MicroVoluntia: A Web Portal for Event-Based and Micro-Volunteering

A

SYNOPSIS

SUBMITTED TO THE

SHETH L.U.J AND SIR M.V. COLLEGE

FOR THE DEGREE

OF

BACHLEOR OF COMPUTER SCIENCE

IN

COMPUTER SCIENCE

BY

BHUMIKA ROHIDAS SHELAR

(Seat No. T114)

UNDER THE GUIDANCE OF

Prof.

DEPARTMENT OF COMPUTER SCIENCE

SHETH L.U.J AND SIR M.V. COLLEGE,

DR. S. RADHAKRISHNAN MARG, ANDHERI EAST, MUMBAI -400069

Year 2025-26

(i) Title : MicroVoluntia: A Web Portal for Event-Based Micro-Volunteering

(ii) Name of student : Bhumika Rohidas Shelar

(iii) Seat no. : T114

(iv) Subject :

(v) Guide name :

Signature of student Signature and seal of guide

Contents of Synopsis

Introduction

With the exponential growth of digital transactions and e-commerce platforms, online payment systems have become a vital component of modern financial infrastructure. However, this growth has also led to an increase in fraudulent activities such as unauthorized transactions, identity theft, and phishing attacks. Traditional fraud detection systems, which rely on predefined rules, often fall short in identifying sophisticated and evolving fraudulent patterns.

This project, titled "AI-Based Fraud Detection in Online Payment System," proposes the development of a secure and intelligent web-based platform that uses Artificial Intelligence (AI) and Machine Learning (ML) algorithms to detect fraudulent transactions in real-time. By analyzing various features such as transaction amount, time, location, device information, and user behavior, the system aims to predict the likelihood of a transaction being fraudulent.

The objective is to enhance the reliability and security of online payment systems by providing accurate fraud detection, timely alerts, and data-driven risk analysis. This platform will help reduce financial losses and build trust among users by ensuring secure digital transactions.

Problem Statement

With the increasing reliance on online payment systems for financial transactions, there has been a corresponding rise in fraudulent activities such as credit card fraud, phishing attacks, identity theft, and account takeovers. Traditional rule-based fraud detection methods are often static and fail to detect complex, evolving, and previously unseen fraudulent behaviors. These systems lack the ability to adapt to new patterns and often generate false positives or miss subtle anomalies.

There is a critical need for an intelligent, adaptive, and real-time solution that can accurately detect and prevent fraudulent transactions without compromising user experience. This project aims to address this problem by developing an AI-powered web-based fraud detection system that leverages machine learning techniques to analyze transaction data, identify suspicious behavior, and provide timely alerts to users and administrators.

Objectives

- To develop a web-based platform that facilitates secure online transactions with integrated fraud detection capabilities.

- To design and implement AI/ML algorithms capable of analyzing transactional data and identifying fraudulent patterns with high accuracy.
- To enable real-time fraud detection and alerting, thereby minimizing financial loss and protecting user accounts from unauthorized access.
- To generate risk scores for each transaction based on parameters such as amount, time, location, device type, and historical behavior.
- To incorporate a feedback mechanism where flagged transactions can be reviewed, allowing the model to learn and improve over time.
- To ensure user-friendly interfaces for both users and administrators, including dashboards for transaction monitoring, alerts, and analytics.
- To enhance system security by integrating user authentication techniques and preventing common vulnerabilities in online payment systems.

Scope Of The Project

The scope of this project is confined to developing a web-based platform that utilizes Artificial Intelligence and Machine Learning techniques to detect fraudulent activities within online payment systems. The platform will include features such as a user-friendly interface for performing transactions, real-time fraud detection through AI models trained on historical transaction data, and a risk scoring system that evaluates the likelihood of fraud based on various factors like transaction amount, time, frequency, location, and device information. Additionally, the system will generate real-time alerts for users and administrators upon detecting suspicious behavior and will offer an admin dashboard for monitoring flagged transactions and analyzing fraud trends. The project will also incorporate essential security features such as user authentication and will support a feedback mechanism to improve the accuracy of the detection model over time.

However, the project does not cover integration with actual banking systems or real-world payment gateways such as Razorpay or PayPal. It is limited to simulated transactions for demonstration purposes. Furthermore, the system will not handle fraud detection outside the domain of online payments, such as insurance or loan fraud. Legal actions, reporting to authorities, and financial recovery post-fraud incidents are beyond the scope of this project. Advanced security measures like biometric authentication or blockchain integration, as well as fraud detection in high-frequency trading or large-scale enterprise systems, are also excluded from the project's boundaries.

Work Plan

The implementation of the AI-Based Fraud Detection in Online Payment System will follow a structured work plan divided into phases. Each phase will focus on specific tasks ranging from requirement gathering to testing and deployment. This approach ensures clarity, proper resource allocation, and efficient progress tracking.

The project will utilize a range of modern tools and technologies to ensure smooth development and effective functionality. For the frontend, HTML5, CSS3, JavaScript, and Bootstrap will be used to design a user-friendly and responsive web interface. The backend will be developed using Python, with Flask or FastAPI as the web framework, allowing seamless integration of the machine learning model. The database will be managed using either MySQL for structured data storage or MongoDB for flexible JSON-based data handling. For developing and training the AI models, libraries such as Scikit-learn, Pandas, NumPy, and XGBoost will be employed. Data visualization for the admin dashboard will be handled using Matplotlib, Seaborn, or Chart.js. The project will be developed using Visual Studio Code and Jupyter Notebook, while version control will be maintained using GitHub. Additional tools like Google Colab may be used for model training, and Postman will assist in API testing. To secure the application, HTTPS protocols and JWT (JSON Web Tokens) will be used for token-based authentication.

The project will apply several important techniques to ensure accurate fraud detection and efficient system performance. Initially, data preprocessing will be conducted to clean the dataset by handling missing values, encoding categorical variables, and normalizing numerical data. Feature engineering will then be carried out to extract relevant attributes from transaction data, such as amount, frequency, location, device information, and time of transaction, which are critical in detecting suspicious patterns. The system will rely on supervised machine learning techniques, where models like Random Forest, Logistic Regression, and XGBoost will be trained on historical transaction datasets. Model evaluation will be based on performance metrics such as accuracy, precision, recall, and confusion matrix to ensure reliability. Once the best-performing model is selected, it will be integrated into the web application's backend to provide real-time fraud predictions. The system will also undergo rigorous testing, including unit testing, system testing, and user acceptance testing, to validate the accuracy and responsiveness of the solution.

Expected Outcome

The proposed project is expected to deliver a functional, intelligent, and secure web-based system capable of detecting and preventing fraudulent transactions in online payment environments. One of the key outcomes is the successful integration of a trained AI model that can accurately classify transactions as legitimate or suspicious based on multiple behavioral and transactional features. The system will provide real-time alerts to users and administrators, allowing timely intervention before potential financial losses occur.

The project will also feature a user-friendly interface for conducting transactions, a risk scoring mechanism to assess threat levels, and an admin dashboard for monitoring

fraud trends. Over time, the system is expected to improve its accuracy through continuous learning from feedback and new data, thus enhancing its adaptability to evolving fraud techniques.

From a practical standpoint, this platform can be applied to small-scale online businesses, e-commerce platforms, digital wallets, or educational payment portals to improve transaction security. The real-world impact includes increased user trust, reduced fraudulent activities, better decision-making through data analytics, and overall enhancement of cybersecurity in financial systems.

Conclusion

In an era where digital transactions have become the norm, ensuring the security and trustworthiness of online payment systems is more crucial than ever. This project, AI-Based Fraud Detection in Online Payment System, addresses the growing challenge of financial fraud by leveraging the power of Artificial Intelligence and Machine Learning. By analyzing transaction patterns and user behavior, the system can effectively identify and prevent fraudulent activities in real-time.

The project is not only technically feasible with the use of readily available tools and datasets but also highly relevant to real-world applications. Its implementation can significantly reduce financial losses, enhance user confidence, and support administrators in making informed decisions through data-driven insights. With continuous improvement and adaptability, the proposed system offers a scalable and impactful solution to combat cyber fraud in digital payment environments.