DEPARTMENT OF APEX INSTITUTE OF TECHNOLOGY

PROJECTPROPOSAL

1. Project Title: -

Online Payment Fraud Detection

2. Project Scope: - (Max 500 words)

The objective of this project is to develop a robust and scalable solution to detect and mitigate fraudulent activities in online payment systems. The system will leverage advanced technologies, including machine learning algorithms, data analytics, and real-time monitoring, to enhance transaction security and protect users from fraud

Data Collection:

Data is the foundation for any fraud detection system. The following sources and types of data will be collected:

a. Transaction Data:

Attributes: Transaction ID, amount, currency, timestamp, location, payment method (credit card, e-wallet, etc.), and merchant details.

Sources: Payment processors, banks, e-commerce platforms, and financial institutions.

b. User Data:

Attributes: Customer ID, account age, transaction history, device ID, IP address, and geolocation.

Sources: Customer databases, application logs, and user profiles.

c. Behavioural Data:

Attributes: Clickstream data, session duration, login frequency, and browsing patterns.

Sources: Website or app analytics tools and behavioural tracking software.

d. Fraud Labels (if available):

Historical data of confirmed fraudulent and non-fraudulent transactions. This is essential for supervised learning models.

Fraud Detection Algorithms:

Fraud detection involves identifying suspicious patterns and anomalies in transaction data using a combination of machine learning models, statistical techniques, and rule-based systems. The choice of algorithm depends on the complexity of the fraud, the availability of label data, and the need for real-time detection

Real-Time Detection and Alerts :

The goal of this project is to design and implement a real-time detection and alert system to identify and mitigate fraudulent activities in online payment systems.
The solution will use advanced algorithms, data processing tools, and notification mechanisms to ensure timely and effective responses to potential threats.

Data Management:

Real-Time Data Ingestion and Processing:

Develop a pipeline to collect transaction data streams from payment gateways, user devices, and backend systems.

Leverage real-time data streaming technologies like Apache Kafka, Apache Flink, or AWS Kinesis for continuous data ingestion and processing.

Ensure data preprocessing (e.g., normalization, transformation) happens in real time.

2. Fraud Detection Engine:

Deploy machine learning models (e.g., Random Forests, Isolation Forests, or Neural Networks) optimized for low-latency detection.

Implement rule-based systems for identifying known fraud scenarios, such as unusual transaction amounts or high-frequency transactions.

Incorporate anomaly detection techniques to flag deviations from a user's normal behaviour

3. Alert Management System:

Develop an alerting mechanism to notify relevant stakeholders (users, administrators) about suspicious transactions.

Support multiple notification channels, including SMS, email, and push notifications.

Prioritize and categorize alerts based on the severity of the threat.

3. Requirements: -

- Software Requirements
  1. Development Tools and IDEs
  2 Real-Time Data Streaming and Processing Tools
  3. Machine Learning and Data Processing
  4. Database Management
  5. Monitoring and Logging

- Hardware Requirements

  NA

STUDENTS DETAILS

Name	UID	Signature
ANKIT KUMAR	21BCS10065	
ADITYA KUMAR	21BCS10345	
GAURANG ADLAKHA	21BCS6204	
UTKARSH PATHAK	21BCS6158	

APPROVAL AND AUTHORITY TO PROCEED

We approve the project as described above, and authorize the team to proceed.

Name	Title	Signature (With Date)
Ramanjot Kaur		