Project Design Phase-II
Technology Stack (Architecture & Stack)

Date	28th November 2023
Team ID	Team-591971
Project Name	Project - Online Payments Fraud Detection using ML
Maximum Marks	4 Marks

Technical Architecture:

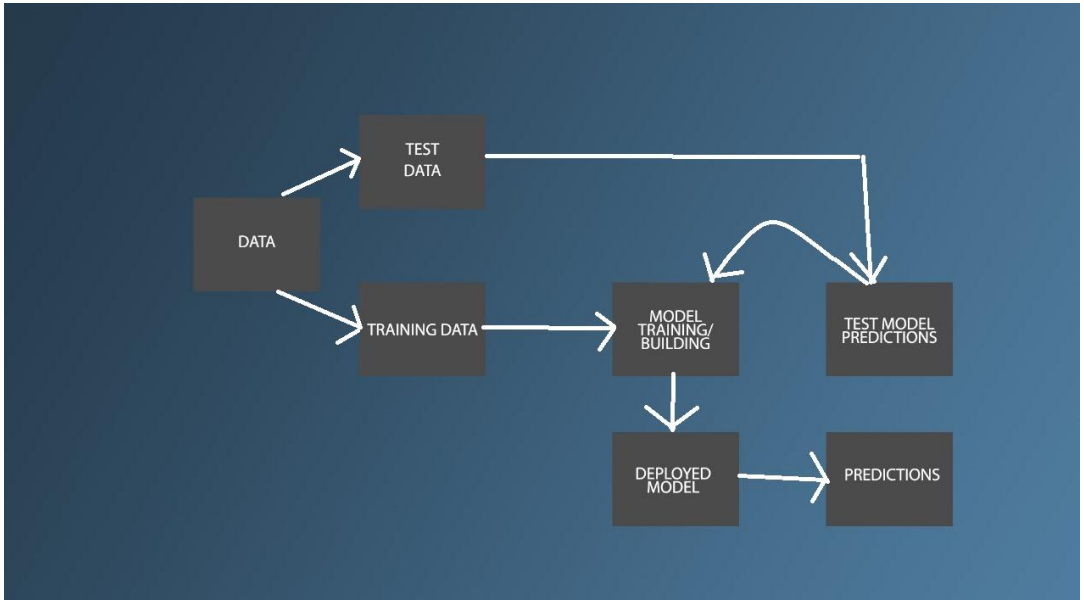

Table-1 : Components & Technologies:

S.No	Component	Description	Technology
1.	User Interface	How user interacts with application e.g. Web UI, Mobile App, Chatbot etc.	HTML, CSS, JavaScript / Angular Js / React Js etc.
2.	Application Logic-1	Logic for a process in the application	Java / Python
3.	Data Collection and Aggregation	Collects data from various sources such as transactions, user behavior, device fingerprints, and more. Aggregates this data for analysis.	APIs, data scraping tools, data lakes, and databases for storage and retrieval.
4.	Machine Learning Models	Algorithms trained to detect patterns of fraudulent behavior based on historical data.	Supervised and unsupervised machine learning algorithms like Random Forest, Logistic Regression, Neural Networks, and clustering

			algorithms.
5.	Behavioral Analytics	Monitors and analyzes user behavior in real-time to detect anomalies or deviations from normal patterns.	Statistical analysis tools, anomaly detection algorithms, and user profiling techniques.
6.	Rules Engine	Implements predefined rules or logic to flag specific behaviors or transactions as potentially fraudulent.	Decision trees, rule-based systems, and scripting languages for defining and executing rules.
7.	Device Fingerprinting	Captures unique device identifiers and characteristics to recognize devices associated with fraudulent activities.	Device ID tracking, browser fingerprinting, and IP geolocation techniques.
8.	Real-time Monitoring and Alerting	Constantly monitors transactions and activities to promptly flag and respond to potential fraud.	Real-time processing systems, event-driven architectures, and alert/notification mechanisms.
9.	Integration and APIs	Enables seamless integration with various systems, databases, and third-party services for enriched data analysis.	RESTful APIs, webhooks, and middleware for connecting different systems.
10.	Machine Learning Model	Purpose of Machine Learning Model	Object Recognition Model, etc.
11.	Dashboard and Reporting	Provides visualizations and reports for insights into fraudulent activities and system performance.	Data visualization tools, reporting frameworks, and dashboard creation platforms.

Table-2: Application Characteristics:

S.No	Characteristics	Description	Technology
1.	Immediate analysis and decision-making on incoming data	Processes transactions or user interactions instantly to flag potential fraud in real-time.	Stream processing frameworks like Apache Kafka or Apache Flink, in-memory databases, and low-latency computing.
2.	Ability to handle increased data volume without compromising performance.	Systems should accommodate growing data streams and user interactions without slowdowns.	Cloud computing, containerization (e.g., Docker, Kubernetes), and scalable database solutions like Cassandra or MongoDB.
3.	Systems that adapt and evolve to new fraud patterns.	Machine learning models that continuously learn from new data to refine detection capabilities.	Reinforcement learning, online learning algorithms, and adaptive model training pipelines.

S.No	Characteristics	Description	Technology
4.	Protection of sensitive data and secure communication channels.	Ensures encryption of data both at rest and in transit to prevent unauthorized access or tampering.	SSL/TLS encryption, secure hashing algorithms (e.g., SHA-256), and cryptographic protocols.
5.	Tailoring the system to specific business needs and fraud types.	Configurable parameters and adaptable rules to fit different fraud scenarios.	Configuration management systems, customizable rule engines, and flexible machine learning frameworks.