International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307 OPEN ACCESS

Available Online at : www.ijsrcseit.com

doi : https://doi.org/10.32628/CSEIT25112469

AI Powered Credit Card Fraud Detection by Using Ensemble Method of Machine Learning

Sankeerthan P[1], Vaishnavi N. M.Sc., M.Phil., (Ph.D.)[2]

[1]Department of Information Technology, Dr. N.G.P Arts and Science College, Coimbatore, Tamil Nadu, India

[2]Assistant Professor, Department of Information Technology, Dr. N.G.P Arts and Science College, Coimbatore, Tamil Nadu, India

ARTICLEINFO

Article History:

Accepted : 13 March 2025

Published: 15 March 2025

Publication Issue

Volume 11, Issue 2

March-April-2025

Page Number

1255-1264

ABSTRACT

The growth of Credit Card (CC) fraud over the last few years necessitates the construction of fraud detection models that are both efficient and robust. This work investigated the use of machine learning models, especially ensemble methods, to improve the detection of CC fraud. We herein introduce an ensemble model that combines various classifiers to solve the dataset imbalance problem that is present in most CC datasets. We employed synthetic over-sampling and under-sampling techniques in certain machine learning algorithms to tackle the same issue. Online transactions have become an essential aspect of life as universe becomes more technological and every industry leverages the web to grow enterprises. Online transactions have been increasing steadily, and this trend is expected to continue. Credit cards are a popular form of internet transaction, but with their widespread use comes a significant drawback: credit card fraud. Since banks are unable to screen every transaction, machine learning is essential to identifying credit card fraud. In our research, we used Kaggle to gather a dataset of 2,844,808 credit card transactions from a European Bank Dataset. There are 492 fraudulent transactions in it; to balance the dataset, we proposed hybrid resampling method and for the detection of credit card fraud, Random Forest Algorithm is employed. The evaluation of the model is evaluated based on accuracy, precision, recall, and F1-score.

Keywords: Credit Card, Ensemble learning, Machine learning, Algorithms, Fraudulent.

Introduction

The rapid digitalization of financial transactions has revolutionized the world economy with unprecedented ease and efficiency. The revolution has, however, been accompanied by a significant increase in credit card fraud, causing heavy financial losses to

individuals, businesses, and financial institutions. Credit card fraud is a general category of criminal behavior encompassing unauthorized transactions, identity theft, and account takeovers, thereby posing a continuous and dynamic threat to the financial ecosystem.

Conventional fraud detection tools are heavily reliant on rule-based systems and pre-defined heuristics to identify suspicious transactions. While these approaches have proven useful up to a point, they are quickly becoming inappropriate for the detection of sophisticated schemes of fraud that typically involve well-advanced techniques such as identity spoofing, synthetic identity theft, and cyber-attacks in coordination. Further, rule-based systems cannot deal with large volumes of transactional data efficiently and cannot detect complicated, dynamic patterns of fraudulent behaviors. As fraudsters continually come up with new ways of avoiding conventional security measures, the need for advanced fraud detection software has never been greater. In response to these challenges, this project proposes the use of an AI-based credit card fraud detection system based on ensemble machine learning techniques. Ensemble learning is a robust approach that employs an array of machine learning models to enhance prediction accuracy and robustness. By using models like Random Forest, Gradient Boosting, and Voting Classifier, the system seeks to enhance fraud detection performance while reducing false positives and false negatives. The ensemble models can process large data sets, detect complex transaction patterns, and respond to changing fraud tactics in real time. The primary objective of this research is to design and implement a high-performance, scalable system for fraud detection that can identify fraudulent transactions with high accuracy. The system will be capable of processing real-time transaction information and provide financial institutions timely insights to effectively mitigate fraud risk. Also, by integrating advanced data analytics techniques, the system will be capable of ongoing learning and updates, and thus continue to be effective in a constantly changing threat landscape. The present research will focus on a number of most critical fraud detection areas like data preprocessing, feature engineering, model selection, and performance estimation. Through the logical analysis of transaction data and utilizing the latest machine learning techniques, the present project aims to create more reliable and effective fraud detection solutions. The results of this research have the potential to significantly enhance fraud protection measures, safeguard monetary funds, and facilitate buyer confidence in electronic money transactions.

LITERATURE REVIEW

Numerous studies in credit card fraud detection have explored different methods to enhance accuracy and eliminate false positives. The following section summarizes literature on fraud detection methods, machine learning methods, and ensemble learning models.

Traditional Fraud Detection Methods:

Rule-based systems have been the prevailing approach to fraud detection. Rule-based systems flag a transaction as fraudulent based on pre-established rules. Their value is, however, capped by their inability to learn and evolve in response to new fraud methods. Statistical approaches like logistic regression and Bayesian networks have been used to detect outliers in transaction patterns. These approaches present some advantage over rule-based systems but still experience problems with high-dimensional data.

Machine Learning-Based Techniques:

Decision Trees, Support Vector Machines (SVM), and Neural Networks are some of the most popular supervised algorithms utilized in fraud detection. These models have been proven to perform very well if they are trained on large sets of tagged data but need to be constantly retrained to avoid a drop in accuracy. Unsupervised learning techniques like clustering algorithms like K-Means and Autoencoders have also been attempted to identify anomalies within transactional data. These models are able to identify

new patterns of fraud without labelled data but have the potential to produce additional false positives.

Ensemble Learning for Fraud Detection:

Researchers have shown in recent research the power of ensemble learning methods to improve fraud detection performance. Techniques like Random Forest, Gradient Boosting, and Voting Classifiers combine several models to improve prediction performance. A study by Liu et al. (2020) showed that the use of ensemble methods is better compared to the application of a single classifier in fraud detection, especially in dealing with imbalanced data sets. XGBoost and LightGBM have proven to be much stronger gradient boosting algorithms that enhance detection rates without incurring high computational costs. The use of real-time fraud detection remains a challenge as it requires the quick processing of large amounts of transactional data. Research indicates that hybrid models integrating machine learning and deep learning architectures (e.g., LSTMs and CNNs) have the potential to enhance real-time fraud detection capability. Big data platforms like Apache Spark and Hadoop have been investigated to create cloud-based fraud detection systems that can process large amounts of transactional data quickly.

Challenges and Future Directions:

Datasets that are class imbalance are a great challenge in fraud detection. Various research work has proposed techniques like Synthetic Minority Over-sampling Technique (SMOTE) to address class imbalance problems. Explainability of Artificial Intelligence (AI) models for fraud detection is also one area of ongoing research. Techniques like SHAP (Shapley Additive explanations) and LIME (Local Interpretable Model-agnostic Explanations) are being investigated to improve model interpretability. Reinforcement learning and federated learning-based continuous learning frameworks have been proposed as possible ways to enhance adaptability and robustness in fraud detection systems.

IMPLEMENTATION PROCEDURE

Implementing a machine learning-powered credit card fraud detection system involves some elementary steps. First, one has to gather an enormous amount of historical credit card transactions that are fraudulent or legitimate. This dataset is used as input to train and test the machine learning model. Some preprocessing activities such as data cleaning, normalization, and feature engineering may be necessary to reshape the data for analysis. Lastly, a prediction model is trained with some machine learning algorithms on the pre-processed data. Logistic regression, decision tree, random forest, support vector machine (SVM), or neural networks are some of the supervised machine learning algorithms that are normally applied for this. The data is typically split between training data and test data in an effort to render the model operational. As the model trains, it becomes proficient at identifying patterns and correlation between features of real and fraudulent transactions. Model performance and model generalization potential could be maximized using hyperparameter tuning and cross-validation strategies. Additional strategies like oversampling or under sampling could be utilized attempting to remove class imbalance common in most fraud detection data sets. Once the model has been trained and validated, it can be put into production to execute in production as either a batch or real-time processor of incoming credit card transactions. The deployed model processes the transactions one at a time and generates a probability or score of the likelihood of the transaction being fraudulent. Cut-offs are employed to label the transactions as valid or fraudulent based on the scores. There needs to be ongoing monitoring and repeated retraining of the model so that it is able to catch up with evolving fraud patterns and operate in the best possible way in the long run. Execution of feedback loop for model updation from fresh labelled data also improves the model to become increasingly accurate and resilient to newer trends of fraud. Lastly, one has to insert the fraud detection system into the existing

system of credit card buying smoothly without crossing the regulatory borders and data protection levels' rates. Audits and testing for the level of effectiveness of the system are instrumental in examining areas of vulnerability to be addressed as well as defining the security level of cardholder transactions.

OBJECTIVES

The objectives of Credit Card Fraud Detection using machine learning are three and aim finally to secure financial transactions against fraud without causing it. The first objective is to develop prediction models that are capable of classifying correctly fraudulent transactions and genuine transactions. This is done by the use of machine learning algorithms to analyze past transaction history to identify patterns, anomalies, and trends with respect to fraud. Second, avoidance of false positives and false negatives in anti-fraud detection is also an objective. False positives occur when legitimate transactions are mistakenly flagged as fraudulent and cause inconvenience to customers, whereas false negatives occur when fraudulent transactions are not detected and cause customers and financial institutions financial loss. Therefore, recall and accuracy need to be balanced so that efficient fraud detection is attained without disrupting legitimate transactions. Moreover, the goal entails frequent updating and training of the fraud detection models to respond to evolving fraud patterns and schemes. This entails applying methods such as regular model retraining, feature engineering, and introducing new sources of data to enhance accuracy and resilience of the detection system in the long run. Moreover, among the primary objectives is enhancing the velocity and efficacy of fraud detection procedures so as to monitor transactions in real-time or near real-time. This entails developing effective and scalable machine learning algorithms in order to handle large amounts of transaction data swiftly and precisely. Adherence to regulatory regimes and data protection acts is also one of the main objectives in detecting credit card fraud. This includes the use of measures for the protection of sensitive customer information and transparency and accountability in applying machine learning models for detecting fraud. Typically, objectives in Credit Card Fraud Detection based on machine learning are to develop accurate, timely, and efficient detection models that are able to accurately pick out fraudulent and genuine transactions with low false positives and false negatives and in accordance with data protection legislation and regulatory needs. Realization of these objectives is highly important for safeguarding financial systems and customers' trust in electronic payment systems.

PROJECT OVERVIEW

Credit card fraud is a wide-ranging problem of particular concern to cardholders and financial institutions. Fraud transactions must be detected early on so that financial loss and users can be protected. With its capacity to analyse huge quantities of data and detect complex patterns, machine learning has also developed as an efficient mechanism for fraud detection. This introduction presents the significance, problems, and answers that come with utilizing machine learning to forecast credit card fraud.

EXISTING SYSTEM

The current credit card fraud detection system based on machine learning includes a range of advanced methods focused on detecting and preventing fraudulent transactions in real-time. Machine learning algorithms are a central part of this system in that they analyse past transaction information to identify patterns that are predictive of fraudulent behaviours. One of the typical methods includes supervised learning techniques like logistic regression, decision trees, and ensemble learning like Random Forests or Gradient Boosting Machines. These techniques are trained on labelled datasets that include fraudulent as well as legitimate transactions and thus learn to identify between the two classes on

the basis of attributes like transaction value, location, time, and user behaviour. Along with supervised learning, unsupervised learning methods such as clustering methods like K-means or density-based methods like DBSCAN are utilized to identify anomalies in transaction data without having labelled examples of fraud. These methods can spot unusual patterns or outliers that vary substantially from the norm, which can be potential cases of fraud. In addition, anomaly detection methods such as Isolation Forests or One-Class SVMs are employed to learn the normal behaviour of authentic transactions and mark any variation from this baseline. Additionally, the credit card fraud detection system commonly uses sophisticated features such as real-time monitoring, adaptive learning, and feature engineering to improve its accuracy continuously and adjust to changing fraud methods. For example, models for anomaly detection can be updated in real time as new data for transactions comes in, so that the system is able to respond rapidly to new patterns of fraud. Feature engineering methods like PCA (Principal Component Analysis) or feature scaling can also be utilized to preprocess the data and identify important features that help to improve the performance of machine learning models. In total, the current credit card fraud detection system utilizes both supervised and unsupervised machine learning algorithms in conjunction with high-level features and methods to effectively detect and eliminate fraudulent transactions in real-time. Through ongoing development of its algorithms and adjustment according to emerging patterns of fraud, the system works to protect consumers and financial institutions from the expanding menace of credit card fraud.

DISADVANTAGES OF EXISTING SYSTEM:

- Data Dependency
- Computational Complexity
- Overfitting
- Interpretability

PROPOSED SYSTEM

The proposed system for machine learning-based credit card fraud detection aims to use advanced algorithms to identify and prevent fraudulent transactions with accuracy in real-time. The system will use past transaction information, including transaction amount, location, time, and user pattern behaviour, to train a machine learning model. The first step is to preprocess the data in order to handle missing values, normalize the features, and potentially perform dimensionality reduction to enhance the performance of the models. Thereafter, multiple machine learning algorithms such as logistic regression, support vector machines (SVM), random forest, or gradient boosting classifiers will be trained on the pre-processed data. The models will then be evaluated on performance measures such as accuracy, precision, recall, and F1-score to determine the best-performing algorithm or group of algorithms. Methods like cross-validation and hyperparameter tuning will also be employed to enhance model performance and generalize well to new data. In the operational phase, the selected model would be applied in a real environment in which it would scan incoming credit card transactions online continuously. Each transaction would be compared to patterns learned and flagged as potentially fraudulent if they demonstrate considerable deviation from normal behaviour. Flagged transactions can go on to further verification processes, such as contacting the cardholder or completely blocking the transaction, depending on the system settings. Furthermore, the system will have feedback loops that recurrently retrain the model based on new data and learn new patterns of fraud over time. With this iterative process, the system will continue to be effective in detecting new and future fraud techniques. In total, the proposed machine learning-based credit card fraud detection system offers a proactive approach to avoiding financial loss and protecting consumers against fraudulent activity. By leveraging the power of machine learning, the system is capable of efficiently

processing enormous amounts of transaction data, identifying suspect patterns, and responding speedily to potential threats and thereby safeguarding the purity of financial transactions and maintaining trust in the financial system.

ADVANTAGES OF PROPOSED SYSTEM:

- Improved Accuracy
- Automatic Feature Learning
- Scalability
- Adaptability

PROPOSED METHODOLOGY AND ALGORITHM :

The steps involved in the methodology for the execution of the suggested fraud detection system are as follows:

Data Collection: The data will be gathered from banks or public sources having labeled transactional data (fraudulent and legitimate transactions).

Data Preprocessing: Missing value handling using imputation methods. Numerical features normalization to uniformize data distribution. Conversion of categorical variables into numerical variables using one-hot encoding or label encoding. Removal of outliers using statistical methods such as the IQR method.

Feature Engineering: Creating new useful features like transaction velocity, spending habit, and geospatial trends. Applying dimensionality reduction methods like PCA to improve the performance of models.

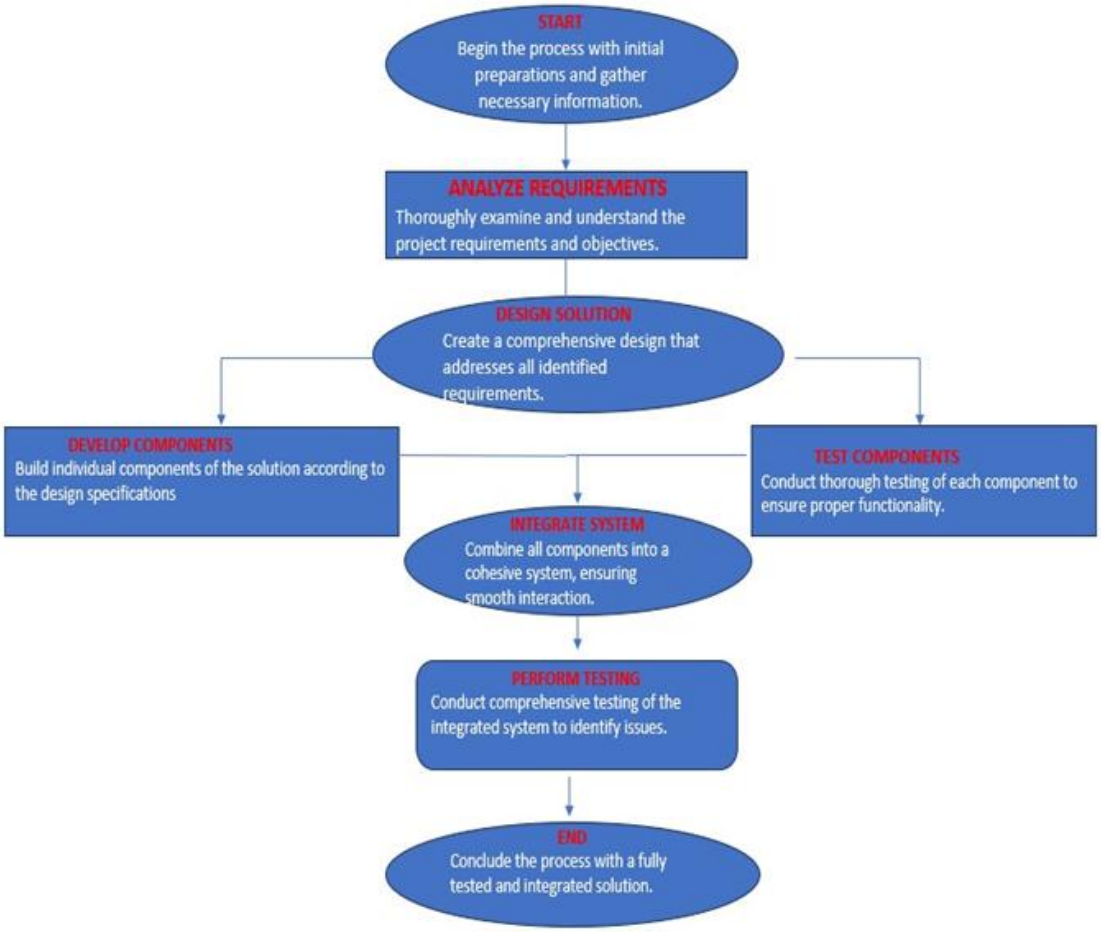
Model Training: Dividing the dataset into training and testing sets via stratified sampling. Training various machine learning models (Random Forest, Gradient Boosting, Voting Classifier) on pre-processed data. Hyperparameter tuning using methods like Grid Search or Bayesian Optimization.

Fraud Detection Algorithm: Developing an ensemble learning framework in which, Random Forest detects transaction anomalies based on decision trees. Gradient Boosting strengthens weak learners to enhance fraud detection. Voting Classifier combines model predictions for better classification accuracy. Utilizing a threshold-based classification system to reduce false positives.

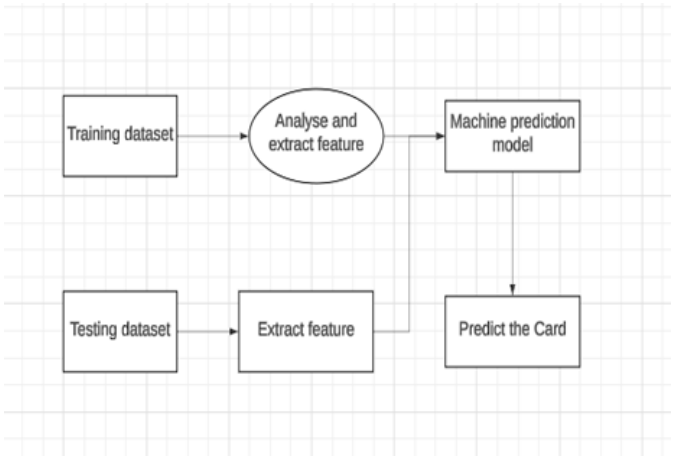
Model Evaluation and Validation: Model evaluation with metrics like Precision, Recall, F1-score, and AUC-ROC. Cross-validation to ensure model generalizability. Comparative analysis with existing fraud detection models.

Deployment and Real-Time Monitoring: Deploying the trained model in a cloud or on-premise setup. Having an automated alert system for risky transactions. Regularly training the model on fresh transactional datato learn changing fraud patterns. The algorithm and methodology are designed to give a scalable, high-performance, and robust fraud detection system that increases the security of financial transactions while reducing financial losses. This method uses the latest machine learning methods and real-time processing features to guarantee sound fraud detection in a constantly changing threat environment.

FLOW CHART



SYSTEM ARCHITECTURE



TECHNIQUES USED IN THIS PROJECT

The suggested fraud detection system applies some of the most important techniques to improve accuracy, efficiency, and real-time processing:

Data Preprocessing Techniques:

Missing Data Handling: Applies statistical imputation or deletes missing values to complete the data.

Feature Scaling & Normalization: Normalizes numerical transaction features via Min-Max Scaling or Standardization to optimize model performance.

Categorical Encoding: Translates categorical variables (e.g., transaction type, location) to numerical representations using One-Hot Encoding or Label Encoding.

Outlier Detection: Removes outliers with statistical techniques such as Z-score and IQR (Interquartile Range).

Feature Engineering:

Transaction Behaviour Analysis: Unnecessarily pulls out patterns including frequency of transactions, average transaction amount, and spending behaviour.

Time-Based Features: Identifies timestamps and intervals between transactions to identify rare patterns.

Device & Location-Based Features: Looks at IP addresses, device IDs, and geography to identify suspicious transactions.

Machine Learning Models & Ensemble Techniques:

Random Forest: Ensemble model based on decision trees for increased accuracy and prevention of overfitting.

Gradient Boosting (XGBoost/LightGBM): Iteratively enhances model performance by building on weak learners.

Voting Classifier: Merges multiple models via majority or weighted voting for enhanced fraud detection.

Logistic Regression: A basic binary classification model for fraud detection.

Imbalanced Data Handling Techniques:

SMOTE (Synthetic Minority Over-sampling Technique): Creates synthetic fraud samples to over-sample the minority class.

Under sampling: Down-samples non-fraudulent transactions to counter class imbalance.

Cost-Sensitive Learning: Imposes greater penalties on misclassified fraudulent transactions.

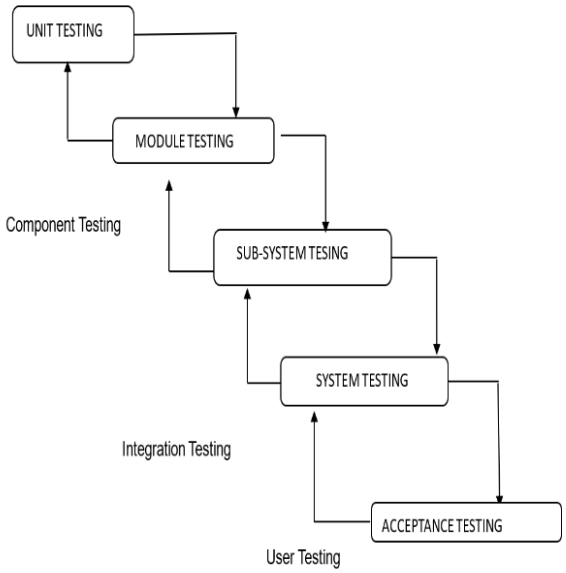
Real-Time Fraud Detection & Model Deployment:

Stream Processing (Apache Kafka/Spark Streaming): Supports real-time transaction monitoring and fraud detection.

Hyperparameter Tuning: Employs Grid Search and Random Search to tune model performance.

Cloud Integration (AWS/GCP/Azure): Hosts the fraud detection model on cloud platforms for scalability.

SYSTEM TESTING AND IMPLEMENTATION



CLIENT-SIDE VALIDATION

There are different client-side validations employed to make sure on the client side that valid data only is input. Client-side validation prevents server time and load to deal with invalid data. Some checks imposed include:

- VBScript is used to make sure only the required fields are filled with appropriate data. Maximum lengths of the form field are defined correctly.
- \tSubmission of forms is not possible without completing the required data so that manual errors of submitting blank fields that are required can be avoided at the client side in order to save the server time and load.
- Tab-indexes are defined based on the requirement and keeping in view the comfort of the user while operating the system.

SERVER-SIDE VALIDATION

Some checks are not applicable to the client side. Checks need to be done at the server side to prevent the system from crashing and notifying the user that some illegal operation has been done or the done operation is forbidden. Some of the server-side checks imposed is:

- Server-side constraint has been applied to validate primary key and foreign key. The value of primary key cannot be repeated. Any attempt to repeat the primary value leads to a message alerting the user regarding those values through the forms using foreign key can be updated only of the current foreign key values.
- User is hinting with proper messages regarding the successful executions or the exceptions at server side.
- ·\tDifferent Access Control Mechanisms have been developed so that a single user should not provoke another. Access rights to different types of users are regulated based on the organizational hierarchy. Only allowed users can log in to the system and can be accessible based on their category. User-name, passwords and rights are managed o the server side.
- Through server-side validation, limitations on many restricted operations are enforced

FUTURE ENHANCEMENT

Deep Learning: Exploring deep learning methods such as LSTMs and CNNs to recognize sequential fraud patterns.

Federated Learning: Developing decentralized AI models to detect fraud in multiple financial institutions while keeping the data private.

Blockchain-Based Security: Improving fraud prevention through blockchain technology by providing secure and transparent transactions.

Explainable AI (XAI): Improve model interpretability using SHAP and LIME to enhance trust and regulatory compliance.

Real-Time Adaptive Models: Developing AI models that continuously learn from new fraud patterns using reinforcement learning.

These techniques guarantee that the fraud detection system is robust, scalable, and capable of identifying fraudulent transactions with high precision while minimizing false positives and false negatives. The following section will cover the proposed methodology and implementation framework for the AI-powered fraud detection system.

CONCLUSION

Advanced fraud detection systems are required due to the growing complexity and frequency of credit card theft. In order to improve detection accuracy and reduce false positives and false negatives, this research presents an AI-powered fraud detection system that makes use of ensemble machine learning approaches. Robust analysis of transactional data is made possible by the use of Random Forest, Gradient Boosting, and Voting Classifiers, which accurately detect fraudulent activity. The suggested system is a useful tool for financial organizations since it is made to be scalable, flexible, and able to detect fraud in real time. Future developments like blockchain security, federated learning, and deep learning integration will fortify fraud prevention measures even more, guaranteeing a more secure environment for online transactions. Through constant adaptation to new fraud strategies, this system seeks to protect financial resources.

References

[1]. Bahnsen, D. Aouada, A. Stojanovic, and B. Ottersten, "Feature engineering strategies for credit card fraud detection," Expert Systems with Applications, vol. 51, pp. 134-142, 2016.

[2]. Panigrahi, P. K. Borah, and K. K. Bhuyan, "Credit card fraud detection using machine learning models and collusion attack analysis," Neural Computing and Applications, vol. 33, pp. 14805-14824, 2021.

[3]. J. West and M. Bhattacharya, "Intelligent financial fraud detection: A comprehensive review," Computers & Security, vol. 57, pp. 47-66, 2016.

[4]. P. Phua, V. Lee, K. Smith, and R. Gayler, "A comprehensive survey of data mining-based fraud detection research," arXiv preprint arXiv:1009.6119, 2010.

[5]. Duman and M. H. Ozcelik, "Detecting credit card fraud by genetic algorithm and scatter search," Expert Systems with Applications, vol. 38, no. 10, pp. 13057-13063, 2011.

[6]. F. Carcillo et al., "Combining unsupervised and supervised learning in credit card fraud detection," Information Sciences, vol. 557, pp. 317-331, 2021.

[7]. L. Liu, J. Chai, and W. Ma, "An adaptive ensemble approach for credit card fraud detection with concept drift," Computational Intelligence and Neuroscience, vol. 2021, pp. 1-10, 2021.

[8]. G. A. Wheeler and J. R. Davidson, "Fraud detection in electronic transactions using machine learning," ACM Transactions on Knowledge Discovery from Data, vol. 15, no. 4, pp. 1-21, 2021.

[9]. Y. Sahin and E. Duman, "Detecting credit card fraud by ANN and logistic regression," IEEE Symposium on Computer and Information Sciences (ISCIS), pp. 1-6, 2011.

[10]. W. K. Lee and J. Stolfo, "Data mining approaches for intrusion detection," USENIX Security Symposium, pp. 79-93, 2000.

[11]. M. S. Nami and M. R. Abdi, "An artificial immune network approach for credit card fraud detection," Applied Soft Computing, vol. 11, no. 1, pp. 1100-1113, 2011.

[12]. J. Wang, Y. Wang, and Y. Wang, "Fraud detection using clustering techniques and machine learning," Journal of Information Security and Applications, vol. 55, pp. 102581, 2020.

[13]. X. Li, J. Lei, and Z. Liu, "Credit card fraud detection using convolutional neural networks," Neural Computing and Applications, vol. 33, pp. 15145-15156, 2021.

[14]. T. Chen and C. Guestrin, "XGBoost: A scalable tree boosting system," Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 785-794, 2016.

[15]. P. R. Clemente and J. L. P. Angelov, "Real-time fraud detection using deep learning techniques," IEEE Transactions on Neural Networks and Learning Systems, vol. 32, no. 10, pp. 4481-4493, 2021.

[16]. Pumsirirat and L. Yan, "Credit card fraud detection using deep learning based on autoencoder and restricted Boltzmann machine," International Journal of Data Science and Analytics, vol. 9, pp. 1-12, 2018.

[17]. F. Provost, T. Fawcett, and R. Kohavi, "The case against accuracy estimation for comparing induction algorithms," Proceedings of the Fifteenth International Conference on Machine Learning (ICML), pp. 445-453, 1998.

[18]. S. Roy, A. Misra, and K. Das, "Hybrid deep learning model for real-time credit card fraud detection," Applied Intelligence, vol. 51, pp. 4541-4557, 2021.

[19]. Van Vlasselaer et al., "APATE: A novel approach for automated credit card fraud detection using network-based anomaly detection," Decision Support Systems, vol. 75, pp. 38-48, 2015.

[20]. P. Dal Pozzolo, O. Caelen, and G. Bontempi, "When is undersampling effective in unbalanced classification tasks?" Machine Learning, vol. 107, no. 8-10, pp. 2473-2505, 2018.