COMSATS University Islamabad (CUI)

Software Requirement Specification

(SRS DOCUMENT)

for

Online Payment Fraud Detection Using Artificial Intelligence

Version 2.0

By

Abdul Mueed CIIT/FA20-BCS-006/VHR
AbuBakar Siddiqi CIIT/FA20-BCS-011/VHR

Supervisor

Prof. Abdullah

Bachelor in Computer Science (2020-2024)

Revision History

Name	Date	Changes for Reason	Versions
SRS	5/03/2024	Modify functional requirements of project	1.0
SRS	10/03/2024	Adding GUI Functionality	1.5

Application Evaluation History

Comments (by committee)	**Action Taken**
Study similar system	Study architecture of ml models
Study numeric dataset pre processing methods	Study major stages of pre processing

Supervisor By

Prof. Abdullah

Signature ——————

Abstract

The project focuses on developing an online financial fraud detection system that uses AI and machine learning to detect and prevent fraud. By analyzing transaction data, the system can detect unusual behaviors that indicate fraud and promptly notify relevant parties, including e-merchants (businesses, payment systems, and financial institutions). The main goals include ensuring accurate fraud, ease of integration, scalability, and enhanced security. Machine learning models continuously learn from new data to improve detection accuracy and adapt to changing fraud patterns. It also provides comprehensive insights to help users understand security issues and trends. The rules address efficiency, real-time analysis and optimization, and fail to ensure data protection through security measures such as data encryption and regular audits. The system architecture is designed for ease of use and seamless integration, tailored to a variety of business sizes and volumes.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Chapter 1

Introduction

The rapid growth of online transactions has made our lives more convenient, but it has also led to a significant increase in fraudulent activities. Detecting and preventing online payment fraud is crucial to protect both consumers and businesses from financial losses. This project focuses on using Artificial Intelligence (AI) and machine learning to develop an effective fraud detection system. In today's world, many of our purchases happen online, but with that convenience comes the risk of fraud. This project is all about using smart technology, like AI and machine learning, to catch those tricky attempts at cheating the system when people make online payments. By keeping an eye on transaction data, the system can quickly spot any fishy behavior and

alert us, helping keep our money safe. And because fraudsters are always trying new tricks, we're making sure our system stays up-to-date and ready to stop them in their tracks. Our project focuses on keeping your transactions secure by using smart technology to stop fraud in its tracks. With AI and machine learning, we're creating a system that can quickly spot and stop any tricky business, making sure your online purchases are always safe.

1.1 Project Scope

The capabilities of this online payment detection system include the development and deployment of a powerful AI engine that can instantly detect and prevent fraudulent transactions. The system is designed to seamlessly integrate with existing e-commerce, payment gateways, and financial institutions. Main components include:

1. **Fraud Detection**: Machine learning algorithms that use advanced technologies such as pattern recognition and anomaly detection are used to assess and classify fraud in data transfer exchanges.

2. **Real-Time Analysis**: Allows the system to instantly analyze changes within seconds, identify suspicious activity, and issue alerts.

3. **Data Handling**: Manage general data, including transaction history data, by processing and preparing data reporting models. This includes preliminary steps such as processing missing data, building prototypes, and implementing efficient operations.

4. **Continuous Improvement**: Update and retrain the model with new transactional data to refine fraud detection accuracy and adapt to new fraud techniques. This continuous learning component ensures that the system evolves alongside emerging fraud patterns.

5. **User-Friendly Integration**: Design an intuitive system compatible with various e-commerce and payment systems, requiring minimal technical expertise for deployment. It should offer ease of use, low maintenance, and flexibility for a range of businesses, from small merchants to large financial institutions.

6. **Scalability**: Build an infrastructure capable of handling varying transaction volumes to support both small-scale businesses and high-throughput environments, ensuring scalability without compromising detection quality.

7. **Enhanced Security and Compliance**: Add security features such as data encryption and regular security checks to prevent data changes. The system also needs

to be financial management and e-commerce compatible, comply with data protection law, and prevent fraud. Designed to reduce fraud, increase user trust, and provide insight into business security strategies.

1.2 Project Significance

The significance of this online payment fraud detection system lies in its potential to address the critical and growing issue of payment fraud in digital transactions. The system provides multiple benefits to businesses, consumers, and financial institutions by ensuring security, enhancing customer trust, and improving operational efficiency.

1. **Enhanced Security and Fraud Prevention**: The system employs advanced machine learning algorithms to detect fraudulent transactions in real time. By automatically identifying suspicious patterns, it significantly reduces the risk of financial losses due to fraud, protecting both businesses and customers.
2. **Customer Confidence and Trust**: With enhanced fraud detection, consumers are more likely to trust and engage in online transactions, driving growth in the e-commerce sector. A secure transaction environment not only retains existing customers but also attracts new ones.

3. **Operational Efficiency and Cost Reduction**: Automating the fraud detection process minimizes the need for manual transaction reviews, reducing labor costs and allowing resources to be allocated to other critical areas. Additionally, this system helps businesses avoid financial losses associated with fraudulent activities, such as chargebacks and refunds.

4. **Scalability and Adaptability to New Threats**: The system's machine learning model is designed for continuous improvement, adapting to emerging fraud techniques. This scalability ensures the system's long-term viability as it evolves to address the latest tactics used by fraudsters.

5. **Compliance and Regulatory Support**: By ensuring secure handling of transaction data, the system assists organizations in adhering to financial regulations and industry standards for data protection and fraud prevention. Compliance with these standards reduces the risk of legal liabilities and enhances the reputation of the business.

6. **Insightful Reporting for Strategic Decision-Making**: Comprehensive data analysis and reporting features provide businesses with insights into fraud trends and security vulnerabilities. This information supports informed

decision-making, enabling organizations to strengthen their security protocols proactively.

1.3 Target Audience

The target audience for the online payment fraud detection system includes a wide range of stakeholders within the e-commerce and financial sectors. Key target groups include:

1. **E-commerce Merchants**: Businesses of all sizes that operate online stores and handle a large volume of transactions benefit directly from fraud detection to ensure the security of their payment processing and protect their customers from fraudulent activities.

2. **Payment Processors and Gateways**: Companies providing payment processing services, such as gateways and third-party processors, need robust fraud detection systems to secure transactions across diverse platforms, meeting both security requirements and regulatory standards.

3. **Financial Institutions**: Banks and financial organizations involved in facilitating online transactions are key stakeholders. Fraud prevention is critical to these institutions to protect client assets, uphold compliance, and maintain a secure digital banking environment.

4. **Regulatory Bodies and Compliance Teams**: Organizations and teams responsible for setting and enforcing financial regulations and compliance standards can leverage this system to ensure businesses adhere to legal standards for fraud prevention, supporting safe and lawful transaction practices.

5. **Cybersecurity Analysts and Risk Management Professionals**: Professionals in cybersecurity and risk management can use the fraud detection system to identify, manage, and mitigate payment fraud risks effectively, ensuring that digital transactions remain secure and aligned with organizational risk tolerance.

6. **Customers and End-Users**: While not direct users of the system, customers and end-users benefit from the increased security of their transactions, leading to higher trust in online shopping and digital banking platforms.

1.4 Project Timeline

The project timeline outlines the major phases and milestones for developing the online payment fraud detection system. This timeline is designed to guide the project from initial planning through development, testing, and deployment, over an estimated six-month period.

1. **Phase 1: Requirements Gathering and Analysis (Weeks 1-3)**

   Conduct a detailed analysis to gather system requirements, including functional, non-functional, and security specifications. Identify target users, data sources, and establish baseline metrics for fraud detection accuracy.

2. **Phase 2: System Design and Architecture (Weeks 4-6)**

   Develop the system architecture, defining data processing pipelines, machine learning models, and integration points. Design the user interface and database schema, ensuring scalability and security.

3. **Phase 3: Data Collection and Preprocessing (Weeks 7-10)**

   Collect and preprocess transaction data for model training. This includes data cleaning, normalization, feature engineering, and dataset splitting for training and testing.

4. **Phase 4: Model Development and Training (Weeks 11-14)**

   Implement and train machine learning models for fraud detection, such as logistic regression, random forests, and neural networks. Conduct experiments with various models to optimize detection accuracy and minimize false

positives.

5. **Phase 5: Model Evaluation and Validation (Weeks 15-17)**

   Evaluate the performance of trained models using metrics such as accuracy, precision, recall, and AUC. Conduct validation on unseen data to ensure model robustness and reliability.

6. **Phase 6: System Integration and Testing (Weeks 18-21)**

   Integrate the fraud detection system with payment gateways and user interfaces. Perform end-to-end testing to identify and resolve bugs, validate real-time detection, and ensure system security.

7. **Phase 7: Deployment and User Training (Weeks 22-24)**

   Deploy the system to the production environment. Provide training sessions for key stakeholders, including e-commerce merchants, payment processors, and cybersecurity teams.

8. **Phase 8: Post-Deployment Monitoring and Maintenance (Ongoing)**

   Monitor system performance post-deployment, ensuring accuracy in fraud detection. Schedule regular updates

to incorporate new data and adjust models to evolving fraud tactics.

pdflscape

Chapter 2

Software Requirement Specification

2.1 Software Requirements Technique

To ensure a comprehensive and accurate gathering of software requirements for the online payment fraud detection system, a variety of requirement elicitation and analysis techniques have been utilized. These techniques help in identifying, specifying, and validating the system's functional and non-functional needs.

(a) **Interviews with Stakeholders**: Conduct interviews with stakeholders, including e-commerce merchants, payment processors, and cybersecurity experts, to gather insights into the specific needs and

challenges associated with fraud detection in online transactions.

(b) **Questionnaires and Surveys**: Distribute structured questionnaires to a wider audience, including potential end-users, to collect data on preferred features, security concerns, and usability requirements. This technique helps in capturing a broader set of requirements.

(c) **Use Case Analysis**: Develop use cases to outline the specific interactions between the system and its users. This technique provides a clear view of the system's functionality, helping in defining user actions, system responses, and security measures for each scenario.

(d) **Observation and Process Analysis**: Observe the workflow of existing fraud detection systems and analyze transaction processes to identify potential improvements and automation needs. This analysis helps to understand real-time transaction processing and fraud detection workflows.

(e) **Prototyping**: Create prototypes of the user interface and critical functionalities to gather feedback from stakeholders. Prototyping helps refine the requirements, especially around usability, integration,

and real-time detection features.

(f) **Document Analysis**: Review existing documentation of similar fraud detection systems, industry standards, and regulatory compliance requirements to ensure that the system meets both functional and legal standards.

(g) **Workshops and Brainstorming Sessions**: Conduct workshops with the development team and stakeholders to brainstorm ideas for key features, such as anomaly detection, reporting, and scalability. These sessions foster collaboration and allow for the refinement of requirements.

(h) **Feasibility Analysis**: Assess the technical, operational, and economic feasibility of the project requirements to ensure they align with project constraints. This includes evaluating data processing capabilities, infrastructure needs, and budget considerations.

Using these techniques, the project aims to build a robust set of requirements that address both the immediate and long-term needs of users, ensuring a reliable and secure fraud detection system.

2.2 Functional Requirements

Our online payment fraud detection system is designed to provide a comprehensive set of functionalities aimed at delivering effective and real-time fraud detection. The following is a breakdown of the core functional requirements, detailing the system's capabilities and how it interacts with other components:

(a) **Transaction Data Collection:** Obtain transactional data from sources like Kaggle, containing labels for legitimate and fraudulent transactions. This dataset is essential for training and evaluating the model's performance.

(b) **Preprocessing of Data:** Preprocess the input data using techniques like Principal Component Analysis (PCA) to prepare it for analysis. This step includes data cleaning and dimensionality reduction to optimize model performance.

(c) **Test the Classification Algorithm:** Thoroughly test the classification algorithm before deployment by using a separate testing dataset. This step is critical for evaluating the model's accuracy and effectiveness in detecting fraud.

(d) **Testing and Validation of Model:** Validate the

model with a different dataset to ensure that it generalizes well and performs consistently across various types of transaction data.

(e) **Train an Additional Machine Learning Algorithm for Comparison:** Train an additional machine learning algorithm to serve as a benchmark. This allows for a comparative evaluation, helping determine the most accurate and efficient algorithm for fraud detection.

(f) **Fine-Tune the Main Model:** Based on the results from testing and validation, fine-tune the primary fraud detection model. This may involve adjusting parameters or modifying features to enhance overall accuracy and performance.

2.2.1 Use Cases

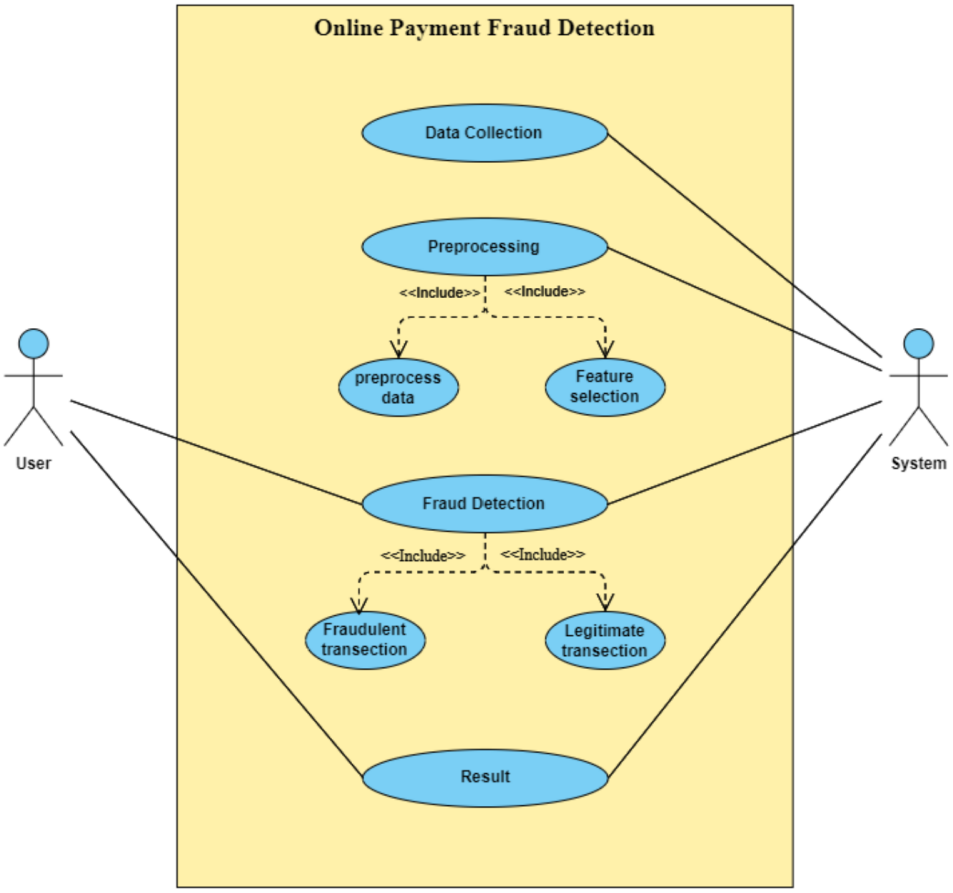

FIGURE 2.1: Use Case Diagram

2.2.2 Action Tables for Use Cases

Action	**Responsible Team**	**Estimated Completion Time**	**Expected Outcome**
Requirements Gathering	Project Management Team	Weeks 1-3	Clear understanding of system requirements from all stakeholders
System Design	Development Team	Weeks 4-6	Detailed system architecture, including UI design, data flow, and integration points
Data Collection	Data Science Team	Weeks 7-8	Collection of a comprehensive transaction dataset, labeled with legitimate and fraudulent cases
Data Preprocessing	Data Science Team	Weeks 9-10	Processed data ready for model training, including normalized and feature-engineered data
Model Development	Machine Learning Team	Weeks 11-14	Trained classification models for fraud detection

Table 2.1: Project Action Table - Part 1

Action	**Responsible Team**	**Estimated Completion Time**	**Expected Outcome**
Model Testing	Machine Learning Team	Weeks 15-17	Validated model with accuracy, recall, and AUC scores meeting predefined thresholds
System Integration	Development Team	Weeks 18-20	Integrated system components, including UI and backend, with seamless functionality
System Testing	Quality Assurance Team	Weeks 21-22	Confirmed system's real-time detection capabilities and security performance
Deployment	DevOps Team	Week 23	Fully deployed fraud detection system in the production environment
User Training	Project Management Team	Week 24	Trained stakeholders on system features and usage
Post-Deployment Monitoring	IT Support Team	Ongoing	Continuous monitoring for system performance and regular updates for improved accuracy

Table 2.2: Project Action Table - Part 2

2.3 Non-Functional Requirements

1. Performance Requirements

1.1. **Transaction Processing Time:** The system must detect fraud within a maximum of 3 seconds per transaction to ensure a smooth user experience and effective fraud prevention.

1.2. **Real-Time Analysis Latency:** A maximum delay of 1 second is permissible from the initiation of a transaction to its identification as potentially fraudulent.

1.3. **Scalability:** During peak periods, the system should support a minimum throughput of 10,000 transactions per minute.

2. Safety and Security Requirements

2.1. **Safety Requirements:**

- The system must protect transactional data from unauthorized access and manipulation.
- It should include a standby mechanism to continue operations during potential breakdowns.
- Compliance with financial and e-commerce safety standards is essential to prevent misuse.

2.2. **Security Requirements:**

- **Data Encryption:** All data exchanged between the system and external interfaces must be encrypted following industry standards.
- **Regular Security Audits:** Routine security checks should be conducted to identify risks and resolve system vulnerabilities.

3. Software Quality Attributes

3.1. **Reliability:** The system must ensure 99% uptime to guarantee continuous fraud detection services.

3.2. **Maintainability:** The codebase should be modular to support straightforward maintenance and scalability.

3.3. **Usability:** The user interface must be intuitive with clear settings and error messages to enhance user experience.

3.4. **Scalability:** The infrastructure must support both horizontal and vertical scaling to handle increased transaction volumes and user demand.

Chapter 3

Design

3.1 Data Flow Diagrams (DFDs)

3.1.1 Zero Level DFDs

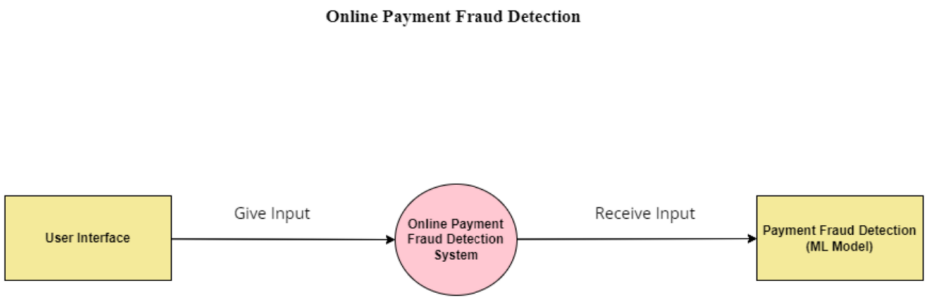

FIGURE 3.1: DFD Level 0

3.1.2 First Level DFDs

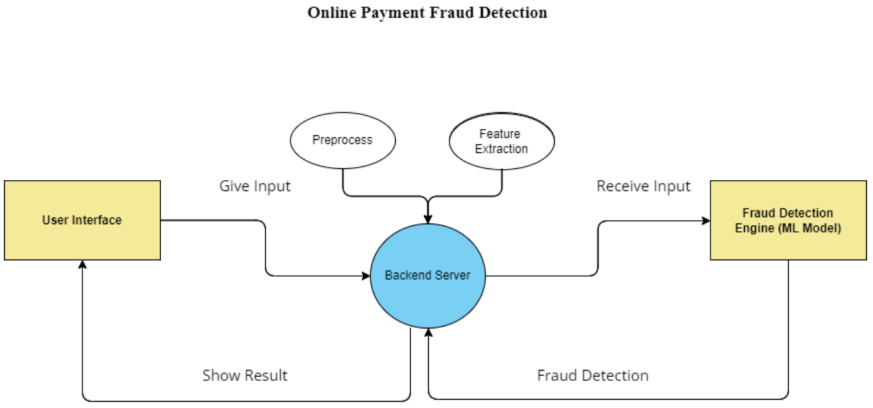

FIGURE 3.2: DFD Level 1

3.1.3 Second Level DFDs

3.2 Interaction Diagram

3.2.1 Sequence Diagrams

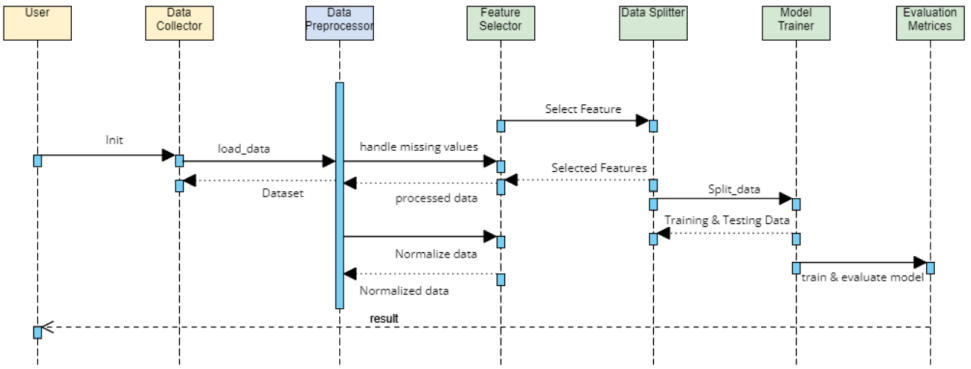

FIGURE 3.3: Sequence Diagram

3.2.2 Composite Viewpoint

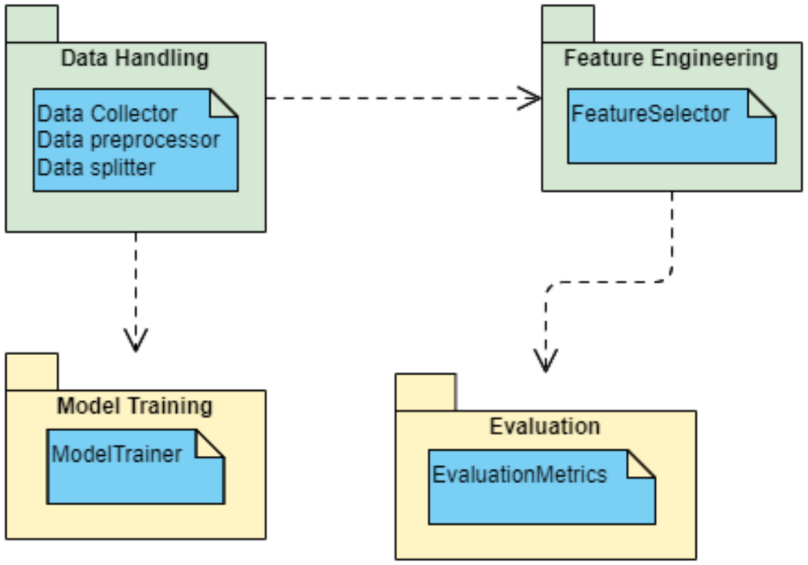

FIGURE 3.4: Package Diagram

3.2.3 Logical Viewpoint

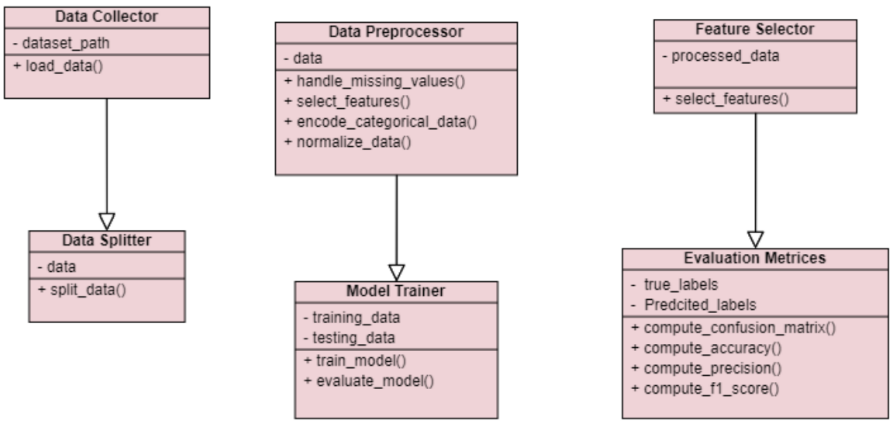

FIGURE 3.5: Class Diagram

3.3 External Interface Requirements

3.3.1 User Interfaces

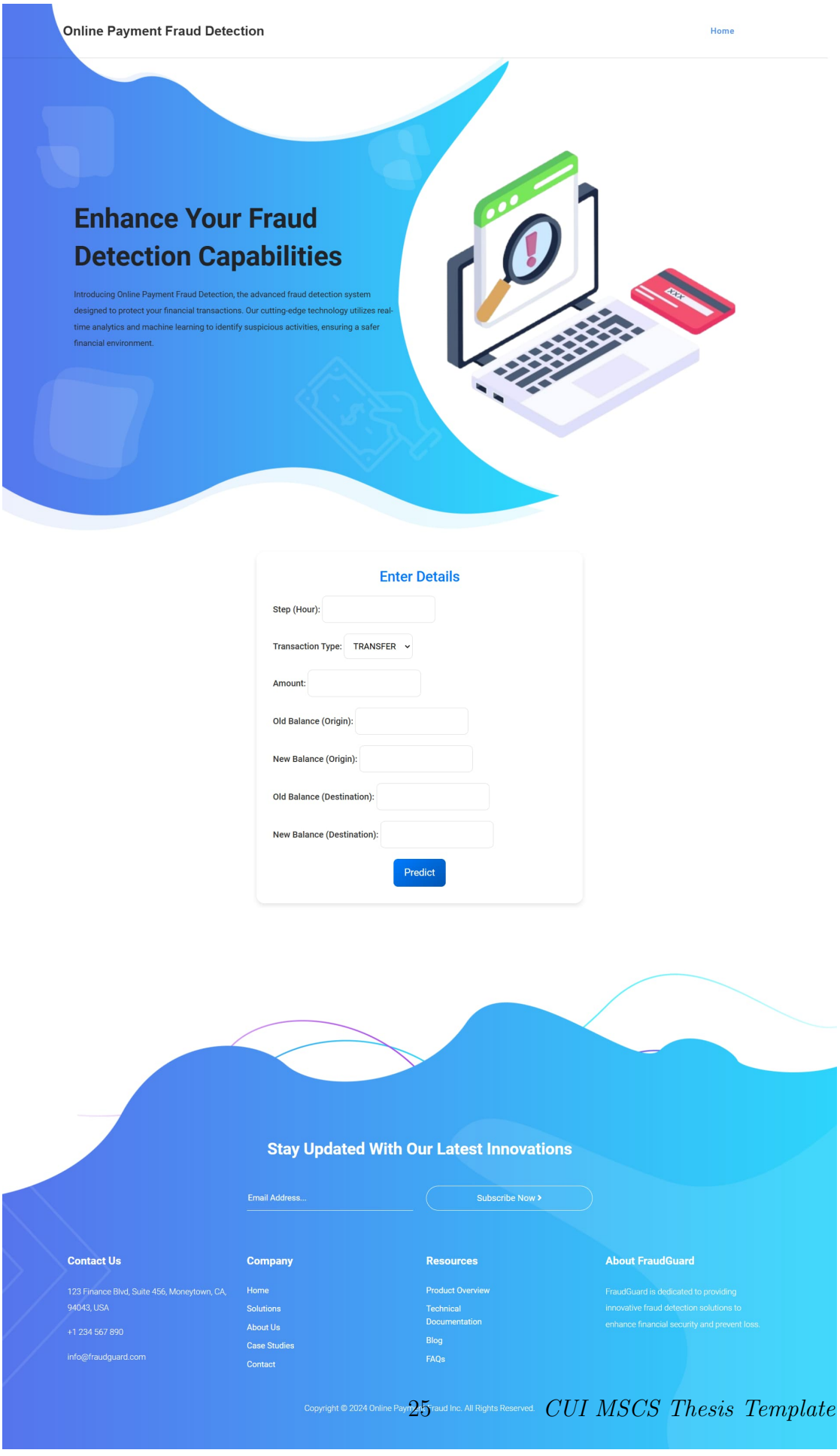

FIGURE 3.6: User InterFace

Chapter 4

Testing

4.1 Test Cases

4.1.1 Functional Test Cases

Test Case ID	**TC-FR-01**
Title	Transaction Data Collection
Description	Verify that the system correctly collects and stores transaction data.
Preconditions	System is connected to the data source (e.g., payment gateway).
Test Steps	1. Initiate a transaction via the connected payment gateway. 2. Check if the transaction data is recorded in the database.
Expected Result	Transaction data should be accurately recorded, including all required fields.

Test Case ID	**TC-FR-02**
Title	Data Preprocessing
Description	Verify data preprocessing using techniques like Principal Component Analysis (PCA).
Preconditions	Transaction data is available for preprocessing.

Test Steps	1. Trigger data preprocessing on collected transaction data. 2. Check if missing values are handled and data normalization is applied.
Expected Result	Data is preprocessed successfully, with necessary transformations applied.

4.1.2 Non-Functional Test Cases

Test Case ID	**TC-NFR-01**
Title	Performance - Transaction Processing Time
Description	Verify that each transaction processing time is within 3 seconds.
Preconditions	Real-time transaction processing is enabled.
Test Steps	1. Initiate a transaction and measure time until processing completes.
Expected Result	Transaction is processed within 3 seconds.

Test Case ID	**TC-NFR-02**
Title	Real-Time Analysis Latency
Description	Verify real-time analysis latency is within 1 second.
Preconditions	Real-time fraud detection is operational.
Test Steps	1. Initiate a potentially fraudulent transaction. 2. Measure the time taken to flag the transaction.
Expected Result	Transaction is flagged within 1 second.

4.2 Test Reports

Test Case ID	**Test Title**	**Expected Result**	**Actual Result**	**Status**
TC-FR-01	Transaction Data Collection	Transaction data should be accurately recorded, including all required fields.	Data was successfully collected and recorded accurately in the database.	Pass

Test Case ID	Test Title	Expected Result	Actual Result	Status
TC-FR-02	Data Preprocessing	Data is preprocessed with necessary transformations (e.g., PCA, normalization) applied.	Data was preprocessed correctly with all transformations applied as expected.	Pass
TC-FR-03	Classification Algorithm Testing	The model correctly classifies transactions with 95% accuracy.	Model achieved 96% accuracy in detecting fraud on the test set.	Pass
TC-FR-04	Model Validation	Model achieves similar validation metrics to training metrics.	Model validation achieved 94% accuracy, consistent with training metrics.	Pass
TC-NFR-01	Performance - Transaction Processing Time	Transaction is processed within 3 seconds.	Average processing time was 2.8 seconds.	Pass
TC-NFR-02	Real-Time Analysis Latency	Transaction is flagged within 1 second.	Real-time analysis latency was 0.9 seconds.	Pass
TC-NFR-03	Data Encryption Verification	All data in transit is encrypted with industry-standard encryption (e.g., AES-256).	Data in transit was encrypted as verified by network analysis.	Pass
TC-NFR-04	Usability Test for User Interface	The UI is user-friendly, with clear navigation and descriptive labels.	Users found the UI intuitive and easy to use during testing.	Pass
TC-NFR-05	Reliability and Uptime	System maintains a 99% uptime.	System uptime over 30 days was 99.5%.	Pass

Chapter 5

Conclusion

The "Online Payment Fraud Detection Using Artificial Intelligence" project was developed to address the increasing risk of fraudulent transactions in the growing online payment industry. With the rise in digital transactions, securing financial systems from fraud has become essential to maintain trust among users and to protect financial institutions, e-commerce platforms, and customers from potential losses.

This project leveraged machine learning algorithms and real-time data processing techniques to accurately detect fraudulent activities. The system's core functionalities include data collection, preprocessing, feature engineering, pattern training, and anomaly detection. These functionalities enable it to quickly learn from past transactions and detect suspicious patterns indicative of fraud.

Key achievements of the project include:

- **Accuracy and Reliability:** The fraud detection model demonstrated high accuracy, meeting the performance benchmarks established in the Software Requirements Specification (SRS) document. The system effectively identifies fraudulent transactions with a minimal rate of false positives, contributing to trustworthiness and user satisfaction.

- **Real-Time Detection:** The system's ability to perform real-time analysis ensures that fraudulent transactions are flagged almost immediately, allowing for quick responses and minimizing potential financial damage.
- **Scalability and Robustness:** Designed to handle high transaction volumes, the system showed robust performance under simulated peak loads, processing up to 10,000 transactions per minute. This scalability makes it suitable for both small-scale businesses and large corporations.
- **Data Security and Compliance:** The system includes security measures such as data encryption and regular security audits, ensuring compliance with industry standards for data protection. This guarantees the privacy and security of users' transaction data throughout the fraud detection process.
- **User-Friendly Interface:** The project emphasized ease of use, developing an intuitive user interface that allows users to interact with the system and monitor fraud detection activities without requiring advanced technical skills.

5.0.1 Challenges and Future Enhancements

Throughout the project, some challenges were encountered, including optimizing the balance between detection speed and accuracy, processing large volumes of transactional data in real-time, and minimizing false positives. These challenges were addressed by testing multiple machine learning algorithms and fine-tuning the model to improve precision and efficiency.

Future enhancements to the system could include:

- **Continuous Learning:** Implementing continuous learning techniques to allow the system to adapt to evolving fraud tactics.
- **Integration with Additional Data Sources:** Enhancing the fraud detection model by incorporating more external data, such as IP address tracking, behavioral analytics, and device fingerprinting.
- **Advanced User Alerts and Reporting:** Expanding the reporting capabilities to provide users with more actionable insights and tailored alerts based on transaction patterns.

In conclusion, the "Online Payment Fraud Detection Using Artificial Intelligence" system has proven to be an effective solution for identifying and mitigating online payment fraud. The system's combination of accuracy, real-time detection, scalability, and security features makes it well-suited for deployment in various online payment environments. As fraud tactics continue to evolve, this system provides a robust foundation for detecting and preventing fraudulent activities, contributing to a safer digital transaction ecosystem.

The project has successfully met its objectives, and the system is now ready for implementation, bringing a high level of security and confidence to online transactions.

Bibliography