IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

CREDIT CARD FRAUD DETECTION USING MACHINE LEARNING

[1]Mr.F.Richard Singh Samuel, [2]C.V.Lalitha, [3]P.Madhu Swetha, [4]D.Madhura

[1]Assistant Professor, [2]Student, [3]Student, [4]Student
[1]Information Technology,
[1]Francis Xavier Engineering College, Tirunelveli, India

Abstract : With a focus on PIN verification, secure transaction processing, and fraud detection, this project proposes a Python-based system for safe financial transactions. The system loads security questions and customer data from Excel sheets using the pandas and scikit-learn libraries.Users enter their PINs, which are then checked via an integer comparison. Users input the transaction amount if it is validated. When a transaction surpasses certain thresholds, such as the daily maximum transaction amount (MTPD), the system asks security questions. Users haven't made many attempts to respond to these queries. Transactions proceed securely after successful verification. In order to detect fraud based on transaction quantities, the system additionally uses a decision tree classifier. With a focus on strong verification and fraud prevention methods in transaction processing, this project provides a flexible framework for safe financial systems.

IndexTerms **-** financial transactions, PIN verification, secure processing, fraud detection, Python, pandas, scikit-learn, Excel data, security questions, customer data, integer comparison, transaction amount, thresholds, machine learning, decision tree classifier.

I.INTRODUCTION

Safe financial transactions are crucial in today's digital world to preserving faith and confidence in the banking system. Ensuring the security of these interactions has become a primary priority for financial institutions as well as customers, given the growing frequency of online transactions. By creating a Python-based system that enables safe transactions and fraud detection, this project solves the requirement for strong security measures. The system has a feature that asks security questions whenever a transaction exceeds certain thresholds, including the daily maximum transaction amount (MTPD), in order to further improve security. In order to confirm the authenticity of the transaction, these questions provide an extra degree of verification. The system uses machine learning algorithms to determine the probability of fraud based on the transaction amount after the security questions are correctly answered. The integration of PIN verification, security questions, and fraud detection algorithms offers a comprehensive method for secure financial transactions, reducing the possibility of fraudulent activities and protecting the interests of clients and financial institutions alike. The objective of this project is to facilitate the creation of reliable and safe financial systems in the digital age by combining cutting-edge technologies with strong security protocols.

II. LITERATURE SURVEY

Fawaz Khaled Alarfaj, et al. [1] have developed a credit card fraud detection system by employing machine learning and deep learning techniques, as well as a comparative analysis of several algorithms like CNN, LSTM, ANN, KNN, and DNN. Their research's impressive accuracy, precision, and AUC scores show how effective these strategies are in real-world fraud detection scenarios. It is important to apply machine learning techniques to enhance fraud detection skills, and the authors provide valuable insights into the application of these technologies in financial security.

Emmanuel Ileberi, et al. [2], have devised a machine learning framework for identifying credit card fraud in online transactions, employing methodologies like SMOTE and AdaBoost. Their investigation highlights the system's efficacy in detecting fraudulent activities, underscoring its practical applicability in safeguarding online financial transactions. The authors stress the significance of utilizing machine learning approaches to bolster fraud detection capabilities, offering valuable insights into the realm of financial security.

Ibomoiye Domor Mienye, et al. [3], have introduced a deep-learning approach for detecting credit card fraud, employing LSTM and GRU networks, MLP, and SMOTE-ENN techniques. Their research demonstrates high sensitivity and specificity in fraud detection, emphasizing the efficacy of deep-learning methods in enhancing financial security. The authors contribute valuable insights into the utilization of advanced technologies for combating fraudulent activities in credit card transactions.

Altyeb Altaher Taha, et al. [4], have introduced an intelligent approach to credit card fraud detection using an optimized light gradient boosting machine. Their research achieves high accuracy, AUC, precision, and F1-score in real-world datasets, highlighting the effectiveness of their method in detecting fraudulent activities. The authors contribute valuable insights into enhancing financial security through the utilization of advanced machine learning techniques.

Andrea Dal Pozzolo, et al. [5] has presented a practical approach to detecting credit card fraud, tackling challenges such as concept drift and class imbalance. Through experiments with real-world datasets, the research demonstrates the effectiveness of the proposed method in fraud detection. The author contributes valuable insights into overcoming obstacles in financial security through innovative approaches.

Daniele Lunghi, et al. [6] has introduced a novel method for credit card fraud detection called Adversary-based Oversampling (ADVO). By leveraging regression-based oversampling and TimeGAN, this approach predicts future fraudulent activities, surpassing traditional methods in effectiveness. The study contributes valuable insights into advancing fraud detection capabilities, highlighting the significance of innovative techniques in enhancing financial security.

Kuldeep Randhawa, et al. [7] have introduced a credit card fraud detection system utilizing machine learning techniques. Their research evaluates hybrid methods that combine AdaBoost and majority voting, with findings indicating majority voting as the most effective approach. The study underscores the significance of leveraging machine learning in enhancing fraud detection capabilities, offering valuable insights for improving financial security.

Suraya Nurain Kalid, et al. [8] has presented a study discussing machine learning techniques for credit card fraud detection. The research recommends leveraging deep learning, ensemble learning, and sampling methods, along with specific metrics for assessing fraud detection and transaction accuracy. The findings contribute valuable insights into the application of machine learning in enhancing financial security and fraud detection capabilities.

Ebenezer Esenogho, et al. [9] has introduced a method for credit card fraud detection utilizing a neural network ensemble classifier and the SMOTE-ENN hybrid data resampling technique. The study demonstrates superior performance in real-world datasets, showcasing the effectiveness of this approach in enhancing fraud detection capabilities and ensuring financial security.

Yuanming Ding, et al. [10] has contributed to improving credit card fraud detection by enhancing the VAEGAN generator with a new oversampling technique. This approach generates diverse minority class data, surpassing other techniques and enhancing fraud detection capabilities.

III.METHODOLOGY

Data Collection:

The dataset for this project consists of customer transaction data stored in Excel sheets. Parameters such as transaction amount, PIN numbers, security questions, and answers are collected from the "credit_cards.xlsx" and "questions and answers.xlsx" files, respectively. These parameters are crucial for identifying potential fraud and ensuring secure transactions.

Data Preprocessing:

The collected data undergoes preprocessing to handle missing values and ensure consistency. Any missing values or inconsistencies in the dataset are addressed to maintain data integrity. Outliers and noise are also identified and handled appropriately to improve model performance. Additionally, data normalization or scaling techniques may be applied to ensure uniformity across different features.

Model Training:

Model training involves selecting suitable algorithms for fraud detection, such as Decision Trees or ensemble methods. In this project, a DecisionTreeClassifier from the scikit-learn library is used for fraud detection. The dataset is split into training and testing sets to evaluate model performance accurately.

Model Evaluation:

The performance of the trained model is evaluated using evaluation measures including F1-score, recall, accuracy, and precision. The accuracy with which the model detects fraudulent transactions is evaluated by these criteria. The model's capacity to identify fraud in actual situations is revealed by the evaluation results.

Recommendation Generation:

Based on user-provided input data, the model can be trained to forecast the probability of fraudulent transactions. In order to ensure quick response to possible security concerns, the system offers recommendations for additional action depending on the discovered fraud possibility. To successfully improve fraud detection capabilities, this recommendation generating approach makes use of learning patterns and previous transaction data.

IV.EXISTING SYSTEM

Manual Record-keeping:

Manual record-keeping is crucial to the upkeep of customer data and transaction histories in traditional credit card systems. Documenting specifics such client PINs, transaction amounts, dates, and merchant details is part of this process. Although keeping records by hand can guarantee data integrity to some degree, it is prone to inefficiencies and human mistake. Furthermore, the use of manual processes restricts scalability and real-time monitoring capabilities, which makes it difficult to quickly identify fraudulent activity.

Security Measures:

Existing credit card systems often employ PIN verification and security questions as primary authentication mechanisms. PIN verification requires customers to enter their personal identification numbers (PINs) to authorize transactions. Similarly, security questions serve as an additional layer of authentication, prompting users to provide answers to predefined questions. While these measures enhance security to some extent, they may not effectively mitigate sophisticated fraud schemes or unauthorized access attempts.

Fraud Detection Techniques:

Traditional fraud detection methods in credit card systems typically rely on rule-based algorithms and manual review processes. These techniques involve predefined rules and thresholds to flag potentially fraudulent transactions based on suspicious patterns or anomalies. However, rule-based approaches may struggle to adapt to evolving fraud tactics and may generate false positives, leading to inconvenience for legitimate cardholders.

Limitations of Legacy Systems:

Legacy credit card systems face several limitations, including scalability challenges, limited real-time monitoring capabilities, and susceptibility to sophisticated fraud schemes. As transaction volumes grow and fraud tactics become more sophisticated, traditional systems may struggle to keep pace with emerging threats. Moreover, manual intervention in fraud detection processes can result in delays and increased operational costs for financial institutions.

Transition to Modern Fraud Detection Systems:

Financial institutions are moving more and more towards sophisticated fraud detection systems driven by artificial intelligence and machine learning in response to changing fraud trends and regulatory requirements. These systems use very precise and accurate algorithms that have been trained on massive volumes of past data to detect fraudulent patterns and abnormalities. Modern fraud detection systems improve operational efficiency and reduce financial risks related to fraudulent activity by automating the detection process and lowering reliance on manual interventions.

V.PROPOSED SYSTEM

Data Loading and Preprocessing:

Using the pandas library for effective handling, the system starts by loading data from external Excel sheets. In order to ensure a smooth transition by handling any exceptions that may occur during data loading, this process involves obtaining both customer data and security questions.

User Authentication:

In order to guarantee the security of online transactions, user authentication is essential. PIN verification and security question authentication are the two main ways the system uses to confirm user identity. When it comes to enhanced security, security question authentication asks users a series of random questions, manages missing values, and sets a limit on the number of attempts. In PIN verification, user input is converted into integers and cross-referenced with recorded PINs.

Transaction Processing:

Transaction processing refers to all of the procedures that go into making safe financial transactions possible. The system guides users through the process by validating the transaction amounts they submit. Additional security measures, such as security questions, are activated based on transaction amounts beyond predetermined thresholds, and security threshold verification guarantees that transactions correspond with specified restrictions.

Fraud Detection Mechanism:

Protecting against harmful activity requires a strong fraud detection technique. The system uses a Decision Tree Classifier with machine learning to identify possible fraud. Based on the transaction amount, the system forecasts the probability of fraud by training the model with past transaction data. Through simulations, this prediction is improved even more, offering insights into possible transactional hazards. The system is strengthened against fraudulent activities during online transactions by integrating security question authentication with fraud detection, which improves the entire security protocol.

VI. ARCHITECTURE EXPLANATION

1. User Interface (UI):

This part stands in for the graphical user interface that allows users to communicate with the system. Forms, input fields, buttons, and other components that enable data entry, result viewing, and system navigation are frequently included. The user interface in your project would be where users enter the transaction amounts, security question answers, and PIN numbers.

2. Credit Card Data Store:

The system of storage used to hold credit card data is represented by this component. Something like MySQL, PostgreSQL, or MongoDB are examples of database management systems (DBMS). Information regarding credit card details, including PINs, transaction histories, and other pertinent data, can be found in the credit card data repository for consumers.

3. Security Questions and Answers Store:

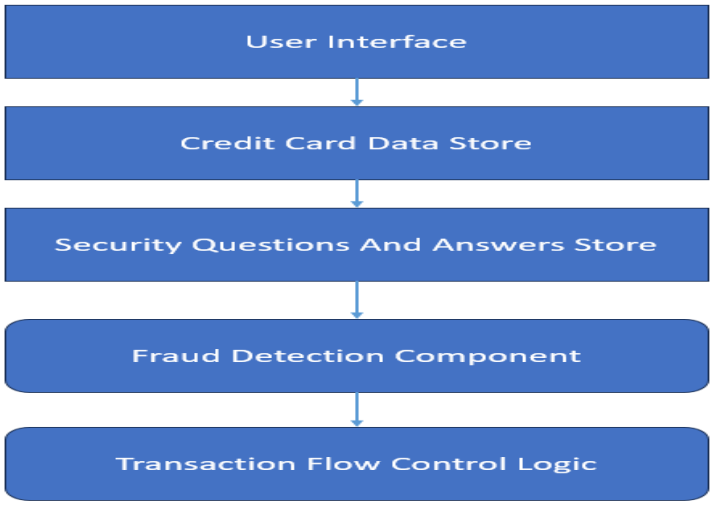
This part is the storage mechanism for security questions and the answers to go along with them, much as the credit card data store. Users' set-up questions and their accurate responses are stored for further security verification. Before completing a transaction, the system can confirm a user's identification thanks to this data storage.

4. Fraud Detection Component:

This part is in charge of identifying any fraudulent transactions or activity occurring within the system. Typically, it analyses transaction data to find patterns suggestive of fraud using machine learning techniques like decision trees, random forests, or neural networks. When it notices any unusual activity, the fraud detection component notifies the system and processes transaction data either in real-time or in batches.

5. Transaction Flow Control Logic:

This part controls how transactions move through the system. The user interface, credit card data storage, security questions and answers store, and fraud detection component are all coordinated by it. Transaction flow control logic guarantees secure and effective transaction processing by adhering to pre-established workflows and business requirements. It manages activities including PIN verification, security question validation, transaction amount comparison with pre-established restrictions, and when needed, activating the fraud detection component.



VII. CONCLUSION

With components for user authentication, fraud detection, and transaction management, the solution described above offers a strong system for safe credit card transactions. Through the use of Excel data handling skills and Python modules like pandas and scikit-learn, the system illustrates a workable solution to major issues with online financial transactions.

The system's core function is to authenticate users using a PIN, which allows for user identity verification. This improves security and lowers the possibility of unauthorised access by guaranteeing that only authorised users can start transactions. Security question integration further strengthens the authentication process by providing an additional degree of validation.Additionally, the system incorporates machine learning.

Additionally, in order to detect and stop fraudulent transactions, the system incorporates machine learning-based fraud detection tools. The integrity of the financial ecosystem is protected by the system's ability to identify anomalies that may be signs of fraud by examining transaction amounts and patterns.

Moreover, the user interface, data stores, and fraud detection component all work together seamlessly thanks to the transaction flow control logic that orchestrates the entire process. In the end, this centralised control system improves customer experience by streamlining transaction processing and increasing operational efficiency.

In summary, the project represents a thorough approach to safe credit card transactions by fusing strong authentication methods with advanced fraud detection strategies and effective transaction handling. Strong security measures are becoming more and more important as online financial transactions continue to grow in popularity. The system provides a scalable and flexible solution to handle changing issues in the digital financial ecosystem by utilising a multidimensional approach that includes user authentication, fraud detection, and transaction management.

VIII. FUTURE SCOPE

1. **Enhanced Authentication Mechanisms**

   With the development of technology, user authentication security may be greatly enhanced by utilising biometric verification techniques like fingerprint or facial recognition. By providing a more reliable and intuitive means of identity verification, these techniques lessen the possibility of unauthorised access to private data.

2. **Integration of Real-Time Data Sources**:

   Useful insights into user behaviour patterns can be gained from real-time data sources including transaction history and behavioural analytics. Through the integration of multiple sources, the fraud detection system gains enhanced adaptability and responsiveness to changing fraud patterns, facilitating prompt identification and mitigation of fraudulent activity.

3. **Dynamic Risk Assessment**:

   Real-time analysis of different transaction-related elements is made possible by the development of dynamic risk assessment algorithms. Through precise risk assessment of each transaction and dynamic security measure adjustment based on perceived risk level, this approach improves the system's overall fraud prevention capabilities.

4. **Advanced Fraud Detection Techniques**:

   Sophisticated methods of identifying fraudulent activity are provided by AI- and machine learning-based approaches like neural networks and anomaly detection systems. These methods help the system detect complicated fraud patterns more accurately and efficiently, which lowers false positives and improves fraud detection capabilities.

5. **Transaction Monitoring and Alerting**:

   It is possible to continuously monitor user transactions for questionable activity by putting in place a thorough transaction monitoring system. Proactively preventing fraudulent transactions can minimise possible losses and ensure the security of financial transactions by rapidly generating notifications for additional investigation.

6. **Integration with Blockchain Technology**:

   Transaction security and transparency are improved by integrating blockchain technology since it produces unchangeable transaction records. The transaction process is made more trustworthy and confident by this integration, which guarantees tamper-proof transaction records and lowers the possibility of fraud or data manipulation.

7. **User Education and Awareness**:

   By encouraging user education and awareness initiatives, users are better equipped to identify any fraudulent activity and adopt safe online security habits. Users can become active participants in fraud prevention efforts and help create a more secure transaction environment by being educated on safe transaction behaviours and how to report suspicious activities.

8. **Regulatory Compliance**:

   To keep the system credible and trustworthy, compliance with security standards and legal requirements is crucial. Users and regulatory agencies alike can have confidence that user data is protected and industry standards are followed when legislation like PCI DSS and GDPR are followed.

9. **Continuous Improvement and Feedback**:

   Adopting a continuous improvement culture requires seeking feedback from users, stakeholders, and security experts as it helps identify areas that require improvement and address emerging dangers. Through active feedback collection and adoption of enhancement proposals, the system can be configured to accommodate evolving user requirements and market trends. This guarantees that the system will always be applicable and efficient in thwarting fraud.

IX.REFERNCES

[1]Y. Abakarim, M. Lahby and A. Attioui, "An efficient real time model for credit card fraud detection based on deep learning", *Proc. 12th Int. Conf. Intell. Systems: Theories Appl.*, pp. 1-7, Oct. 2018.

[2]H. Abdi and L. J. Williams, "Principal component analysis", *Wiley Interdiscipl. Rev. Comput. Statist.*, vol. 2, no. 4, pp. 433-459, Jul. 2010.

[3]V. Arora, R. S. Leekha, K. Lee and A. Kataria, "Facilitating user authorization from imbalanced data logs of credit cards using artificial intelligence", *Mobile Inf. Syst.*, vol. 2020, pp. 1-13, Oct. 2020.

[4]A. O. Balogun, S. Basri, S. J. Abdulkadir and A. S. Hashim, "Performance analysis of feature selection methods in software defect prediction: A search method approach", *Appl. Sci.*, vol. 9, no. 13, pp. 2764, Jul. 2019.

[5]B.Bandaranayake,"Fraud and corruption control at education system level: A case study of the Victorian department of education and early childhood development in Australia", *J. Cases Educ. Leadership*, vol. 17, no. 4, pp. 34-53, Dec. 2014.

[6] J. Błaszczyński, A. T. de Almeida Filho, A. Matuszyk, M. Szeląski and R. Słowiński, "Auto loan fraud detection using dominance-based rough set approach versus machine learning methods", *Expert Syst. Appl.*, vol. 163, Jan. 2021.

[7]B. Branco, P. Abreu, A. S. Gomes, M. S. C. Almeida, J. T. Ascensão and P. Bizarro, "Interleaved sequence RNNs for fraud detection", *Proc. 26th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, pp. 3101-3109, 2020.

[8]F. Cartella, O. Anunciacao, Y. Funabiki, D. Yamaguchi, T. Akishita and O. Elshocht, "Adversarial attacks for tabular data: Application to fraud detection and imbalanced data", *arXiv:2101.08030*, 2021.

[9]S. S. Lad, I. and A. C. Adamuthe, "Malware classification with improved convolutional neural network model", *Int. J. Comput. Netw. Inf. Secur.*, vol. 12, no. 6, pp. 30-43, Dec. 2021.

[10]V. N. Dornadula and S. Geetha, "Credit card fraud detection using machine learning algorithms", *Proc. Comput. Sci.*, vol. 165, pp. 631-641, Jan. 2019.

[11]I. Benchaji, S. Douzi and B. E. Ouahidi, "Credit card fraud detection model based on LSTM recurrent neural networks", *J. Adv. Inf. Technol.*, vol. 12, no. 2, pp. 113-118, 2021.

[12]Y. Fang, Y. Zhang and C. Huang, "Credit card fraud detection based on machine learning", *Comput. Mater. Continua*, vol. 61, no. 1, pp. 185-195, 2019.