Project Design Phase-I
Solution Architecture

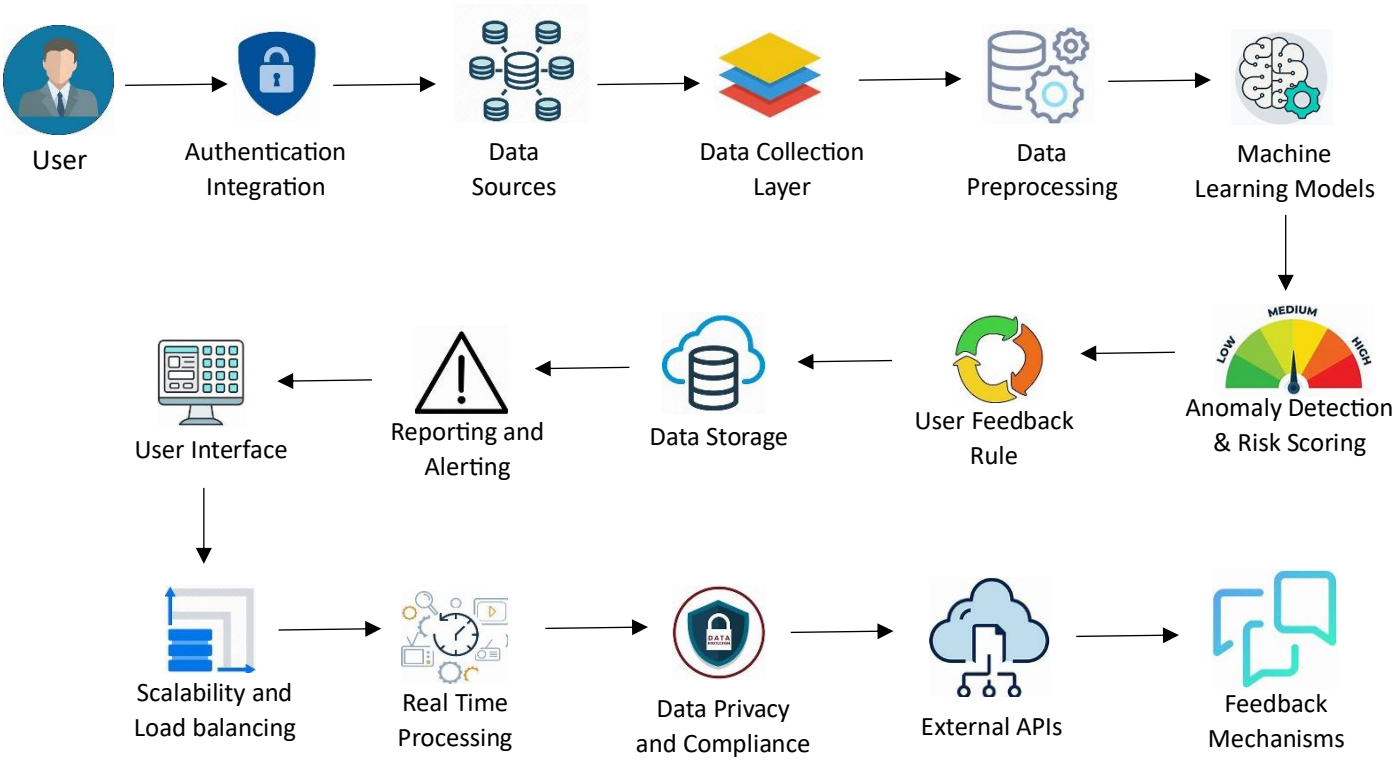
Date	19 September 2022
Team ID	Team 7.5
Project Name	Develop an AI system that verifies user identities based on their online behavior patterns, adding an extra layer of security
Maximum Marks	4 Marks

Solution Architecture:

Solution architecture is a complex process – with many sub-processes – that bridges the gap between business problems and technology solutions. Its goals are to:

- Find the best tech solution to solve existing business problems.
- Describe the structure, characteristics, behavior, and other aspects of the software to project stakeholders.
- Define features, development phases, and solution requirements.
- Provide specifications according to which the solution is defined, managed, and delivered.

Solution Architecture Diagram:



Project Overview:

The objective of this project is to enhance security by using AI to verify user identities based on their online behaviour patterns. This system will analyse user actions, habits, and interactions to detect anomalies and ensure that only legitimate users gain access.

I. Solution Structure and Characteristics:

1. Data Collection:

- The system will gather data from various sources, including user interactions with websites, applications, and devices.
- Data will include user behaviour, such as keystrokes, mouse movements, navigation patterns, login history, and device information.

2. Data Preprocessing:

- Clean, transform, and normalize the collected data for analysis.
- Convert data into a suitable format for machine learning.

3. Machine Learning Models:

- Develop AI models to analyze user behavior patterns.
- Utilize supervised and unsupervised learning techniques, such as anomaly detection and pattern recognition.
- Train models on historical user data and legitimate behavior.

4. Anomaly Detection:

- Implement anomaly detection algorithms to identify suspicious activities.
- Classify behavior as normal or abnormal based on deviation from established patterns.

5. Risk Scoring:

- Assign risk scores to user actions based on the level of deviation from normal behavior.
- Higher risk scores trigger additional security measures.

6. Authentication Integration:

- Integrate the AI system with the existing authentication process.
- Implement multi-factor authentication (MFA) for high-risk activities.

7. User Feedback Loop:

- Create a feedback loop to continuously improve the system by learning from false positives and negatives.

II. Development Phases:

Phase 1 - Requirements Gathering:

- Define the specific needs of the organization.
- Identify data sources and integration points.
- Determine performance and security requirements.

Phase 2 - Data Collection and Storage:

- Set up data collection mechanisms.
- Create data storage infrastructure for collected user behavior data.

Phase 3 - Data Preprocessing:

- Develop data preprocessing pipelines.
- Ensure data quality and consistency.

Phase 4 - Machine Learning Model Development:

- Build and train machine learning models.
- Fine-tune models based on initial results.

Phase 5 - Anomaly Detection and Risk Scoring:

- Implements anomaly detection algorithms.
- Develops a risk scoring system.

Phase 6 - Integration and Testing:

- Integrates the AI system into the existing authentication process.

- Conducts extensive testing and validation.

Phase 7 - User Feedback and Improvement:

- Implements feedback mechanisms.
- Continuously monitors and enhances the system's accuracy.

III. Solution Requirements:

1. Data Privacy:

- Ensures compliance with data privacy regulations.
- Anonymizes and protects user data.

2. Scalability:

- Ensures the system can handle a growing number of users and data.
- Load balancing distributes incoming data and requests to maintain performance.

3. Real-time Processing:

- Provides real-time analysis for immediate threat detection.
- Critical for timely security responses.

4. Flexibility:

- The system is made adaptable to changing user behavior patterns.

5. Reporting and Alerting:

- Generates reports and alerts for security administrators.
- Alerts can be sent via various communication channels.

6. User-Friendly:

- Provides user interfaces for system administrators and end-users.
- Administrators can configure the system and review reports.

V. Project Stakeholders:

- IT teams, security teams, legal compliance, and end-users.
- Management and Executives, External service providers, Project team, Finance Team, User support team