ABBOTTABAD UNIVERSITY OF SCIENCE AND TECHNOLOGY

SOFTWARE REQUIREMENTS SPECIFICATION

(SRS DOCUMENT)

Data encryption in database

Version 1.0

BY

Name : Rizwan Ali

Section : BSCS - 3D

Teacher : Sir Jamal Abdul Ahad

Subject : DSA

Signature :

Table of Contents

1. Introduction

1.1 Purpose

The purpose of this system is to securely handle user data during the signup process, ensuring that sensitive information (such as passwords, email addresses, and other personal details) is encrypted before it is stored in the database. This is to ensure data privacy and compliance with security standards.

1.2 Document Conventions

This document follows standard SRS formatting, with sections describing functional and non-functional requirements, including security and performance considerations.

1.3 Project Scope

- The project involves the following:
- Fetching data from a web signup page (e.g., user name, email, password, etc.)
- Encrypting sensitive data using strong encryption algorithms
- Storing the encrypted data securely in the database

1.4 References

- AES Encryption Standard
- OWASP Security Guidelines
- Web Application Security Best Practices

2. Overall Description

2.1 Product Perspective

The system is a component of a web-based application where users can register by providing their personal data. The system will encrypt sensitive data before storing it in the database.

2.2 User Classes and Characteristics

- End Users: Individuals who are registering on the website (new users).
- Admin Users: Users who have permission to manage and view the stored data (e.g., user support or system administrators).

2.3 Operating Environment

- Web-based application (browser)
- Server-side technology: PHP/Node.js/Python, etc.
- Database: MySQL, MongoDB, or any other relational database.

2.4 Design and Implementation Constraints

- The system must comply with industry security standards (e.g., AES-256 encryption, SSL/TLS for data transmission).
- The user data will be stored in an encrypted format to ensure privacy.
-

2.5 Assumptions and Dependencies

- The application will be connected to the internet, with no disruptions to the network.
- The database server supports encrypted data storage.
- The encryption keys will be stored securely using a key management system.

3. System Features

3.1 Data Collection and Validation

- The system shall collect user data from a signup form (e.g., username, email, password, phone number).
- Input validation will be performed on the user data to ensure correctness (e.g., valid email format, strong password checks).

3.2 Data Encryption

- Encryption Algorithm: AES-256 encryption will be used to encrypt sensitive data (passwords, personal details) before storing it in the database.
- Encryption Process: The system will encrypt user data on the server-side before saving it in the database.
- The encryption will be done using a secure key, and a unique encryption key will be generated for each user.

3.3 Data Storage

- The encrypted user data will be stored in the database.
- The database will store the encrypted password and any other sensitive information.
- Data will be stored securely, and only encrypted information will be persisted (no plain-text data).

3.4 User Authentication

The system will authenticate users based on encrypted credentials during login. The user’s inputted password will be compared against the encrypted password in the database.

4. External Interface Requirements

4.1 User Interfaces

- Signup Page: The UI will consist of standard fields such as username, password, email, and phone number.
- Error Messages: Display appropriate error messages for invalid input (e.g., weak password, invalid email format).

4.2 Software Interfaces

- Web Framework: The system will interact with the chosen web framework (e.g., Django, Express, Flask).
- Encryption Library: The system will use an encryption library (e.g., PyCryptodome, OpenSSL) to perform AES encryption.

4.3 Hardware Interfaces

The system should be compatible with standard server environments (e.g., AWS, Apache, Nginx).

5. Quality Attributes

5.1 Security

- The system will use AES-256 encryption to ensure data privacy and security.
- Passwords and other sensitive data will never be stored in plain text.
- Secure transmission protocols (e.g., TLS/SSL) will be used for data in transit.

5.2 Performance

- The encryption and decryption processes should not affect the performance of the system.
- The system should be optimized to handle multiple signup requests concurrently.

5.3 Usability

- The signup process should be straightforward and user-friendly.
- The user should be informed of any validation errors promptly.

5.4 Reliability

- The system will ensure that data is securely encrypted before being stored in the database.
- The system will ensure data consistency, with no loss during the encryption or storage process.

6. Appendices

B: Analysis Model

This section can include a detailed model of how the data encryption will work, flow diagrams, and any relevant data models.