Project Synopsis

Secure Web-Based Organ Donation Management System

Project Overview

This project aims to develop a web-based application for hospitals to manage organ donations and requests in a secure, transparent, and efficient manner. The platform will allow individuals to register as organ donors and patients in need to request organs. A core feature of the system will be secure storage and controlled access to sensitive documents such as death certificates and medical records, ensuring only authorized hospital administrators can access them using secure methods such as OTP-based access.

Objectives

- Facilitate easy registration for organ donors and patients in need.
- Maintain a waiting list for requested organs.
- Allow uploading of death certificates to initiate the donation process.
- Automatically notify hospital admins when a potential organ is available.
- Enable document storage with strict access control mechanisms (OTP or time-bound access).
- Ensure the security and privacy of all user data and uploaded documents.

Key Features

1. Donor Registration Form:
   - Personal information, organs willing to donate, consent checkbox, and ID upload.

2. Recipient Registration Form:
   - Personal and medical details, required organ, contact info, and automatic addition to waiting list.

3. Death Certificate Upload:

- Triggered upload by authorized person, secure storage, and admin notification.

4. Notification System:

- Admin is alerted about donor availability; patients are notified for matching organs.

5. Secure Document Storage:

- Encrypted document storage, admin-only access with OTP or time-limited secure links.

6. Admin Dashboard:

- Full control to manage lists, approve matches, track access, and manage files securely.

Technology Stack

- Frontend: HTML, CSS, JavaScript (React or Angular)
- Backend: Node.js / Python (Flask or Django)
- Database: MySQL / MongoDB
- File Storage: AWS S3 / Firebase Storage (with encryption)
- Authentication: JWT + OTP (Email/SMS)
- Notifications: Email API (SendGrid/SMTP)
- Security: HTTPS, Encrypted file storage, Role-based access control

Security Focus

- End-to-end encryption of documents.
- Role-based access (admin vs public users).
- OTP-based temporary access for document viewing.

- Use of signed URLs for time-limited access.

- Secure storage and logging of data access activities.

Expected Outcome

The proposed system will streamline the organ donation and request process while ensuring the highest level of security for sensitive documents. It will improve coordination between donors, patients, and hospitals, ultimately saving lives and building trust in the donation system.