**Phase – 2 SUBMISSION**

**TEAM 11**

**CREDIT CARD FRAUD DETECTION**

Designing an innovative credit card fraud detection system involves several steps, from data collection and preprocessing to implementing advanced machine learning algorithms.

**Overview of the complete process:**

Split the dataset into training, validation, and test sets. The training set is used to train the model, the validation set is used for hyper parameter tuning, and the test set is reserved for final evaluation.

Creating an innovative credit card fraud detection system involves a comprehensive process with several key steps:

**1. Data Collection:** Gather historical credit card transaction data, including both legitimate and fraudulent transactions, along with relevant features like transaction amount, location, and time.

**2. Data Preprocessing:** Clean the data by handling missing values and outliers, normalize or scale numeric features, and encode categorical variables into numerical representations.

**3. Feature Engineering:** Create new features to enhance fraud detection, such as aggregating transaction history and identifying anomalies in transaction patterns.

**4. Data Splitting:** Divide the dataset into training, validation, and test sets for model development and evaluation.

**5. Model Selection:** Choose an appropriate machine learning or deep learning model, considering options like logistic regression, decision trees, random forests, support vector machines, or neural networks.

**6. Model Training:** Train the selected model using the training data while addressing class imbalance using techniques like oversampling, under sampling, or synthetic data generation.

**7. Hyper parameter Tuning:** Optimize the model's hyper parameters using the validation dataset to improve performance.

**8. Model Evaluation:** Assess the model's performance on the test dataset using metrics like precision, recall, F1-score, and ROC-AUC.

**9. Threshold Setting:** Determine a classification threshold that balances false positives and false negatives based on business requirements.

**10. Deployment:** Deploy the trained model in the production environment, integrating it with credit card processing systems.

**11. Monitoring and Maintenance:** Continuously monitor model performance, retraining it periodically to adapt to changing fraud patterns.

**12. Alerts and Reporting**: Implement alerting systems for flagged transactions, investigating them manually or automatically.

**13. Feedback Loop:** Establish a feedback loop between the fraud detection system and the fraud investigation team to improve accuracy.

**14. Documentation and Compliance**: Thoroughly document the process, ensuring compliance with data privacy regulations and security standards.

**15. Scalability**: Design the system to scale with transaction volume growth and evolving fraud tactics.