INTELLIGENT FRAUD ANALYTICS FOR SECURE FINANCIAL TRANSACTIONS

[1]Dr. D. Nagesh Babu,[2]Karpoorapu Vani Priya,[3]Inaganti Shakila,[4]Gorla Govardhana Kumar

[1]Associate Professor, Dept of Computer Science and Engineering, St. Ann's College of Engineering and Technology, Chirala-523187, India.

[2,3,4]B. Tech Student, Dept of Computer Science and Engineering, St. Ann's College of Engineering and Technology, Chirala-523187, India.

ABSTRACT

Fradulent activities in financial transactions pose significant challenges to businesses and consumers leading to substantial financial losses in digital payment systems. Traditional Rule based methods are ineffective against fraud patterns. This presents a comprehensive machine learning framework aimed at real-time fraud detection and prevention in transactions. In this project we used advanced algorithms and large datasets to identify fraudulent behaviour with high accuracy and minimal false positives. This methodology begins with the collection and preprocessing of transaction data, a range of classification algorithms including logistic regression, decision trees, random forests are employed to build predictive models.

KeyWords: Machine Learning, Decision Tree Classifier, Random Forest, Logistic Regression, Python, Numpy, Pandas, Flask.

INTRODUCTION

Fradulent activities in financial transactions have become increasingly serious issue in today's digital economy, affecting businesses, consumers and overall stability of financial systems. Traditional Fraud detection systems rely on rule-based approaches and manual monitoring which are ineffective against evolving fraud patterns. So Machine Learning techniques provide an effective solution by learning patterns from historical data and identifying hidden relationships associated with fraudulent behaviour and accurately classify transactions as genuine or fraudulent. Such systems improve security, reduce financial losses and enhance trust in digital payment systems.

In this project a machine learning based credit card detection system is developed using PCA -transformed transaction features to ensure data privacy. The system allows users to securely log in and input transaction details, which are analyzed

using trained model and predict whether a transaction is fraudulent or legitimate.

LITERATURE REVIEW

Recent years I studied papers related to fraud detection, In that I got some limitations. In that first paper Dal Pozzolo et al. (2015) it is mainly focuses on dataset creation rather than model improvement and limited discussion on real-time fraud detection. Later in the second paper Bahnsen et al. (2013)a cost sensitive decision trees for fraud detection which requires cost estimation which is difficult in practice and less effective if costs change over time. Next in the third paper Carcillo et al. (2021) which is scalble framework for fraud detection requires advanced infrastructure and resources. So, the project I developed overcome all the limitations and to develop Intelligent Fraud detection system using machine learning algorithms from historic data to learn fraud patterns.

RELATED WORK

In this project we use python for the core logic of the fraud detection system. It receives the transaction data from the frontend and performs data preprocessing. Based on learned transactions patterns trained by the different machine learning algorithms the model predicts whether the transaction is fraud or legitimate. We use flask for frontend to provide an interactive interface for user interaction with the fraud detection system to predict the transactions as fraud or not fraud.

EXISTING SYSTEMS

The Existing credit card fraud detection system mainly rely on rule based methods and manual verification techniques. The system use predefined rules such as transaction limits and location mismatch. The traditional systems also use basic statistical methods that compare current transactions with past customer behaviour. While these approaches are effective foe known fraud patterns, they struggle to detect new and evolving fraud techniques. Due to the rapid increase in transaction volume, existing systems face challenges in accuracy and real-time detection. This creates a need for more intelligent and automated fraud detection system.

PROPOSED SYSTEM

The proposed system introduces a machine learning–based credit card fraud detection system to overcome the limitations of traditional methods. Instead of relying on fixed rules, the system learns patterns from historical transaction data and automatically classifies transactions as fraudulent or legitimate.

The system allows users to securely log into the application and enter transaction feature

values obtained from the dataset. These input values are preprocessed using standard scaling and then analysed by a trained machine learning model, such as a Decision Tree classifier. The model predicts fraud in real time based on learned transaction behavior.

This approach improves detection accuracy, reduces false positives, and adapts to changing fraud patterns. The proposed system is efficient, scalable, and suitable for practical fraud detection applications.

ARCHITECTURE

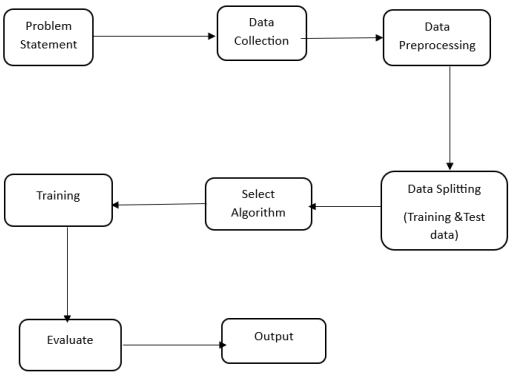

Fig1: System Architecture

METHODOLOGY

1. **Data Collection Module** Collects the credit card fraud detection dataset. Contains PCA-transformed features (V1–V28) and transaction amount. Includes class label (Fraud /Not Fraud)

2. Data Preprocessing Module In Preprocessing Module Handles missing and inconsistent values, Prepares clean data for model training

3. Model Training Module

The third step is Trains machine learning models using preprocessed data, Learns transaction patterns for fraud detection. Optimizes model parameters for better accuracy

4. Model Evaluation Module

Evaluates models using precision, recall, accuracy. Compares different models to select the best one Focuses on reducing false positives

5. Prediction Module

Takes 29 input values for a new transaction. Predicts whether the transaction is Fraud or Genuine. Provides real-time fraud detection capability

6. Web Application Module

User-friendly interface for transaction input. Displays prediction results clearly. Integrates trained ML model with frontend

RESULTS AND DISCUSSIONS

Fig2: Web Page of Fraud Detection System

The webpage serves as a landing page for fraud detection system application.

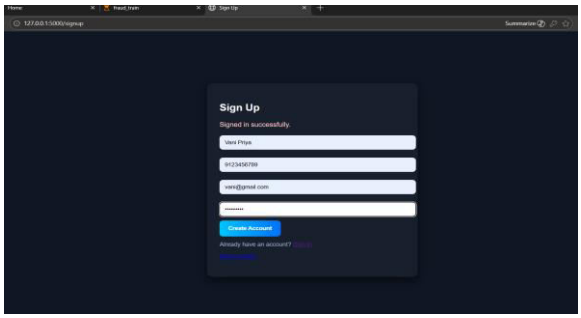

Fig 3: Sign Up page

In signup page, the new user created account by entering the credentials.

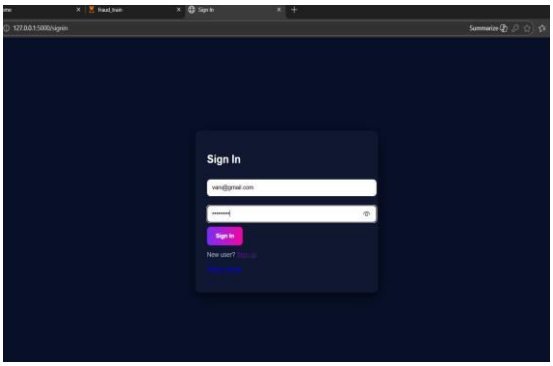

Fig 4: Sign in page

In sign in page the login in to the system by entering the credentials.

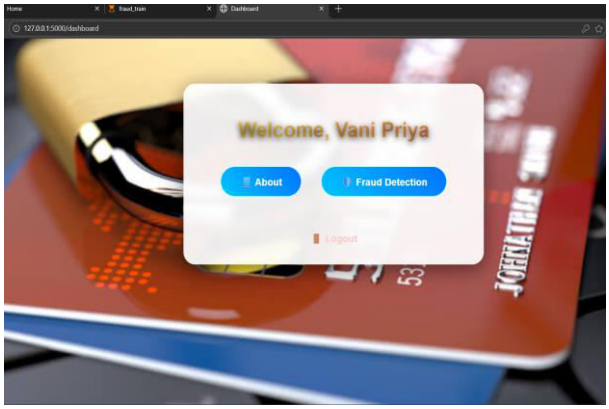

Fig 5: Dashboard of fraud detection system

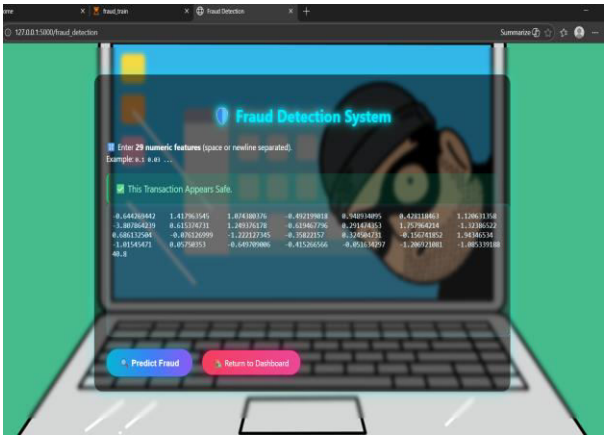

Fig 6: Fraud Detection Page

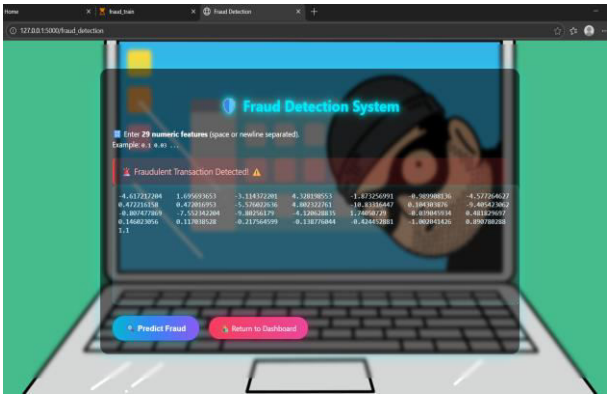

Fig 7: Fraud Detection Page

In this page, the user enter the input and the predict the transaction as fraud or not fraud.

CONCLUSION AND FUTURE ENHANCEMENTS

The project successfully demonstrates the use of machine learning to identify fraudulent transactions. Users log into the system and provide transaction details in the form of 28 PCA values and transaction amount. These inputs are processed using a trained Decision Tree model to classify transactions as fraudulent or legitimate. The system is efficient, easy to use, and suitable

for real-time deployment. Overall, the project enhances transaction security and helps reduce financial losses caused by credit card fraud.

In future, the fraud detection system can be deployed in real world situations in banks and E-Commerce websites to predict whether the transactions as Fraud or Not Fraud.

REFERENCES

1. Harini, D. P. (2013). Two Level Intrusion Detection For Detecting Intruders in Multitier Web Applications. *International Journal of Engineering & Science Research*, *3*, 472-478.

2. Tiwari, S., Sarma, W., & Srivastava, A. (2022). Integrating Artificial Intelligence with Zero Trust Architecture: Enhancing Adaptive Security in Modern Cyber Threat Landscape. International Journal of Research and Analytical Reviews, 9, 712-728.

3. Dey, S., Sarma, W., & Tiwari, S. (2023). Deep learning applications for real-time cybersecurity threat analysis in distributed cloud systems. World Journal of Advanced Research and Reviews, 17(3), 1044-1058.

4. Sarma, W., Srivastava, A., & Sresth, V. AI-Driven Cybersecurity for Iot Ecosystems: Leveraging Machine Learning for Proactive Threat Detection and Autonomous Defense Mechanisms.

5. Sarma, W., & Nagavalli, S. (2021). Reimagining Industry Solutions with AI and Machine Learning: Transforming E-Commerce through Intelligent Systems for Automation and Optimization Independent Researcher 1 Independent Researcher 2 Independent Researcher

6. Srivastava, A., Sarma, W., & Nagavalli, S. Reimagining Industry Solutions with AI and Machine Learning: Transforming E-Commerce through Intelligent Systems for Automation and Optimization.

7. Sarma, W., Nagavalli, S. P., & Sresth, V. (2020). Leveraging AI-Driven Algorithms to Address Real-World Challenges in E-Commerce: Enhancing User Experience, Fraud Detection, and Operational Efficiency. International Journal of Research and Analytical

Reviews, 7, 2348-1269.

8. Dey, S., & Sarma, W. (2020). Automating cybersecurity with AI/ML: Defending against advanced threats.

9. Nagavalli, S. P., Tiwari, S., & Sarma, W. (2024). Redefining Data Privacy in the Age of Artificial Intelligence: Ethical Frameworks, Technological Innovations, and Regulatory Challenges.

10. Shaikh, A. K., & Nazir, A. (2020). A novel dynamic approach to identifying suspicious customers in money

transactions. International Journal of Business Intelligence and Data Mining, 17, 143–158. https://doi.org/10.1108/IJBIDM-01-2020-0001

11. Kassem, R. (2014). Detecting asset misappropriation: A framework for external auditors.

International Journal of Accounting, Auditing and Performance Evaluation, 10(1),142.https://doi.org/10.1504/IJAAPE.2014.058123

12. Omair, B., & Alturki, A. (2020). Taxonomy of fraud detection metrics for business processes. IEEE Access, 8, 71364–71377. https://doi.org/10.1109/ACCESS.2020.2981234

13. Achary, R. (2023). Fraud detection in banking transactions using machine learning. 2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE). IEEE.

14. Ajayi, A. J. (2025). The impact of AI on cyber security in digital currency transactions. SSRN Electronic Journal.

15. Brown, J. (2022). Explainable AI for transparent fraud detection in financial systems. Journal of Financial Analytics, 18(4), 223–235.

16. Cook, A. (2023). AI in financial services: Risk management and fraud detection. AI Tech International Journal, 1(1), 1–7.