Analysis of Machine and Deep Learning Approaches for Credit Card Fraud Detection

P. Divya, D. Palanivel Rajan, and N. Selva Kumar

Abstract In modern days, digitalization increased more demand because of faultless, ease, and convenient use of payment online. More people are choosing to pay the money through online mode through a safe gateway in e-commerce or e-trade. Today's reality seems we are on the fast-growing to a cashless society. As indicated by the World Bank Report in the year of 2018 most of transactions are non-cash and also increased to 25%. Because of so many banking and financial companies spending more money to develop a application based on current demand. False transactions can happen in different manners and can be placed into various classifications. Learning approaches to classification play an essential role in detecting credit card fraud detection through online mode. There will be two significant reasons for the challenges of credit card detection. In the first challenge as the usage of the card has normal behavior or any fraudulent and second as most of the datasets are misrepresented for challenging to classify. In this paper, we investigate the machine and deep learning approaches usage of credit card fraud detection and other related papers and that merits and demerits and, of course, discussed challenges and opportunities.

Keywords Pay online · Credit card · Machine learning · Deep learning · Fraud detection

P. Divya · N. Selva Kumar
CSE Department, Coimbatore Institute of Engineering and Technology, Coimbatore, Tamil Nadu, India
e-mail: divisrecme@gmail.com

N. Selva Kumar
e-mail: mselvaa618@gmail.com

D. Palanivel Rajan (✉)
CSE Department, CMR Engineering College Kandlakoya (V), Hyderabad, Telangana, India
e-mail: palanivelrajan.d@gmail.com

A. Kumar and S. Mozar (eds.), *ICCCE 2020*, Lecture Notes in Electrical Engineering 698, https://doi.org/10.1007/978-981-15-7961-5_24

1 Introduction

Financial Fraudulent has created significant influences in day to day life and financial sectors. Fraudulent activities are lead to reduce the impact of financial sectors and also digitalization. Many financial institutions are worked to protect the people's money in various ways to address the issues. However, Intruders has conceived new technology against the protective models. Credit card fraud has increased gradually in many ways and its leads to financial loss and trust in all banking sectors. People are using to consuming the financial products for the benefits like as

1. Ease of use
2. Keep Customer credit history
3. Protection of Purchases

Detection for fraud involves finding scarce fraud activities as early as possible among different legitimate transactions. Techniques of fraud detection are rapidly developing to conform throughout the world with different emerging fraudulent techniques [1].

Nevertheless, the emergence of new techniques for fraud detection becomes much more complicated due to the current extreme limitation of the exchange of opinions in fraud prevention [2, 3]. The Fig. 1 represents the overall Financial Fraud Categorization.

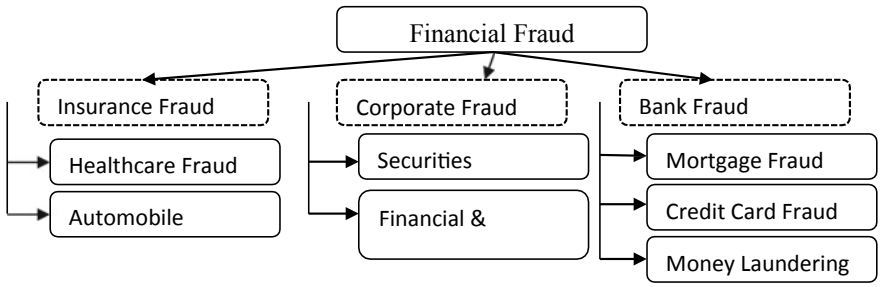

Fig. 1 Financial fraud categorization

1.1 Credit Fraud Detection Using Machine Learning Work Process

1.1.1 Collecting Data

First, the information gathering is very important because its strengthen the model. The precision of the model relies upon the measure of information on which it is

prepared because accurate information has gives better performs. For distinguishing cheats explicit to a specific business, you have to enter an ever-increasing number of measures of information into your model. This will prepare your model so that it distinguishes extortion exercises explicit to your business flawless.

1.1.2 Extricating Features

Feature extraction is basic operation to removing the data of every single string related to an unrelated or unnecessary data for efficient computation. These can be the area from where the exchange is made, the personality of the client, the method of installments, and the system utilized for exchange.

1.1.3 Character

This parameter is utilized to browse a client's email address, versatile number, and so forth, and it can check the FICO assessment of the financial balance if the client applies for an advance.

1.1.4 Area

It checks the IP address of the client and the misrepresentation rates at the client's IP address and dispatching address.

1.1.5 Method of Payment

It checks the cards utilized for the exchange, the name of the cardholder, cards from various nations, and the paces of misrepresentation of the ledger utilized.

1.1.6 System

It checks for the quantity of versatile numbers and messages utilized inside a system for the exchange (Fig. 2).

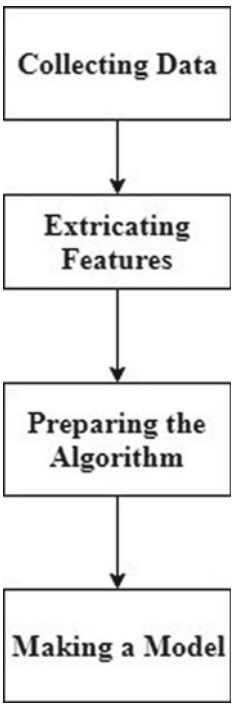

Fig. 2 Credit fraud detection using machine learning work process

1.1.7 Preparing the Algorithm

Once you have made an extortion location calculation, you have to prepare it by giving clients information with the goal that the misrepresentation discovery calculation figures out how to recognize fraud and authenticate exchanges.

1.1.8 Making a Model

Once you have prepared your misrepresentation discovery calculation on a particular dataset, you are prepared with a model that works for distinguishing 'deceitful' and 'non-false' exchanges in your business. The benefit of Machine Learning in extortion recognition calculations is that it continues improving as it is presented to more information. There are numerous strategies in Machine Learning utilized for extortion recognition. Here, with the assistance of some utilization cases, we will see how Machine Learning.

2 Challenges of Credit Fraud Detection

Fraud detection mechanisms are trim to several difficulties and problems listed here. In terms of achieving the best results, an active fraud detection strategy must be able to tackle these challenges.

2.1 Importance of Misclassification

Different misclassifying failures have various meanings in the function of fraud prevention. This is not a harmful to mislabel a fraudulent activity as cheating as usual to detect a fraudulent payment. Even though the classification failure will be identified in more inquiries over the first instance.

2.2 Cost-Efficient of Fraud Detection

The system should take into account both the cost of fraudulent behavior that is detected and the cost of preventing it.

2.3 Imbalanced Data

Credit card fraud detection data has imbalanced nature. It means that minimal percentages of all credit card transactions are fraudulent. This causes the detection of fraud transactions very difficult and imprecise.

2.4 Lack of Flexibility

Classification algorithms are usually faced with the problem of detecting new types of standard or fraudulent patterns. The supervised and unsupervised fraud detection systems are inefficient in detecting new patterns of healthy and fraud behaviors, respectively.

2.5 Overlapping Data

Many transactions may be considered fraudulent, while they are Normal (false positive) and reversely, a fraudulent transaction may also seem to be legitimate (False negative). Hence obtaining a low rate of a false positive and false negative is a crucial challenge of fraud detection systems [4–6].

3 Methods of Machine Learning for Credit Fraud Detection Algorithms

3.1 Logistic Regression

It is a directed learning system that is utilized when the choice is unmitigated. It implies that the outcome will be either 'misrepresentation' or 'non-extortion' if exchange happens. Let us consider a situation where exchange happens, and we have to check whether it is a 'fake' or 'non-fake' exchange [7]. There will be given arrangement of parameters that are checked, and, based on the likelihood determined, we will get the yield as 'misrepresentation' or 'non-extortion.'

3.2 Decision Tree

It is utilized where there is a requirement for the grouping of strange exercises in exchange for an approved client. These calculations comprise of imperatives that are prepared on the dataset for arranging misrepresentation exchanges. For example, consider the situation where a user creates transactions. The system will create a decision tree to predict the probability of fraud based on the transaction made [8].

3.3 Random Forest

It multiple decision tree trees to improve the outcomes. Every choice of tree checks for various conditions. They are prepared on arbitrary datasets, and, because of the preparation of the choice trees, each tree gives the likelihood of the exchange being false and non-extortion [9].

3.4 Neural Networks

Neural Networks is an idea enlivened by the working of a human brain. Neural systems in Deep Learning uses various layers for calculation. It utilizes psychological registering hat aides in building machines equipped for utilizing self-learning calculations that include the utilization of information mining, design acknowledgment, and standard language preparation. It is prepared on a dataset going through various layers a few times. It gives more precise outcomes than different models as it utilizes psychological registering, and it gains from the examples of approved conduct and along these lines recognizes false and trustful exchanges [10].

3.5 Artificial Immune System

Artificial Immune System (AIS) is an ongoing subfield dependent on the organic analogy of the insusceptible framework. Artificial Immune System expanded the accuracy, decline the expense, and framework preparing time. Liking between antigens was determined to utilize a novel technique in the AIS-based Fraud Detection Model [11].

3.6 Support Vector Machines

SVM is a regulated learning model with related learning calculations that can examine and perceive designs for grouping and relapse tasks. SVM is a double classifier. The fundamental thought of SVM was to locate an ideal hyper-plane that can isolate occurrences of two given classes, straight. This hyper plane was thought to be situated in the hole between some minor cases called bolster vectors. Presenting the piece capacities, the thought was stretched out for straight in divisible information. A portion of work speaks to the spot result of projections of two information focuses on a high dimensional space [12].

3.7 Bayesian Network

Bayesian Network is built to display the conduct of dishonest clients, and the next model is developed, accepting the client as real. At that point, exchanges are named fake on-false by these systems. Bayes rule creates the likelihood of misrepresentation for any approaching transaction. Bayesian Network needs preparing of

information to work and require high handling speed. BN is more precise and a lot quicker than neural organize [13].

3.8 Hidden Markov Model

The Hidden Markov Model is a limited arrangement of states, every one of which is related to a likelihood circulation. Many probabilities represent advances among the states called progress probabilities. In a specific express, a result or perception can be produced, as indicated by the related likelihood dispersion. It is just the result, not the state unmistakable to an outer on looker, and like these states are "covered up" to the outside; subsequently, the name Hidden Markov Model. HMM uses cardholder's expenditure behavior to detect fraud. Dissimilar cardholders have their different expenditure behavior [14].

3.9 Autoencoders

Autoencoders is an unsupervised Neural Network. It is an information pressure calculation which takes the information and experiencing a compacted portray a land gives the recreated output [15]. Autoencoders, it gives a decent precision. Be that as it may, on the off chance that we investigate Precision and Recall of the dataset, it is not performing enough (Tables 1 and 2).

3.10 Advantage of Using Machine Learning in Credit Fraud Detection

3.10.1 Speed

Machine Learning is broadly utilized on account of its quick calculation. It examines and forms information and concentrates new examples from it inside no time. For individuals to assess the information, it will take a ton of time, and assessment time will increment with the measure of information [16].

3.10.2 Adaptability

As an ever-increasing number of information is nourished into the Machine Learning-based model, the model turns out to be progressively exact and influential in the forecast.

Table 1 Different machine learning method used in credit fraud detection

References no.	Methods	Learning approaches	Advantages	Disadvantages
7	Logistic regression	Supervised	Velocity variables to discover more characteristics of the algorithm	Cost of retraining the classifier
8	Decision Tree	Supervised	High agility Easily build a system	Accuracy is low compared to neural network
9	Random Forest	Supervised	Very fast in detection training time is less	Accuracy is low compared to the neural network
10	Neural Network	Supervised	High accuracy High speed in detection	It takes a considerable amount of training time
11	Artificial Immune System	Unsupervised	High accuracy in pattern predications and easy to integrate with another system	Memory generation phase & calculation of affinity is time-consuming
12	Support Vector Machines	Unsupervised	SVM is resilient Gives a distinctive solution	Reduced speed in detection process Accuracy is medium
13	Bayesian Network	Unsupervised	High accuracy High speed in detection	It takes a tremendous amount of training time
14	Hidden Markov Model	Unsupervised	High speed in detection process	Accuracy is low
15	Autoencoders	Unsupervised	It gives a decent precision	Precision and recall was not good
16	Machine Learning Hybrid BGWO	Supervised	The huge amount of data sets Less predictive	Precision and recall was not good
17	Hybridization of swarm intelligence	Supervised	Imbalance data sets	Precision and recall was not good

Table 2 Different types of evaluation criteria for credit card fraud detection

Evaluation criteria	Formula	Description
Accuracy	$\frac{TP+TN}{TP+TN+FP+FN}$	Accuracy is the percentage of correctly categorized credit card fraud detection
Precision	$\frac{TN}{FP+TN}$	The ability of a classification model to return only related
Recall	$\frac{TP}{TP+FN}$	The ability of a classification model to identify all related occurrences
F1 measure	$2 * \frac{Sensitivity * Specificity}{Sensitivity + Specificity}$	The distinct metric that pools recall and precision using the harmonic mean
Receiver operating characteristic	True positive rate plotted against false positive rate	Plots the true positive rate versus the false positive rate as a function of the model's threshold for classifying a positive

3.10.3 Effectiveness

Machine Learning calculations play out the excess assignment of information examination and attempt to discover concealed examples redundantly. Their productivity is better in giving outcomes in examination with manual endeavors. It dodges the event of bogus positives, which means its effectiveness.

3.10.4 Open Issues

While charge card extortion recognition has increased wide-scale consideration in writing, there are yet a few issues (various noteworthy open issues) that face specialists and have not been tended to before adequately.

3.11 Nonexistence of Standard and Complete Charge Card Benchmark or Dataset

Master Card is intrinsically private property because making an appropriate benchmark for this design is very troublesome. Small datasets can cause a misrepresentation recognition framework to learn extortion stunts or ordinary conduct in part. Then again, the absence of a standard dataset makes the correlation of different systems risky or inconceivable. Numerous scientists utilized datasets that are just allowed to creators and cannot be distributed to protection contemplations [17].

3.11.1 Nonexistence of Standard Calculation

There is not any fantastic calculation known in Visa extortion writing that beats all others. Each technique has its possess focal points and burdens, as expressed in past areas. Joining these calculations to help each other's advantages and spread their shortcomings would be of incredible intrigue.

3.11.2 Nonexistence of Appropriate Measurements

The impediment of the right measurements to assess the after effect so extortion location framework is yet an open issue. The nonexistence of such measurements causes in eptitude of specialists and professionals in looking at changed methodologies and deciding the need for most effective extortion discovery frameworks.

3.12 Lack of Versatile Visa Misrepresentation Location Frameworks

Albeit heaps of explores have been researched MasterCard extortion recognition field, there are none or constrained versatile methods that can learn in formation stream of exchanges as they are directed. Such a framework can refresh its inner model and systems over a period without should be relearned disconnected. Subsequently, it can include different cheats (or standard practices) promptly to display learning misrepresentation deceives and recognize them after that as quickly as time permits.

4 Conclusion

Credit fraud detection is one of major problem in the banking process. False exercises are uncommon occasions that are difficult to display and in steady advancement. The massive volume of exchanges happening in day to day activity, and it is necessary to use machine learning-based automated tools to use and predict the fraudulent activities in the banking transaction. In this paper, we present a comparative study of different machine learning techniques such as logistic regression, decision tree, random forest, neural network, artificial immune system, support vector machines, Bayesian network, hidden Markov model, autoencoders are presented with advantage and disadvantage.

References

1. Roy A, Sun J, Mahoney R, Alonzi L, Adams S, Beling P (2018) Deep learning detecting fraud in credit card transactions. In: 2018 systems and information engineering design symposium SIEDS 2018, pp 129–134
2. Thennakoon A, Bhagyani C, Premadasa S, Mihiranga S, Kuruwitaarachchi N (2019) Real-time credit card fraud detection using machine learning. In: Proceedings of the 9th international conference on cloud computing, data science & engineering (confluence), pp 488–493
3. Sinayobye JO, Kiwanuka F, Kaawaase Kyanda S (2018) A state-of-the-art review of machine learning techniques for fraud detection research. In: Proceedings - international conference on software engineering, pp 11–19
4. Pillai TR, Hashem IAT, Brohi SN, Kaur S, Marjani M (2018) Credit card fraud detection using deep learning technique. In: Proceedings - 2018 4th international conference on advances in computing, communication & automation ICACCA 2018, pp 1–6
5. Popat RR, Chaudhary J (2018) A survey on credit card fraud detection using machine learning. In: Proceedings of the 2nd international conference on trends in electronics and informatics, ICOEI 2018, no ICOEI, pp 1120–1125
6. Rajora S et al (2019) A comparative study of machine learning techniques for credit card fraud detection based on time variance. In: Proceedings of the 2018 IEEE symposium series on computational intelligence SSCI 2018, pp 1958–1963
7. Rushin G, Stancil C, Sun M, Adams S, Beling P (2017) Horse race analysis in credit card fraud- deep learning, logistic regression, and gradient boosted tree, pp 117–121. IEEE
8. Zeager M, Sridhar A, Fogal N, Adams S, Brown D, Beling P (2017) Adversarial learning in credit card fraud detection, pp 112–116. IEEE
9. Mahmoudi N, Duman E (2015) Detecting credit card fraud by Modified Fisher Discriminant Analysis. Expert Syst Appl 42:2510–2516
10. Halvaiee N, Akbari M (2014) A novel model for credit card fraud detection using Artificial Immune System. Appl Soft Comput 24:40–49
11. Vlasselaer V, Bravo C, Caelen O, Eliassi-Rad T, Akoglu L, Snoeck M, Baesens B (2015) APATE: a novel approach for automated credit card transaction fraud detection using network based extensions. Decis Support Syst 75:38–48
12. Zareapoor M, Shamsolmoali P (2015) Application of credit card fraud detection: based on bagging ensemble classifier. In: International conference on intelligent computing, communication & convergence, pp 679–685
13. Bahnsen AC, Aouada D, Stojanovic A, Ottersten B (2016) Feature engineering strategies for credit card fraud detection. Expert Syst Appl 51:134–142
14. Harkous H, Bardawil C, Artailand H, Daher N (2018) Application of hidden Markov model on car sensors for detecting drunk drivers. In: 2018 IEEE international multidisciplinary conference on engineering technology (IMCET), Beirut, pp 1–6. https://doi.org/10.1109/imcet.2018.8603030
15. Luoand T, Nagarajan SG (2018) Distributed anomaly detection using autoencoder neural networks in WSN for IoT. In: 2018 IEEE international conference on communications (ICC), Kansas City, MO, pp 1–6. https://doi.org/10.1109/icc.2018.8422402
16. Velliangiri S (2019) A hybrid BGWO with KPCA for intrusion detection. J Exp Theor Artif Intell. https://doi.org/10.1080/0952813X.2019.1647558
17. Velliangiri S, Karthikeyan P (2019) Hybrid optimization scheme for intrusion detection using considerable feature selection. Neural Comput Appl. https://doi.org/10.1007/s00521-019-04477-2