Financial Fraud Detection System

Session: 2022 - 2026

Team Members

Rizwan Yaqoob 2022-CS-176
Abdullah Chaudhary 2022-CS-204
Hasnain Ali 2022-CS-174
Arham Imran 2022-CS-209

Course

Database Systems CS-262L

Instructor

Syed Numan Babar

Submission Date

Friday, May 10, 2024

University Of Engineering And Technology Lahore,
Department of Computer Science

Abstract

This digital age has transformed traditional monetary transactions, shifting the majority of financial exchanged to electronic platforms. But also there still some forms of traditional monetary transactions happening. The Financial Fraud Management System (FFMS) is developed to address a need to detect and prevent fraudulent activities in financial transactions. Utilizing rule-based system to detect and prevent fraudulent activities not only in traditional transactional data but also in digital financial transactions.

The FFMS operates on a comprehensive set of predefined rules derived from different fraud patterns and typical fraudulent behaviors. These rules are designed to analyze transactional data of accounts, flagging the transactions that display any fraudulent activity. This approach helps minimizing the risk of financial loss.

The system is equipped with an intuitive dashboard that allows financial analysts to monitor transactions actively. Receive information about the transactions that mitigate potential threats.

The FFMS provides a reliable and efficient solution to combat financial fraud, ensuring the safety of electronic financial transactions in an increasingly digital world.

Acknowledgement

We, the members of Team (ID. 4), would like to express our deepest appreciation to our esteemed course teacher, Sir Syed Khaldoon, Ph.D., for his invaluable guidance and profound insights throughout the duration of our Database course. His expertise, persistent dedication, and constant evaluations of our progress had a profound influence on our approach to this project. His timely insights were particularly helpful in refining our strategies and overcoming technical challenges. We are also immensely thankful to our lab instructors, Sir Nazeef and Syed Babar, for their hands-on assistance in the lab sessions. Special thanks to Sir Babar, who helped us grasp complex database concepts such as joins and subqueries, enhancing our technical proficiency and understanding. Additional special thanks to Sir Nazeef, whose direct involvement was instrumental in finalizing our database project schema, which was pivotal in the completion of this project

Contents

List of Figures

Introduction

In the rapidly evolving financial landscape, the prevalence of digital transactions has increased exponentially. With this surge in digital transactions, ranging from ATM withdrawals to mobile wallet exchanges, there emerges a significant rise in the potential for financial fraud. Financial fraud poses grave risks to both consumers and financial institutions, affecting trust and causing substantial financial losses. To combat these challenges, our project focuses on the development of a Rule-Based Financial Fraud Detection System designed specifically to monitor and analyze transactional data across various mediums including ATM transactions, credit and debit cards, cash transactions, mobile wallets, and account-to-account or account-to-merchant transfers.

This project aims to leverage the rule-based approach, which utilizes predefined criteria to evaluate transactional behaviors and identify anomalies that could indicate fraudulent activities. By implementing this system, we aim to enhance the security measures of financial institutions and provide a robust framework that helps in the early detection and prevention of potential frauds.

The detection system is built upon a solid foundation of transactional rules derived from historical data analysis, industry standards. These rules address various aspects of a transaction such as frequency, amount, location discrepancies, and unexpected patterns that deviate from a user's typical behavior. Moreover, the project encompasses the creation of a user-friendly interface that allows user to add, delete , update transactional data that can be further analyzed. It also uses PowerBI dashboard for visualization and analytics of transactional data.

Methodology

Database Design

We've structured Database to effectively manage and analyze transactional data.

Entity-Relationship Diagram(ERD):

Our ERD includes the main entities like 'Transactions', 'User', 'Account', 'Merchant', 'Bank', 'Branch', 'ATM', 'Card', 'Location', etc. As shown in the following figure.

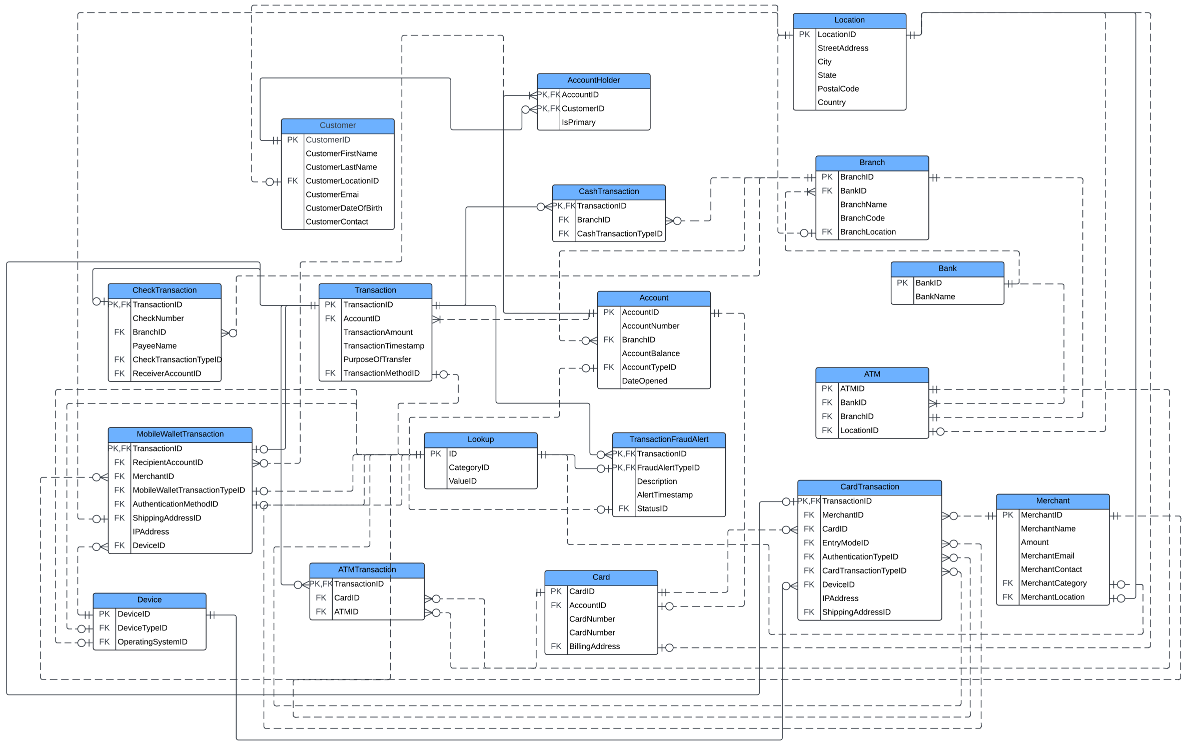


Figure 1: Entity Relationship Diagram (ERD).

Database Schema

This database schema is designed to support efficient data retrieval and integrity. Tables are indexed appropriately. Foreign keys are used to maintain referential integrity. The following is the schema of our database.

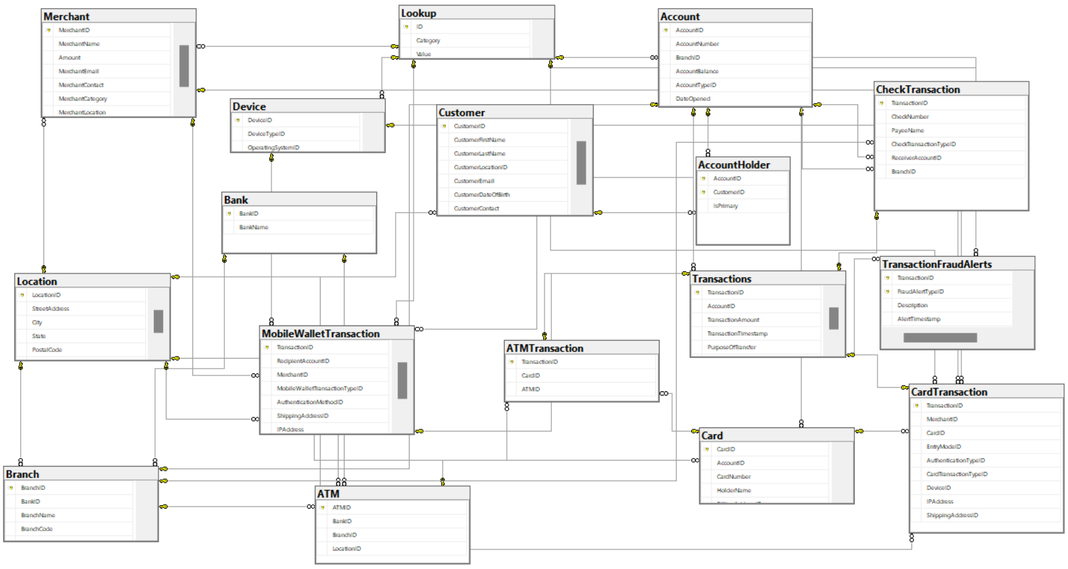


Figure 2: Database Schema Diagram.

Data Collection

Data for the Financial Fraud Detection System is collected and synthesized from multiple sources to create a robust dataset for analysis. We simulate transactional data streams by combining real elements with synthetic data. This includes using the names of the top 10 famous banks globally and popular online merchants like Netflix, Spotify, and Disney, paired with real-world locations in various countries. On the other hand, data such as customers, accounts, transactions, ATM locations, and bank branches are meticulously created using the Python library Faker. This hybrid approach not only ensures the authenticity of the bank and merchant contexts but also preserves individual privacy and introduces variability that is essential for thorough testing and simulation of diverse fraud scenarios.

System Design

Our system design incorporates both frontend and backend components to ensure usability and robust functionality. The design emphasizes scalability and security, facilitating efficient data handling and user management while providing a seamless user experience.

Frontend Design

The frontend of our system is developed using ReactJS, providing a responsive and intuitive interface for system administrators to populate and manage transaction data effectively. In addition to basic data management, Power BI is integrated to enable system administrators to monitor alerts and view analytics on a comprehensive dashboard. This powerful combination aids in real-time decision-making and enhances the overall monitoring capabilities of our system.

Backend Design

The backend is developed using modern JavaScript frameworks to ensure secure and reliable connections between the frontend interfaces and the SQL database. The use of Microsoft Azure Cloud Service for hosting our SQL database ensures that our data storage solutions are both scalable and secure. This deployment not only supports global accessibility but also provides the flexibility needed to handle large volumes of data efficiently, which is crucial for the real-time processing demands of fraud detection.

Dataflow Diagram

Dataflow diagram of this project is given as

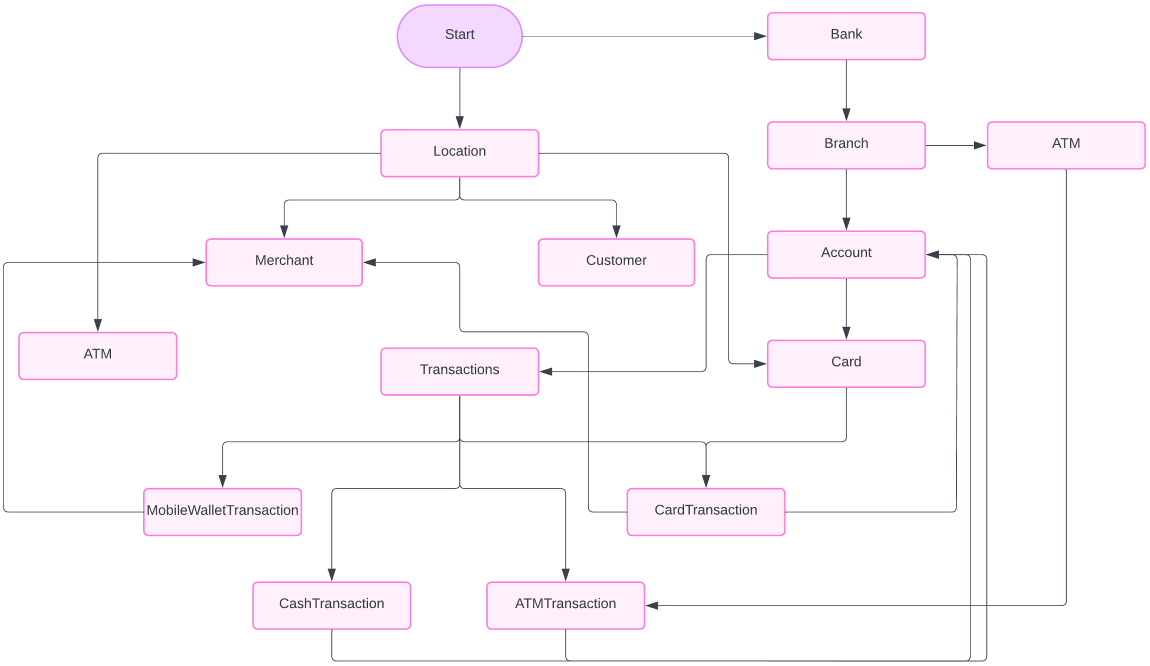


Figure 3: Data Flow Diagram.

Tools & Technologies Used

- **Frontend:**
  - React: Used for building the user interface.
  - Power BI: Employed for creating interactive dashboards and analytics.
- **Backend:**
  - Javascript: Utilized for backend services to handle business logic and data manipulation.
  - Python: Used for dummy data creation
  - Azure: Serves as the primary database system to store and manage transactional data.
- **Development Tools:**
  - Gitlab: Used for version control to manage code changes and collaboration.
  - Notion: Employed for project management to track progress, organize documentation, and coordinate tasks among team members.
  - Lucidchart: Used for ERD Creation and also for the creation of Data Flow Diagram.
  - Visual Studio SQL Server Ingration Service : Used for ETL (Extract-Transform-Load) Operation that was performed on the above database to convert it into data warehouse which was used to analyze transaction data.

System Description

Overview of the Final System

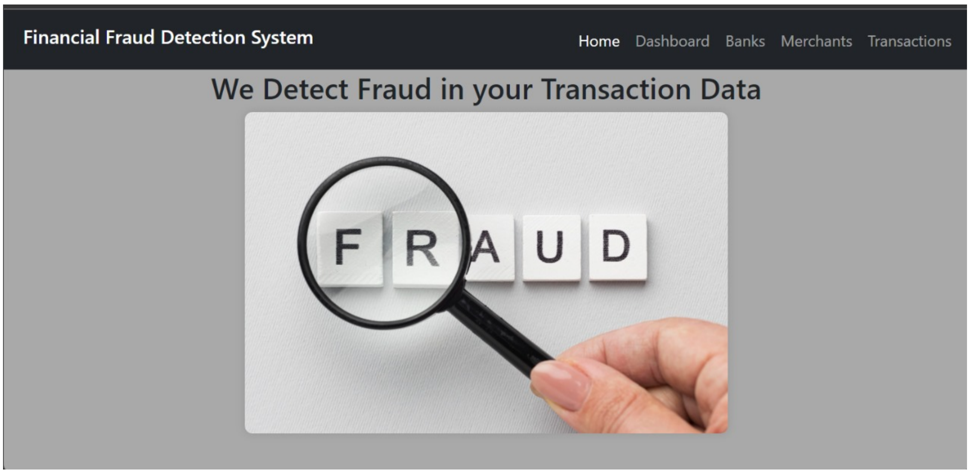
The Financial Fraud Detection System is designed to identify and prevent fraudulent transactions across various payment platforms, including ATMs, mobile wallets, and online banking. The system integrates a sophisticated frontend for user interactions, a powerful backend for processing data, and a secure database for storing transaction records and user information. Technologies used include React for the frontend to ensure a responsive user experience, Javascript in the backend for robust data processing, and Azure cloud service for reliable data management.

Features and Functionalities

- **Web-based Application:** Used for the CRUD operations of data so that new data can be analyzed.
- **Fraud Detection Algorithms:** SQL queries was used to analyze transactional data/.
- **Dashboard PowerBI:** Offers comprehensive dashboards with real-time analytics and interactive tools for deep dives into transaction data.

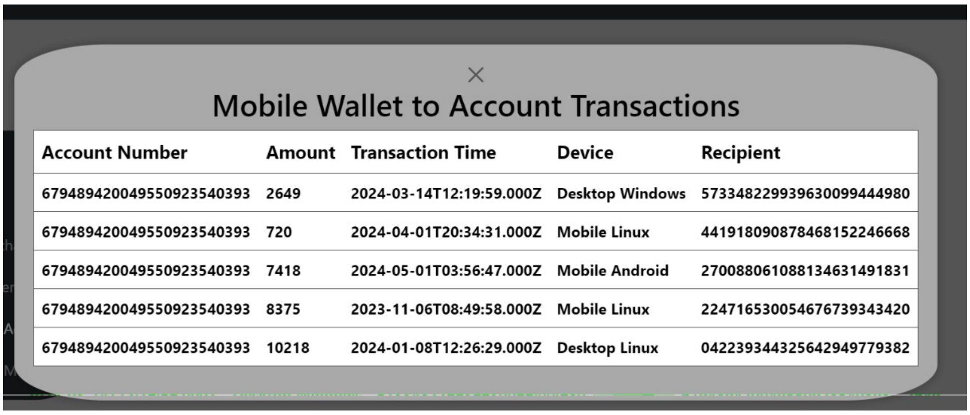
User Interface Screenshots

Below are screenshots that demonstrate key functionalities of the system.


Financial Fraud Detection System

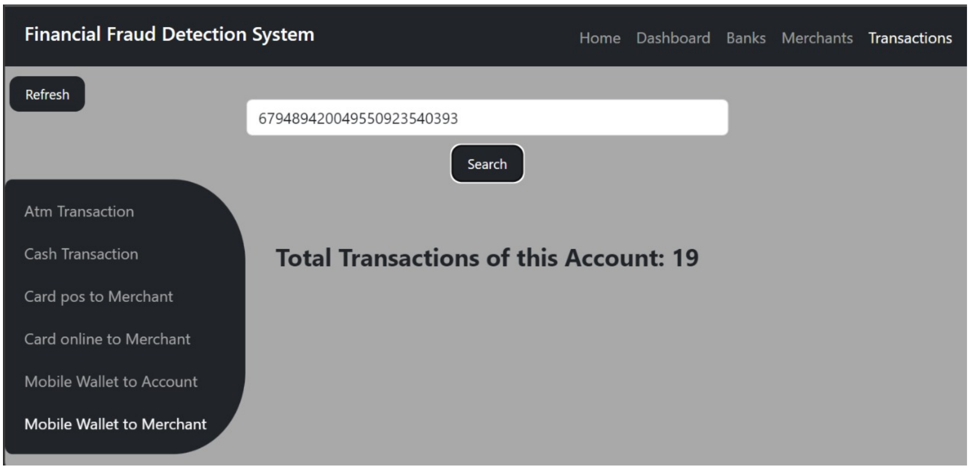
We Detect Fraud in your Transaction Data

Figure 4: Web Application Homepage


Mobile Wallet to Account Transactions

Account Number	Amount	Transaction Time	Device	Recipient
679489420049550923540393	2649	2024-03-14T12:19:59.000Z	Desktop Windows	573348229939630099444980
679489420049550923540393	720	2024-04-01T20:34:31.000Z	Mobile Linux	441918090878468152246668
679489420049550923540393	7418	2024-05-01T03:56:47.000Z	Mobile Android	270088061088134631491831
679489420049550923540393	8375	2023-11-06T08:49:58.000Z	Mobile Linux	224716530054676739343420
679489420049550923540393	10218	2024-01-08T12:26:29.000Z	Desktop Linux	042239344325642949779382

Figure 5: Account Mobile Wallet Transactions



679489420049550923540393

Total Transactions of this Account: 19

Figure 6: Account Homepage

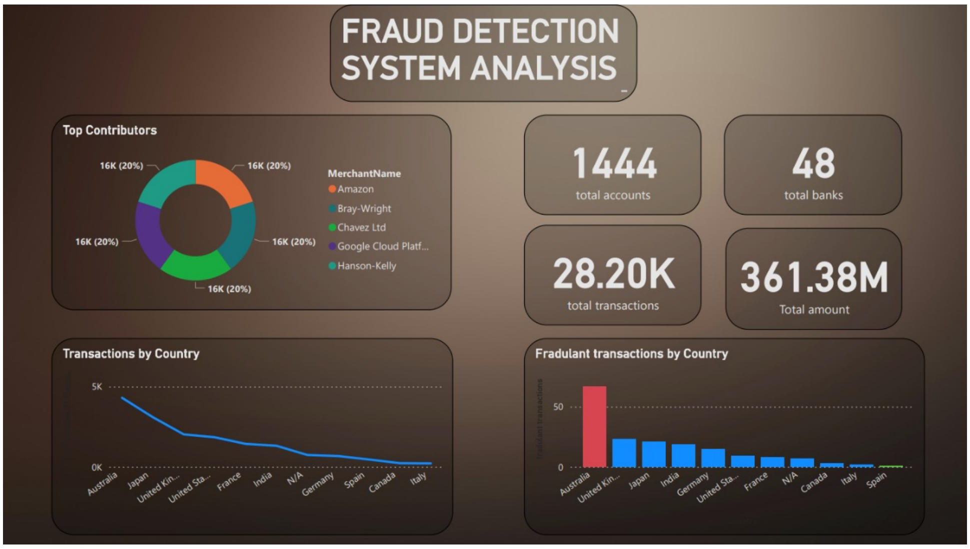


Figure 7: PowerBi Dashboard Transactions Data

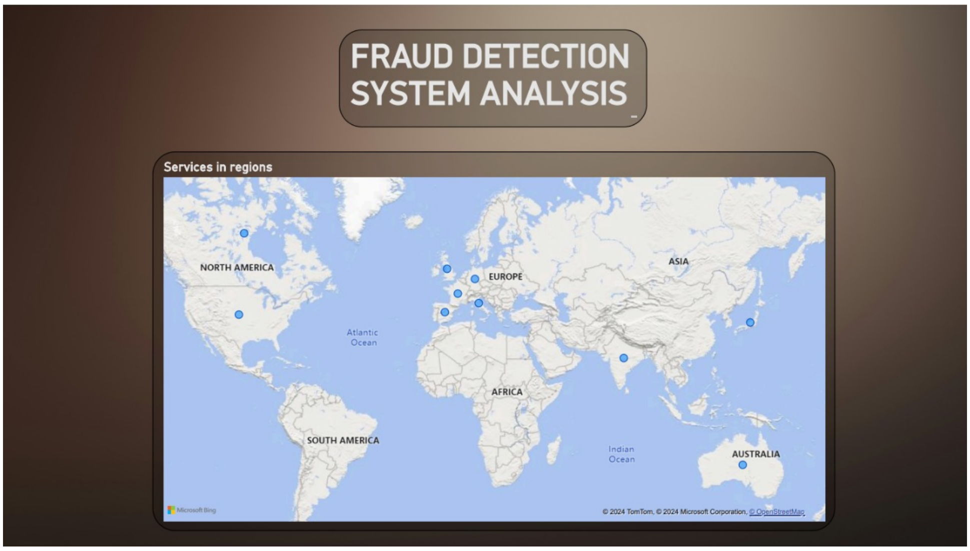


Figure 8: PowerBI Dashboard Map highlighting Countries Affected by Fraudulent Transactions

Challenges and Solutions

Technical Challenges

- **I/O Storage of tables**

  Challenge: Multiples tables were created like TransactionTypes, AccountTypes, MerchantCategoryType, etc. It would take a lot of storage to store all of these tables that only store Enum entries.

  Solution: A single table was implemented that was called Lookup that had 3 attributes. ID, Category that was like TransactionType, AccountType, MerchantCategoryType. And Value which stores DepositTransaction, SavingsAccount, OnlineService. A single table was implemented to accumulate all of these tables.

- **Scalability of the System:**

  Challenge: How to adopt different types of transactions like transaction to account, merchant, ATM transactions, card transactions, CashTransactions.

  Solution: A single table was created for transaction. Then different tables were created like ATMTransaction, CashTransaction and many more which had 1-1 relation with transaction.

- **Create Dummy Data:**

  Challenge: How to create dummy data that looked like orignal.

  Solution: Python library faker was used to create SQL commands that inserted dummy data in SQL server.

- **Online Database Server**

  Challenge: How to communicate through database online so that different devices can connect to a single database.

  Solution: Microsoft Azure web service was integrated with Azure Data studio in which database was deployed so that it can be connected with different devices.

Problem-Solving Approaches

- **Iterative Development and Feedback:**

  Approach: Employed agile development methodologies, conducting different versions of erd, business rules that were based on Course teacher's feedback.

  Outcome: This approach allowed for continuous improvement in system features and user interface based on real-user feedback, leading to a more robust and user-friendly application.

Conclusion

In conclusion, the development of the Financial Fraud Detection System has successfully demonstrated the capability to detect and prevent fraudulent activities across multiple transaction platforms efficiently. Through the integration of database design. The project has not only achieved its primary objectives but has also set the groundwork for future enhancements. Furthermore, the experience gained and lessons learned from this project provide valuable insights that can be applied to other areas within the field of financial technology. The successful collaboration among team members and effective problem-solving approaches adopted are testaments to the project's sound management and technical strategies. Overall, the Financial Fraud Detection System stands as a testament to the potential for technology to improve security and efficiency in financial transactions, making it a valuable asset in the ongoing fight against financial fraud.