LBS INSTITUTE OF TECHNOLOGY FOR WOMEN

Poojappura, Thiruvananthapuram, Kerala-695012

CSD 334 MINIPROJECT

Academic Year : 2024-2025	
Programme :Computer Science &Engineering	**Degree: B Tech**
Semester and Class : S6 CS1	**Regulation: 2019**
Names(Roll Nos)	**Aleena Sabu(12)** **Amina R(13)** **Anjali Krishna T J(17)** **Aparna S S(24)**
Title/ Area	**UPI Fraud Detection**
Miniproject Coordinator	**Prof Janisha A**
Guided By:	**Dr Lekshmy P L**

Signature **Signature**

(Miniproject Guide) **(Miniproject Coordinator)**

ABSTRACT

The rapid adoption of Unified Payments Interface (UPI) platforms has significantly transformed digital payments by providing users with unparalleled convenience, speed, and accessibility. These systems have simplified financial transactions, promoting a cashless economy and increasing user engagement. However, the exponential growth of UPI transactions has also introduced vulnerabilities, leading to a surge in fraudulent activities such as phishing, identity theft, and unauthorized access to accounts. Such activities result in severe financial losses for users and institutions, undermine trust in digital ecosystems, and create challenges in ensuring the security of payment infrastructures. This project aims to address these challenges by designing and developing a machine learning-based fraud detection system tailored for UPI platforms. The primary objective is to enable real-time detection and prevention of fraudulent transactions, ensuring both the safety and trustworthiness of digital payments. The methodology comprises six integral components: data collection, data preprocessing, feature engineering, machine learning model training, real-time fraud detection, and an alert system. Initially, transaction data is gathered and carefully cleaned to eliminate inconsistencies and enhance its reliability. Relevant features, such as transaction frequency, timing, and geographical patterns are extracted to capture potential indicators of fraud.
A robust machine learning model, powered by the XGBoost algorithm, is then trained on this data to classify transactions as either legitimate or fraudulent with high accuracy. This model is seamlessly integrated into the UPI framework, enabling continuous real-time fraud detection. The system's user interface is developed using Python-based frontend frameworks to ensure an intuitive and user-friendly experience, while the backend utilizes Python, Jupyter Notebook- for efficient data handling and analysis.

References

1. S. Sharma, R. Gupta, and A. Verma, "*Secure UPI: Machine Learning-Driven Fraud Detection System for UPI Transactions,"* presented at the 2023 IEEE International Conference on Machine Learning and Applications (ICMLA), San Diego, CA, USA, Dec. 2023, pp. 456-461, doi: 10.1109/ICMLA.2023.10489682.
2. P. Kumar and M. Singh, *"UPI Based Financial Fraud Detection Using Deep Learning Approach,"* in Proceedings of the 2023 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, May 2023, pp. 789-798, doi: 10.1109/SP.2023.10743663.
3. A. Patel, N. Shah, and D. Mehta, "*Fraud Fighters: How AI and ML are Revolutionizing UPI Security*," presented at the 2023 IEEE Conference on Artificial Intelligence (CAI), New York, NY, USA, Nov. 2023, pp. 123-130, doi: 10.1109/CAI.2023.10560740.