**Student Name:** Swetha C

**RegisterNumber:** 613023243053

**Institution:** Vivekanandha College of Technology for Women

**Department:** B.Tech Artificial Intelligence and Data Science

**Date of Submission:** 25.04.2025



# ProblemStatement

In today’s digital economy, the exponential rise in online and card-not-present transactions has led to a significant increase in credit card fraud, resulting in billions of dollars in financial losses annually There is a critical need for an intelligent, adaptive, and scalable solution that can accurately detect and prevent fraudulent transactions in real-time without compromising the customer experience. This project aims to develop an AI-powered credit card fraud detection and prevention system that leverages machine learning and data analytics to identify suspicious patterns, mitigate risks, and ensure secure financial transactions for both businesses and consumers.

# 2.Objectives of the Project

# To develop an AI-powered system that can accurately detect and prevent fraudulent credit card transactions in real time.

# To analyze transaction patterns using machine learning algorithms to differentiate between legitimate and suspicious activities.

# To reduce false positives and negatives, ensuring that genuine customer transactions are not wrongly flagged or declined.

# 3.Scope of the Project

# Features to Include:

# Real-time fraud detection

# Behavioral analysis

# Transaction pattern monitoring

# Alert system for suspicious activity

# Machine learning model updates

# Limitations/Constraints:

# False positives/negatives

# Requires large datasets

# Privacy concerns

# High initial setup cost

# Limited by model accuracy

# 4.Data Sources

# Kaggle Credit Card Fraud Detection: Real-world data, highly imbalanced, PCA-transformed features, great for binary classification Task

* **IEEE-CIS Fraud Detection**:Large-scale, rich in features (identity + transaction), ideal for deep learning and feature engineering.
* **PaySim:** Simulated mobile transactions, well-structured, good for behavioral analysis and fraud pattern detection.

**5.High-Level Methodology**

* **Data Collection and Preparation**: A vast amount of historical transaction data is gathered. This data includes legitimate and fraudulent transactions, along with various features like transaction amount, time, location, merchant details, and user behavior.
* **Feature Engineering**: Relevant features that can help distinguish between fraudulent and legitimate transactions are identified and created. This might involve creating new features based on combinations of existing ones or using domain expertise to extract meaningful signals.
* **Model Selection and Training:** Various machine learning and deep learning algorithms are explored and selected based on the characteristics of the data and the specific requirements of the fraud detection system. 1.Supervised Learning 2.Unsupervised Learning 3.Deep Learning 4.Ensemble Learning
* **Model Evaluation and Validation:** The trained model's performance is rigorously evaluated using separate datasets that were not used during training.
* **Real-time Monitoring and Scoring:** Once a satisfactory model is developed, it is deployed into a real-time transaction processing system. As new transactions occur, the model analyzes their features and assigns a risk score indicating the likelihood of fraud.
* **Decision and Action**: Based on the risk score, appropriate actions are taken. Transactions with high-risk scores might be flagged for manual review, require additional authentication from the cardholder, or even be blocked to prevent potential fraud.
* **Continuous Learning and Adaptation**: Fraudsters constantly evolve their techniques, so the AI system must adapt to these changing patterns. This involves continuously monitoring the model's performance, retraining it with new data, and potentially updating the features and algorithms used.
* **Integration with Security Systems**: The AI-powered fraud detection system is often integrated with other security systems and fraud prevention tools to create a comprehensive defense strategy.

**6.ToolsandTechnologies**

## **Programming Language**: Python

## **Notebook/IDE**: Google Colab, VS Code

# Libraries: pandas , numpy, scikit-learn , PyOD , Matplotlib

# 7.TeamMembersandRoles

# Team Leader:

* Indhumathi.E **Project Manager:** Oversees the project timeline and tasks ,Coordinates Communication between Members

**Team Members:**

* Joshika.S **Designer Creative Lead**: Ensure aesthetic consistency , Help with multimedia Elements
* Janani.S **Reasearch Lead:** Gathers and organizes relavent information,Ensures data is accurate and well documented
* Swetha.C **Presenter Lead**: Prepares and delivers presentations ,Handles public speaking or video narration ,Supports writing and editing for clarity

## Jaya.S **Technical Lead:** Handles coding,technical tools,experiment setup,Ensure functionality of Technical ascepts , Seaborn , Plotly