



Project Proposal

AI-Based Real-Time Fraud Detection in Digital Service Requests

Prepared By

Name: Majed Al Jebrel

ID No.:

Name: Ahmed Abutalib

ID No.: 243002097

Submitted in fulfillment of the requirements for the degree Master
of Science in Artificial Intelligence

At

Collage of Informatics

Midocean University

UAE

Supervisor Name: Amjad Qatish

Collage of Informatics, Midocean University, Comoros

Email: mr.ahmadabutalib@gmail.com

Email: majedaljebrel@gmail.com

1. Project Overview

The growth of digital services in sectors such as e-commerce, financial technology (FinTech), and online platforms has transformed user experiences—but also introduced significant vulnerabilities. One of the most pressing challenges is the increasing sophistication of fraud. Fraudulent activities such as unauthorized transactions, account takeovers, and false refund claims lead to substantial financial losses and erode user trust.

Traditional fraud detection systems rely heavily on predefined rules and manual reviews. These approaches often fail to detect new or evolving fraud tactics, generate high false-positive rates, and cannot scale with large volumes of data. With the advent of Artificial Intelligence (AI), particularly machine learning (ML) and deep learning (DL), it has become possible to detect complex, hidden fraud patterns in real time. This project aims to develop a robust AI-powered system that leverages behavioral and transactional data to detect fraudulent requests as they occur.

2. Project Goal

The primary goal of this research is to develop an intelligent fraud detection model capable of identifying fraudulent digital service requests in real time while maintaining a low false positive rate. The project aims to:

- Improve fraud detection accuracy using advanced ML/DL techniques.
- Minimize disruptions to legitimate users by reducing false alarms.
- Build a flexible, adaptive framework that evolves with changing fraud strategies.

3. Approach

To reach the project goal, the work will be divided into four main stages:

1. Data Collection:

Gather data from digital services such as user requests, transaction history, device info, and previous fraud cases. If real data is not available, public or simulated datasets will be used.

2. Data Preparation:

Clean the data by removing errors or missing values. Then organize and combine the data into a consistent format so it's ready for analysis.

3. Model Building:

Try different machine learning models like Logistic Regression, Random Forest, and XGBoost. Also test deep learning models like LSTM if needed. Special techniques will be used to handle the small number of fraud cases compared to normal ones.

4. Evaluation:

Test the models using important metrics like Precision, Recall, and F1-Score. The goal is to detect fraud accurately without wrongly blocking real users. The best model will be chosen for the final result

4. Project Steps and Timeline (8 Weeks)

Week Task

- 1 Data acquisition and initial cleaning**
- 2 Data integration and preparation**
- 3 Exploratory Data Analysis (EDA)**
- 4 Feature engineering and selection**
- 5 Model selection and baseline training**
- 6 Model evaluation and hyperparameter tuning**
- 7 Final testing and performance validation**
- 8 Report writing and framework proposal**

5. Expected Results

This research is expected to produce the following outcomes:

- A validated AI model that can detect fraud in real-time or near-real-time across digital platforms.**
- Clear identification of the most effective modeling techniques (ML or DL) for fraud detection under class imbalance conditions.**
- A refined set of features that significantly improve fraud detection accuracy.**
- Quantitative performance improvements over baseline rule-based or traditional systems.**
- A high-level adaptive framework for continuous learning and model retraining to maintain long-term relevance.**

6. Resources Needed

To execute the project successfully, the following resources will be required:

- **Software Tools:** Python, Jupyter Notebook, Scikit-learn, TensorFlow or PyTorch, XGBoost, pandas, NumPy, matplotlib.
- **Hardware:** A high-performance local machine with GPU support or access to cloud computing platforms (e.g., Google Colab, AWS, or Azure ML).
- **Datasets:** Historical request data with labeled fraud instances, behavioral logs, and device/network metadata. In the absence of real data, simulated or open-source datasets may be used.
- **Expert Guidance (Optional):** Feedback from fraud detection professionals or data scientists familiar with ML/DL in cybersecurity contexts.