

The background image shows a person wearing a dark hoodie, sitting at a desk and using a laptop. The person's face is obscured by a black silhouette. The background is filled with various terms related to cyber security and fraud, such as 'IDENTITY THEFT', 'PHISHING', 'CODE', 'INTRUDER', 'HACKER', 'VIRUS', 'FRAUD', 'SPYWARE', 'PASSWORD', and 'M'. There are also some numbers and binary code scattered around. The overall color scheme is dark with greenish-yellow highlights.

CREDIT CARD FRAUD DETECTION

DATA SCIENCE PROJECT-FRAUD DETECTION
PHASE 1

TEAM MEMBERS:

ABINAYA.R

ANBARASI.S

BHUVANA SURUTHI.K

GAYATHRI.M

PROBLEM DEFINITION:

Credit card fraud is a significant issue in the financial industry, costing billions of dollars annually. Detecting fraudulent transactions is crucial to mitigate financial losses and protect consumers. This paper presents a comprehensive module for credit card fraud detection using machine learning and data analytics techniques. The module encompasses data preprocessing, feature engineering, model training, and real-time transaction monitoring. By leveraging historical transaction data and advanced algorithms, our module can effectively identify and prevent fraudulent activities, enhancing the security of credit card transactions.

DESIGN THINKING:

1. DATA PREPROCESSING:

- Data cleaning: Removing duplicates, handling missing values.

- Data transformation: Scaling and normalization.

- Feature selection: Identifying relevant features for fraud detection.

- Handling imbalanced data: Resampling techniques.

2.FEATURE ENGINEERING:

Creating new features: Combining existing ones or extracting meaningful information.

Dimensionality reduction: Reducing the number of features while preserving information.

3.MODEL TRAINING:

Supervised learning: Using labeled data to train models (e.g., logistic regression, decision trees, random forests).

Unsupervised learning: Employing anomaly detection algorithms (e.g., Isolation Forest, One-Class SVM) for detecting unusual patterns.

Ensemble methods: Combining multiple models for improved accuracy.

4.EVALUATION:

Metrics: Using appropriate metrics (e.g., precision, recall, F1-score, ROC AUC) to assess model performance.

Cross-validation: Ensuring model robustness and generalization.

5.REAL-TIME TRANSACTION MONITORING:

Deploying the trained model in a real-time environment.Continuously monitoring incoming transactions for potential fraud.

6.ALERTING MECHANISM: Notifying relevant stakeholders when suspicious activity is detected.

MODEL UPDATES:

Periodically retraining the model to adapt to evolving fraud patterns.Incorporating new data and feedback from fraud analysts.

DEPLOYMENT:

Integrating the fraud detection module into existing banking systems.Ensuring scalability and low latency for real-time processing.By implementing this module, financial institutions can enhance their ability to detect and prevent credit card fraud, safeguarding the interests of both customers and the institution itself.