ACROPOLIS
Enlightening wisdom

Synopsis Presentation
on

Intelligent Fraud Detection System Using Machine Learning

Guided By:

Prof.Ankita Agrawal

Presented By:

Priyanshu Yadav (0827IT211091)

Shubhra Jain (0827IT211109)

Shyamsundar (0827IT211111)

Yashika Rahinj (0827IT211134)

ACROPOLIS
Enlightening wisdom

Contents

1. Introduction

1.1 Overview

- Fraudulent activities in bank transactions are an increasing concern in our quickly changing digital world.
- Offering serious risks to both financial institutions and their clients.
- Traditional rule-based systems frequently struggle to recognize and stop these more complex fraud schemes.

1.2 Purpose

- Machine learning has become a powerful technique to handle this problem, with classification at its core.
- This study seeks to investigate the use of logistic regression in the particular context of detecting bank transaction fraud.
- While highlighting its benefits, drawbacks, and practical use in the financial industry.

ACROPOLIS
Enlightening wisdom

2. Literature Review

S. No.	Name of Solution/System	Features	Drawback
1	Random Forest	Fast training and prediction	Sensitive to noisy data and outliers
2	Logistic Regression	Simple, interpretable model	Struggles with large feature sets and interactions
3	Decision Trees (CART)	Handles missing values well	Prone to overfitting without pruning
4	Neural Networks	Learns complex, non-linear patterns	Computationally intensive
5	XGBoost	High-performance gradient boosting	Dependent on smartphones and internet

3. Problem Statement

- **Reduce reliance on manual fraud detection**
  Minimize human involvement in detecting fraud by automating the process using machine learning.

- **Ensure real-time fraud detection**
  Implement a system capable of detecting fraud as transactions occur, with immediate alerts.

- **Adapt to changing fraud patterns**
  Design a system that evolves with emerging fraud techniques and continuously learns from new data.

- **Handle large transaction datasets efficiently**
  Build a system capable of processing and analyzing high volumes of transaction data without performance degradation.

- **Minimize false positive rates**
  Ensure that legitimate transactions are not incorrectly flagged as fraudulent, reducing customer friction and operational overhead.

4. Proposed Solution

- **Fraud detection with machine learning models**
  Train algorithms like Random Forest or XGBoost on labeled transaction data to classify transactions as fraudulent or legitimate.

- **Automated fraud detection**
  Develop an automated pipeline that processes incoming transactions and applies the trained model without manual intervention.

- **Real-time transaction analysis**
  Deploy the model in a real-time environment where transactions are evaluated immediately, and suspicious activities are flagged instantly.

- **Adaptive fraud detection**
  Continuously retrain the model with new transaction data to adapt to evolving fraud patterns.

4. Proposed Solution

- **Scalable system design**
  Implement a cloud-based infrastructure to handle large transaction volumes efficiently, ensuring the system scales as transaction data grows.

- **Reduce false positives**
  Optimize machine learning models and fine-tune detection thresholds to minimize legitimate transactions being incorrectly flagged as fraud.

- **Detect new and unseen fraud tactics**
  Leverage anomaly detection techniques to identify emerging fraud schemes that have not been observed in historical data.

- **Provide real-time decision-making support**
  Develop a real-time fraud detection system that can provide instant feedback on transactions, enabling immediate actions by fraud analysts or automated systems.

ACROPOLIS
Enlightening wisdom

5. Objectives

- **Identify fraudulent transactions accurately**
  Use machine learning algorithms to detect fraudulent activities within large datasets of financial transactions.

- **Detect fraud in real-time**
  Implement a system capable of immediately identifying and responding to potential fraudulent transactions as they occur.

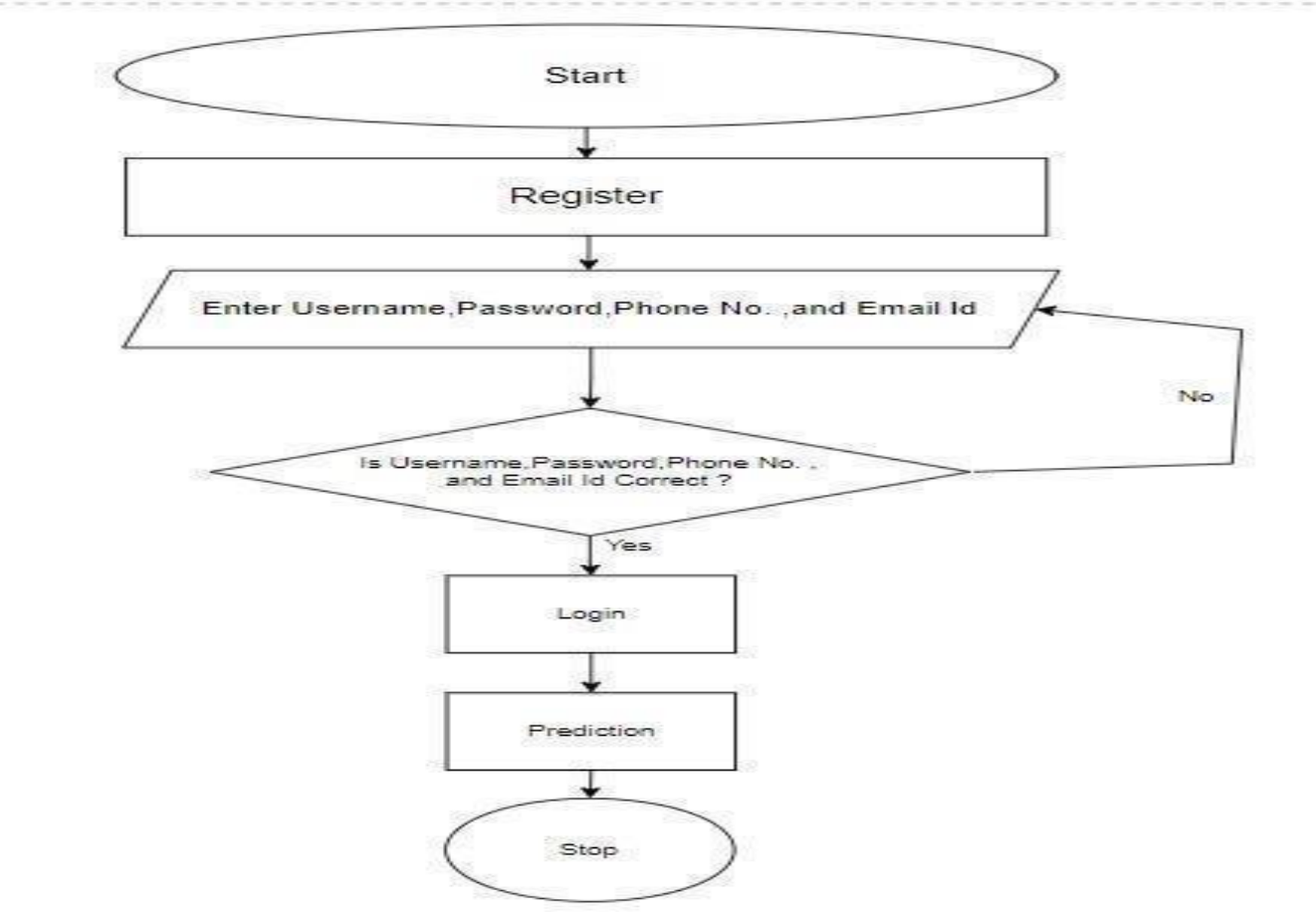
- **Adapt to evolving fraud patterns**
  Continuously enhance the fraud detection model to detect emerging fraud techniques and trends over time.

- **Optimize the system for scalability**
  Build a solution that can scale efficiently to handle high transaction volumes, ensuring performance remains optimal as data grows.

- **Improve decision-making with minimal false positives**
  Fine-tune the system to minimize false positives, ensuring that legitimate transactions are not flagged as fraudulent.

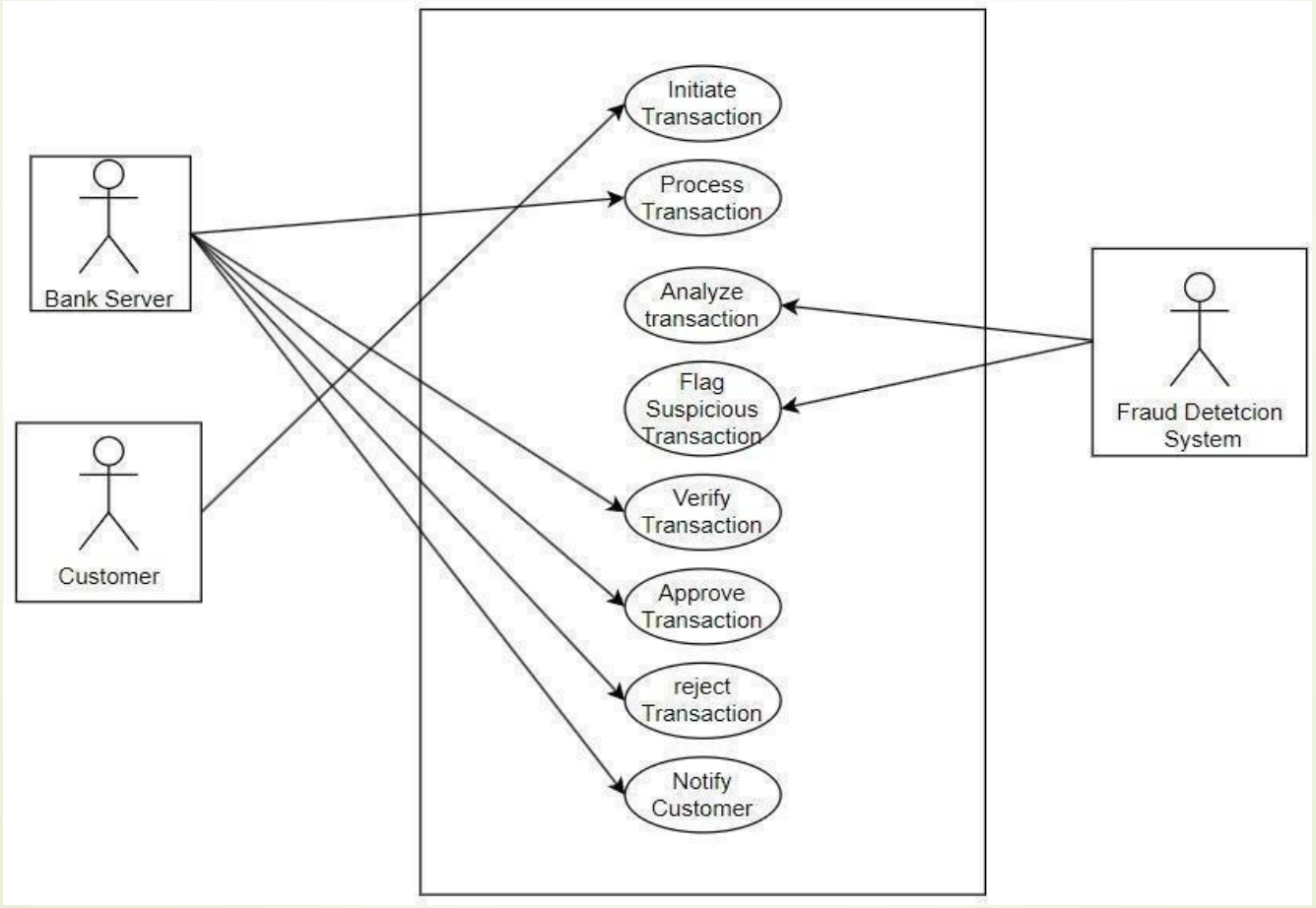
6. Theoretical Analysis

6.1.1 Flowchart:



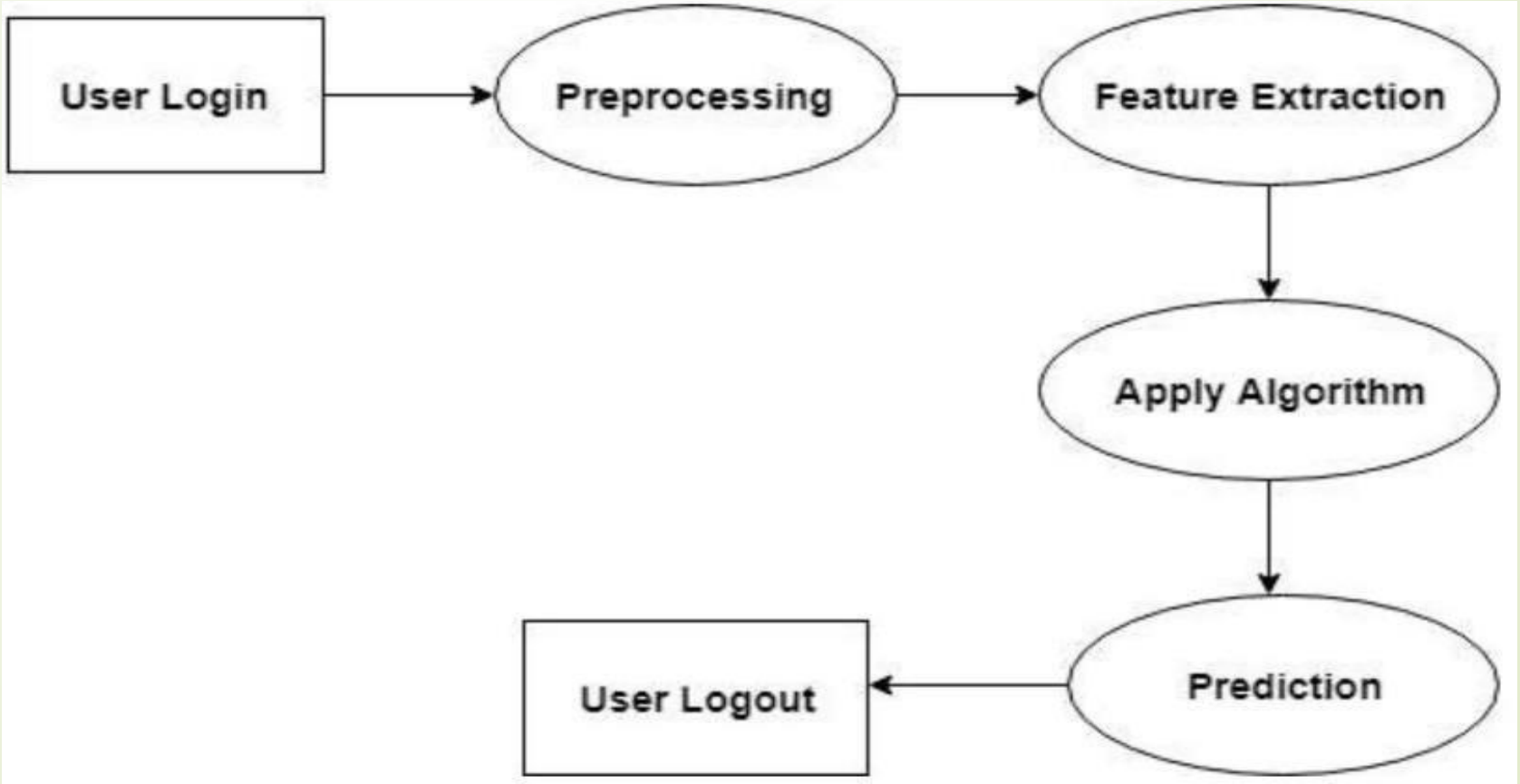
6. Theoretical Analysis

6.1.2 Use Case Diagram:



6. Theoretical Analysis

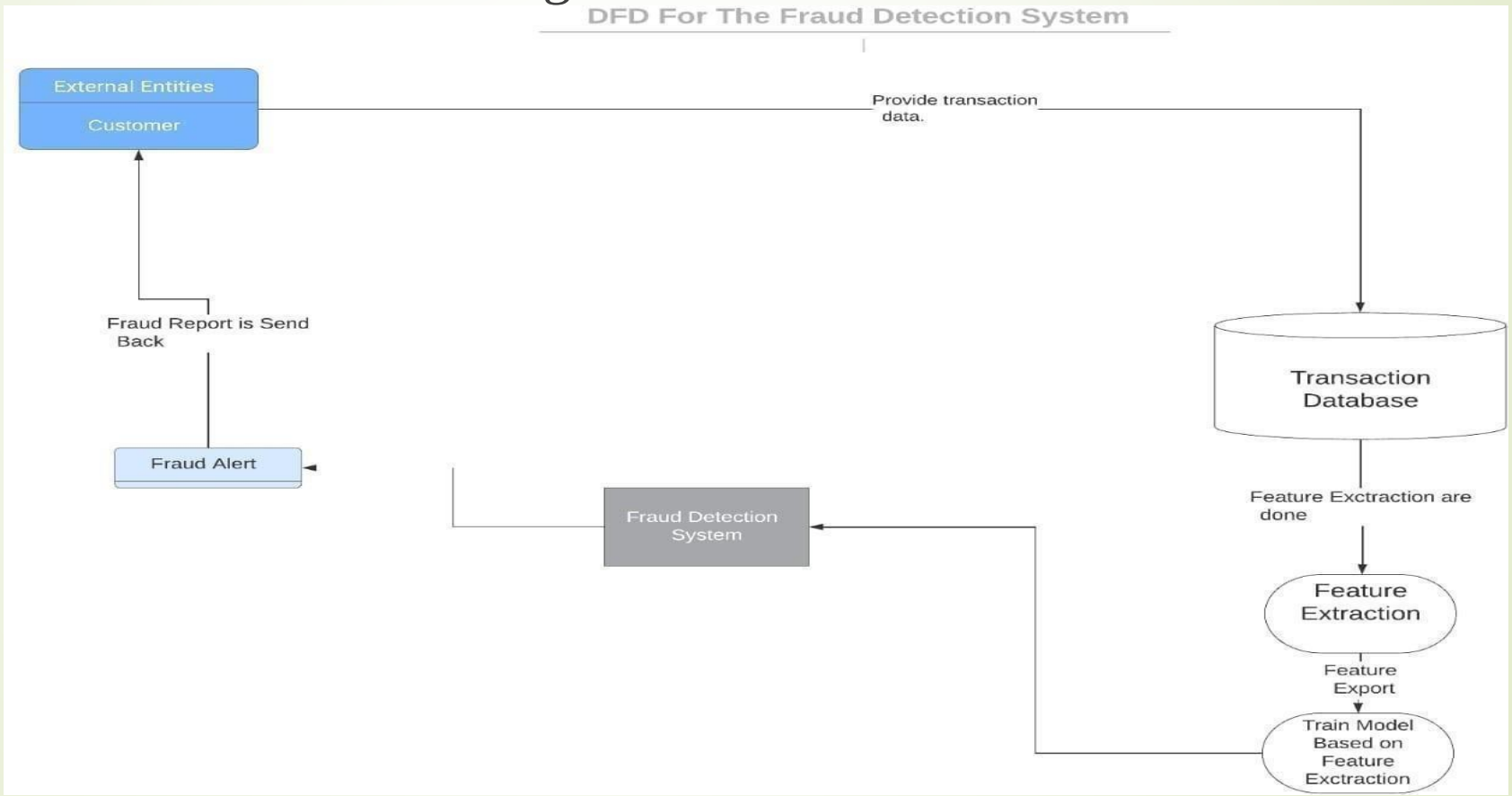
6.1.3 Block Diagram:



ACROPOLIS
Enlightening wisdom

6. Theoretical Analysis

6.1.4 Detailed Block Diagram:



6. Theoretical Analysis

6.2 Software Requirements:

Python: It offers a rich ecosystem of libraries and frameworks that are well-suited for image recognition, data preprocessing, and model development. Data Management and Processing

Pandas: Pandas is a Python library used for data manipulation and analysis. It can be beneficial for handling datasets and preprocessing.

NumPy: NumPy is another Python library for numerical computing. It's useful for performing operations on multidimensional arrays, which are common in image data.

ACROPOLIS
Enlightening wisdom

Applications

1. **Anomaly Detection**: Identifies transactions that deviate from typical spending patterns, signaling potential fraud.
2. **Real-Time Fraud Prevention**: Flags suspicious transactions instantly, preventing fraudulent activities.
3. **Classification Models**: Uses labeled data to classify transactions as legitimate or fraudulent, improving predictive accuracy.
4. **Ensemble Learning**: Combines multiple models to enhance fraud detection by reducing errors and improving robustness.
5. **Clustering Techniques**: Groups similar transactions, helping to spot outliers that may indicate fraudulent behavior.
6. **Deep Learning**: Detects complex, non-linear fraud patterns in large datasets using neural networks.
7. **Risk Scoring**: Assigns a risk score to each transaction, automatically flagging or blocking high-risk activities.
8. **Adaptive Learning**: Continuously updates the model based on new data to stay ahead of evolving fraud tactics.

REFERENCES

1. https://www.tutorialspoint.com/scikit_learn/index.htm
2. https://en.wikipedia.org/wiki/Data_analysis_for_fraud_detection
3. https://en.wikipedia.org/wiki/Credit_card_fraud
4. https://www.itransition.com/machine-learning/fraud-detection

ACROPOLIS
Enlightening wisdom

Thank You

Queries ?