GUARDIAN SHIELD: ADVANCED FRAUD DETECTION

# PROJECT ABSTRACT

This project introduces a comprehensive web application developed using Flask, integrating fraud detection and payment URL safety assessment functionalities. The system includes user registration with Google reCAPTCHA for enhanced security. The user data is stored in an SQLite database with hashed and salted passwords.

Upon registration, users receive a one-time password (OTP) for verification via email. The verification process ensures the legitimacy of user accounts. The application also features a login system with password encryption using bcrypt.

The fraud detection module utilizes an ensemble machine learning model (Random Forest Classifier + Decision Tree Classifier) trained to predict fraudulent activities in financial transactions. Users can upload CSV files containing transaction data, and the system generates predictions for each transaction. Additionally, the application provides visualizations and statistics for a user-friendly interface.

Furthermore, the system incorporates a payment URL safety assessment feature. Users can input a website URL, and the application employs a logistic regression model to assess the safety of the given URL. The results include a safety score and probability values.

The web application adheres to best practices for data security and user authentication. It employs various libraries for data manipulation, machine learning, and visualization, such as Pandas, NumPy, Seaborn, and Scikit-Learn. The inclusion of a Google reCAPTCHA during registration enhances security measures, mitigating the risk of automated attacks.

The project serves as a versatile and robust tool for both financial institutions seeking fraud detection solutions and users concerned about the safety of payment-related websites. Its modular design allows for easy expansion and integration of additional security features.