Software Requirements Specification (SRS)

Phishing Detection and Automated Mitigation System

1. Purpose

The purpose of this project is to design and implement a Phishing Detection and Automated Mitigation System that can securely analyze email content, identify phishing attempts, and automatically apply suitable mitigation actions without requiring manual intervention.

The system is intended to demonstrate how modern security platforms use automation, containerization, and secure API-based integrations to protect users from phishing attacks. Instead of focusing on complex algorithms, this project emphasizes strong system architecture, secure design principles, and automated security workflows that are commonly used in real-world environments.

2. Functional Requirements

2.1 User Authentication

- The system shall allow users to create an account through a secure signup process.
- The system shall allow registered users to log in using authenticated credentials.
- The system shall manage user sessions using secure, token-based authentication mechanisms.

2.2 Email Account Integration

- The system shall provide users with the option to connect their email account to the platform.
- The system shall use OAuth 2.0 to request permission for accessing email data.
- The system shall never request, store, or process user email passwords.
- The system shall securely store OAuth access and refresh tokens in an encrypted format.

2.3 Email Retrieval

- The system shall retrieve emails from the connected inbox using the Gmail API.
- The system shall extract relevant email components such as sender information, subject, body content, and embedded links.
- The system shall support both periodic and on-demand email scanning.

2.4 Phishing Detection

- The system shall analyze email content to identify phishing-related indicators.
- The system shall calculate a phishing risk score based on predefined detection rules.
- The system shall classify emails into one of the following categories: Safe, Suspicious, or Phishing.
- The system shall record all indicators and rules used during the detection process for transparency and audit purposes.

2.5 Automated Mitigation

- The system shall automatically apply mitigation actions based on the classification result.
- The system shall quarantine or isolate emails identified as phishing.
- The system shall block malicious senders or URLs when applicable.
- The system shall notify users or system administrators when phishing threats are detected.
- The system shall support rollback or reversal of mitigation actions in cases of false positives.

2.6 Logging and Reporting

- The system shall log all phishing detection and mitigation activities.
- The system shall maintain detailed audit logs for security monitoring and review.
- The system shall allow administrators to view and review historical phishing incidents.

---

3. Non-Functional Requirements

3.1 Performance Requirements

- The system shall analyze emails within a reasonable time frame without causing noticeable delays to users.
- The system shall support multiple users simultaneously without significant performance degradation.

3.2 Security Requirements

- The system shall not store any plaintext credentials.
- The system shall encrypt sensitive data stored in the database.
- The system shall process untrusted email content only within isolated Docker containers.
- The system shall enforce proper access control for administrative and sensitive operations.

3.3 Reliability and Availability

- The system shall ensure that incomplete jobs or orphaned containers are not left running.
- The system shall maintain consistency between the system’s internal state and actual execution results.

3.4 Scalability

- The system shall support horizontal scaling of email analysis workers.
- The system shall allow new phishing detection rules to be added without requiring major architectural changes.