**Project Proposal: AI-Based Credit Card Fraud Detection System**

**Project Title**: Credit Card Fraud Detection Using Machine Learning

**Submitted By**: Aaminah Binte Farooq

**Course**: AI

**Instructor**: Ms Mehak Mazhar

**Submission Date**: March 8, 2025

**1. Project Overview**

* **Project Topic**:  
  This project focuses on building a machine learning-based system to detect fraudulent credit card transactions. It will use a dataset containing labeled transactions (legitimate or fraudulent) and explore various machine learning algorithms, such as Logistic Regression and Random Forest, to predict fraudulent activity.
* **Objective**:  
  The main goal of this project is to develop a robust fraud detection system that can accurately classify transactions as legitimate or fraudulent. The system will be evaluated using various metrics, including accuracy, precision, recall, and AUC (Area Under the Curve), and the aim is to achieve high detection rates while minimizing false positives and negatives.

**2. Game Description**

* **Original Game Background**:  
  Credit card fraud detection is a critical problem in the financial industry. Given the large volume of transactions processed daily, traditional methods of fraud detection (e.g., rule-based systems) are often insufficient. Instead, machine learning models can learn patterns from historical transaction data and identify fraudulent transactions more effectively.
* **Innovations Introduced**:
  + **Dataset Sampling**: To handle the highly imbalanced nature of the dataset (with fraud being <1% of all transactions), the project applies **undersampling** to balance the classes for better training and model performance.
  + **AI Model Development**: This project innovates by integrating both traditional machine learning algorithms (Logistic Regression) and more advanced algorithms (Random Forest) to compare performance and accuracy in fraud detection.
  + **Impact on Complexity**:  
    These innovations will increase the complexity of the project by incorporating class imbalance handling, feature selection, and model comparison for better fraud detection.

**3. AI Approach and Methodology**

* **AI Techniques to be Used**:
  + **Logistic Regression**: A simple yet effective linear model for binary classification (fraud vs. legitimate).
  + **Random Forest Classifier**: A more advanced ensemble learning technique to improve model accuracy and robustness.
  + **Evaluation Metrics**: Precision, Recall, F1-Score, AUC, Confusion Matrix, Accuracy.
  + **Optional**: If time permits, the model can be extended to use reinforcement learning for continuous learning from new fraudulent data.
* **Heuristic Design**:
  + The heuristics will focus on the following:
    - **Transaction Amount**: Fraudulent transactions tend to have higher amounts.
    - **Time Feature**: Temporal analysis could reveal unusual transaction times associated with fraud.
    - **PCA Features**: Since the dataset includes PCA-transformed features, heuristics will focus on outliers in these features as they may indicate fraudulent behavior.
* **Complexity Analysis**:
  + The time complexity of training models like Logistic Regression is relatively low (O(n)), whereas Random Forest can be more time-consuming (O(n \* log(n))).
  + Handling the imbalanced dataset adds complexity, requiring careful evaluation of performance metrics and optimization to minimize false positives and negatives.

**4. Game Rules and Mechanics (Modified to Fit Fraud Detection)**

* **Modified Rules**:
  + **Data Preprocessing**: Transaction data will be cleaned (e.g., handling missing values, scaling features) and balanced through undersampling.
  + **Model Evaluation**: Models will be evaluated on the basis of accuracy, precision, recall, F1-score, and AUC.
  + **Fraud Detection**: Fraud is determined based on the classifier’s output: 0 for legitimate and 1 for fraudulent transactions.
* **Winning Conditions**:  
  The project “wins” when the models can correctly detect fraudulent transactions with minimal false positives or negatives. The success is measured by high precision, recall, and AUC scores, as well as low false alarms in real-world scenarios.
* **Turn Sequence**:
  + Data Collection: Collect and preprocess the dataset.
  + Model Training: Train the models using balanced data.
  + Evaluation: Use metrics to evaluate and compare models.
  + Fine-Tuning: If needed, fine-tune the models for better performance.

**5. Implementation Plan**

* **Programming Language**: Python 3.x
* **Libraries and Tools**:
  + **Pandas**: For data manipulation and analysis.
  + **NumPy**: For numerical computations.
  + **Scikit-learn**: For machine learning algorithms and metrics.
  + **Seaborn/Matplotlib**: For data visualization and evaluation plots.
  + **Jupyter Notebooks**: For interactive development and visualization.
* **Milestones and Timeline**:
  + **Week 1-2**: Data collection, exploration, and preprocessing (handling missing values, balancing dataset).
  + **Week 3-4**: Model training using Logistic Regression and Random Forest classifiers. Start with baseline models.
  + **Week 5-6**: Model evaluation (precision, recall, confusion matrix, AUC) and tuning (hyperparameter optimization if necessary).
  + **Week 7**: Final testing and comparison of models. Prepare visualizations (ROC curves, confusion matrix).
  + **Week 8**: Finalize project, prepare documentation, and write report.

**6. References**

* **Books and Research Papers**:
  + *"Pattern Recognition and Machine Learning"* by Christopher M. Bishop.
  + *"Machine Learning Yearning"* by Andrew Ng.
  + *"Hands-On Machine Learning with Scikit-Learn and TensorFlow"* by Aurélien Géron.
* **Online Resources**:
  + Kaggle: Credit Card Fraud Detection Dataset
  + Scikit-learn Documentation: <https://scikit-learn.org>