`

A

Project report on

**FRAUD DETECTION AND PREVENTION SYSTEM**

****

Submitted by (Group 4):

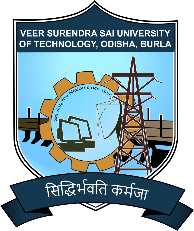
Nikhil Mohanty - 2206151007

Ujjwal Dash - 2002081060

Sambit Behera - 2206151003

Jitu Malik - 2206151010

Bikash Kumar Behera - 2206151019



Veer Surendra Sai University of Technology, Burla

**Project Overview**

In this project, we are tasked with developing a fraud detection and prevention system using machine learning. The primary goal is to differentiate between legitimate and fraudulent transactions. We have chosen to implement logistic regression as the machine learning algorithm for this task and have obtained our dataset from Kaggle. The dataset consists of binary labels, with '0' indicating legitimate transactions and '1' indicating fraudulent transactions. To provide a user-friendly interface for input, we have utilized HTML and CSS to create a user interface.

**Project Steps**

**1. Data Collection**

We collected our dataset from Kaggle, ensuring that it is clean and relevant to our problem.

**2. Exploratory Data Analysis (EDA)**

We conducted an initial exploration of the dataset to gain insights into its characteristics, including statistics, distributions, and feature relationships.

**3. Data Preprocessing**

Data preprocessing tasks such as handling missing values, scaling features, and encoding categorical variables were performed as needed.

**4. Data Splitting**

We divided our dataset into training and testing sets to assess the model's performance on unseen data.

**5. Model Selection**

Logistic regression was chosen as the primary machine learning algorithm due to its suitability for binary classification tasks like fraud detection.

**6. Model Training**

We trained our logistic regression model on the training data, fine-tuning it to achieve optimal performance.

**8. Model Evaluation**

We evaluated the model's performance on the testing dataset using various metrics such as accuracy, precision, recall, F1-score, and ROC-AUC.

**9. Deployment**

The trained model was deployed within an HTML/CSS-based web interface, allowing users to input their transaction information.

**10. User Interaction**

Users can submit transaction details through the interface, and the model provides predictions regarding the legitimacy of the transaction.

**11. Continuous Monitoring**

To ensure ongoing effectiveness, we established a feedback loop to monitor the model's real-world performance and adapt it as needed

**Connection of Frontend with Backend**

Connecting the frontend and backend through MongoDB involves setting up a communication pathway that allows web application's frontend (HTML, CSS) to interact with the backend (typically implemented in a server-side language like Python or Node.js) and access data stored in MongoDB. Below is a step-by-step guide on how to establish this connection.

**Conclusion**

The fraud detection and prevention system, built on logistic regression and a user-friendly HTML/CSS interface, serves as a vital tool in identifying and mitigating fraudulent transactions. It is designed to evolve and adapt to new threats as fraudsters modify their techniques. By adhering to best practices and continuously monitoring its performance, we aim to maintain the system's effectiveness in safeguarding against fraudulent activities.

REFERENCES:

* Dataset 🡪 <https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud>
* Logo 🡪 <https://app.logo.com/dashboard/logo_2c9b3a96-0fb4-43d4-8969-264a18d7a656/your-logo-files>
* Images 🡪 <https://wallpapercave.com/wp/wp9764093.jpg>
* Machine Learning 🡪https://en.wikipedia.org/wiki/Logistic\_regression