minority Oversampling in Boosting (RAMO) methods were proposed afterwards, however, it caused the issue of classification while considering the increased number of iterations, and the researchers have suggested that the ensemble classifier could perform well in contrast to single-classifier when used with imbalance datasets.

4 Model Design

The centralised approach is one of the commonly adopted methods for credit card fraud detection. A fraud detection system (FDS) becomes inefficient when the limited datasets are available and the limited detection period. Banks and other financial centres cannot share their data on a central server due to GDPR. Users' privacy can still be compromised even if the "anonymised" dataset is locally on servers as it could be reversed-engineered. Therefore, to cope with this challenge we are using FL in our research model as this gives the capability to train the real-time data locally on the edges devices and trained model is centrally shared among all other banks and research centres that can effectively enhance the accuracy of fraudulent transactions.

Secondly, in our research model, we will be using the ANN algorithm to find better evaluation matrix's on clients' data in combination with Federated learning to achieve higher accuracy. Furthermore, this model will play an essential role to accomplish the privacy of the user's data in the given hybrid model approach.

4.1 Proposed Model with Federated Learning and ANN

In our FL model, the following steps are involved in training the model until all participants achieve the full transition:

- Clients selection
  Based on the eligibility criteria, the server selects the participating clients.
- Broadcasting
  In this stage, the chosen client downloads our model. It will be an artificial neural network mode.
- Computation phase
  In this stage, all the participant devices compute the model-update by executing the program provided by the server.
- Aggregation
  In this stage, the server performs the aggregation of the updates from the device.
- Model-update
  In this, the shared server performs aggregation of the clients update locally and update the shared model.
- Model Outline

The proposed model of federated learning with ANN can be classified into three phases followed one after the other until the last phase is completed, and the cycle continues. We will start from Step one as follows:

Table 1 Review comparison

Ref	Methods	Dataset name	Pros	Cons	Accuracy
[4]	Deep learning, Logistic-regression	Nigeria bank	It helped to improve real-life entries of transactions	It doesn't work if the transactions are not based on the real-time	95% for detecting fraudulent transactions
[17]	ANN, annealing	UCI websites	Effective results once trained with ANN	Time-consuming when trained with annealing simulations	92% for detecting fraudulent transactions
[23]	KNN, NB, L.R., D.T., CFLANN	Europeans cardholders	CFLANN reduces mean-squared error	KNN is time-consuming	97.56% for detecting fraudulent transactions
[15]	RF-1, RTRF, RF-2, CRF	Chinese E-commerce firm	R.F. performs well in comparison with other D.T. algorithms	Data imbalance is the lacking	96.77% accuracy and 89.46% precision
[18]	Support vector machine, neural networks	Chinese financial institution	Overall performance of CCFD is enhanced	Time-consuming process	99.21% accuracy and recall of 95.20%
[19]	Random forest (R.F.), logistic regression, SVM, D.T., KNN,	Credit card from European datasets	Classification methods produce higher accuracy in prediction	It requires classification of anomalies earlier	Overall accuracy is achieved higher in contrast to random forest
[20]	R.F., SVM	Credit card from European datasets	Produces better results compared to other classification metrics	This approach is not a long term solution	R.F. produces higher accuracy in static-learning while L.R. produces higher accuracy in incremental-learning
[5]	SVM, neural networks, decision tree	UCI websites	SVM produces optimal results in classification	The model training is time-consuming	Higher accuracy is produced by SVM
[22]	SVM, KNN	Datasets from financial institutions	It helps to classify the transactions in real-life	In-depth knowledge is required for the algorithm to predict in real-life situations	91% accuracy by SVM and 72% by KNN
[25]	SVM	Banks datasets	SVM doesn't overfit	Time-consuming for training model	SVM performs well in contrast to the hybrid B.P. model
[9]	SVM, KNN, Naive Bayes (NB)	UCSD FICO datasets	The more negligible alteration doesn't impact much on the model implementation	Time-consuming for training model Sometimes the prediction is not accurate. KNN is sensitive to noise-datasets	20% accuracy by SVM, 15% by NB and 10% by KNN
[12]	KNN	UCI websites	No need to have predictive-model prior classification	Fraud is not detected while transactions. It is difficult to monitor the system	72% accuracy is achieved by the KNN
[53]	R.F., blockchain	Synthetically created	Privacy-preserving approach	Limited privacy	84.92% recall while using R.F
53]	Gossip learning	Spambase binary classification	Privacy-preserving approach	Less effective due to decentralised nature	95%-LR 96% SVM
[55]	Federated Learning	European cardholders	Privacy-preserving approach	System heterogeneity	95.5% AUC

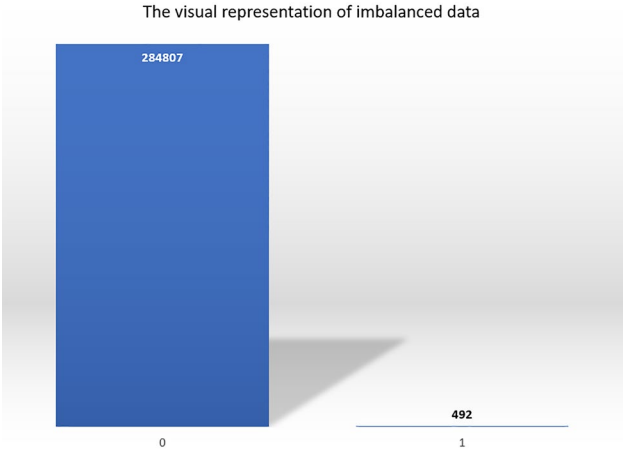

Fig. 3 It shows the ratio of imbalance of the data has in the dataset used in most of the research on our table. 284,807 transactions are genuine, whereas 492 were a fraud

Step 1

This step involves the distribution of our model (ANN) from the central server to the respective correspondence banks or financial institutions. It is displayed as "Black Brain" in Fig. 4. Once the individual banks receive the model, it starts training the model with the available datasets locally. The training process is illustrated below, where the trained model is represented as differentiated by colors for the bank (A-purple, B-blue, C-green and D-red). Digit "1" shows the first phase of sending process of our model to the banks.

Step-2

On completing step-1, step-2 starts simultaneously to send a trained model from banks to the central server of the federated learning model. On the server, all models from the respective banks are combined and form an "upgraded model" as illustrated in Fig. 5.

Step-3

Step-3 is the last step of our proposed model, reflecting the sending of "upgraded model" (formed by the mean average of all corresponding trained models from different banks) to the individual bank separately. Furthermore, on receiving the model by the banks, it is trained locally as step-1. Once the training is completed, it is sent back to the server. The process is repeated cyclically until the expected outcome is ensured (Fig. 6).

Cycle Repetition

After completion of step-3, the process is continued by sending the trained model to the server as the first step explained. Again, the server takes the mean-average of all banks, and it is sent to individual banks again. According to our hypothesis, this repeated training process repeatedly can ensure higher accuracy in CCFD. The overall process is represented in Fig. 7.

The model is commonly and collaboratively shared by banks and other research centres where the data is kept locally to their database. However, just the trained model is shared among all participants, not actual data. The central server will be trained mutually by all participants, resulting in better classification than the individual model trained locally. In simple words, the learning pattern is

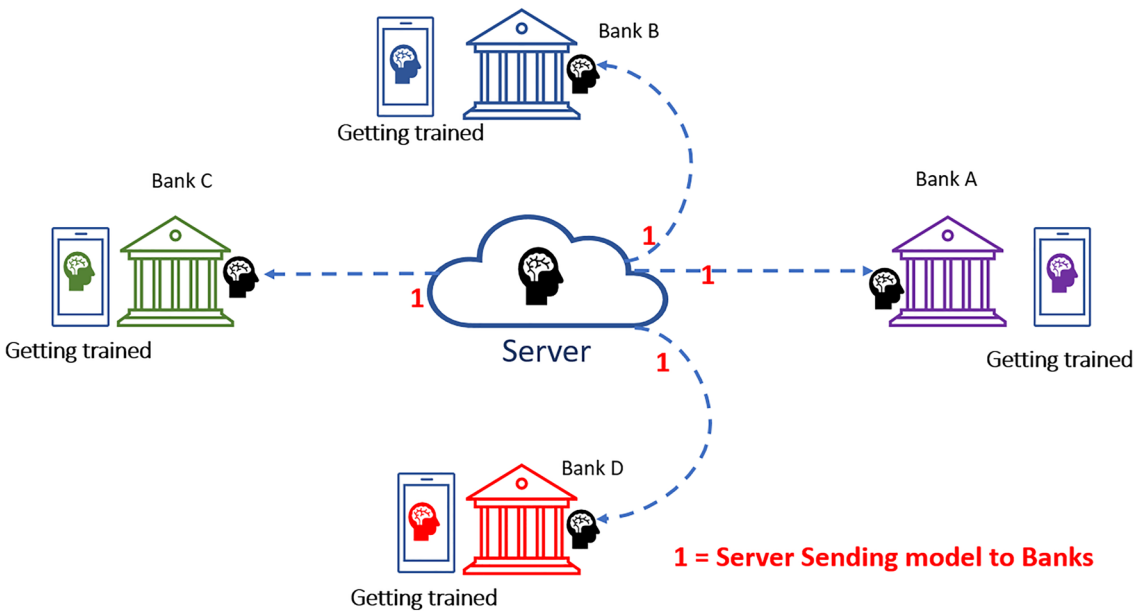

Fig. 4 : Step 1 of the proposed model

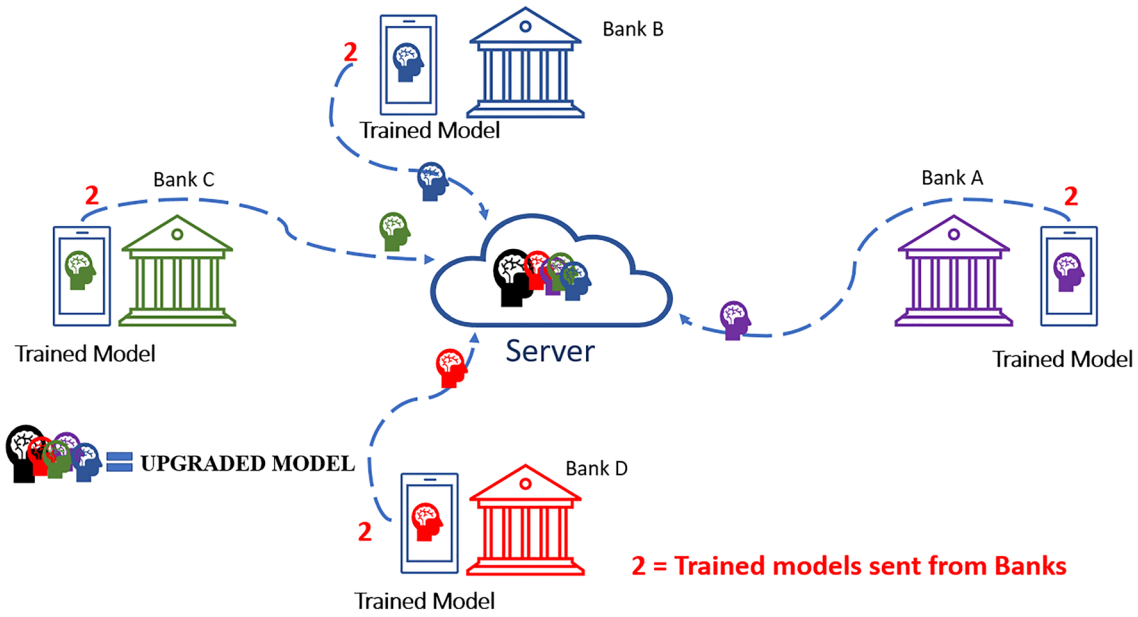

Fig. 5 Step 2 of the proposed model

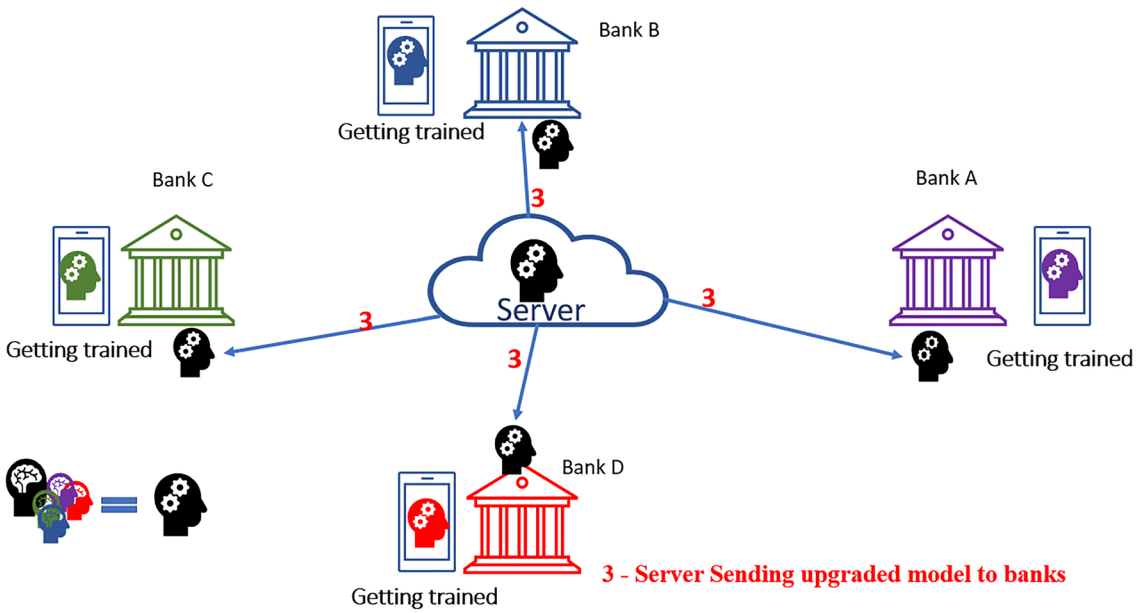

Fig. 6 Step 3 of the proposed model

learnt locally at each client-side, and these learnt patterns are aggregated together in the central server. It is trained from the mutual inputs from all participants. This central model is shared back to all participants, and fraud detection is performed accordingly. By performing the steps mentioned above, FL can significantly enhance fraud detection accuracy, and simultaneously, the privacy of the customer's data is preserved by using the FL, which will incorporate the data according to GDPR.

5 Proposed Method

In this review paper, we found that the usage of supervised learning is common practice among researchers. SVM, KNN, Naïve-Bayes, logistic-regression and DT models are highly used. We also see that the hybrid approach gives a better performance than if usage of a single algorithm/classifier. As it can be observed, various experiments

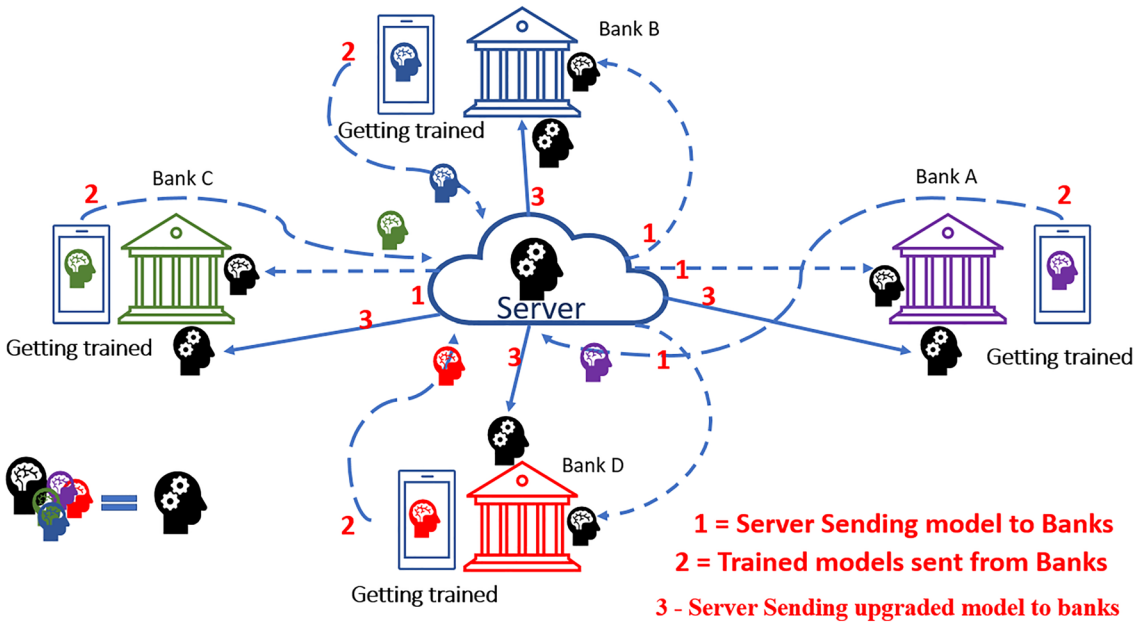

Fig. 7 Full model

that are performed on the CCFD in the previous section, although different ML models are proven to be effective in this process however due to data imbalance and heterogeneity, CCFD is always challenging, and models are unable to yield higher accuracy. The factor of data imbalance and heterogeneity could be enhanced for higher volume of data and also the real-time fraudulent patterns are observed constantly, so the model is updated with the potential feature variables. The use of real-time datasets involves privacy issues as the banks and financial institutions are obliged to follow GDPR rules. Our proposed solution suggests the use of a privacy-preserving approach of using the datasets for effective ML model training. Following is the flow chart of the proposed solution that will follow each step as shown, and eventually, it performs an iterative process.

Figure 8 shows our proposed methodology following number of steps from beginning to the end. Data splitting is performed into training, validation and testing with the percentage of 75%, 15% and 15% respectively across the whole dataset. Machine learning algorithm is used on the training data. In our proposed topology, we have used FL framework for model training. In this architecture, model is sent from FL central server to the local server comprising of local devices. The model sent at local devices is trained separately and eventually the trained model is sent back to the FL server and aggregated together. This process is repeated to keep the model updated with the latest patterns. In this framework, only the trained model from the local devices is shared to the FL server and the data is remained secured locally on devices. Once the model is trained, it can be evaluated for performance analysis by testing and validation data. And the trained model from the real time transaction data can be effectively used for CCFD.

Our proposed solutions involve the use of a federated learning concept that follows the framework for banks and financial institutions to collaborate for training the ML model. In this process of collaboration, the model is trained locally on each participant, and the trained model is combined centrally without data. The mean average of the trained model is repeated across the participants for training and keep learning new patterns from the variety of data. In this process, the data is not shared; instead, only the trained model is combined centrally. It follows the data privacy concept, where the data is secured (not shared), but at the same time ML model is trained from the datasets. Experiments show that the use of Deep learning algorithms has produced effective outcomes in CCFD. Our proposed solution outlines the use of an artificial neural network with the F.L., which can bring up model training on the bigger scale real-time datasets where privacy is ensured, and the trained model can promise the optimal CCFD. Although work has been done on ANN for CCFD, however, it is based on lab-based datasets. Our proposed solution is novel in the sense that it uses the hybrid approach that is based on using real-time data in a privacy-preserving manner. The use of ANN for effective detection and federated learning for providing the framework of data privacy will provide a hybrid approach which is a novel contribution.

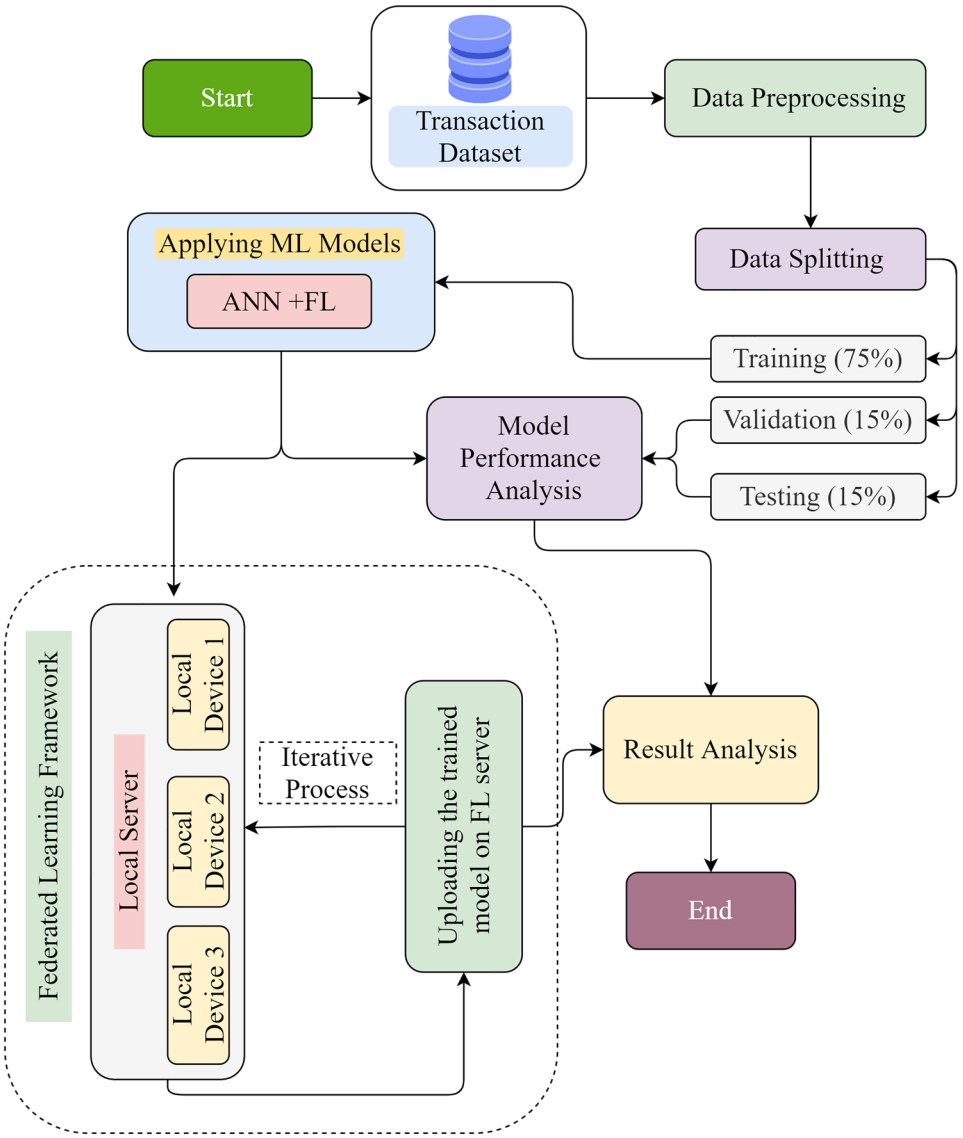

Fig. 8 It shows our proposed methodology. In this model, transaction data can be used for preprocessing and applying ML models. Data splitting, processing, and using the ML model in FL framework is used for data privacy and effective model performance analysis

6 Conclusion

This review paper explores the various techniques been used for CCFD. It can be analysed that the ML techniques are a great way to enhance the accuracy of CCFD. However, we need large datasets to train the model to avoid the issue of data imbalance. The use of real-time datasets can provide us with more variety of data, while privacy remains an issue. According to our proposed method, we can utilise the real-time datasets to train the model in a privacy-preserving manner. A Federated learning framework with ANN can enhance the capability of the ML model to detect fraudulent transactions. The proposed hybrid approach can alter the way of CCFD in an effective manner while utilising the real-life datasets and give a new horizon in the field of the banking and finance industry. The proposed method can help the finance institutions and banks to utilise the real-time datasets by the mutual collaboration that would give a collective benefit for developing an effective system for CCFD. Although the proposed method is effective in terms of CCFD while using the real-time datasets in a privacy-preserving way, however, it has limitations when it comes to real-life deployment. All banks and financial institutes have their own rules and regulations, and they are quite strict about it. Adapting the proposed method will be challenging as every bank and finance institutes have their own limitations, and they rely on their internal resources rather than using a centralised approach. Although data is not shared centrally, even the trained model will be going to learn patterns that can be possibly decoded by hackers. Therefore, while keeping the limitations in place, there still needs to be work done for gaining the confidence of banks and financial institutes to adopt this technology.

Author Contributions RBS significantly contributed to the conceptual parts of the paper's contribution to the knowledge. VS and PS assisted with report improvement and review, as well as providing guidance on manuscript drafting.

Funding Not applicable.

Availability of Data and Material Not applicable.

Declarations

Conflict of Interest The authors declare that they have no competing interests.

Ethics Approval Not applicable.

Consent to Participate Not applicable.

Consent for Publication Not applicable.

References

1. Lucas Y, Portier P-E, Laporte L, et al. Multiple perspectives HMM-based feature engineering for credit card fraud detection. In: ACM, 2019. p. 1359–1361.
2. Duman E, Elikucuk I. Solving credit card fraud detection problem by the new metaheuristics migrating birds optimization. Berlin: Springer; 2013.
3. Botchey FE, Qin Z, Hughes-Lartey K. Mobile money fraud prediction—a cross-case analysis on the efficiency of support vector machines, gradient boosted decision trees, and Naïve Bayes algorithms. Information. 2020;11:383. https://doi.org/10.3390/info11080383.
4. Ogwueleka FN. Data mining application in credit card fraud detection system. J Eng Sci Technol. 2011;6:311–22.
5. Sriram Sasank JVV, Sahith GR, Abhinav K, Belwal M. Credit card fraud detection using various classification and sampling techniques: a comparative study. In: IEEE, 2019. p. 1713–1718.
6. Ojugo AA, Nwankwo O. Spectral-cluster solution for credit-card fraud detection using a genetic algorithm trained modular deep learning neural network. JINAV J Inf Vis. 2021;2:15–24. https://doi.org/10.35877/454RI.jinav274.
7. Majhi SK, Bhatachharya S, Pradhan R, Biswal S. Fuzzy clustering using SALP swarm algorithm for automobile insurance fraud detection. J Intell Fuzzy Syst. 2019;36:2333–44. https://doi.org/10.3233/JIFS-169944.
8. Darwish SM. An intelligent credit card fraud detection approach based on semantic fusion of two classifiers. Soft Comput. 2019;24:1243–53. https://doi.org/10.1007/s00500-019-03958-9.
9. Sobanadevi V, Ravi G. Handling data imbalance using a heterogeneous bagging-based stacked ensemble (HBSE) for credit card fraud detection. Singapore: Springer; 2020.
10. Li C, Ding N, Dong H, Zhai Y. Application of credit card fraud detection based on CS-SVM. Int J Mach Learn Comput 2021;11(1).
11. Olowookere TA, Adewale OS. A framework for detecting credit card fraud with cost-sensitive meta-learning ensemble approach. Sci Afr. 2020;8:e00464. https://doi.org/10.1016/j.sciaf.2020.e00464.
12. Itoo F, Meenakshi SS. Comparison and analysis of logistic regression, Naïve Bayes and KNN machine learning algorithms for credit card fraud detection. Int J Inf Technol. 2020;13:1503–11. https://doi.org/10.1007/s41870-020-00430-y.
13. Awoyemi JO, Adetunmbi AO, Oluwadare SA. Credit card fraud detection using machine learning techniques: a comparative analysis. IEEE, 2017. p. 1–9
14. Alam MN, Podder P, Bharati S, Mondal MRH. Effective machine learning approaches for credit card fraud detection. Cham: Springer; 2021.
15. Vynokurova O, Peleshko D, Bondarenko O, Ilyasov V, Serzhantov V, Peleshko M. Hybrid machine learning system for solving fraud detection tasks. In: 2020 IEEE third international conference on data stream mining & processing (DSMP), IEEE; 2020. p. 1–5.
16. Rai AK, Dwivedi RK. Fraud detection in credit card data using unsupervised machine learning based scheme. In: IEEE, 2020. p. 421–426.
17. Dubey SC, Mundhe KS, Kadam AA. Credit card fraud detection using artificial neural network and back propagation. In: 2020 4th international conference on intelligent computing and control systems (ICICCS). IEEE; 2020. p. 268–273.
18. Patidar R, Sharma L. Credit card fraud detection using neural network. Int J Soft Comput Eng (IJSCE), 2011;1(32–38).
19. Dhankhad S, Mohammed E, Far B. Supervised machine learning algorithms for credit card fraudulent transaction detection: a comparative study. In: IEEE, 2018. p. 122–125.
20. Puh M, Brkic L. Detecting credit card fraud using selected machine learning algorithms. In: Croatian Society MIPRO, 2019. p. 1250–1255.
21. Varmedja D, Karanovic M, Sladojevic S, et al. Credit card fraud detection—machine learning methods. In: IEEE, 2019. p. 1–5.
22. Zhu H, Liu G, Zhou M, Xie Y, Abusorrah A, Kang Q. Optimizing weighted extreme learning machines for imbalanced classification and application to credit card fraud detection. Neurocomputing. 2020;407:50–62. https://doi.org/10.1016/j.neucom.2020.04.078.
23. Jemima Jebaseeli T, Venkatesan R, Ramalakshmi K. Fraud detection for credit card transactions using random forest algorithm. Singapore: Springer; 2020.
24. Dighe D, Patil S, Kokate S. Detection of credit card fraud transactions using machine learning algorithms and neural networks: a comparative study. In: IEEE, 2018. P. 1–6.
25. Mishra MK, Dash R (2014) A comparative study of Chebyshev functional link artificial neural network, multi-layer perceptron and decision tree for credit card fraud detection. In: IEEE, p. 228–233
26. Rtayli N, Enneya N. selection features and support vector machine for credit card risk identification. Procedia Manuf. 2020;46:941–8.
27. Xuan S, Liu G, Li Z, Zheng L, Wang S, Jiang C. Random forest for credit card fraud detection. In: 2018 IEEE 15th international conference on networking, sensing and control (ICNSC). IEEE; 2018, p. 1–6.

28. Worobec K. The definitive overview of payment industry fraud. In: Ukfinance.org.uk. 2021. https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202021-%20FINAL.pdf.
29. Jakaite L, Schetinin V, Maple C. Bayesian assessment of newborn brain maturity from two-channel sleep electroencephalograms. Comput Math Methods Med. 2012;2012:629654–7. https://doi.org/10.1155/2012/629654.
30. Jakaite L, Schetinin V, Maple C, Schult J. Bayesian decision trees for EEG assessment of newborn brain maturity. In: The 10th annual workshop on computational intelligence UKCI 2010. 2010. https://doi.org/10.1109/UKCI.2010.5625584
31. Jakaite L, Schetinin V, Schult J. Feature extraction from electroencephalograms for Bayesian assessment of newborn brain maturity. In: Proceedings of the 24th IEEE international symposium on computer-based medical systems. 2011. https://doi.org/10.1109/CBMS.2011.5999109
32. Jakaite L, Schetinin V, Schult J. Feature extraction from electroencephalograms for Bayesian assessment of newborn brain maturity. In: 24th International symposium on computer-based medical systems (CBMS), 2011. p. 1–6. https://doi.org/10.1109/CBMS.2011.5999109
33. Nyah N, Jakaite L, Schetinin V, Sant P, Aggoun A. Evolving polynomial neural networks for detecting abnormal patterns. In: 2016 IEEE 8th international conference on intelligent systems (I.S.), 2016. p. 74–80. https://doi.org/10.1109/IS.2016.7737403.
34. Nyah N, Jakaite L, Schetinin V, Sant P, Aggoun A. Learning polynomial neural networks of a near-optimal connectivity for detecting abnormal patterns in biometric data. In: 2016 SAI computing conference (SAI), 2016. p. 409–413. https://doi.org/10.1109/SAI.2016.7556014.
35. Schetinin V, Jakaite L. Classification of newborn EEG maturity with Bayesian averaging over decision trees. Expert Syst Appl. 2012;39(10):9340–7. https://doi.org/10.1016/j.eswa.2012.02.184.
36. Schetinin V, Jakaite L. Extraction of features from sleep EEG for Bayesian assessment of brain development. PLoS ONE. 2017;12(3):1–13. https://doi.org/10.1371/journal.pone.0174027.
37. Schetinin V, Jakaite L, Nyah N, Novakovic D, Krzanowski W. Feature extraction with GMDH-type neural networks for EEG-based person identification. Int J Neural Syst. 2018. https://doi.org/10.1142/S0129065717500642.
38. Hassan MM, Billah MAM, Rahman MM, Zaman S, Shakil MMH, Angon JH. Early predictive analytics in healthcare for diabetes prediction using machine learning approach. In: 2021 12th international conference on computing communication and networking technologies (ICCCNT). IEEE; 2021. p. 01–05.
39. Hassan MM, Peya ZJ, Mollick S, Billah MAM, Shakil MMH, Dulla AU. Diabetes prediction in healthcare at early stage using machine learning approach. In: 2021 12th international conference on computing communication and networking technologies (ICCCNT). IEEE; 2021. p. 01–05.
40. Kong M, Li L, Wu R, Tao X. An empirical study of learning based happiness prediction approaches. Hum Centric Intell Syst. 2021;1(1–2):18.
41. Hassan M, Akter L, Rahman M, Zaman S, Hasib K, Jahan N, Smrity R, Farhana J, Raihan M, Mollick S. Efficient prediction of water quality index (WQI) using machine learning algorithms. Hum Centric Intell Syst. 2021;1(3–4):86.
42. Schetinin V, Jakaite L, Krzanowski WJ. Prediction of survival probabilities with Bayesian decision trees. Expert Syst Appl. 2013;40(14):5466–76. https://doi.org/10.1016/j.eswa.2013.04.009.
43. Schetinin V, Jakaite L, Krzanowski W. Bayesian learning of models for estimating uncertainty in alert systems: application to air traffic conflict avoidance. Integr Comput Aided Eng. 2018;26:1–17. https://doi.org/10.3233/ICA-180567.
44. Jakaite L, Schetinin V, Hladuvka J, Minaev S, Ambia A, Krzanowski W. Deep learning for early detection of pathological changes in X-ray bone microstructures: case of osteoarthritis. Sci Rep. 2021. https://doi.org/10.1038/s41598-021-81786-4.
45. Wen H, Huang F. Personal loan fraud detection based on hybrid supervised and unsupervised learning. In: 2020 5th IEEE international conference on big data analytics (ICBDA). IEEE; 2020. p. 339–343.
46. Li W, Lin S, Qian X, et al. An evidence theory-based validation method for models with multivariate outputs and uncertainty. SIMULATION. 2021;97:821–34. https://doi.org/10.1177/00375497211022814.
47. Zięba M, Tomczak SK, Tomczak JM. Ensemble boosted trees with synthetic features generation in application to bankruptcy prediction. Expert Syst Appl. 2016;58:93–101. https://doi.org/10.1016/j.eswa.2016.04.001.
48. Vynokurova O, Peleshko D, Bondarenko O, et al. (2020) Hybrid Machine Learning System for Solving Fraud Detection Tasks. IEEE, pp 1–5
49. Rejwan BS, Schetinin V. Deep neural-network prediction for study of informational efficiency. In: Arai K, editor. Intelligent systems and applications. IntelliSys 2021. Lecture notes in networks and systems, vol. 295. Cham: Springer; 2022. https://doi.org/10.1007/978-3-030-82196-8_34.
50. Visa credit cards in circulation 2020|Statista. In: Statista. 2021. https://www.statista.com/statistics/618115/number-of-visa-credit-cards-worldwide-by-region/.
51. Mastercard: credit cards in circulation 2021|Statista. In: Statista. 2021. https://www.statista.com/statistics/618137/number-of-mastercard-credit-cards-worldwide-by-region/. Accessed 24 Nov 2021.
52. Hegedűs I, Danner G, Jelasity M. Decentralized learning works: an empirical comparison of gossip learning and federated learning. J Parallel Distrib Comput. 2021;148:109–24. https://doi.org/10.1016/j.jpdc.2020.10.006.
53. Ostapowicz M, Żbikowski K. Detecting fraudulent accounts on blockchain: a supervised approach. Cham: Springer; 2019.
54. Danner G, Berta Á, Hegedűs I, Jelasity M. Robust fully distributed minibatch gradient descent with privacy preservation. Secur Commun Netw. 2018;2018:1–15. https://doi.org/10.1155/2018/6728020.
55. Yang W, Zhang Y, Ye K, et al. FFD: a federated learning based method for credit card fraud detection. Cham: Springer; 2019.
56. Ostapowicz M, Żbikowski K. Detecting fraudulent accounts on blockchain: a supervised approach. In: International conference on web information systems engineering. Springer, Cham; 2020. p. 18–31.
57. Carneiro N, Figueira G, Costa M. A data mining based system for credit-card fraud detection in e-tail. Dec Support Syst. 2017;95:91–101. https://doi.org/10.1016/j.dss.2017.01.002.