Project Planning Phase-II

Technology Stack (Architecture & Stack)

Date	27 October 2023
Team ID	Team-593390
Project Name	Online Payments Fraud Detection Using ML
Maximum Marks	5 Marks

Technical Architecture :

The technical architecture for online payment fraud detection through machine learning encompasses a comprehensive system that covers data ingestion, preprocessing, model development, training, deployment, real-time data processing, model monitoring, a decision engine, alerting mechanisms, feedback loops, security provisions, scalability measures, integration capabilities, compliance adherence, and an ongoing commitment to continuous improvement. This architecture is designed to effectively identify and thwart fraudulent transactions while ensuring the utmost data security and compliance with regulatory standards. It achieves these objectives by harnessing the power of machine learning models, real-time data streams, and automated decision-making processes..

Online Payment Fraud Detection Using ML

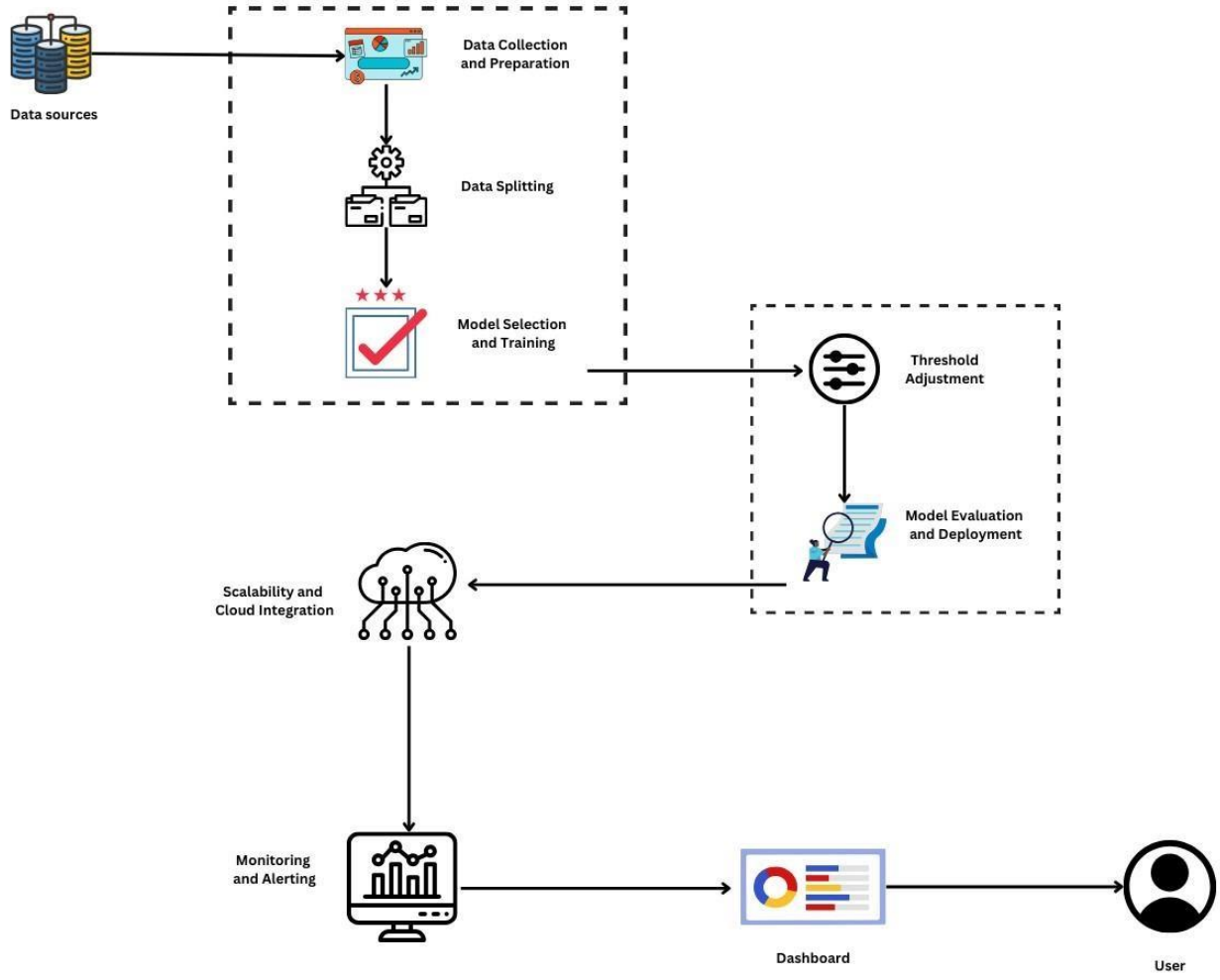

Table-1 : Components & Technologies :

S.No	Component	Description	Technology
1.	User Interface	Creating a user-friendly and effective user interface (UI) for online payments fraud detection system is crucial for ensuring that users can easily interact with and make sense of the application.	HTML, CSS, JavaScript, BootStrap
2.	Database	Database contains Transaction, User information and Logs table. With a range of primary and foreign keys to associate each table with all attributes.	SQL, NO-SQL
3.	Application Logic-1	Logic for a process in the application	Python
4.	Application Logic-2	Application logic may maintain the state of the application, including user sessions, context, and data persistence.	Python
5.	Verification Process	Logic for a process in the application	Bank Information
6.	Cloud Database	Database Service on Cloud	IBM, IBM Cloudant etc.
7.	Machine Learning Model	The purpose of a machine learning (ML) model is to make predictions or decisions based on data. ML models are designed to automatically learn patterns and relationships within a dataset and use that knowledge to make informed predictions or decisions without being explicitly programmed.	Classification Model
8.	Infrastructure (Server / Cloud)	Application Deployment on Local System / Cloud Local Server Configuration Cloud Server Configuration	Local, Cloud Foundry, Kubernetes, etc.

Table-2: Application Characteristics :

S.No	Characteristics	Description	Technology
1.	Open-Source Frameworks	Open-source machine learning and data science frameworks to streamline your development and model-building process. These frameworks provide a wide range of tools, libraries, and resources to help you work efficiently and effectively.	Python, Pandas, Numpy, XGBoost
2.	Security Implementations	Implement strong user authentication methods such as multi-factor authentication (MFA) to ensure that only authorized users can access accounts and perform transactions. Enforce role-based access control (RBAC) to restrict access to sensitive systems and data to authorized personnel only.	User Authentication and Authorization
3.	Scalable Architecture	Consider using cloud services like AWS, Azure, or Google Cloud for scalability and elasticity, allowing you to adapt to varying workloads.	Google Cloud, AWS, Flask
4.	Availability	Justify the availability of application (e.g. use of load balancers, distributed servers etc.)	Amazon RDS (Relational Database Service) and Google Cloud SQL
5.	Performance	Good performance in online fraud detection requires a combination of advanced technologies, effective machine learning models, and robust processes for continuous improvement. Regular testing, optimization, and adaptation to evolving fraud patterns are key to maintaining high performance levels.	Caching mechanisms to store frequently accessed data and reduce response times, Optimizing machine learning model performance for real-time classification.