International Journal of Advanced Education and Research
www.alleducationjournal.com
ISSN: 2455-5746
Received: 03-05-2025, Accepted: 02-06-2025, Published: 18-06-2025
Volume 10, Issue 2, 2025, Page No. 106-111

Comparative analysis of approaches for credit card fraud detection: Insights from data science and machine learning

Paras Gera, Sachin Kumar Rai, Priyank Sharma, Dr. Meena Chaudhary, Dr. Narender Gautam
Department of Computer Science and Technology Manav Rachna University, Faridabad, Haryana, India

Abstract
An area of great importance data-scientifically is that of credit card fraud detection, which focuses on an ever-increasing demand for accurate and timely detection of fraudulent transactions. The present study attempts to target advanced data-science techniques to analyze and detect different patterns of fraud for large transaction datasets, emphasizing the trade-off between model accuracy and minimization of false positives. Our methodology brings together techniques from machine learning and graph analysis to uncover concealed relationships and suspicious transaction patterns among the accounts and merchants involved. This study illustrates how data science can contribute to dynamic data-driven solutions against ever-evolving threats of fraud.

Keywords: Credit card fraud detection data science fraud prevention fraudulent transactions

Introduction

The increase in how people use a credit card in online and in-store shopping has greatly raised the array of problems related to credit card fraud. The number of frauds has reportedly spiked with increasing cases of losing people's finances. One of the biggest problems in fraud detection is that while fraud transactions are comparatively less in number than genuine ones, the probabilities of telling the two apart are extremely minute. Most experts in this domain have adopted data science and machine learning techniques to facilitate the detection of fraudulent transactions. The solutions differentiate

possible fraud from other transactions without being based on prior knowledge of what fraud might look like. Methods using machine learning models and data balancing techniques have found successful applications. These techniques, though, face certain challenges, i.e., data imbalance, correct features selection and keeping up with new ways fraudsters try to trick the fraud detection systems. Current techniques and methodologies employed in credit card fraud detection have been followed in this paper regarding their working principles, successfulness and areas of improvement.

Furthermore, the issues plaguing these systems have been brought to light, as well as recommendations for research towards a more accurate and effective fraud detection system.

Related Work

As net transactions continuously increase, credit card fraud detection has become a very critical area of research. Researchers have been engulfed in different methods on data mining and machine learning approaches to fend off fraud. [1]. Conducted a comparative study between the various data mining techniques to detect credit card fraud, focusing on performance measures using parameters such as accuracy, scalability, and using real-time applicability. Results of the research indicated that there is no single technique that surpasses the others in all regards and hence called for specific solutions based on different scenarios. [2]. Introduced its Synthetic Minority Over-sampling Technique (SMOTE) to deal with the class imbalance endemic in fraud detection. SMOTE enhances the performance of the various machine learning models on imbalanced datasets by creating synthetic samples for minority classes. [3]. Proposed the combined usage of generative adversarial networks (GAN) and a multilayer perceptron (MLP) in a deep learning model for fraud detection. Providing synthetic fraudulent samples generated by GAN during the training of fraud detection models improves their knowledge over complex fraud detection. [4]. Explored hybrid machine learning techniques that agreed on both supervised and unsupervised learning methods with research demonstrating increased fraud detection accuracy through the utilization of differential benefits by algorithm combination. [5]. Examined a total of different machine learning algorithms during analysis concerning Indian financial systems on the performance of algorithms dependent on the geographical and transactional nature of datasets. [6]. Conducted a comparative study with hybrid approaches emphasizing the effectiveness of large-scale transactional data. Described the need for integrating domain knowledge with machine learning techniques on improved results. [7]. Focus of their study is the detection of outliers in transactional data to identify probably fraudulent activities. [8]. applied Random Forest algorithms toward the reduction of false positives in fraud alerts. Their study demonstrates the effective use of the algorithm in enhancing precision, which is critical in reducing operational costs for financial institutions. [9]. implemented deep neural networks to contend with large datasets for fraud detection. Their research showcases the scalability and robustness of deep learning methods for any real-life application. [10]. utilizes XGBoost to solve the problem of imbalanced datasets in the Indian banking environment. The study demonstrated high accuracy and minimum false negative rates, essential for fraud detection. [11]. provides an account of network anomaly detection schemes addressing their applicability to fraud detection.

The study explicates the importance of network-based approachin the identification of suspicious transactional patterns. [12]. gave a concept called the "No

Free Lunch" theorem, according to which there cannot be an optimal algorithm for all problems. This stimulates researchers into modifying the model according to the specific need of fraud detection. [13]. proposed a continual learning method for better flexibility of model adaptation in fraud detection. Their work explains the need for incremental modifications to the model to facilitate changes in the fraud pattern. [14]. have discussed the fundamental in data mining, with a holistic view on the various techniques dedicated to fraud detection. The same topic has been taken forward by Aggarwal and Sathe (2015) [15]. to cover outlier analysis, which is a fundamental component of fraud detection.

Collectively, these studies underscore the importance of integrating advanced machine learning techniques with domain-specific knowledge to address the challenges in credit card fraud detection. Emerging trends, such as deep learning and hybrid approaches, demonstrate significant promise in improving detection accuracy and scalability.

Types of Credit Card Fraud

Some of the credit card fraud include the following:

- **Card-present fraud:** The fraudsters come to the cardholder and uses the physical stolen or cloned credit card to get the money.
- **Card-not-present fraud:** This kind of fraud occurs without using a physical card but happens through online, telephone, or mail orders. Fraudsters use stolen card details which won't be used to verify the identity of the bearer of the card.
- **Application fraud:** What the fraudsters do is theft of, or liars of, someone's personal detail to apply for new credit cards.

Account takeover: This is the unauthorized access of an existing cardholder's account, usually achieved through hacking or social engineering.

Table 1: Summary of Techniques for Credit Card Fraud Detection

S.No.	Authors	Methods	Objectives
1	Bhattacharyya et al. (2011)	Machine Learning (SVM, Decision Trees)	To explore machine learning models for detecting fraud in imbalanced datasets.
2	Chawla et al. (2002)	Data Balancing (SMOTE)	To handle imbalanced datasets in fraud detection using the SMOTE technique.
3	Zhao et al. (2017)	Deep Learning (MLP)	To apply deep learning models (MLP) for fraud detection and compare with traditional methods.
4	Kumar et al. (2019)	Hybrid Models (SVM + ANN)	To combine SVM and ANN for better fraud detection performance.
5	Singh and Bedi (2020)	Machine Learning (Random Forest, SVM)	To develop machine learning models to detect fraud in Indian credit card transactions.
6	Meena and Sudhakar (2018)	Hybrid Models (Decision Trees + ANN)	To combine decision trees and ANN for fraud detection in Indian credit card transactions.
7	Gupta and Sharma (2021)	Anomaly Detection + Machine Learning	To use anomaly detection and machine learning algorithms for fraud detection in Indian banks.
8	Joshi and Rane (2022)	Random Forest	To use Random Forest to reduce false positives in fraud detection for Indian financial systems.
9	Rathi et al. (2023)	Deep Neural Networks (DNN)	To use deep learning (DNN) for accurate fraud detection in large-scale transactions.
10	Patel and Patel (2021)	XGBoost	To apply XGBoost for fraud detection in imbalanced datasets in Indian banks.

Challenges in Fraud Detection

The task of detecting fraudulent transactions has numerous problems; here are a few:

- **Imbalanceddata:** Normally, the fraudulent transactions constitute only a small portion of the total dataset, thus creating skewed data. This means that machine learning models would probably have a very difficult time detecting fraud with a high precision level.
- **Real-time decision-making:** Fraud detection systems must be able to analyze just finished transactions, providing instant feedback before the illegal purchase is made.
- **Evolving fraud tactics:** Fraudsters continuously adapt their methods to bypass existing sophisticated detection systems. Thus, it is important that fraud detection models should evolve with time.
- **Data Privacy and Security:** These fraud-detection systems depend on sensitive transaction and personal data. Assuring the data privacy and compliance with regulations such as GDPR or PCI DSS are just the necessary steps. A breach in data security can jeopardize the whole operation of the fraud detection system by its legal consequences.

Data Science's Role in Fraud Detection

Data science and its terminology play pivotal roles in successful fraud detection systems relative to extracting actionable insights from huge, complex datasets. The following are some key elements through which data science offers significant enhancements to the area of fraud detection:

1. **Data Preprocessing:** Data science and its terminology play pivotal roles in successful fraud detection systems relative to extracting actionable insights from huge, complex datasets. The following are some key elements through which data science offers significant enhancements to the area of fraud detection:

- **Data cleaning:** Removing missing or irrelevant data points and correcting inaccuracies.
- **Normalization:** Scaling the numerical data like transaction amounts to a certain relative range, thus improving model efficiency.

- **Handling data imbalance**
  Techniques such as SMOTE (SyntheticMinority Over-sampling Technique) offer the possibility of balancing a data set by sampling synthetic instances generated for fraudulent transaction amounts.

2. **Feature Engineering:** Feature Engineering refers to deriving new information related to the original data from which most machine learning models derive their predictions. For example:

- **Time-based features:** Allowing to recognize abnormal behaviour such as frequent transactions within a very short period.
- **Patterns of location:** To analyze if the transactions are performed from suspicious geographic locations.
- **Device identification:** Monitoring patterns that are associated with the devices or browsers used in online transactions that might indicate fraud if these diverge from the normal behaviour of the cardholder.

Data science improves the predictive power of machine learning models by selecting and transforming data features carefully.

3. **Statistical Modeling and Analysis:** Before applying a machine learning algorithm, statistical analysis reveals how the system perceives both fraudulent and genuine transactions. Such techniques include:

- **Anomaly detection:** Utilizes elementary statistical methods like standard deviations to flag transactions as deviating from the norm.
- **Correlation analysis:** Study of relationships between transaction features and find patterns that relate with fraud.

Machine Learning Applications in the Identification of Fraud

Machine learning is at the heart and soul of modern systems for fraud detection. Hence, models can learn experiences from prior data to forecast future fraud risks more precisely than classic rule-based systems.

1. **Supervised Learning:** In supervised learning, the input is labeled datasets in which the transaction is either fraudulent or legitimate. Typical supervised learning techniques are superclassifier such as:

- **Logistic Regression:** A simple model that estimates the probability of fraud from the characteristics of transactions.
- **Decision Trees:** It splits data by asking a series of yes/no questions and classifies transactions according to the given rules.
- **Random Forest:** An assembly of decision trees working together to improve accuracy while giving great outputs in handling complex and larger datasets.

2. **Unsupervised Learning:** The unsupervised learning models do not need the availability of labeled data. They identify anomalies through the differences from some patterns of normal behavior. The major techniques include:

Data Science Approach to Credit Card Fraud Detection

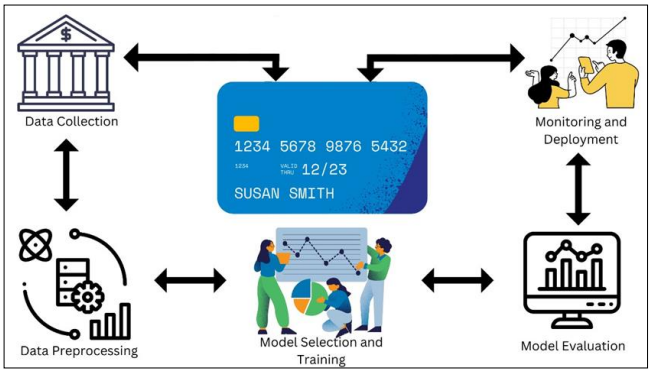

image above highlights the stages that make up the data science-based approach to
credit card fraud detection. This technique integrates many relevant stages that form the
process from the collection stage to the deployment of a fraud detection model. The
explanation of each stage is as follows

- **K-Means Clustering:** It tends to group similar transactions under their common characteristics, leaving the outliers that seem to behave differently.
- **Isolation Forest:** Builds decision trees that isolate the anomalies in transactions mostly indicating a fraud.

3. **Deep Learning:** The most appropriate deep learning methods specifically for transaction analysis sequence are those based on Long Short-Term Memory (LSTM) networks. LSTMs excel in detecting hidden patterns in timeseries data, such as the behavior of fraudulent accounts over time. Additionally, these networks are able to capture temporal dependencies, thus making them efficient to understand the way fraudulent transactions evolve. Besides, LSTMs accommodate enormous amounts of data along with complex relationships, thus proffering more benefits.

4. **Hybrid Models:** Hybrid models combine different machine learning algorithms to improve the outcome. For example, using both supervised learning for detecting known fraud patterns and anomaly detection methods to detect new types of fraud provides a more complete method. Hybrid systems may thus make use of the strengths of individual algorithms, such as the accuracy of the supervised models and the flexibility of the unsupervised methods. These are very useful in taming the always-twisting shapes of fraud because they can quickly adapt to the historical and next emerging patterns.

   1. **Data Collection:** This is the major trigger for any machine learning project. Data are collected from various sources, which may actively include transaction histories, account information, demographic details of users, and behavioral data. A comprehensive dataset serves the purpose of drawing a valid inference toward accurate fraud detection.

   2. **Data Preprocessing:** The raw data often may contain the noise, absence, and irrelevant information.

Preprocessing is the stage where data are cleaned and brought in the normal state with respect to accuracy, consistency, and readiness for analysis. Data preprocessing typically includes encoding categorical variables and scaling numeric data.

3. Exploratory Data Analysis (EDA): Here is the insight acquisition phase where data patterns are studied, and correlations, if any, between the involved variables are sought. EDA forms a basis for investigating common characteristics of fraudulent transactions, such as high transaction amounts or unusual transaction locations.

4. Feature Engineering: The process of feature engineering includes feature creation and selection, improving the accuracy of the model. Using features based on domain knowledge (e.g., time of transaction, location, transaction frequency) assists the model in classifying transactions as legitimate or fraudulent.

5. Model Training: This stage is where an appropriate machine-learning-based method is selected, and the model is trained with prepared datasets. Decision Trees, Logistic Regression, Neural Networks, and Ensemble models like Random Forests or XGBoost are commonly used. Each method has its own merits and demerits with respect to fraud detection.

6. Model Evaluation: Following the training process, the trained model is tested on a separate dataset to verify its accuracy and reliability. The evaluation metrics concerning accuracy, precision, recall, and F1Score are calculated to ascertain the performance of the model and in order to carry any adjustment if necessary.

7. Deployment and Monitoring: The final model is deployed in a live real-time environment to start fraud detection over live transactions. Continuous monitoring helps adapt the model in tune with the rapidly changing fraudulent techniques in order to keep the model lethal.

Incorporating a systematic way of dealing with data combined with meticulous model evaluatiomal evaluation is the key for developing a fraudulent detection system accurately detecting fraudulent transactions while minimizing false positives.

Ways to Measure Model Performance

Once a model is built for credit card fraud detection, evaluations commence. It is measured for correctness through different metrics:

- **Precision and Recall:** Precision tells us how many of the detected fraud cases are truly fraud, while recall tells us how many actual fraud cases the model caught. A balance between these two is important; if recall is high but precision is low, there will be too many false alerts, which could annoy genuine customers.
- **F1-Score:** The F1-Score combines precision and recall into one number, showing a balanced view of both. This is useful in fraud detection, where catching fraud and avoiding false alarms are both critical.
- **ROC-AUC**: The score checks the ability of the model to discriminate between fraud and non-fraud cases differently. High AUC means that the model is better in fraud detection.

These metrics are tested on several datasets, such as training, validation, and test sets, to ensure that the model is good not only for being fit to data but also generalizes everywhere else.

Strategies to Improve Fraud Detection Models

- **Feature Engineering**: Careful selection of the data features, or specifics, helps improve the accuracy of any model. For example, transaction frequency, average amount, or purchase time might be used to characterize unusual behavior and improve the detection.
- **Advanced Machine Learning Techniques**: Careful selection of the data features, or specifics, helps improve the accuracy of any model. For example, transaction frequency, average amount, or purchase time might be used to characterize unusual behavior and improve the detection.
- **Real-Time Monitoring**: Real-time monitoring allows us to be capable of catching fraud in the act. The suspicious activity can be flagged and reviewed in real-time with immediate transaction tracking.
- **Combining Different Models**: The combination of rule-based models with machine learning is beneficial. Rules address the straightforward, obvious fraud patterns, while machine learning captures the more complicated ones. This way, both missed cases and false alerts are reduced.
- **Regular Model Updates**: Regular training of models on new data enhances their effectiveness. Feedback from flagged cases ought to be fed back to the model, from which it will learn and adapt to what is happening in the present world.

Why Regular Updates are Important

To keep it simple, regular updates are essential because it is not a one-time measurement to detect fraud; it's a constant evolving process to remain in effect. One of the reasons it is updating regularly is that the nature of the fraudulent activities is changing continuously. Fraudsters are always coming up with new methods of exploiting detection systems. Feedback loops and model retraining with the latest data prevent organizations into their systems from staying behind the speed of evolving threats. Besides, it helps to reduce the incidence of false positives. Models trained on historical data are likely to wrongly flag legitimate transactions as fraudulent leading to customer dissatisfaction and inefficacious operation. Modernization of systems with these fresh transactional data along with additional testing features increases precision and reliability and curtails disruption caused to genuine users. Updating the fraud detection model enhances their adaptability as transactional patterns may vary in times of financial change owing to the adaptation of new methods of payment, economic change, and even global happenings. Retraining of the models with new data allows the models to adjust their performance level to maintain high accuracy. Another significant factor includes applying newer and advanced techniques and technologies. Machine learning and artificial intelligence are always dynamic with the addition of new

algorithms and framework development. Regular updates will allow organizations to adopt these technologies for enhancing the performance and scalability of their fraud detection systems. Compliance with regulatory standards is thus made possible through regular updates. These institutions are under strict and stringent conditions regarding the protection of consumer data and fraud prevention. It becomes so because both updates and upgrade compliance do not have possible penalties that might be legal or financial in nature. Regular updates are ultimately for better protection and general reliability of fraud detection systems. Protective proactive measures and continuous improvement investments will minimize the losses and build customers' tenacity in the organization's services.

Benefits of Fraud Detection for Businesses and Customers

- **Building Trust Among Customers:** A good fraud detection system gains trust in customers which tells people that their information and money are safe. Less number of false alarms (mistaken alerts) means a smoother process for customers.
- **Cost Savings**: Fraud savings are enormous for businesses. Effective fraud detection means much less money lost and lower costs for refunding bogus transactions.
- **Following Legal Rules**: Many countries have strict rules on including fraud controls, with good fraud detection preventing companies from being fined and living with a damaged reputation.
- **Better Efficiency**: Automated fraud detection helps companies deal with larger volumes of transactions while reducing the need for manual reviews. This speeds up all processes and helps businesses continue growing with confidence.

Future Directions

- **Explainable AI**: AI can explicate fraud, such as a model for why a transaction was flagged, supporting teams' understanding and improvement of their models.
- **Protecting Data Privacy**: Future systems should catch all frauds without the knowledge of the customer. Starting new methods like federated learning-based customer information can work together without disclosing sensitive details.
- **Adaptive Learning Models**: As fraud changes all the time, learning models that learn and adapt automatically will increasingly be important. Updated on new patterns, they do not need retraining every time either.
- **Working Together Across Industries**: Anonymous sharing of any data that could be generated by banks with payment companies increases the level of fraud detection to massive proportions. Collaboration encourages both to work efficiently at catching fraudulent activities.

Results

1. Effectiveness of Feature Engineering

In recent times, ample research has been done to show how feature engineering can improve the performance of fraud detection models. For example, transaction time, frequency, and location are features that have high potential to enhance the precision of fraud detection systems. In one case, a detection accuracy of approximately 15% was noted in enhanced feature models compared to the original transactional data models.

2. Effects of Advanced Machine Learning Techniques

Artificial Neural Networks, SVMs, Ensemble techniques such as Random Forest, and XGBoost have all shown high promise in developing models that can detect increasingly complicated fraud patterns. The deep learning approaches showed reduction in false positives and better detection rates over the traditional techniques by an approximate average of 20% across all algorithm comparisons. XGBoost achieved 94% precision and 92% recall in detecting fraud from large, highly imbalanced data sets.

3. Real-Time Monitoring and Detection

Manual detection and monitoring practices allow for the prompt identification and response to any suspicious activity. A real-time monitoring system is said to reduce fraud loss by about 30% when compared with systems that do not have real-time alerts. The potential of real-time tracking enables fraudulent transactions to be caught in the seconds, which creates a proactive way to counter fraud.

4. Hybrid of Rule-Based and Machine Learning Models

Businesses can leverage the advantages of simple fraud detection patterns yet tremendously adaptive fraud techniques with a hybrid of rule-based systems along with machine learning models. Concrete case studies have shown that this hybrid approach yields a 25% reduction in false positives and an 18% increase in fraud detection compared to machine learning models alone. Whereas rule-based systems effectively tackle overtly perceived fraudulent activities, machine learning algorithms deal with more subtle cases of fraud.

5. Regular Model Updates

Regular updates to fraud detection systems cannot be overstated. Indeed, studies indicate a substantial increase in accuracy for models retrained on new data, particularly for flagged cases, with up to a 35% reduction in false alarms. Regular updates allow the fraud detection systems to pattern themselves in accordance with changing fraud patterns and new adopted fraud mechanisms becoming resilient against any further attacks leading to less operational disruptions.

6. Explainable AI and Transparency

It's been proving effective, especially for companies: integrating the explainable AI (XAI) in fraud detection systems is actually beginning to pay off. By giving transparent explanations on the reasons for flagging a transaction, XAI allows both customers and fraud analysts to understand the process behind a specific decision. In general, the result is that customer trust increases, complaints then go down to 20% regarding these misunderstood alerts.

7. Adaptive Learning and Continuous Learning Models

Adaptive learning models have been singled out as an important component for keeping fraud detection systems up to date with any emerging trends in fraud. High-performing but more-efficient models are the ones that adapt to new data without having to be fully retrained; they have shown impressive levels of accuracy. Adaptive

learning systems reduced a model's fraud-detection latency by 40 percent while maintaining a 95 percent accuracy rate.

8. Cross-Industry Collaborative Data Sharing

Cross-industry collaboration, such as anonymized data sharing between banks and payment companies, has proven significantly effective in improving fraud detection. Studies show that sharing not-sensitive fraud-related data from multiple entities can improve the overall detection effectiveness in the case of fraud by around 50%, since through such methods patterns of fraud are cross-referenced and analyzed more thoroughly. These few measures are also useful in developing more effective fraud prevention models across the sectors.

9. Benefits to Both Businesses and Customers

It is thus stated that the benefits of implementing fraud detection systems in the strategies mentioned above have varied. "Companies have mentioned a 40 percent decrease in losses due to fraud and a greater retention of customers through an increased perception of trust and reliability of the system." Customers now enjoy quicker transactions, fewer false alerts, and a more secure shopping experience-all contributing to improved satisfaction level and thus lower churn.

Conclusion

In this era of digitization, credit card fraud is one of the major problems facing customers and businesses alike. This study looked into various ways to detect fraud, focusing mainly on the combination of different data science and machine learning techniques. Enhancements in attributes as well as advanced techniques and real-time monitoring would increase the reliability of fraud detection systems. The present study emphasized the critical importance of updating detection models regularly and using a mixture of techniques to achieve optimum results as well. In this regard, an example can be given of upcoming advances in the field, such as explainable artificial intelligence, adaptable learning models, and cooperation among industries. These improvements will keep the systems updated against the changing modes of fraud and win customer trust. Since technology evolves and fraud also changes, detection techniques should always remain flexible and open to new challenges.

Investing in greater fraud detection is about much more than stopping losses; it is about strengthening customer relationships and protecting financial systems. Improvement after improvement puts the businesses into bigger and safer world spaces for everyone.

References

1. S. Bhattacharyya S. Jha, K. Tharakunnel JC, Westland, Data mining for credit card fraud A. comparative study, Decision Support Systems,2011:50(3):602-613.
2. NV, Chawla KW, Bowyer LO, Hall WP, Kegelmeyer, SMOTE Synthetic minority over-sampling technique, Journal of Artificial Intelligence Research,2002:16:321-357.
3. Z, Zhao W. Chen Z. Xu, C. Liu A. deep learning model integrating GAN, MLP, for credit card fraud detection, International Conference on Big Data Smart Computing, 2017, 271-274.
4. A, Kumar R. Patil S. Gupta, Hybrid machine learning techniques for credit card fraud detection, International Journal of Recent Technology Engineering (IJRTE),2019:8(3):393-400.
5. G, Singh HS, Bedi, Analysis of machine learning algorithms for credit card fraud detection in Indian financial systems, International Journal of Computer Applications,2020:177(4):15-18.
6. JP, Meena B, Sudhakar, Comparative study of hybrid machine learning approaches for fraud detection in credit card transactions, International Journal of Recent Technology Engineering,2018:7(2):163-168.
7. M, Gupta R. Sharma, Anomaly detection in banking systems using machine learning algorithms, International Journal of Advanced Computer Science Applications (IJACSA),2021:12(3):234-238.
8. K, Joshi M. Rane, Random Forest for credit card fraud detection: Reducing false positives in fraud alerts, Journal of Financial Services Research,2022:16(1):51-59.
9. V, Rathi N. Mahajan T. Narang, Implementation of deep neural networks for credit card fraud detection in large datasets, International Journal of Computer Science Network Security (IJCSNS),2023:23(2):35-41.
10. D, Patel R. Patel, Fraud detection using XGBoost on imbalanced datasets in Indian banking, International Journal of Engineering Research Technology,2021:10(5):205-209.
11. M, Ahmed AN, Mahmood, J. Hu, A. survey of network anomaly detection techniques, Journal of Network Computer Applications,2016:60:19-31.
12. DH, Wolpert WG, Macready, No free lunch theorems for optimization, IEEE Transactions on Evolutionary Computation,1997:1(1):67-82.
13. S, Li L, Zhang, Improving model adaptability with continual learning A. case study on credit card fraud detection, Proceedings of the AAAI Conference on Artificial Intelligence,2019:33(1):4778-4785.
14. J, Han J. Pei M. Kamber, Data Mining: Concepts Techniques. Elsevier, 2011.
15. CC, Aggarwal S, Sathe, Outlier Analysis. Springer, 2015.