SOFTWARE REQUIREMENTS SPECIFICATION (SRS)

UPI Fraud Detection System

SUBMITTED BY,

ALEENA SABU - 12

AMINA R - 13

ANJALI KRISHNA TJ - 17

APARNA SS - 24

TABLE OF CONTENTS

1. INTRODUCTION

Unified Payments Interface (UPI) is a revolutionary digital payment system that has transformed the way financial transactions are conducted, offering users speed, convenience, and accessibility. However, with its rapid adoption, there has been a significant rise in fraudulent activities such as phishing, identity theft, and unauthorized transactions, posing severe financial and security challenges. To combat these issues, UPI fraud detection technologies are essential for ensuring the safety and trustworthiness of digital payment systems.

1.1 Our Plan

- Develop a software system capable of detecting fraudulent UPI transactions.
- Utilize machine learning models like XGBoost for accurate classification of transactions.
- Incorporate secure frameworks to validate transaction integrity and maintain transparency.
- Design a real-time monitoring and alert system for suspicious activities.
- Create a user-friendly interface to help administrators and users track fraud detection.

1.2 Motivation

- According to recent studies, UPI transactions have experienced exponential growth, leading to a parallel increase in fraudulent activities.
- Financial fraud not only causes monetary losses but also damages user trust in digital payment platforms.
- With the growing reliance on cashless economies, there is a pressing need for a robust fraud detection system to ensure security and prevent unauthorized transactions.
- This motivated us to develop a scalable, efficient, and real-time fraud detection solution to protect users and institutions from potential threats.

2. OBJECTIVE

This project aims to develop a fraud detection system for UPI platforms, enabling secure and trustworthy digital transactions. The system focuses on real-time detection of fraudulent activities by analyzing transaction data, identifying unusual patterns, and classifying transactions as legitimate or fraudulent. It emphasizes scalability, privacy, and responsiveness, ensuring effective integration with existing UPI platforms and providing enhanced security for users.

3. FUNCTIONAL REQUIREMENTS

1. Data Collection: Gather and load UPI transaction data, ensuring it is relevant and sufficient for fraud detection.

2. Data Preprocessing: Clean the dataset by handling missing values, duplicates, and outliers.

3.Feature Engineering: Create additional features like transaction patterns, location consistency, and device usage.

4. Fraud Detection Model: Build machine learning models capable of classifying transactions as fraudulent or non-fraudulent.

5. Model Evaluation: Assess models using metrics such as accuracy, precision, recall, and F1-score.

6. Real-Time Detection: Implement a system to detect fraudulent transactions in near real-time.

7. Visualization: Develop visualizations to display fraud distribution, transaction trends, and model insights.

8. Alert Notifications: Create an alert system to notify stakeholders when fraud is detected.

9. System Integration: Ensure seamless integration of the fraud detection system with existing UPI payment gateways.

4. NON-FUNCTIONAL REQUIREMENT

1. Performance: Achieve low-latency processing, ensuring fraud detection occurs in real-time or near real-time.

2. Scalability: Design the system to handle increasing data volumes, scaling to millions of ransactions.

3. Accuracy: Maintain high fraud detection accuracy.

4. Reliability: Ensure the system provides consistent and dependable results under varying workloads.

5. Security: Protect sensitive customer and transaction data, complying with privacy laws like GDPR.

6. Usability: Provide an intuitive user interface for stakeholders to review flagged transactions and insights.

7.Maintainability: Use modular, well-documented code to simplify updates, such as retraining models or adding features.

8. Portability: Ensure the system can be deployed across various platforms, including cloud-based environments.

9. Auditability: Maintain logs of transactions, model predictions, and alerts for future audits and regulatory compliance.

5. SOFTWARE SPECIFICTIONS

Programming languages

Python is a powerful and versatile language due to its simplicity and extensive library support. Its large community and resources ensure easy problem solving and scalability for both small experiments and production level systems.SQL is used to handle transaction databases for fraud detection.

Machine learning frameworks

Scikit-learn was utilized for implementing models like Decision Tree, Random Forest, and Gradient Boosting, as well as for data preprocessing, model evaluation.The XGBoost framework was employed to build the XGBoost model, leveraging its advanced features such as efficient handling of missing data, regularization, and parallel processing, which contributed to its superior performance. Pickle is Used for serializing and saving machine learning models to disk for reuse.

Computer vision frameworks and libraries

OpenCV is a versatile and widely used computer vision library that can be leveraged for a variety of image processing tasks.OpenCV is lightweight, efficient, and integrates seamlessly with Python, making it an essential tool for basic and advanced image processing.

Libraries for Data Processing and Visualization

NumPy and Pandas are used for handling and processing datasets.Matplotlib and Seaborn provides visualization of fraud patterns and insights.Scipy is used for advanced statistical analysis.

Hardware specifications

Processor : Intel i5 (8th Gen)

RAM :8 GB (for small datasets).

System type :64-bit operating system,x64-based processor

6. CONCLUSION

In conclusion it is evident that the XGBoost model outperforms the other models in terms of accuracy. It consistently demonstrated superior predictive capabilities, making it the most suitable choice for detecting fraudulent transactions in this context. This model can serve as a valuable tool in financial institutions, enabling them to proactively identify and prevent fraudulent activities, thereby safeguarding both businesses and customers from potential financial losses.