Software Requirements Specification

for

Credit Card Fraud Detection System (CCFDS)

Version 1.0 approved

Prepared by Raj Srivastava

KIET Group of Institutions

Ghaziabad, Uttar Pradesh

30-10-2023

Table of Contents

1. Introduction

The Broad use of digital transactions in today's global economy has led to a significant increase in credit card fraud. Fraudsters employ sophisticated techniques to exploit vulnerabilities in payment systems, causing substantial financial losses to both individuals and organizations. In response to this escalating threat, the development of Credit Card Fraud Detection has become paramount. This abstract provides an overview of the key components, methodologies, and challenges associated with Credit Card Fraud Detection System.

Credit Card Fraud Detection Systems are advanced computational tools designed to identify and prevent fraudulent credit card transactions in real-time or during post-transaction analysis. These systems leverage a combination of data analytics, machine learning algorithms, and artificial intelligence techniques to analyse vast amounts of transaction data and detect suspicious activities. Key components of Credit Card Fraud Detection System include data preprocessing, feature engineering, model training and evaluation, and decision-making engines.

Data preprocessing is crucial in ensuring the accuracy and effectiveness of Credit Card Fraud Detection System. It involves data cleansing, normalization, and transformation to prepare the transaction data for analysis. Feature engineering is the process of selecting and creating relevant features from the dataset, which are then used to train machine learning models. Commonly used algorithms in Credit Card Fraud Detection System include logistic regression, decision trees, random forests, support vector machines, and neural networks. These models are trained on historical transaction data labelled as either genuine or fraudulent.

Evaluation of Credit Card Fraud Detection System models is essential to measure their performance accurately. Metrics such as accuracy, precision, recall, and F1-score are used to assess how well the system distinguishes between genuine and fraudulent transactions. To further enhance the accuracy of detection, some systems employ anomaly detection techniques, which identify deviations from normal transaction patterns.

In conclusion, Credit Card Fraud Detection Systems are indispensable tools in the fight against credit card fraud. They combine data analysis, machine learning, and AI to identify suspicious transactions, protect consumers, and mitigate financial losses for businesses. As fraudsters continue to evolve their tactics, ongoing research and development in this field are essential to stay ahead of emerging threats and ensure the security of digital payment systems.

1.1 Purpose

This System helps the people or vendors to protect them from credit card fraud which will happening in everyday on every website

1.2 Scope

i. Data Collection and Integration:
   - Gathering and integrating data from various sources, including transaction records, user profiles, and historical data.

ii. Data Preprocessing:
   - Cleaning and preprocessing the data to handle missing values, outliers, and inconsistencies.
   - Feature engineering to create relevant features for fraud detection.

iii. Model Development:
   - Building machine learning or deep learning models for fraud detection.
   - Exploring and selecting appropriate algorithms, such as logistic regression, random forests, support vector machines, or neural networks.
   - Training and fine-tuning models using historical data.

iv. Real-time Monitoring:
   - Implementing real-time or near-real-time monitoring of credit card transactions.
   - Developing alerting mechanisms to flag suspicious transactions.

v. Anomaly Detection:
   - Creating algorithms for anomaly detection to identify unusual or suspicious patterns in transaction data.
   - Utilizing statistical and machine learning techniques to identify deviations from normal behavior.

vi. Rule-Based Systems:
   - Implementing rule-based systems to capture known fraud patterns.
   - Defining rules and thresholds for various transaction parameters.

vii. Model Evaluation:
   - Assessing the performance of the fraud detection models using metrics like precision, recall, F1-score, and ROC curves.
   - Conducting cross-validation and benchmarking against baseline models.

viii. Model Deployment:
   - Deploying the trained models into a production environment where they can process incoming transactions in real time.
   - Ensuring scalability and low latency for processing a large volume of transactions.

ix. Regulatory Compliance:
   - Ensuring that the system complies with relevant industry regulations and data privacy laws, such as GDPR or PCI DSS.

x. Security and Privacy:

- Implementing robust security measures to protect sensitive data and prevent unauthorized access to the system.
- Ensuring that customer data is handled with care and in compliance with privacy regulations.

1.3 Definitions, Acronyms and Abbreviations

-SRS: Software Requirement Specifications
-FCCDS: Credit Card Fraud Detection System

1.4 References

- https://www.ijitee.org/wp-content/uploads/papers/v10i6/C84000110321.pdf
- https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud
- Credit Card Fraud Detection Based on Transaction Behaviour, by John Richard D. Kho Larry A. Veam published by Proc of the 2017 IEEE Region 10 Conference, (TENCON) Malaysia November 5-8 -2017
- CLIFTON PHUA1 VINCENT LEE1 KATE SMITH1&ROSS GAYLER2 A Comprehensive Survey of Data Mining-based, Fraud, Detection, Research published by School of Business Systems Faculty of Information Technology Monash University Wellington Road Clayton Victoria 3800 Australia

2. Overall Description

The rapid growth of digital transactions in today's global economy has led to a significant increase in credit card fraud. Fraudsters employ sophisticated techniques to exploit vulnerabilities in payment systems, causing substantial financial losses to both individuals and organizations. In response to this escalating threat, the development of Credit Card Fraud Detection has become paramount. This abstract provides an overview of the key components, methodologies, and challenges associated with Credit Card Fraud Detection System.

Credit Card Fraud Detection Systems are advanced computational tools designed to identify and prevent fraudulent credit card transactions in real-time or during post-transaction analysis. These systems leverage a combination of data analytics, machine learning algorithms, and artificial intelligence techniques to analyse vast amounts of transaction data and detect suspicious activities. Key components of Credit Card Fraud Detection System include data preprocessing, feature engineering, model training and evaluation, and decision-making engines.

Data preprocessing is crucial in ensuring the accuracy and effectiveness of Credit Card Fraud Detection System. It involves data cleansing, normalization, and transformation to prepare the transaction data for analysis. Feature engineering is the process of selecting and creating relevant features from the dataset, which are then used to train machine learning models. Commonly used algorithms in Credit Card Fraud Detection System include logistic regression, decision trees, random forests, support vector machines, and neural networks. These models are trained on historical transaction data labelled as either genuine or fraudulent.

Evaluation of Credit Card Fraud Detection System models is essential to measure their performance accurately. Metrics such as accuracy, precision, recall, and F1-score are used to assess how well the system distinguishes between genuine and fraudulent transactions. To further enhance the accuracy of detection, some systems employ anomaly detection techniques, which identify deviations from normal transaction patterns.

In conclusion, Credit Card Fraud Detection Systems are indispensable tools in the fight against credit card fraud. They combine data analysis, machine learning, and AI to identify suspicious transactions, protect consumers, and mitigate financial losses for businesses. As fraudsters continue to evolve their tactics, ongoing research and development in this field are essential to stay ahead of emerging threats and ensure the security of digital payment systems.

3. External Interface Requirements

3.1 Hardware Interface

Processor: Pentium i3 or higher.

RAM: 4 GB or higher.

Hard Disk Drive: 20 GB (free).

Peripheral Devices: Monitor, Mouse and Keyboard

3.2 Software Interface

Operating system: Windows 8/10.

IDE Tool: PyCharm

Coding Language: Python 3.6

APIs: NumPy, Pandas, PySpark, Matplotlib

4. Other Non-Functional Requirements

4.1 Software System Attributes

4.1.1 Reliability

- The system should have an uptime of at least 99.9%.
- Regular maintenance and updates should not disrupt user access.
- Error handling should provide meaningful messages to users.

4.1.2 Availability

- User can access the software easily and use it without any problem.
- A hassle free experience provide user a better experience.

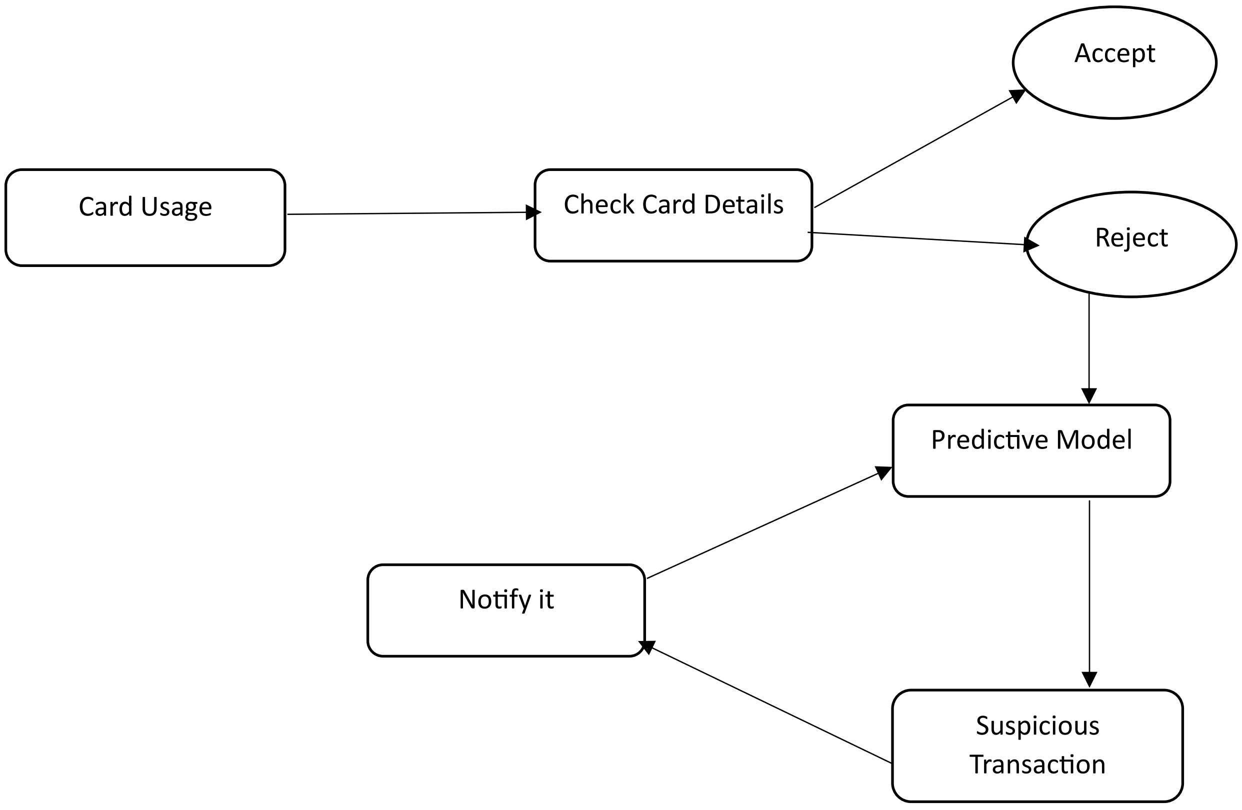
4.1.3 Performance

- The system should respond to user interactions within 2 seconds.
- The system should support a minimum of 1000 concurrent users.

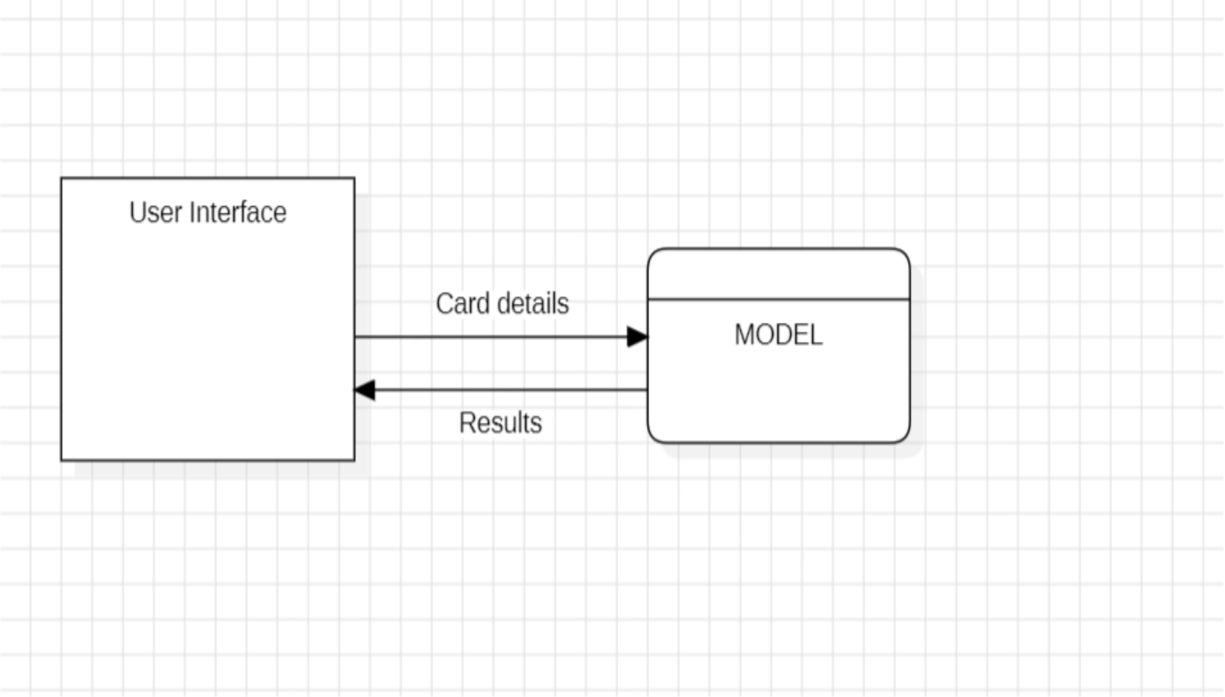
4.1.4 Maintainability

- The Software should always be corrective maintenance.
- Changes of hardware, operating system and software dependency does not impact.

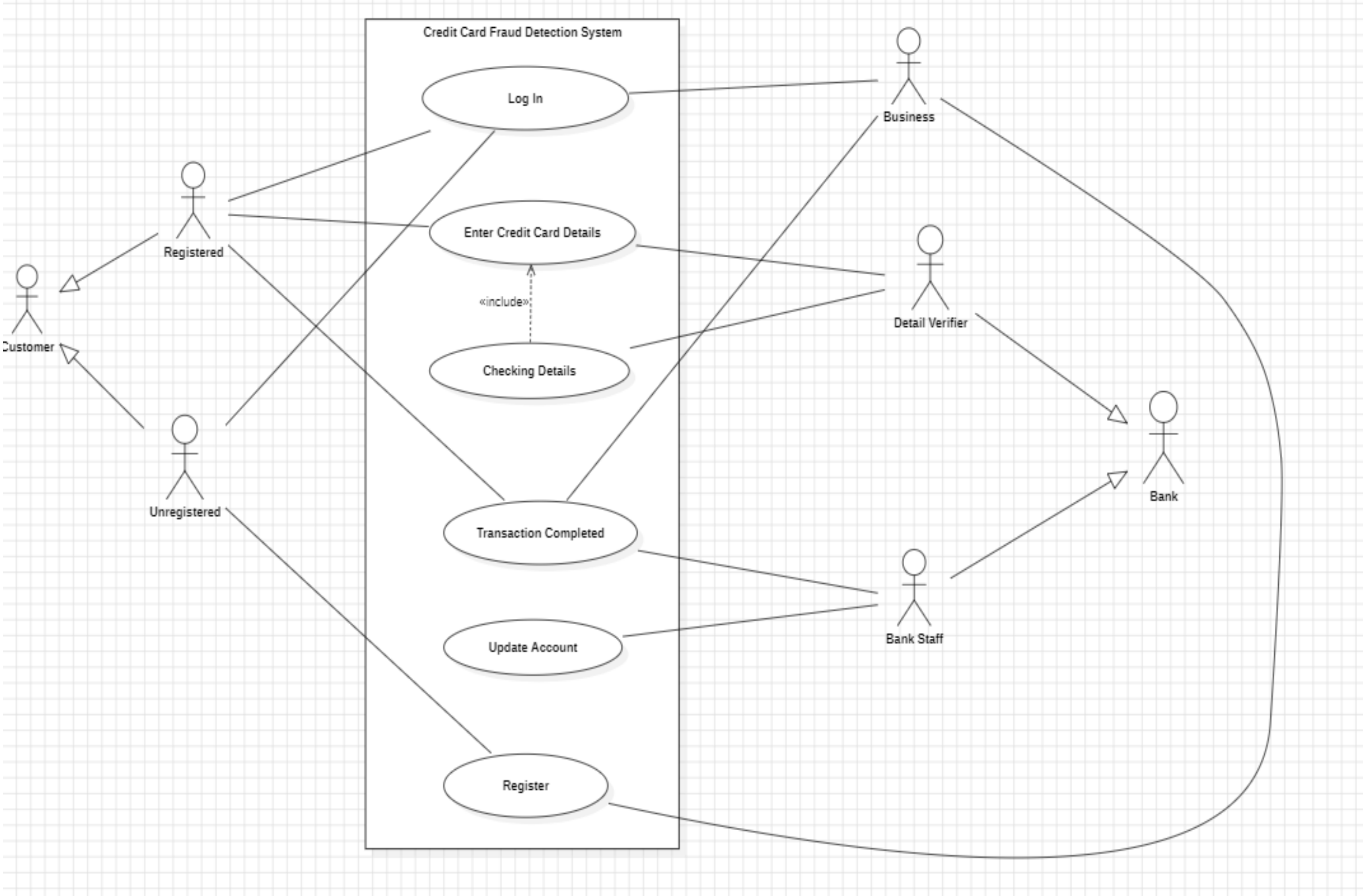
5. Flow Diagram



6. Data Flow Diagram:-



7. Use Case Diagram:-


Credit Card Fraud Detection System
Log In
Enter Credit Card Details
«include»
Checking Details
Transaction Completed
Update Account
Register
Registered
Customer
Unregistered
Business
Detail Verifier
Bank
Bank Staff