Software Requirements Specification

Secure Academic File Access Tracker

Prepared by : **SUBIKSHA S K**

1. INTRODUCTION

1.1 Purpose

This document describes the software requirements for the Secure Academic File Access Tracker, a system developed for educational institutions such as colleges and universities. The main objective of this system is to secure academic documents, control access based on user roles, and monitor all file access activities. By doing so, the system ensures data confidentiality, accountability, and transparency in academic file management.

1.2 Scope

- The Secure Academic File Access Tracker is a web-based application that enables secure storage and controlled access to academic files, including notes, question papers, project reports, and certificates.
- The system provides role-based access for Admin, Staff, and Students, allowing only authorized users to view or download files.
- It maintains a comprehensive audit log that records details such as the user who accessed a file, the action performed, and the date and time of access.
- An administrative dashboard is also provided to help monitor users, files, and overall access activities efficiently.

1.3 Definitions, Acronyms, and Abbreviations

- **SRS** – Software Requirements Specification
- **RBAC** – Role-Based Access Control
- **Admin** – System administrator
- **Audit Log** – Record of file access activities
- **UI** – User Interface

2. OVERALL DESCRIPTION

2.1 Product Perspective

The Secure Academic File Access Tracker is a web-based system designed to replace traditional manual or unsecured methods of sharing academic files.
It follows a client–server architecture with a centralized database that securely stores user information, academic files, and access logs.

2.2 User Classes

- **Admin** – Responsible for managing users, roles, academic files, and access logs
- **Staff** – Uploads and manages academic files
- **Student** – Views and downloads authorized academic files

2.3 Operating Environment

- Web browsers such as Chrome, Edge, and Firefox
- Server-based backend application
- Centralized relational database
- Secure server-side file storage

3. SYSTEM WORKFLOW

- Students register or log in to the system, after which their role is verified. Once authenticated, students can view and download permitted academic files, and each access is recorded in the audit log.
- Staff members log in to upload academic files, manage access permissions, and review student access reports.
- Administrators log in to manage users and roles, monitor files, review complete access logs, and generate reports.

4. FUNCTIONAL REQUIREMENTS

4.1 Student Module

- Log in using registered credentials
- View a list of authorized academic files

- Download permitted files
- Log out securely

4.2 Staff Module

- Log in using staff credentials
- Upload academic files
- Update or remove uploaded files
- Control file visibility for students
- View file access statistics

4.3 Admin Module

- Log in using administrator credentials
- Create, edit, and delete user accounts
- Assign and manage user roles
- View all uploaded academic files
- Monitor and analyze access logs
- Generate access and usage reports

5. NON-FUNCTIONAL REQUIREMENTS

5.1 Security

- Passwords must be stored in encrypted form
- Role-based access control must be strictly enforced
- Unauthorized access must be prevented

5.2 Performance

- File access requests should be processed efficiently
- The system should support multiple users simultaneously

5.3 Usability

- The interface should be simple and user-friendly
- Easy navigation across all modules
- Responsive design for different devices

5.4 Reliability

- Data integrity must be maintained at all times
- Audit logs must be accurate and tamper-proof
- Backup and recovery mechanisms should be supported

6. FUTURE ENHANCEMENTS

- File encryption for improved security
- OTP-based or multi-factor authentication
- Alerts for suspicious access activities
- Graphical dashboards for access analytics

7. CONCLUSION

The Secure Academic File Access Tracker offers a secure, scalable, and efficient solution for managing academic files with complete access traceability.

By preventing unauthorized access and maintaining detailed audit logs, the system enhances data security and accountability, making it well-suited for academic institutions.