

Project Design Phase-I

Solution Architecture

Date	26 october 2023
Team ID	8.1
Project Name	System that uses AI for real-time data classification, leak detection, and prevention to enhance data security.
Maximum Marks	4 Marks

Solution Architecture:

Goals:

- Find the best technology solution to enhance data security.
- Describe the system's structure, behavior, and features to stakeholders.
- Define development phases and requirements.
- Provide specifications for system definition, management, and delivery.

Components:

1. **Data Ingestion and Preprocessing:**
 - Data sources (databases, file systems, network traffic).
 - Data preprocessing modules.
2. **Data Classification:**
 - Machine learning models.
 - Labeled data for model training.
3. **Real-time Data Classification:**
 - Real-time processing modules.
 - Streaming or event-based data handling.
4. **Anomaly Detection and Leak Prevention:**
 - Anomaly detection algorithms.
 - Preventive measures (access controls, encryption, data masking).
5. **Alerting and Monitoring:**
 - Alerting mechanisms.
 - Dashboards for system monitoring.
6. **Incident Response and Investigation:**
 - Automated incident response modules.
 - Forensic analysis tools.
7. **Feedback Loop and Model Improvement:**
 - Feedback collection mechanisms.
 - Automated model retraining.
8. **Integration with Existing Security Infrastructure:**
 - Integration with firewalls, SIEM systems, and DLP solutions.
9. **User Access Controls and Authentication:**
 - User authentication and access control modules.
 - Multi-factor authentication.
10. **Compliance and Reporting:**
 - Compliance reporting tools.
 - Data compliance checks.

Scalability and Performance:

- Scalable architecture to handle large data volumes.
- High-performance computing resources.

Documentation and Training:

- Comprehensive documentation for administrators and users.
- Training resources for effective system use and maintenance.

This architecture outlines the key components and their interactions in the AI-based data security system, aligning technology solutions to enhance data security and provide a framework for defining, managing, and delivering the system.