Proceedings of the 4th International Conference on Signal Processing and Machine Learning
DOI: 10.54254/2755-2721/51/20241172

Credit card transaction fraud detection based on machine learning

Yuxin Jiang

Department of Economics, University of Michigan - Ann Arbor - 500 S State St, Ann Arbor, MI 48109, US

yyyuxin@umich.edu

Abstract. The rise of e-commerce payment systems has been swift due to our society's rapid advancement. However, the transparency and vulnerability of the internet have opened new avenues for illicit access, resulting in a significant surge in financial fraud cases, particularly credit card transaction fraud. Detecting and mitigating such incidents has become crucial. One branch of artificial intelligence, machine learning, offers a potent solution. It operates by utilizing various algorithms and models that rely on established patterns and reasoning without explicit instructions. By processing vast amounts of historical data, machine learning models can identify underlying data relationships, allowing them to make accurate predictions based on input data. Therefore, it emerges as a highly effective method for credit card transaction fraud detection. This paper reviews the research methods for credit card fraud, introduces credit card transaction fraud detection data sets, and outlines machine learning algorithms and models related to credit card fraud detection. It also considers the future prospects for machine learning development and possible challenges.

Keywords: Credit Card Transaction, Fraud Detection, Machine Learning, Deep Learning.

1. Introduction

Due to the ease of completing transactions online by entering credit card information, credit card transaction fraud has become one of the biggest risks facing the global financial industry. Credit card transaction fraud means using other people's credit card information or the falsification of credit card information to conduct illegal transactions through crooked means. With the global popularity of innovative systems for online payment like Paypal, as well as the rapid growth of top businesses like Amazon and Flipkart (which together accounted for 80% of India's online retail business in 2015), and Jingdong and Alibaba (which together accounted for more than 70% of China's market in 2016), e-payments are reaching a large number of new consumers. It is a gold mine for online crooks. The Nielsen Report indicates that global losses increased from around $8 billion in 2010 to $21 billion in 2015 as a result of credit card fraud. In 2017, unauthorized credit card operations reached a staggering 16.7 million victims. Additionally, according to the Federal Trade Commission, there were 40% more credit card fraud claims in 2017 than there were in 2016. The states with the highest number of such crimes per capita were California and Florida, which respectively reported about 13,000 and 8,000 cases. By 2020, this amount is predicted to increase to $31 billion. The harm caused by a data breach is immeasurable.

© 2024 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2755-2721/51/20241172

If credit card fraud occurs frequently, leading to the theft of funds and finally loss of customer adherence and brand reputation, organizations, banks, merchants, and customers will all face a great crisis.

The danger of credit card fraud is not only a small financial loss but also carries a lot of significant negative impacts. For cardholders, it can lead to the disclosure of their identity information, substantial loss of property, and even affect their personal credit records. For banks, if the supply chain between the bank and the credit card customer is broken, the bank has to bear the risk of not getting the money. From the perspective of legal risk, the essence of credit card cash is that the cardholder is maliciously lending money, which is, to some extent, suspected of fictitious loan fraud. From the financial system risk, the cumulative effect caused by credit card fraud not only affects the effect of the national control of excess currency liquidity but also leads to credit card overdrafts after the formation of a large number of overdue bad debts, disrupting the normal financial order. Therefore, credit card fraud brings incalculable risks and losses to people's economic and social lives.

Fraudulent incidents manifest in various forms across multiple industries. For making as accurate a decision as possible, most fraud detection techniques mix several datasets in order to create a connected overview of legitimate and fraudulent payment information. Factors like device identification, internet protocol address, geographic location, "BIN" number, global latitude and longitude, historical transaction records, and actual transaction data must be taken into this decision. For example, if there are anomalies in a transaction, such as geographically suspicious IP addresses, or the hardware and software configuration of unfamiliar payment devices, the fraud detection system will be alarmed. In actuality, this means that, based on the analysis results and the data at their disposal, merchants and card issuers employ a set of operational guidelines or analytical algorithms to identify fraud.

There are a number of analytical methods and detecting techniques available for credit card transaction fraud, including obtaining pre-build fraud risk assessments from external anti-fraud organizations; estimating the likelihood that a transaction is fraudulent by using predictive machine learning algorithms that learn from historical data; and setting criteria that every transaction must satisfy for approval, such as no OFAC alerts[1], matching SSN[2], and remaining below the deposit and withdrawal threshold.

Certainly, there are some issues in the existing methods of credit card transaction fraud detection. It is challenging for us to mine the potential information between various components to derive the most precise causes and conclusions because of the numerous correlated factors involved in credit card transaction fraud. Moreover, because of the high level of confidentiality surrounding credit card transactions, reproducing the majority of published research in this field is infeasible. Additionally, the task of credit card transaction fraud detection remains difficult due to the ever-evolving nature and patterns of fraudulent transactions. Therefore, machine learning with good data mining capability is a good method. Creating machine learning models that can operate at their best and achieve a high level of precision in detecting credit card transaction fraud is significant.

Machine learning constitutes a subset of artificial intelligence where computers gain knowledge from previous experiences (data) and enhance their predictive capabilities without the need for explicit programming. Machine learning has become the most commonly used technology in fraud detection in light of its less time expenditure, more accurate results, and diverse applications.

This paper presents common datasets for credit card transaction fraud detection, including traditional fraud detection techniques, and advanced algorithms based on machine learning. Finally, after analyzing and summarizing these methods of fraud detection, the paper discusses the future research and development of machine learning.

2. Datasets

Since credit card transaction information is personal and private, the information is more difficult to obtain, which poses a great challenge to researchers. Fortunately, Carcillo, Fabrizio [3] proposed a credit card fraud detection dataset. Many researchers have presented some algorithms based on this dataset for detecting fraudulent credit card transactions. There are a total of 284,807 transactions in this dataset during two days in September 2013 from cardholders in Europe, of which 492 are fraudulent. The

DOI: 10.54254/2755-2721/51/20241172

validation of the proportion of positive and negative fraud samples in this dataset is not balanced due to the relatively small proportion of fraud cases in life, with fraud data representing 0.172% of all transactions. This dataset provides transaction time and transaction amount as well as other PCA features to avoid privacy, and ultimately use the Area of Precision Recall Curve (AUPRC) to evaluate the algorithm performance. As Figure 1[3], in order to get the distribution of the fraud and normal transactions (normal:0; fraud:1) and check for its class imbalance, it outputs the pie chart of their possibility.

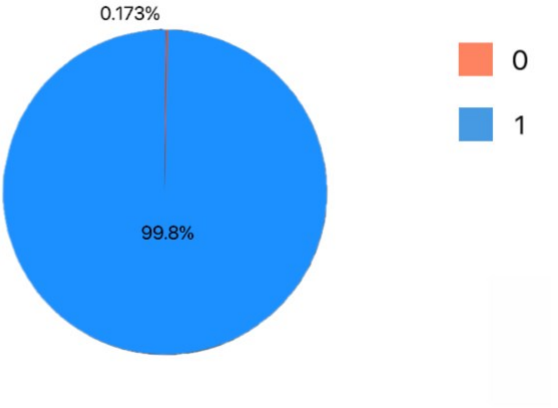

Figure 1. Distribution of Fraud and Normal Transactions.

In the credit card fraud data distribution graph shown in Fig. 1, the red color indicates fraudulent data and the blue color indicates normal data. Due to the low percentage of fraud samples, there is a serious sample imbalance problem, which brings great challenges to the credit card fraud detection task.

As Figure 2[3], the relationship between time and fraud is observed by drawing two line graphs of the change in non-fraudulent transaction counts over time and the change in transaction counts with fraudulent behavior over time.

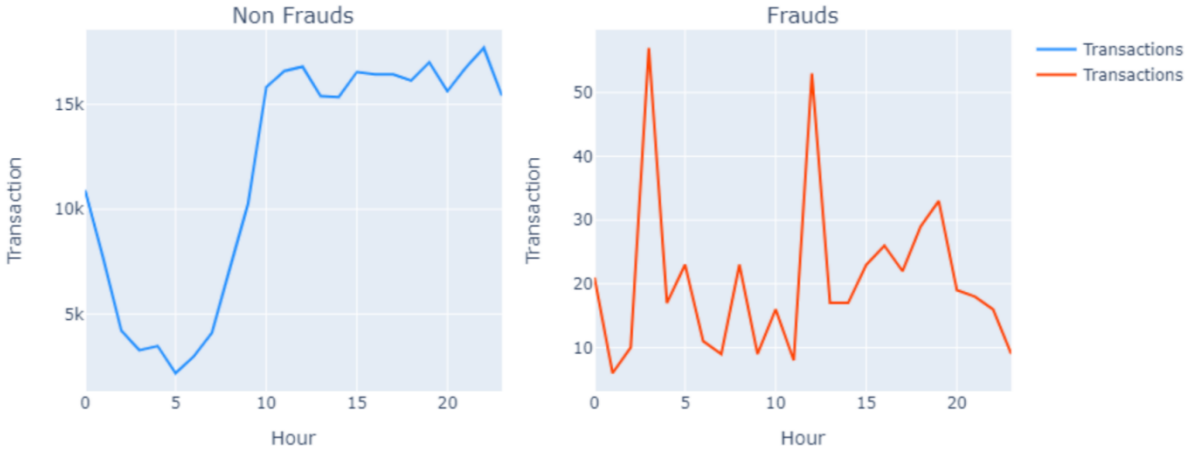

Figure 2. Transaction Count with Non Frauds and Frauds over Time.

DOI: 10.54254/2755-2721/51/20241172

3. Method

In the development history of credit card transaction fraud detection, there are numerous traditional ways, such as card security features, risk scores, and so forth. As artificial intelligence has grown so fast last several years, AI-related algorithms have found extensive application in fraud detection systems, leading to significant enhancements in the accuracy and efficiency of detection results.

3.1. Card Security Features

Faced with the occurrence of increasing cases of transaction fraud, enterprises, and banks use many tools and technologies to judge and detect fraud.

For example, the credit card network has developed many security functions, including address authentication services [4], 3-D security [5], CVV [6] card verification, etc. These features are designed to determine whether a consumer is a cardholder by viewing or validating their personal identity or registration information. However, these security functions will increase a certain degree of friction in the consumption process, slow down the consumption speed of customers, and complicate the purchase process. For address authentication, the user identity can be verified by comparing whether the user's consumption location is consistent with the previous records, or by asking the consumer to enter the mailing address and confirm whether it is correct. Even though the grid planning methodology used in urban planning and the quantification of geographic areas through zip codes has made the delineation of the address system simple and clear in much of North America, there are still significant problems. For example, renaming of roads, construction of multiple residences at the same address, multiple different designations for the same residence, and errors in user input due to address information being too long can complicate the address validation process and cause great inconvenience to the user. For 3-D security, it requires customers to supply extra details of identification, such as a password or a single-use code, to successfully finalize a transaction, apart from the standard card information. This additional layer of security greatly reduces the feasibility of cybercriminals using stolen card information to conduct online transactions. Nevertheless, there are two significant drawbacks to 3D security. Firstly, it can lead to customers abandoning their purchases during the checkout process due to its perceived complexity, resulting in a substantial decrease in conversion rates. Secondly, the implementation of 3D security can be costly, as merchants may have to bear payment fees for each transaction. Another widely used verification method is CVV (Card Verification Value). The CVV is a three- or four-digit code located on the rear side of a credit card, providing an additional layer of security when making online purchases. This code is known only to the cardholder. However, while shopping online, consumers may inadvertently expose their CVV to unfamiliar websites or malware, potentially leading to CVV theft. Additionally, during in-person transactions, if someone else sees the CVV, it increases the risk of later credit card theft. Therefore, some e-commerce companies led by Amazon cancel these verification steps like above, in order to ensure the purchase experience of customers. If there are too many verification steps before payment, it leads to customer attrition; while if the identity of the customer cannot be accurately verified, it increases the likelihood of transaction fraud. Therefore, one of the challenges facing credit card fraud detection technology is how to confirm someone's identity before a transaction as concisely as possible.

3.2. Risk Scores

Risk scores [7] determine the likelihood of transaction fraud by using statistical models to evaluate many factors in each transaction. Typically, these models produce a numerical score that signifies the probability of a transaction being fraudulent. A higher score suggests a more suspicious order. Merchants can use these risk scores to make educated guesses about specific user actions to minimize potentially fraudulent transactions, or to use additional security measures to ensure that every transaction is risky again. If the risk score of any one transaction is greater than a set threshold, it will be defined as fraudulent and rejected. In order to determine the risk score as accurately as possible, we need to consider and test a variety of risk factors, such as bank identification number country matching, city/state and zip code matching, proxy detection, distance between IP address and billing address, IP addresses in high-

DOI: 10.54254/2755-2721/51/20241172

risk countries, and so on, which are derived from past transaction records. Subsequently, these data undergo preprocessing, which includes tasks such as data cleaning to eliminate duplicate entries, address missing values, and identify any anomalous data points. Following preprocessing, machine learning algorithms [8] like dimensionality reduction, logistic regression, Naive Bayes, decision trees, and support vector machines come into play to construct risk-scoring models. These models learn patterns and trends related to potential risks by analyzing historical data. Once the model is constructed, it undergoes a training and validation phase. To evaluate the model's performance and validity, a number of metrics are examined, such as F1-score, accuracy, precision, and recall. Finally, upon deployment of the model in a real-world setting, transactions are continuously monitored in real-time to detect potential risky behavior. If a suspicious transaction is identified, the model generates an associated risk score to indicate the level of potential risk. Organizations utilizing risk scoring can capitalize on precise fraud scores to establish an appropriate strategy for responding to risks. This approach aims to lower the probability of fraud incidents transpiring and mitigate the aftermath in case fraud does take place. At the same time, tra*n*saction fraud can be comprehensively evaluated and prioritized just with a single number, greatly reducing the cost of manual review. In essence, this tool aids in safeguarding merchants against the detrimental effects of credit card fraud, which encompasses financial losses, harm to reputation, strained relationships with payment processors and card issuers, and more.

3.3. AI Fraud Detection System

Machine learning [9] has a significant impact on the field of identifying and preventing online fraud. It involves employing a set of artificial intelligence (AI) algorithms that are educated using historical data from your records. These algorithms then propose risk-related rules that can be enforced. These rules serve to either authorize or block specific user actions, such as instances of suspicious logins, identity theft, or fraudulent transactions. During the training process of the machine learning system, it's essential to flag past instances of both fraudulent and legitimate cases. This step is crucial to minimize instances of false positives and enhance the precision of the risk rules. In practice, the algorithmic model can be continuously optimized by user-generated data, and finally, the prediction accuracy of the model can be improved over time.

In the early stages of research on machine modeling, researchers used simple algorithms for abnormal transaction detection like logistic regression, k-nearest neighbor, decision trees, etc. With the passage of time and advancement in technology, researchers have improved and developed more advanced algorithms, such as neural networks.

A study was carried out by Khatri et al. [10] to assess how well different machine-learning methods detect fraudulent credit card transactions. They explored several machine learning approaches including decision trees, k-nearest neighbor, logistic regression, random forest, and naive Bayes. The researchers employed a dataset created from European cardholders that was substantially class-imbalanced to evaluate the effectiveness of these methods. Precision, which was calculated for each classifier in their experiments, served as the main performance metric. The findings of the experiment showed that DT achieved a precision of 85.11%, KNN reached 91.11%, LR showed 87.5%, and RF exhibited 89.77% precision, while NB lagged behind with a precision of 6.52%. We could see because KNN considers neighbors, its result is 3.61% higher than LR’s.

V. Dornadula, S. Geetha et al [11] also applied a number of machine learning algorithms to tackle the challenge of credit card fraud. In order to address the dataset's significant skew, the researchers utilized the SMOTE sampling technique. They considered several machine learning methods, including DT, LR, and Isolation Forest (IF). The primary performance metric examined was accuracy. Through their improvement, the outcomes revealed that DT achieved an accuracy of 97.08%, while LR reached an accuracy of 97.18%.

Navanshu Khare et al [12] developed a system for credit card transaction fraud detection by employing multiple machine learning algorithms, which included LR, DT, RF, and support vector machine (SVM). To gauge the effectiveness of every machine learning approach, the researchers utilized classification accuracy as their performance metric. The experimental results indicated that LR achieved

DOI: 10.54254/2755-2721/51/20241172

an accuracy of 97.70%, DT reached 95.50%, SVM showed 97.50%, and RF excelled with an accuracy of 98.60%. Despite these favorable outcomes, the authors maintained that implementing sophisticated pre-processing methods could potentially further enhance the performance of these classifiers.

Different machine learning methods have similar accuracy and have achieved good results so far. It models the elements to be observed, which include KNN, SVC, NB, DTC, RFC, XGB, LGB, GGC, ABC, and LR, produces statistical plots of their correlated predicted and actual results with their precision, recall, f1-score, and support respectively, and summarizes the accuracy of all model results as Figure 3.

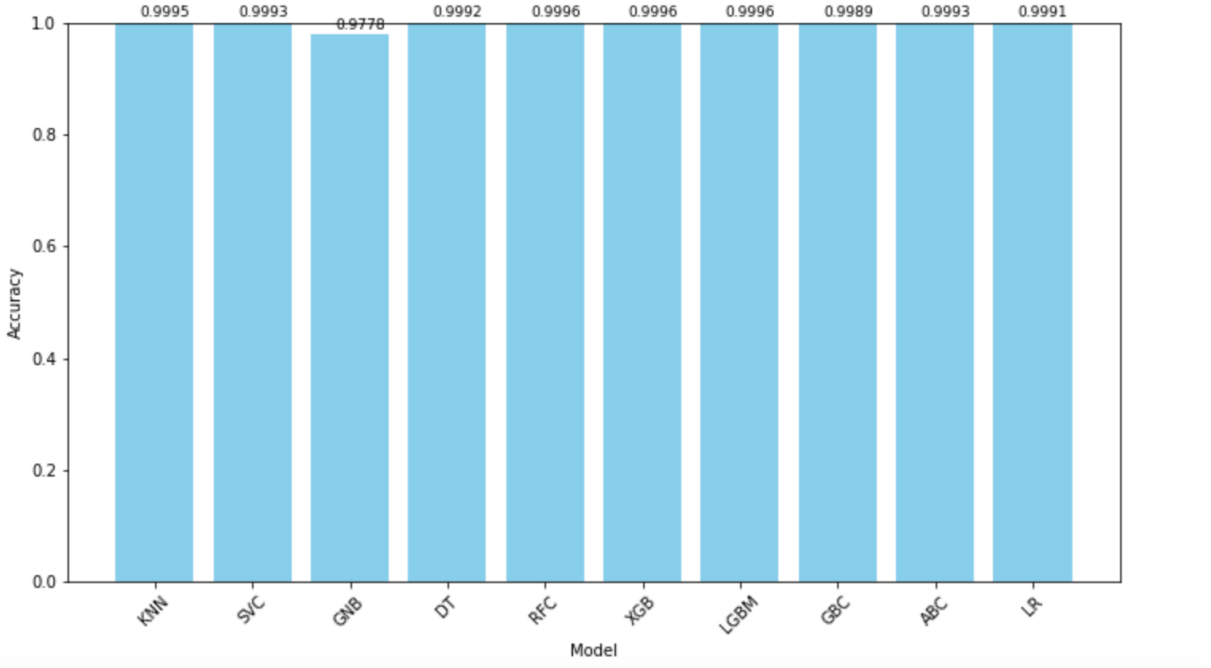

Figure 3. Model Comparison.

In addition to these common algorithms, with the joint efforts of Warren McCulloch, Geoffrey Hinton [13], and other researchers, deep learning, a branch of machine learning, has been proposed to significantly improve the work efficiency of the machine model. Within deep learning, various techniques and architectures are employed, including artificial neural networks [14], autoencoders, deep belief networks, generative adversarial networks, convolutional neural networks, and recurrent neural networks. Deep learning harnesses neural networks to mimic the human brain's ability to process data and make decisions. In the above algorithms, the artificial neural network algorithm (ANN) is separated into the training part and the testing part. The first step of the training part is to load and read the dataset and then it will be scaled, normalized, and segmented. After preprocessing the data, ANN starts training and analyzing the model and predicting the fraudulent behavior. When getting the results, the trained data is stored for testing later. The testing part of the process is roughly the same as the training part, and the only difference is that the stored training model will be used to test and classify the data. Compared to the SVM and KNN algorithms, ANN is able to achieve 99.92% [10] accuracy and is most appropriate for detecting credit card fraud. However, even though ANN could reach such a high accuracy rate, its precision and recall are lower than SVM.

3.4. Application

Running an AI-driven method for credit card transaction fraud detection requires satisfying a lot of crucial conditions, which will guarantee that the model receives the best detection score possible.

DOI: 10.54254/2755-2721/51/20241172

To achieve the purpose of training high-quality machine learning models, a significant number of internal historical records is necessary. Therefore, without enough valid and invalid previous transaction data, it is impossible to run the models and get accurate results. In other words, the quality of the inputs determines the performance of the training process. Using dimensionality reduction and data enrichment strategies is a common approach since it is rare that the training set contains two classes of medium-volume data samples.

The quality of previous data may skew the models. This argument means that if the information collector does not organize the data neatly and appropriately, or even mixes the data of fraudulent transactions with the data of normal transactions, it is possible to cause significant deviations in the output results. Fraud detection will only be effective if you have an adequate number of well-organized and impartial data, as well as business logic that exactly matches the machine learning model you choose. Therefore, the use of machine learning in AI models needs to be based on excellent data sets.

4. Conclusion

In general, the detection of credit card transactions based on machine learning has good results. This paper introduces methods like k-nearest neighbors, k-means, random forest classifier decision tree classifier, and naive Bayes, which exhibit strong performance in this field. However, these algorithms have their drawbacks. For example, first of all, machine learning algorithms have high requirements for the quality of collected data. If the data's source is unreliable, the results will necessarily be incorrect. Second, it needs to collect a large amount of user data, which is inefficient and expensive for trial operation. Besides, data is essential in machine learning, serving as one of its core pivots, but the way data is collected has raised significant privacy concerns. Some major corporations have collected user data without their knowledge, using it for their own commercial benefit. In light of these problems and challenges, future research could explore the development of lightweight models and methods that require smaller sample sizes, aiming to reduce application costs and enhance processing speed. Simultaneously, it is essential to persist in studying deep learning and effectively implementing this advanced and powerful approach for precise credit card transaction fraud detection.

Research on machine learning is still ongoing. But in the meantime, there are some guidelines[15] we should keep in mind to minimize the incidence of credit card transaction fraud. First, never click on a link that asks you for personal information, even though it looks like your bank is sending you this message. In addition, when making an online payment, check to see if the website address begins with "https://" (a standard communication protocol for the secure transmission of data) and verify that it is an official URL. Besides, you can keep track of changes in your accounts by monitoring them manually. For example, you can set up alerts at your card issuer for various transactions, like receiving text alerts when a transaction exceeds $20. Once you realize that you have not made a payment, but you receive a text alert, you can immediately know that someone has made a purchase using your credit card. Finally, when you discover that a thief has used your credit card to make a purchase, you should immediately report the theft to the local authorities and the credit card company. The faster you report the theft, the less likely you are to be held responsible for fraudulent purchases.

References

[1] Yenouskas, Joseph F., and Tierney E. Smith. "Fair Credit Reporting Act Litigation Developments on Standing." The Business Lawyer 76 (2021):2-3.

[2] Komuves, Flavio L. "We've Got Your Number: An Overview of Legislation and Decisions to Control the Use of Social Security Numbers as Personal Identifiers." J. Marshall J. Computer & Info. L. 16 (1997): 525-537.

[3] Dal Pozzolo, Andrea, et al. "Learned lessons in credit card fraud detection from a practitioner perspective." Expert systems with applications 41.10 (2014): 4915-4928.

[4] Save, Prajal, et al. "A novel idea for credit card fraud detection using decision tree." International Journal of Computer Applications 161.13 (2017): 3.

DOI: 10.54254/2755-2721/51/20241172

[5] Bouch, Anthony. "3-D Secure: A critical review of 3-D Secure and its effectiveness in preventing card not present fraud." University of London, Londra, erişim 8 (2011): 39-63.
[6] Barker, Katherine J., Jackie D'amato, and Paul Sheridon. "Credit card fraud: awareness and prevention." Journal of financial crime 15.4 (2008): 404-405.
[7] Bhatla, Tej Paul, Vikram Prabhu, and Amit Dua. "Understanding credit card frauds." Cards business review 1.6 (2003): 13.
[8] Popat, Rimpal R., and Jayesh Chaudhary. "A survey on credit card fraud detection using machine learning." 2018 2nd international conference on trends in electronics and informatics (ICOEI). IEEE, 2018: 3-5.
[9] Ileberi, Emmanuel, Yanxia Sun, and Zenghui Wang. "A machine learning based credit card fraud detection using the GA algorithm for feature selection." Journal of Big Data 9.1 (2022): 1-5.
[10] Khatri, Samidha, Aishwarya Arora, and Arun Prakash Agrawal. "Supervised machine learning algorithms for credit card fraud detection: a comparison." 2020 10th international conference on cloud computing, data science & engineering (confluence). IEEE(2020): 680-683.
[11] Dornadula, Vaishnavi Nath, and Sa Geetha. "Credit card fraud detection using machine learning algorithms." Procedia computer science 165 (2019): 631-641.
[12] Khare, Navanshu, and Saad Yunus Sait. "Credit card fraud detection using machine learning models and collating machine learning models." International Journal of Pure and Applied Mathematics 118.20 (2018): 825-838.
[13] Asha, R. B., and Suresh Kumar KR. "Credit card fraud detection using artificial neural network." Global Transitions Proceedings 2.1 (2021): 35-41.
[14] Mathew, Amitha, P. Amudha, and S. Sivakumari. "Deep learning techniques: an overview." Advanced Machine Learning Technologies and Applications: Proceedings of AMLTA 2020 (2021): 599-608.
[15] Lee, Jen Grondahl, and Gini Graham Scott. “Preventing credit card fraud: A complete guide for everyone from merchants to consumers.” Rowman & Littlefield, 2017: 113-123.