

---

## **PROJECT TOPIC: ANOMALY DETECTION IN FRAUDULENT CREDIT TRANSFER**

---

**Group No.:170**

**Project Group Members:**

1. Anish Khandelwal (B-09 / 201500093)
2. Prashant Dhangar (C-42 / 201500503)
3. Vijay Kaushal (F-67 / 201500783)
4. Yash Kumar Gupta (B-72 / 201500820)

**Project Supervisor:** Mr. Vikash Sawan, Assistant Professor

---

**About the Project:** Objective 1: Perform in-depth analysis on the dataset to identify potential fraudulent transactions and distinguish them from legitimate ones.

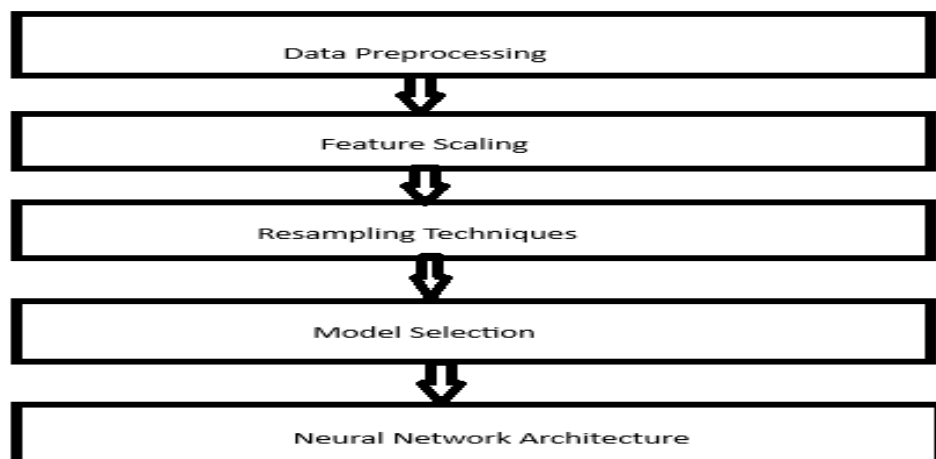
Objective 2: Visualize and compare fraudulent and genuine transactions based on various features.

Objective 3: Implement machine learning models to detect fraudulent activities and evaluate their performance metrics.

Objective 4: Handle class imbalances using sampling techniques or class weights to improve model performance.

**Motivation:** Detecting fraud in credit card transactions is essential for maintaining financial security. The project focuses on analysing the dataset, visualizing transaction patterns, and employing machine learning for effective fraud detection. Key steps include exploring data, handling outliers and missing values through preprocessing, and visualizing to identify crucial features. Machine learning models, tailored for handling class imbalances, play a central role. Iterative model evaluation, updating, and enhancement ensure adaptability to evolving fraud tactics. Emphasis on system security underscores data sensitivity.

**Project Planning:**



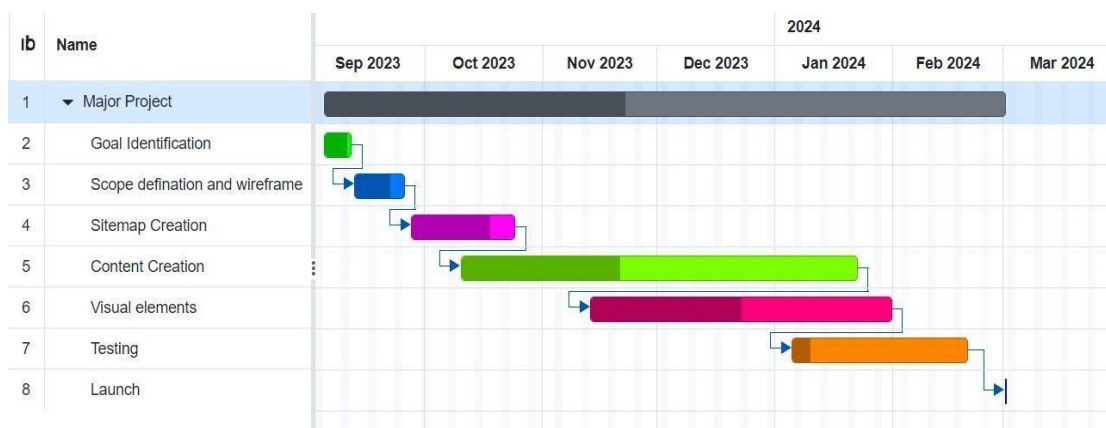
**Data Preprocessing:** The preprocessing phase involved handling missing values and outliers, which significantly improved the quality of the data, making it more suitable for analysis.

**Feature Scaling:** Applying normalization and standardization techniques to the features resulted in enhanced model performance and better convergence during the training process.

**Resampling Techniques:** Using both oversampling and under sampling methods helped in creating a balanced class distribution, preventing the model from being biased towards the majority class.

**Model Selection:** Testing various algorithms such as logistic regression and random forest allowed us to identify the best-performing model that provided the most accurate predictions for fraud detection.

**Neural Network Architecture:** The implementation of a deep learning model with multiple layers enabled the system to learn intricate patterns within the data, leading to highly accurate predictions for fraud detection.



### Tools required:

#### ➤ Hardware Requirements:

1. RAM(4GB)
2. Processor i3 intel
3. Storage (512 GB)

#### ➤ Software Requirements:

1. Operating system (windows 10)
2. Machine learning Libraries: Scikit-learn, TensorFlow, Keras
3. Google Colab/Jupyter Notebook
4. Python Libraries: Pandas, NumPy, Matplotlib, Seaborn

**Signature of Project Supervisor:** \_\_\_\_\_