

Credit Card Fraud Detection Techniques: A Review

Shishobitveer Singh Sohal

Department of Computer Science & Engineering
DAVIET, Jalandhar

Abstract— Prediction Analysis (PA) refers to an approach using which the upcoming prospect can be predicted from the previous occurred events. This technique has two phases namely feature extraction and classification process. The detection of fraud in credit card using PA becomes challenging because of the complexity in datasets. There are numerous classification methods that are implemented in state-of-art schemes in order to detect the frauds in credit card. The prediction analysis is a DM (data mining) method which is useful for future forecasting on the basis of current information. This research is carried out to perform the CCFD (credit card fraud detection) on the basis of recent information. The data of credit card is available in an enormous volume form. Consequently, it becomes difficult to establish association among diverse features that have impact on the predictive accuracy. The various machine learning and deep learning models are reviewed in this paper for the credit card fraud detection. The machine learning and deep learning model techniques has various phases which include pre-processing, feature extraction and classification.

Keywords—component; formatting; style; styling; insert (key words)

Date of Submission: 26-07-2022

Date of acceptance: 09-08-2022

I. INTRODUCTION

The accelerated evolution of information technology has deeply influenced the consumption patterns of folks in fintech-led digital life and has transformed the growth model of the conventional finance sector to some degree. Particularly, in the current era of digital services, the incidents of transaction fraud are more frequent than ever and cause significant financial losses. Hence, there is the need of an efficient fraud detection system for banking institutions and finance companies to trace or track transactions done over the internet. Various fraud detection systems are intended to mine doubtful transaction patterns from multiple transaction records and use them to trace or track inflowing transactions. Credit card fraud detection has drawn the interest of the machine-learning and artificial intelligence communities, where plenty of automatic approaches have been presented. It has been observed that machine learning can mine these patterns with high effectiveness [1]. This task can be perceived as a function of supervised binary classification. In simple way, a well-run classification framework can be trained using a large number of payment logs to identify fraudulent transactions. Even though machine learning has made phenomenal breakthroughs in the detection of fraudulent transactions, fraud detection systems will continue to improve, and even small developments can mitigate vast economic losses.

1.1.1 Types of credit card fraud

Credit card frauds can take various shapes and forms. This includes fraud in which payment card details are used to commit fraud. The reasons for credit card fraud also vary. Some of the commonly existing credit card fraud types are discussed as follows:

- i. Application Fraud: Application to an issuing bank exposes fraud when someone applies for a credit card with a fake ID [2]. This can be partially or completely synthetic identity, known as identity fraud, or theft of someone else's identity, known as identity theft. Application fraud is a perfect example of identity crime. The key component of application fraud is address. This is where the credit card will be directed and retrieved by the deceiver.
- ii. Electronic or Manual Credit Card Imprints: This type of credit card fraud is initiated by using credit card score. In these attacks, a fraudster scans the information available on the card's magnetic stripe. Later, he uses this information to decode the false card or to conduct fraudulent transactions.
- iii. CNP (Card Not Present) Fraud: A fraudster knowing about someone's card expiry date and account number can commit such fraud against him. This fraud can be initiated through phone, mail or internet. This basically means that the fraudster accesses someone's card in real time without getting hold of the credit card.
- iv. Counterfeit Card Fraud: Fraud occurs when someone clones sensitive information and security features from an existing card to reproduce it on a duplicate counterfeit card, for example, the magnetic stripe on the card [3]. It is quite common to use these cards for spending in countries that have not yet provided for authentication via chip, as per the EMV standard.

v. **Lost and Stolen Card Fraud:** Lost and stolen fraud stems from a lost or stolen route, when someone steals a physical credit card or obtains it through other means. Then, either the agent himself or a third party (organized crime) illegally purchases goods or services using this card on behalf of the legitimate card owner. Before the card is stolen, the perpetrator may try to run his victim side to obtain the PIN number with the victim's card.

1.2 Credit Card Fraud Detection Model

With the continuous development of e-commerce transactions in the past few years, credit card fraud detection has become a popular subject of research in the area of fraud detection. In general, detecting frauds is extremely problematic due to two main issues: class imbalance and data dynamic changes. The class imbalance issue associated with the detection of credit card frauds has been analyzed for a long time. Re-sampling is amongst the most well-performing techniques [4]. Simply put, it is possible to balance a training data set by eliminating some instances from the majority class (that is, under-sampling) or creating some samples for the minority class (that is, oversampling). Besides this, ensemble techniques like bagging, boosting, and stacking, are also frequently adopted to problem solution to class imbalance issue [5]. Cost-sensitive learning is an alternative approach of dealing with this by imputing various misclassification error costs to various classes, and the minority class is typically assigned with a greater cost. Some works treat the data dynamic variation issue as concept drift. Their ultimate goal is to early detect the presence of concept drift and to adaptively update a classifier to prepare for new assumptions. There are intrinsic distinguishing features between fraudulent and honest transactions. As a result, it is also important to have a powerful characterization capable of distinguishing fraudulent transactions from truthful ones, while the methods of fraud are constantly changing [6]. As illustrated in Figure 1, constructing an efficient credit card fraud detection model involves a few essential steps that substantially impact identification.

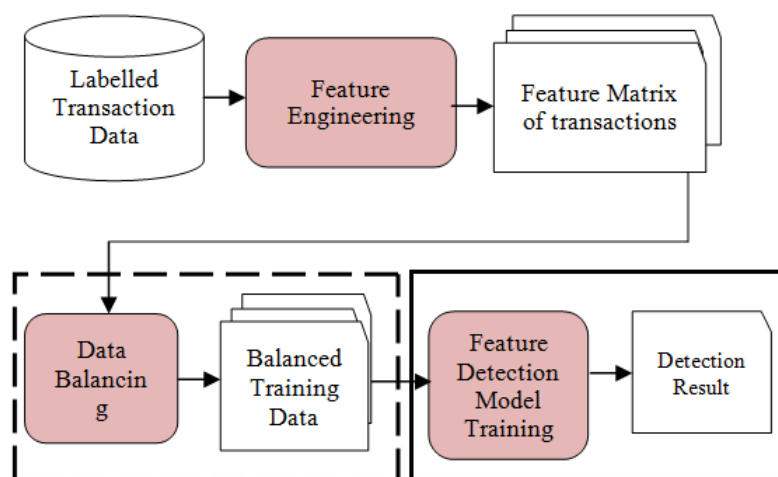


Figure 1: Credit Card Fraud Detection Model

The important blocks of the credit card detection architecture are detailed below:

i. **Feature engineering:** The first step is feature engineering which aims to extract informational characteristics of the transaction behavior of users. Rough attributes like time and date of payment and value of transactions may not portray the transactional behavior of card owners and impostors efficiently [7]. The most common approach is to adopt a transaction aggregation technique to extract some fresh attributes. Transactions are grouped based on a selected session, card number, payment type and merchant code to extract aggregated features. The next step is to compute the number of payments and the overall money spent on those payments. One transaction with rough attributes is turned into a feature matrix with more informercial aggregation attributes, followed by a cycle of transaction aggregation.

ii. **Data Balancing:** The next after feature engineering is to train a classifier as a binary classification function. Nevertheless, the learned classifier recognizes maximum number of fraudulent transactions as real ones when class imbalance issue is not treated [8]. This is because majority of classifiers are contingent on the default theory of a balanced data set, and therefore, the learned decision boundary show inclination towards the class with extra instances. Therefore, tackling the problem of class imbalance has turned into an imperative step prior to training a fraud detection framework. Data sampling is one of the most frequently used methods to deal

with the problem of class imbalance. In particular, the idleness of actual transactions can be reduced by using the under-sampling method which accelerates the model training process. Random under-sampling is one of the most well-known under-sampling techniques for its ease and efficiency. Nevertheless, these sampling techniques don't address the spatial distribution of examples from distinct classes. An under-sampling technique called gaussian mixture can be implemented to test more useful examples and, thus, enhance the productivity of the classification architecture. However, if the data set contains significantly fewer fraudulent transactions than authentic, an up-sampling method, like SMOTE, should be used to highlight the fraudulent transactions [9].

iii. **Fraud Detection Model Training:** After tackling the class imbalance problem, training a fraudulent transaction detection framework as a binary classifier can be done with a comparatively balanced data set. Many machine learning methods, like SVM RF, CNN, and Recurrent Neural Networks (RNNs), have been fruitfully used for fraudulent transactions' detection. Most of them are related to representation learning. Their objective is to discover a better characterization of the input through learning the alterations of the data that isolate the aspects of changeover in the data and hold maximum information [10]. In particular, deep representation learning along deep neural networks has achieved unprecedented success in multiple fields in the past few years because of some innovative compositions.

1.2.1. Machine Learning Methods for Credit Card Fraud Detection

Machine learning methods have been progressively used to detect frauds related to credit cards.

Because extremely unbalanced data and diffuse patterns influence the prediction accuracy of standard ML algorithms, and some non-static data breach the norms of classic clustering and classification techniques, there has been an augmented research interest in using new techniques to deal with this challenge in current years [11]. Both supervised and unsupervised techniques have been put forward for detecting credit card frauds. Non-supervised methods include outlier/anomaly detection methods that treat any transaction as fake that does not comply with the majority. Supervised techniques are undoubtedly the most well-performing methods in fraud detection, which leverage labeled transactions to train a classifier. The feature vectors of genuine transactions are classified, or sometimes the posterior of the classifier is analyzed to detect frauds. Researchers have tested many classification algorithms in terms of credit card transactions for fraud detection. Some most common algorithms for credit card fraud detection are discussed as follow:

a. **AdaBoost:** Boosting, being an ML algorithm, aims to generate highly accurate models by combining multiple ingenious or incorrect architectures. The AdaBoost algorithm is applied alongside other ML methods to enhance their classification performance [12]. The AdaBoost approach outputs a weighted sum. In order to do so, the outputs of the independent boosted models are combined. This mathematical representation of this technique is provided below:

$$G_N(x) = \sum_{t=1}^N g_t(x) \quad (1)$$

where g_t denotes a weak learner (simple classifier) outputting a prediction given an input vector x . t be an iteration. $h(x_n)$ is used to represent the prediction of a weak learner for each training instance [13]. Next, at each t , a weak learner is chosen and multiplied by a coefficient β_t to calculate the training error, L_t , as follows:

$$L_t = \sum_n L[G_{t-1}x_n + \beta_t h(x_n)]$$

where G_{t-1} be a classifier boosted at iteration $t - 1$ and $\beta_t h(x_n)$ be a weak treated for the final framework.

b. **Random Forest:** Random Forest is related to supervised learning algorithm. Its principle is to create a number of decision trees through the selection of random samples and random attributes. Lastly, the classification results of many decision trees are obtained based on the rule that the minority is inferior to the majority. On contrary to a single decision tree, random forest is able to efficiently mitigate the risk of overfitting, successfully balance the error for imbalanced data, and rapidly decide the significance of features [14]. A random forest is a classifier comprising an array of tree-configured classifiers $\{h(\mathbf{x}, \Theta_k), k = 1, \dots\}$ where $\{\Theta_k\}$ are independently uniformly distributed random vectors and each tree has cast one unit vote for the most well-known class on the input. For each tree in the random forest a new training set is produced by drawing it with replacements from the new training set. Then, features are selected randomly at each node for growing tree on the new training set. The resultant trees are not pruned.

c. Support vector machines (SVM): The SVM is a non-probabilistic linear classification algorithm which is able to learn for discriminating the data comes under two classes. For this, the linear boundary recognized as hyperplane is searched due to which the margin amid two known classes is increased. In case, the input denotes an array x that has n attributes which indicated that it is a point in n -dimensional space. A linear surface of dimension $n-1$ is discovered using Support vector machines for dividing two clouds of n -dimensional points that comes in the two classes [15]. The hyperplane parameters are optimized for increasing its distance from the closest point which is a problem whose solution is required to mitigate a quadratic error function. Though, SVM is a linear classifier, the nonlinear kernel trick can be utilized to carry out the nonlinear classification process. Furthermore, the adjustment of this model can be easily done in case the separation of two classes is not performed clearly in n -dimensional space by relaxing the hard margin constraint in the context of a soft margin [16]. The Support Vector Machine is adaptable for dealing with multiclass problems in various ways, generally with the integration of a bank of SVM classifiers.

II. EASEOF USE

2.1 Credit Card Fraud Detection using Machine Learning

M. R. Dileep, et.al (2021) suggested two algorithms: DT (Decision Tree) and (Random Forest) to detect the frauds in credit card [17]. Afterward, an analysis was performed on actual world credit card facts group taken from a financial institution. These algorithms were evaluated on the data samples. The initial algorithm focused on developing a tree against the activities which the user performed, and this tree was implemented to recognize the scams. The latter one aimed to generate a user activity-based forest which was useful to recognize the fraud. The results indicated that the suggested approach offered higher precision to detect frauds in credit cards.

A. A. Taha, et.al (2020) introduced an intelligent technique recognized as OLightGBM (optimized light gradient boosting machine) in order to detect fraud in credit card [18]. This algorithm was an integration of BHO (Bayesian-based hyper-parameter optimization) for enhancing the components of LightGBM (light gradient boosting machine). Two publically available datasets, in which frauds and authentic payments were contained, applied in the quantification of the introduced technique.

The results validated that the introduced technique performed more effectively in comparison with the classic techniques. This accuracy of this technique was calculated 98.40%, AUC (Area under receiver operating characteristic curve) was 92.88%, precision was 97.34% and F1-score was found 56.95%.

A. Salazar, et.al (2019) constructed a novel technique with the objective of detecting frauds in credit cards on the basis of dynamics of the card transactions [19]. Two or 3 variables were utilized to describe subspaces. The LQDA (linear and quadratic discriminant analysis) and RF (random forest) were considered as a single classification algorithm. The AI (alpha integration) algorithm was exploited to fuse all the outcomes for every subspace for acquiring an entire outcome. This technique led to maximize the accuracy to detect the CCF after fusing and employing the temporal dependence of card transactions.

D. Devi, et.al (2019) recommended a cost-sensitive WRF (weighted random forest) algorithm in order to detect the fraud in credit card effectively [20]. A CF (cost-function) was employed while training every tree in bagging so that more weight was allocated to the minority instances during training. The predictive potential of the minority class examples was considered to assign rank to the trees. Two datasets were applied to compare the recommended algorithm against the traditional algorithms. An evaluation was conducted on this algorithm concerning G-mean, F-measure and AUC (Area under receiver operating characteristic curve) values. The experimental outcomes proved that the recommended algorithm was applicable as compared to others.

Table

Author	Year	Technique Used	Findings	Limitations
M. R. Dileep, et.al	2021	DT (Decision Tree) and (Random Forest) algorithms	The results indicated that the suggested approach offered higher precision to detect frauds in credit cards.	It was complex to create a categorized data among spurious data and investigate the dependencies. Thus, the scope of this approach was restricted.
A. A. Taha, et.al	2020	OLightGBM (optimized light gradient boosting machine)	This accuracy of this technique was calculated 98.40%, AUC (Area under receiver operating characteristic curve) was 92.88%, precision was 97.34% and F1-score was found 56.95%.	The efficacy of this technique was mitigated in case the entire data consisted of fraud transactions.
A. Salazar, et.al	2019	LQDA (linear and quadratic discriminant analysis) and RF	This technique led to maximize the accuracy to detect the CCF after fusing and employing the temporal	This technique was unable of separating two classes credit card transactions.

		(random forest)	dependence of card transactions.	
D. Devi, et.al	2019	WRF (weighted random forest) algorithm	The experimental outcomes proved that the recommended algorithm was applicable as compared to others.	This algorithm was not performed well in case of datasets of high dimensionality.

2.2 Credit Card Fraud Detection using Deep Learning

G. K. Arun, et.al (2020) projected a new DL (deep learning) based C-LSTM (convolutional long short term memory) technique to detect fraud in credit card [21]. This algorithm was deployed to pre-process and classify the data. The transactions were classified on the basis of pre-processed data for detecting the occurrence of frauds in credit cards. The experimental results exhibited that the projected technique performed well and yielded an accuracy around 94% on German credit dataset and 94.65% on CCFD (credit card fraud detection) dataset.

Z. Li, et.al (2020) developed an innovative type of LF (loss function) called FCL (full center loss), in which distances and angles among attributes were taken in account [22]. It resulted in supervising the DRL (deep representation learning) at extensive level. Two datasets: private and public were executed in the experimentation for evaluating the developed approach against the conventional techniques. The experimental results depicted the stability of the developed approach over others for detecting the frauds in credit cards.

X. Zhang, et.al (2019) formulated a DL (deep learning) model with a novel feature engineering procedure on the basis of HOBA (homogeneity-oriented behavior analysis) [23]. This model was computed on a real time dataset. The outcomes of experiment demonstrated that the formulated model worked effectively and feasibly to detect the CCF (credit card fraud). This model was capable of recognizing more deceitful transactions in comparison with other methods and offered lower FPR (false positive rate). Moreover, the formulated model was assisted in protecting interests of consumer and mitigating the fraud losses and regulatory costs.

C. Charitou, et.al (2020) investigated a new GAN (generative adversarial network) on the basis of semi-supervised learning of SAE (sparse auto-encoders) to detect fraud in credit cards [24]. The experimental outcomes indicated that the investigated model was more efficient as compared to other ML (machine learning) algorithms namely LR (logistic regression), RF (random forest) and MLP (multi-layer perceptron). This model had generated optimal outcomes on other domains which faced an issue of class imbalance.

2.2 Table

Author	Year	Technique Used	Findings	Limitations
G. K. Arun, et.al	2020	DL (deep learning) based C-LSTM (convolutional long short term memory) technique	The experimental results exhibited that the projected technique performed well and yielded an accuracy around 94% on German credit dataset and 94.65% on CCFD (credit card fraud detection) dataset.	The efficacy of the projected technique was found lower due to the ineffective hyper-parameter tuning methods.
Z. Li, et.al	2020	FCL (full center loss)	The experimental results depicted the stability of the developed approach over others for detecting the frauds in credit cards.	The developed approach was ineffective to deal with the drift problem.
X. Zhang, et.al	2019	HOBA (homogeneity-oriented behavior analysis)	This model was capable of recognizing more deceitful transactions in comparison with other methods and offered lower FPR (false positive rate).	It is impossible to evaluate the computing cost of the formulated model due to which a larger variable was created.
C. Charitou, et.al	2020	GAN (generative adversarial network)	The experimental outcomes indicated that the investigated model was more efficient as compared to other ML (machine learning) algorithms. This model had generated optimal outcomes on other domains which faced an issue of class imbalance.	The performance of this model was found poor on synthetic data.

2.3 Credit Card Fraud Detection using General Techniques

C. Sudha, et.al (2021) devised a MVE (majority vote ensemble) algorithm to detect the frauds in credit card accurately [25]. The major goal of this algorithm was to integrate behavior, operational and transactional attributes into a single attribute. The WMSP (Web Markov Skeleton Process) was deployed to determine the behavior of users as fraud or authentic. RF (Random Forest) was utilized to gather and classify the operational attributes and SVM (Support Vector Machine) for transactional attributes. The devised algorithm made the implementation of the outcomes obtained from utilized algorithms for predicting the frauds. The results of

experiments exhibited that the devised algorithm offered higher accuracy to detect the frauds in credit cards.

J. Forough, et.al (2020) established an ensemble model on the basis of sequential modeling of data in which DRNN (deep recurrent neural network) and a new voting system relied on ANN (artificial neural network) algorithms were implemented for detecting frauds in credit card [26]. Thereafter, the voting algorithm was trained using a new algorithm. Two real time datasets were executed in the simulation. The simulation outcomes depicted that the established model was more adaptable in contrast to other methods.

E. Esenogho, et.al (2022) suggested an effectual technique for detecting the frauds in credit card in which a NNE (neural network ensemble) algorithm and a hybrid DR (data resampling) technique was executed [27]. The ensemble technique was constructed with LSTM (long short-term memory) in AdaBoost (adaptive boosting) algorithm. Moreover, a SMOTE-ENN (synthetic minority oversampling technique and edited nearest neighbor) algorithm was employed to develop the hybrid technique. A real time dataset was considered to compute the suggested technique. The experimental results revealed the supremacy of the LSTM ensemble approach over other technique as this approach offered a sensitivity upto 99.6% and specificity of 99.8%.

2.3 Table

Author	Year	Technique Used	Findings	Limitations
C. Sudha, et.al	2021	MVE (majority vote ensemble) algorithm	The results of experiments exhibited that the devised algorithm offered higher accuracy to detect the frauds in credit cards.	The accuracy of this algorithm was mitigated in case of least amount of labeled samples.
J. Forough, et.al	2020	a new voting system	The simulation outcomes depicted that the established model was more adaptable in contrast to other methods.	The major limitation of this model was its unsuitability in a real time scenario.
E. Esenogho, et.al	2022	NNE (neural network ensemble) algorithm and a hybrid DR (data resampling) technique	The experimental results revealed the supremacy of the LSTM ensemble approach over other technique as this approach offered a sensitivity upto 99.6% and specificity of 99.8%.	The suggested technique was incapable of predicting the frauds related to known impostors and their previous activities.
			credit cards.	
J. Forough, et.al	2020	a new voting system	The simulation outcomes depicted that the established model was more adaptable in contrast to other methods.	The major limitation of this model was its unsuitability in a real time scenario.
E. Esenogho, et.al	2022	NNE (neural network ensemble) algorithm and a hybrid DR (data resampling) technique	The experimental results revealed the supremacy of the LSTM ensemble approach over other technique as this approach offered a sensitivity upto 99.6% and specificity of 99.8%.	The suggested technique was incapable of predicting the frauds related to known impostors and their previous activities.

III. Conclusion

The main objective of data mining is to dig out the valuable information from publicly available rough or unprocessed data collected from numerous sources. The prediction, on the other hand, aims to forecast the future possibilities on the basis of the historic episodes. The two main tasks in data mining are feature extraction and classification. Over the past few years, researchers have put forward many classification schemes for the detection of credit card related scams. The existing methods of the feature extraction are not efficient enough to establish relationships among features. The machine learning are the best performing algorithms for the credit card fraud detection. In future, transform learning algorithms will be applied for the credit card fraud detection.

References

- [1]. A. Agrawal, S. Kumar and A. K. Mishra, "A Novel Approach for Credit Card Fraud Detection," 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom), 2015, pp. 8-11
- [2]. Y. Lucas et al., "Dataset Shift Quantification for Credit Card Fraud Detection," 2019 IEEE Second International Conference on Artificial Intelligence and Knowledge Engineering (AIKE), 2019, pp. 97-100
- [3]. N. Carneiro, G. Figueira and M. Costa, "A data mining based system for credit-card fraud detection in e- tail", Decision Support Systems, vol. 95, no. 7, pp. 91-101, March 2017
- [4]. F. Carcillo, Y. L. Borgne, O. Caelen, Y. Kessaci and G. Bontempi, "Combining unsupervised and supervised learning in credit card fraud detection", Information Sciences, vol. 2, no. 12, pp. 568-572, 16 May 2019
- [5]. M. Nur-E-Arefin and M. S. Islam, "Application of Computational Intelligence to Identify Credit Card Fraud," 2018 International Conference on Innovation in Engineering and Technology (ICIET), 2018, pp. 1-6
- [6]. A. Srivastava, M. Yadav, S. Basu, S. Salunkhe and M. Shabad, "Credit card fraud detection at merchant side using neural networks," 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), 2016, pp. 667-670
- [7]. A. Roy, J. Sun, R. Mahoney, L. Alonzi, S. Adams and P. Beling, "Deep learning detecting fraud in credit card transactions," 2018 Systems and Information Engineering Design Symposium (SIEDS), 2018, pp. 129-134
- [8]. T. Choudhury, G. Dangi, T. P. Singh, A. Chauhan and A. Aggarwal, "An Efficient Way to Detect Credit Card Fraud Using Machine Learning Methodologies," 2018 Second International Conference on Green Computing and Internet of Things (ICGCIoT), 2018, pp. 591-597
- [9]. N. Kalaiselvi, S. Rajalakshmi, J. Padmavathi and J. B. Karthiga, "Credit Card Fraud Detection Using Learning to Rank Approach," 2018 International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC), 2018, pp. 191-196
- [10]. S. Xuan, G. Liu, Z. Li, L. Zheng, S. Wang and C. Jiang, "Random forest for credit card fraud detection," 2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC), 2018, pp. 1-6
- [11]. C. V. Priscilla and D. P. Prabha, "Influence of Optimizing XGBoost to handle Class Imbalance in Credit Card Fraud Detection," 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), 2020, pp. 1309-1315
- [12]. S. Benson Edwin Raj and A. Annie Portia, "Analysis on credit card fraud detection methods," 2011 International Conference on Computer, Communication and Electrical Technology (ICCCET), 2011, pp. 152-156
- [13]. R. R. Papat and J. Chaudhary, "A Survey on Credit Card Fraud Detection Using Machine Learning," 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI), 2018, pp. 1120-1125
- [14]. J. O. Awoyemi, A. O. Adetunmbi and S. A. Oluwadare, "Credit card fraud detection using machine learning techniques: A comparative analysis," 2017 International Conference on Computing Networking and Informatics (ICCN), 2017, pp. 1-9
- [15]. S. Wang, G. Liu, Z. Li, S. Xuan, C. Yan and C. Jiang, "Credit Card Fraud Detection Using Capsule Network," 2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC), 2018, pp. 3679-3684
- [16]. K. Modi and R. Dayma, "Review on fraud detection methods in credit card transactions," 2017 International Conference on Intelligent Computing and Control (I2C2), 2017, pp. 1-5
- [17]. M. R. Dileep, A. V. Navaneeth and M. Abhishek, "A Novel Approach for Credit Card Fraud Detection using Decision Tree and Random Forest Algorithms," 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), 2021, pp. 1025-1028
- [18]. A. A. Taha and S. J. Malebary, "An Intelligent Approach to Credit Card Fraud Detection Using an Optimized Light Gradient Boosting Machine," in IEEE Access, vol. 8, pp. 25579-25587, 2020
- [19]. A. Salazar, G. Safont and L. Vergara, "A New Method for Fraud Detection in Credit Cards Based on Transaction Dynamics in Subspaces," 2019 International Conference on Computational Science and Computational Intelligence (CSCI), 2019, pp. 722-725
- [20]. D. Devi, S. K. Biswas and B. Purkayastha, "A Cost-sensitive weighted Random Forest Technique for Credit Card Fraud Detection," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2019, pp. 1-6
- [21]. G. K. Arun and K. Venkatachalapathy, "Convolutional Long Short Term Memory Model for Credit Card Detection," 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA), 2020, pp. 1168-1172
- [22]. Z. Li, G. Liu and C. Jiang, "Deep Representation Learning With Full Center Loss for Credit Card Fraud Detection," in IEEE Transactions on Computational Social Systems, vol. 7, no. 2, pp. 569-579, April 2020
- [23]. X. Zhang, Y. Han and Q. Wang, "HOBA: A novel feature engineering methodology for credit card fraud detection with a deep learning architecture", Information Sciences, vol. 12, no. 12, pp. 2945-2956, 16 May 2019
- [24]. C. Charitou, A. d. Garcez and S. Dragicevic, "Semi-supervised GANs for Fraud Detection," 2020 International Joint Conference on Neural Networks (IJCNN), 2020, pp. 1-8
- [25]. C. Sudha and D. Akila, "Majority vote ensemble classifier for accurate detection of credit card frauds", Materials Today, vol. 1, no. 5, pp. 2149-2163, 4 March 2021

- [26]. J. Forough and S. Momtazi, "Ensemble of deep sequential models for credit card fraud detection", *Applied Soft Computing*, vol. 3, no. 19, pp. 8545-8551, 7 Nov. 2020
- [27]. E. Esenogho, I. D. Mienye, T. G. Swart, K. Aruleba and G. Obaido, "A Neural Network Ensemble With Feature Engineering for Improved Credit Card Fraud Detection," in *IEEE Access*, vol. 10, pp. 16400-16407, 2022