# SMART PATIENT DATA SECURITY SYSTEM

**A SOCIALLY RELEVANT MINI PROJECT REPORT**

***Submitted by***

**UVASHREE S [211423104709]**

**VAISHALI S [211423104710]**

***in partial fulfillment for the award of the degree***

***of***

**BACHELOR OF ENGINEERING**

**in**

**COMPUTER SCIENCE AND ENGINEERING**

****

**PANIMALAR ENGINEERING COLLEGE**

**(An Autonomous Institution, Affiliated to Anna University, Chennai)**

**OCTOBER 2025**

**BONAFIDE CERTIFICATE**

Certified that this project report **“SMART PATIENT DATA SECURITY SYSTEM”** is the bonafide work of **UVASHREE S (211423104709), VAISHALI S (211423104710)** who carried out the project work under my supervision.

**Signature of the HOD Signature of the Supervisor**

**Dr L. JABASHEELA, M.E., Ph.D., Mrs. SHARMILA S M.E.[Ph.D.,]**

PROFESSOR AND HEAD, ASSISTANT PROFESSOR,

Department of CSE Department of CSE

Panimalar Engineering College, Panimalar Engineering College, Chennai – 600 123 Chennai – 600 123

Submitted for 23CS1512 – Socially Relevant Mini Project Viva-Voce Examination held on...........................

**INTERNAL EXAMINER EXTERNAL EXAMINER**

**DECLARATION BY THE STUDENT**

We **UVASHREE S [211423104709], VAISHALI S [211423104710]** , hereby declare that this project report titled "**SMART PATIENT DATA SECURITY SYSTEM**", under the guidance of **Mrs. Sharmila M.E.[Ph.D.,],** is the work done by us and we have not plagiarized or submitted to any other degree in any university by us.

**SIGNATURE OF THE STUDENTS**

**UVASHREE.S [211420104709]**

**VAISHALI.S [211420104710]**

**ACKNOWLEDGEMENT**

We express our deep gratitude to our respected **Secretary and Correspondent Dr.P.CHINNADURAI, M.A., Ph.D.,** for his kind words and enthusiastic motivation, which inspired us a lot in completing this project.

We express our sincere thanks to our **Directors Tmt. C. VIJAYARAJESWARI, Dr.C.SAKTHIKUMAR,M.E., Ph.D., and Dr. SARANYASREE SAKTHIKUMAR**

**B.E.,M.B.A.,Ph.D.,** for providing us with the necessary facilities for completion of this

project.

We also express our gratitude to our Principal **Dr.K.MANI, M.E., Ph.D.,** for his timelyconcern and encouragement provided to us throughout the course.

We thank the HOD of CSE Department, **Dr.L.JABASHEELA, M.E., Ph.D.,** for the support extended throughout the project.

We would like to thank our Project Coordinator **Dr.V.SUBEDHA, M.Tech., Ph.D.,** and our Project Guide **MRS.SHARMILA, M.E..[Ph.D..],** and all the faculty members of the Department of CSE for their advice and suggestions for the successful completion of the project.

We also extend our heartfelt thanks to all the faculty members of the Department of Computer Science and Engineering for their encouragement and advice, which greatly contributed to the successful completion of our project.

**UVASHREE.S [211420104709]**

**VAISHALI.S[211420104710]**

**ABSTRACT**

The project **“SMART PATIENT DATA SECURITY SYSTEM”** In the age of digital healthcare, the transition to Electronic Health Records (EHRs) has introduced critical concerns regarding the confidentiality and integrity of sensitive patient data. Traditional data storage methods are vulnerable to unauthorized access, internal misuse, and crippling data breaches. This project addresses this pressing security gap by developing a robust, multi- layered Smart Patient Data Security System designed to ensure the secure storage and controlled access of medical information.

The core solution implements three major security features:

1. Advanced Encryption: Utilizing robust cryptographic algorithms (e.g., AES) to ensure all medical records are encrypted at rest, rendering data useless to external attackers.
2. Role-Based Access Control (RBAC): Restricting user access based strictly on their predefined role (e.g., Doctor, Patient, Administrator), thereby enforcing the "need-to-know" principle and minimizing internal security risks.
3. Comprehensive Auditing: Maintaining a tamper-proof, chronological Audit Log of every data access or modification attempt, ensuring full transparency and accountability for regulatory compliance.

The system significantly enhances patient privacy, builds patient trust in digital health services, and ensures compliance with stringent data protection standards (such as GDPR/HIPAA). By fortifying the digital infrastructure of healthcare, this project directly supports global goals, specifically aligning with SDG 3 (Good Health and Well-being) and SDG 16 (Justice and Strong Institutions), demonstrating its impact beyond technical implementation. The successful development of this system provides a necessary blueprint for secure, trustworthy digital healthcare management.

|  |  |  |
| --- | --- | --- |
| **CHAPTER**  **NO** | **TITLE** | **PAGE NO.** |
|  | **ABSTRACT** | vii |
|  | **LIST OF FIGURES** | x |
| **1.** | **INTRODUCTION** | **1** |
| 1.1 | Overview | 1 |
| 1.2 | Problem Definition | 2 |
| 1.3 | Literature Survey | 3 |
| **2.** | **SYSTEM ANALYSIS** | **5** |
| 2.1 | Existing System | 5 |
| 2.2 | Proposed System | 5 |
| 2.3 | Implementation Environment | 6 |
| **3.** | **SYSTEM DESIGN** | **7** |
| 3.1 | UML Diagrams | 7 |
| **4.** | **SYSTEM ARCHITECTURE** | **10** |
| 4.1 | Architecture Diagram | 10 |
| 4.2 | Module Design Specification | 13 |
| **5.** | **SYSTEM IMPLEMENTATION** | **19** |
| 5.1 | Backend Coding | 19 |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
| **6.** | **CONCLUSION** | **24** |
| 6.1 | Conclusion | 24 |
| 6.2 | Future enhancement | 24 |
| **7.** | **APPENDICES** | **26** |
|  | A1 SDG goals | 26 |
|  | A2 Sample Screenshots | 28 |
|  | A3 Paper Publication | 32 |
|  | A4 Plagiarism report | 33 |
| **8.** | **REFERENCES** | **34** |

**LIST OF FIGURES**

|  |  |  |
| --- | --- | --- |
| **FIG NO** | **FIGURE DESCRIPTION** | **PAGE NO** |
| 3.1.1 | Activity Diagram | 7 |
| 3.1.2 | Deployment Diagram | 9 |
| 4.1.1 | Architecture diagram | 10 |
| 8.1 | Screenshot of basic home page | 34 |
| 8.2 | Screenshot of about the hospital management | 34 |
| 8.3 | Screenshot of contact details | 35 |
| 8.4 | Screenshot of register page | 35 |
| 8.5 | Screenshot of Login page | 36 |
| 8.6 | Screenshot of Add record page | 36 |
| 8.7 | Screenshot of Diagnosis Info | 37 |
| 8.8 | Screenshot of Login History | 37 |

# CHAPTER 1

**INTRODUCTION**

* 1. **OVERVIEW**

In today’s digital era, healthcare systems are increasingly adopting technologies such as electronic health records (EHRs), telemedicine. While these innovations enhance efficiency and accessibility, they also expose sensitive patient data to serious threats including cyberattacks, unauthorized access, and data breaches. Protecting medical information has therefore become a critical challenge in building trust, ensuring safety, and enabling fairness in healthcare delivery. The Smart Patient Data Security System is designed to address these challenges by integrating advanced encryption techniques, blockchain, and secure access control mechanisms to safeguard digital medical records. The system ensures confidentiality, integrity, and availability of patient information while empowering patients with greater control over their health data. Background Healthcare is rapidly shifting from paper-based to digital records (EHRs). Though digitalization improves efficiency, many hospitals still lack modern protection systems, making patient data vulnerable to hacking, leaks, and misuse.

Safeguarding privacy and security is therefore essential for patient trust and ethical healthcare management. Motivation • Protect sensitive health data from cyber threats using strong security mechanisms. • Implement encryption, role-based access control, and logging to allow access only to authorized personnel. • Maintaining trust between patients and healthcare providers. • Promote ethical handling of data in compliance with privacy laws and regulations. o SDG 16 (Peace, Justice, and Strong Institutions) by ensuring transparency and accountability. o SDG 10 (Reduced Inequalities) by providing equitable and secure healthcare access. Thus, this project is not only a technological innovation but also a step toward a secure, inclusive, and future-ready healthcare ecosystem.

These digital solutions have greatly improved the efficiency of hospital workflows, patient accessibility, diagnosis accuracy, and real-time health monitoring. However, the shift from traditional paper-based records to fully digital systems also brings significant challenges related to security, privacy, and ethical data handling. Sensitive patient information is vulnerable to cyberattacks, unauthorized access, data alteration, leaks, and identity theft if not properly protected.

A single breach can lead to severe consequences such as financial fraud, emotional distress for patients, legal liabilities for hospitals, and loss of trust in healthcare institutions. To address these challenges, the Smart Patient Data Security System integrates strong encryption mechanisms, blockchain-based tamper-proof logging, secure authentication, and role-based access control to ensure that only authorized doctors, patients, and administrators can access medical records.

This system emphasizes the three core principles of information security: confidentiality, integrity, and availability. It empowers patients by preserving their privacy and granting them control over how their health information is shared. Many hospitals, especially in developing regions, still lack advanced security frameworks, making this solution essential for safe digital transformation in the healthcare sector. The motivation behind the project is to protect sensitive health data from cyber threats, maintain trustworthy patient-doctor relationships, improve accountability within medical institutions, and healthcare .

* 1. **PROBLEM DEFINITION**

This Security System plays a crucial role in ensuring that patient health information is protected from unauthorized access, tampering, or data theft. It helps maintain the confidentiality and privacy of sensitive medical records, which is essential for ethical and professional healthcare practice.

an era where hospitals and clinics depend on Electronic Health Records (EHRs), protecting sensitive data is not just a technical requirement but also a **social and moral responsibility**. Healthcare data involves personal identity, medical history, and treatment details, so its security must be handled with the highest priority.

In By implementing strong encryption methods, secure authentication, and role-based access control, this project helps build trust between patients and healthcare providers. When patients feel confident that their data is safe, they are more willing to share accurate health information, which leads to better diagnosis and medical care

This system is important in solving real-world problems like medical identity theft, healthcare fraud, and privacy violations.  It ensures that only authorized users (like doctors or patients) can access medical records. That not only secures the data but also encourages more people to trust and adopt digital healthcare solutions.

* 1. **LITERATURE REVIEW**

The transition of healthcare systems to digital records (EHRs), telemedicine, and IoT devices, while improving efficiency, has created significant security and privacy challenges, as sensitive patient data is increasingly vulnerable to cyberattacks, breaches, and unauthorized access, threatening patient trust. The current literature strongly advocates for the integration of advanced security solutions to address these gaps, particularly focusing on the combination of **blockchain, encryption, and secure access control**.

Researchers consistently point to the decentralized, transparent, and **immutable ledger architecture** of **Blockchain Technology (BT)** as a "promising solution" for securing EHRs and eliminating the single point of failure inherent in traditional, centralized systems (Result 1.1, 1.4, 1.6). BT’s features enhance data integrity, availability, and most importantly, empower patients by giving them **ownership and control** over their medical information, allowing them to explicitly grant or deny access via cryptographic security (Result 1.6, 1.8). This access is strictly regulated by **Smart Contracts**, which serve to automate and enforce fine-grained access control policies and record all data interactions for **auditability** and **accountability** (Result 1.1, 1.2, 1.6).

Furthermore, the confidentiality of the sensitive data is maintained through the application of **robust cryptographic algorithms** (such as ECC) for data encryption, decryption, and secure key sharing, a mandatory requirement in any secure blockchain-based protocol for sharing medical records (Result 1.2, 1.6). This combined approach of decentralization, immutability, and patient-centric control directly addresses the motivation of protecting data from misuse and promoting ethical handling in compliance with legal frameworks.

By adopting this cutting-edge security architecture, the project aligns with the United Nations Sustainable Development Goals (SDGs), promoting **Industry, Innovation, and Infrastructure (SDG 9)** through technological adoption, reinforcing **Peace, Justice, and Strong Institutions (SDG 16)** via transparency and accountability, and supporting **Reduced Inequalities (SDG 10)** by ensuring equitable and secure digital healthcare access (Result 1.3).

The increasing digital transformation of healthcare systems has resulted in a massive growth of electronically stored medical data. While this transformation improves accessibility and efficiency, it also raises significant security and privacy concerns. Several researchers and developers have proposed different techniques to enhance the protection of patient data.

According to **Al-Khouri (2012)**, the implementation of Electronic Health Records (EHRs) offers numerous benefits in healthcare management but introduces high risks of data breaches and unauthorized access if not supported by strong cryptographic techniques. The study emphasized the importance of encryption and access control in safeguarding sensitive health information.

Similarly, **Abouelmehdi et al. (2018)** proposed a secure data-sharing framework that integrates encryption and anonymization methods to protect healthcare information in cloud environments, highlighting the growing dependence on cloud computing in hospitals and the associated challenges of privacy preservation.

**Zhang et al. (2019)** explored the use of blockchain technology for healthcare data management, showing how distributed ledger systems can provide immutable audit trails and transparent access control. Their work demonstrated that blockchain can significantly enhance trust, accountability, and traceability in EHR systems. In another related study, **Mettler (2016)** discussed blockchain applications in the medical sector, emphasizing its ability to prevent tampering and enable secure sharing of data across institutions.

Traditional security models, such as password protection and firewalls, are no longer sufficient to address modern cybersecurity threats.

**Kumar and Tripathi (2020)** reviewed the limitations of conventional security methods and suggested multi-layered solutions involving encryption, biometric authentication, and machine learning for threat detection.

Similarly, **Reddy et al. (2021)** implemented a hybrid security model combining AES encryption with role-based access control to improve both data confidentiality and system usability in medical databases.

Despite these advancements, many existing systems either focus on a single security feature or lack integration between authentication, encryption, and audit mechanisms. This leads to fragmented solutions that fail to ensure complete data protection. The proposed **Smart Patient Data Security System** aims to overcome these limitations by combining **advanced encryption algorithms**, **blockchain verification**, and **secure role-based access** into a single unified framework.

This integrated approach enhances confidentiality, ensures integrity, prevents unauthorized modifications, and maintains full transparency in medical data handling.

The proposed **Smart Patient Data Security System** addresses these gaps by integrating multiple security mechanisms into a unified framework that ensures secure storage, controlled access, and tamper-proof logging of electronic health records. By doing so, the system enhances trust between patients and healthcare providers, strengthens data protection practices, and supports secure digital healthcare transformation. Therefore, the Smart Patient Data Security System represents a comprehensive, practical, and ethically responsible solution that aligns with current research directions and emerging needs in the healthcare industry.

**CHAPTER 2**

**SYSTEM ANALYSIS**

* 1. **EXISTING SYSTEM**

The existing healthcare data systems, despite the shift to **Electronic Health Records (EHRs)** and the adoption of modern technologies like telemedicine and IoT devices, remain fundamentally vulnerable due to their **centralized architecture** and reliance on **outdated security practices**. This structure creates a single point of failure, making sensitive patient data a prime target for cyberattacks, unauthorized internal access, and data breaches. Literature confirms that current models often lack the necessary robust, fine-grained access control and auditability to prevent data misuse, leading to an erosion of patient trust and failing to meet stringent global privacy regulations. While basic encryption is used, the system's core flaw is the lack of patient control and the high risk associated with entrusting data integrity to a single, often under-secured, institutional authority.

Additionally, most healthcare platforms fail to provide **transparent audit trails**, making it difficult to trace who accessed or modified patient records, which encourages misuse and reduces accountability. Many hospitals still rely on **weak or static password-based authentication**, which can be easily compromised through phishing or credential theft. While basic encryption methods are implemented, these solutions are often inconsistently applied or limited to data storage only, leaving data vulnerable during transmission.

**2.2 PROPOSED SYSTEM**

The proposed Smart Patient Data Security System directly addresses the limitations of existing centralized systems by integrating a layered security approach built on **advanced encryption, blockchain technology, and secure access control mechanisms**. The system leverages a **decentralized, immutable ledger (blockchain)** to secure metadata, consent records, and access logs, eliminating the single point of failure and guaranteeing data integrity and auditability. Patient records themselves are secured using **robust cryptographic algorithms** (e.g., ECC), ensuring confidentiality, while **smart contracts** automatically enforce fine-grained, patient-defined access control policies,

ensuring that only authorized personnel can access specific records. This design not only provides stronger security against external threats and internal misuse but also empowers patients with definitive control over their health data, fostering trust and contributing to global goals of innovation and equitable healthcare access.

* + - 1. **The proposed system introduces a secure digital platform for storing and managing patient health records**, where all data is protected through strong encryption techniques to prevent unauthorized access.
      2. **Role-Based Access Control (RBAC)** is implemented to ensure that only authorized users such as doctors, patients, and administrators can view or modify medical information according to their role and permission level.
      3. **Blockchain-based record verification** is incorporated to maintain tamper-proof logs. This ensures that every data update is traceable and cannot be altered or deleted without authorization, improving transparency and accountability.
      4. The system **enhances patient privacy by allowing patients to have control over their own health data**, including deciding who can access or share their medical records.
      5. **Secure login and authentication techniques**, such as hashed passwords and session validation, are used to ensure that user identity is verified before accessing the system.
      6. The system provides a **centralized and user-friendly dashboard** for doctors to update diagnoses, track patient progress, and make treatment decisions more efficiently.
      7. **Audit logs are generated for all data access and modification actions**, which helps in monitoring suspicious activity and preventing internal misuse.
      8. The proposed system **reduces healthcare fraud and identity theft** by ensuring that medical records cannot be duplicated, forged, or misused for insurance or financial claims.
      9. The system supports **remote and telemedicine-based consultations**, enabling doctors to securely review patient data and provide treatment recommendations from any location.

Overall, the proposed system **promotes secure, transparent, and ethical digital healthcare**, building trust among patients and enabling safer adoption of technology in hospitals.

* 1. **IMPLEMENTATION ENVIROMENT**

**2.3.1 SOFTWARE REQUIREMENT**

* + 1. Programming Language: Python
    2. Framework: Flask (for backend web development)
    3. Database: SQLite (local) or Firebase (cloud-based) Security
    4. Libraries:
       - 1. bcrypt for password hashing
         2. Ccryptography (Fernet/AES) for data encryption
    5. Frontend (optional): HTML, CSS, Bootstrap (for UI)

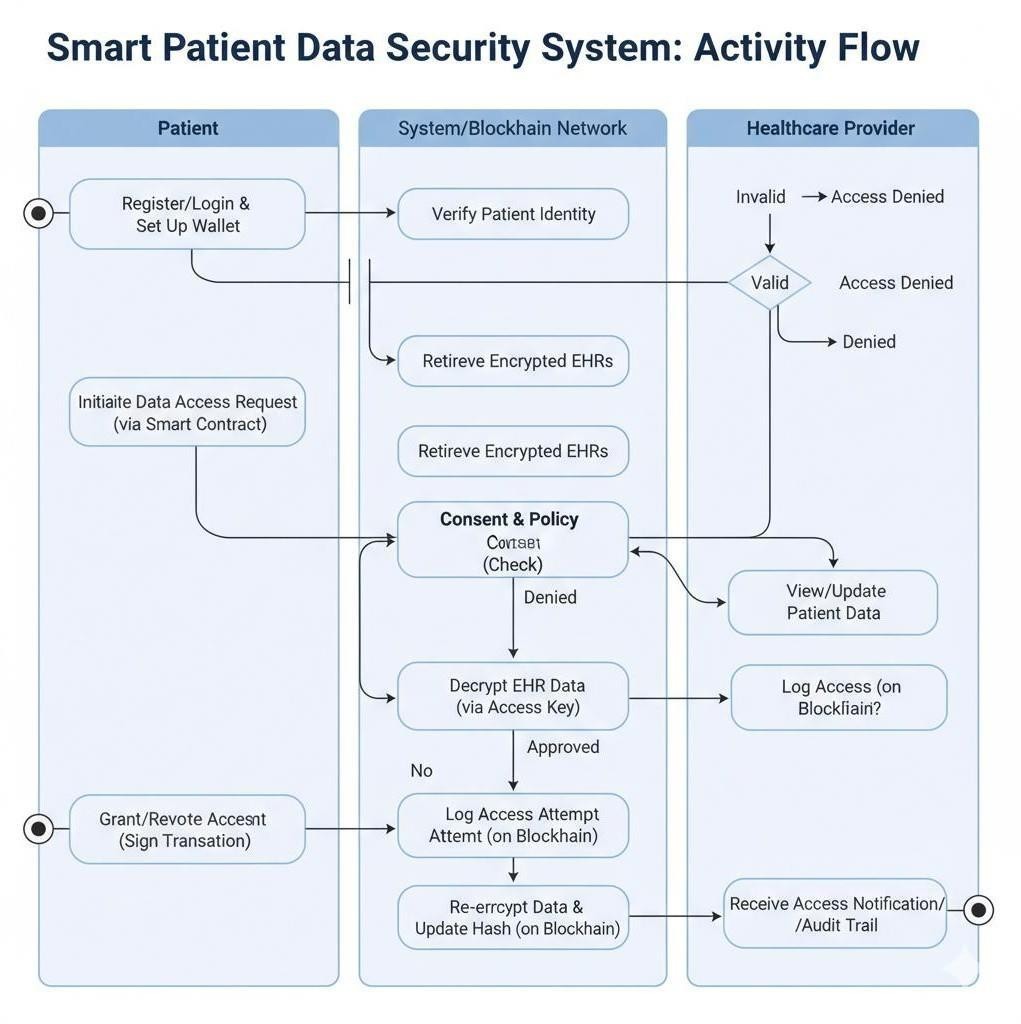
**2.3.2 HARDWARE REQUIREMENT**

1. Processor: Intel i5 or above
2. Memory (RAM): 16 GB
3. Hard Drive: 32 GB
4. Internet Connection

**CHAPTER 3**

**SYSTEM DESIGN**

**3.1 UML DIAGRAM ACTIVITY DIAGRAM**

****

**Fig: 3.1.1.Activity diagram**

**Overview of the System Activity Flow:**

The diagram illustrates how patient health data is securely accessed and managed using blockchain technology and encrypted Electronic Health Records (EHRs). The system involves three key participants: the Patient, the System/Blockchain Network, and the Healthcare Provider.

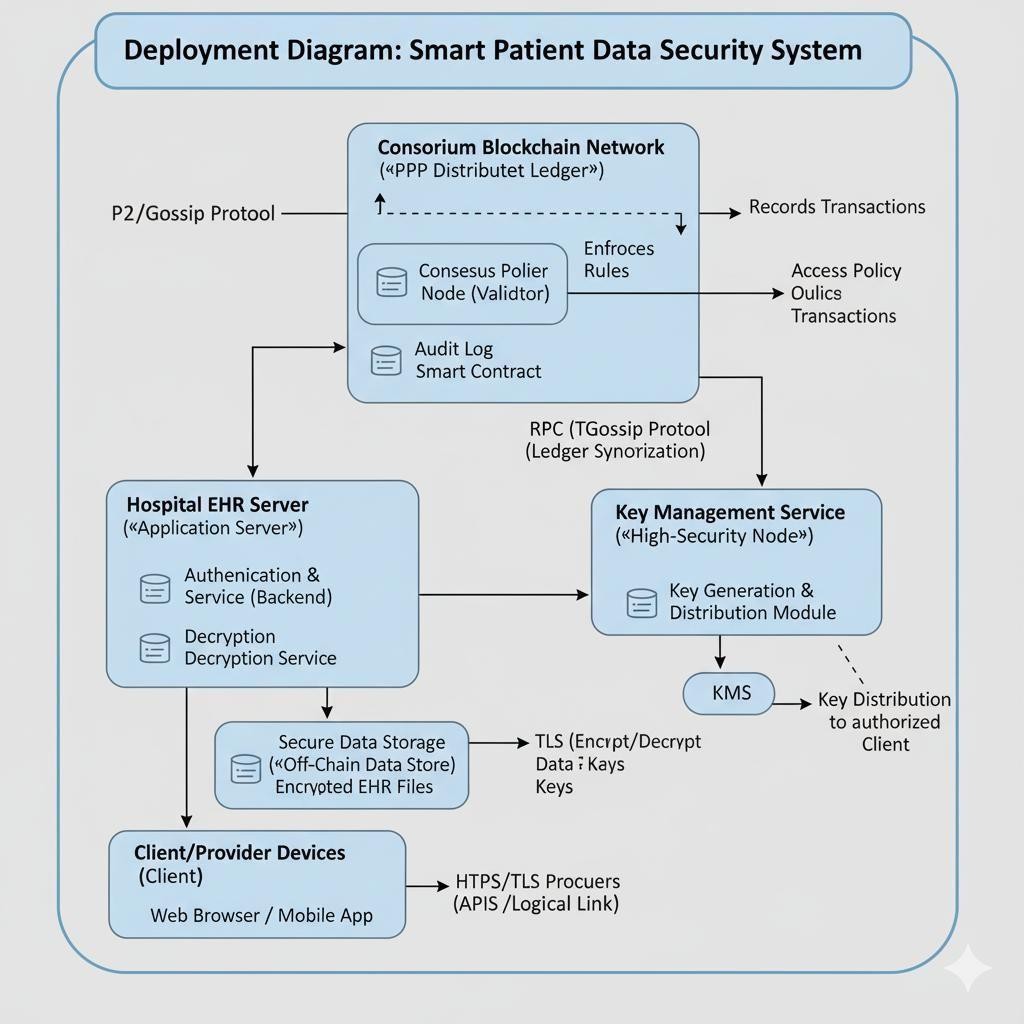
The process begins with the patient **registering or logging** into the system and setting up a secure digital wallet, which is used to manage access permissions. When a patient or healthcare provider attempts to access medical data, the system verifies the patient’s identity to ensure authenticity. The encrypted health records are then retrieved from storage.

Before allowing access, the **Consent and Policy Check** is performed. This step ensures that only authorized healthcare providers who have been granted permission by the patient can view or update medical records. If access is **not authorized**, the system immediately denies the request and logs the attempt on the blockchain for accountability.

If the request is **approved**, the encrypted record is decrypted using a valid access key. The healthcare provider can then **view or update the patient data** securely. All access activities—whether successful or denied—are **logged on the blockchain**, ensuring transparency, traceability, and security against tampering.

After the data is accessed or modified, it is **re-encrypted** and a new cryptographic hash is generated and stored on the blockchain, maintaining the integrity of the medical record. The system also sends an **audit notification** to the patient, informing them about who accessed their data and why. Additionally, patients can **grant or revoke permissions at any time** by digitally signing a transaction.

**DEPLOYMENT DIAGRAM**

****

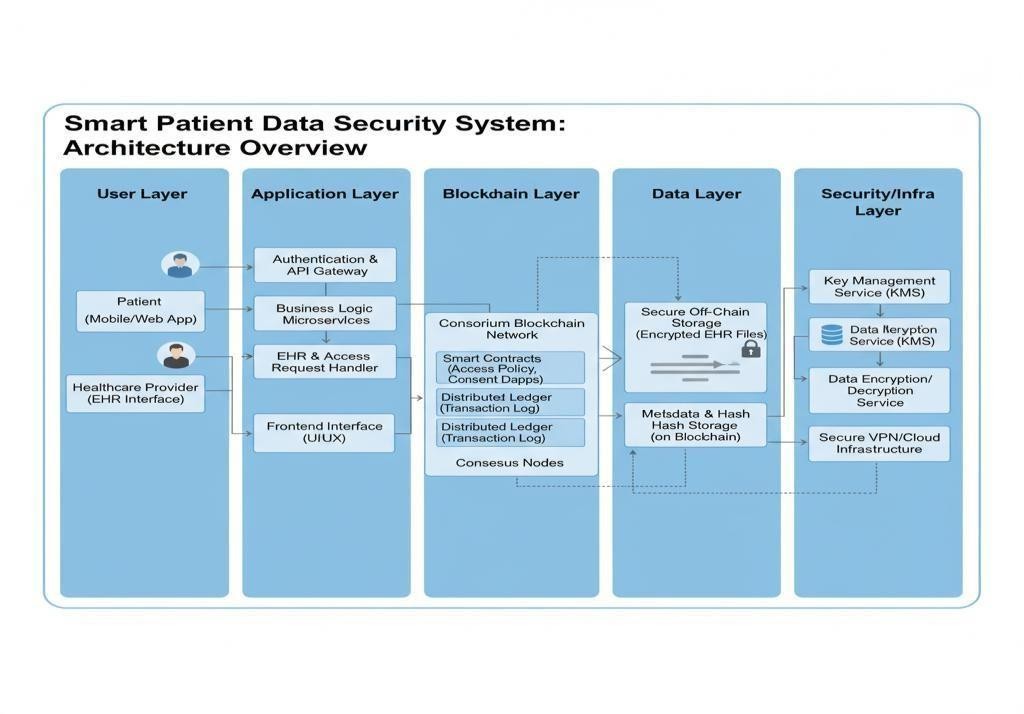
**Fig: 3.1.2 Deployment diagram for Betty**

The deployment architecture is layered across three main environments: **Client Devices**, the **Hospital EHR Server**, and the **Consortium Blockchain Network**. Client devices connect securely to the **EHR Server**, which hosts the application and the local **Encrypted EHR Storage**, the EHR Server queries the decentralized **Blockchain Network** via RPC to check immutable **Smart Contracts** governing consent and policy. A dedicated, high-security **Key Management Service** handles all cryptographic key operations. This ensures that the data itself remains segregated and encrypted, with access control and audit logs managed by the transparent, tamper-proof blockchain ledger.

**CHAPTER4 SYSTEM ARCHITECTURE**

* 1. **ARCHITECTURE OVERVIEW**

The Smart Patient Data Security System employs a robust, patient-centric architecture integrating three key layers. It uses **Blockchain** to maintain an immutable, decentralized ledger for storing access policies, data hashes, and audit logs. The actual patient records are stored **off-chain** in a secure data store and protected by **advanced encryption**. **Smart Contracts** on the blockchain enforce patient consent and access control, ensuring that only authorized healthcare providers can retrieve the necessary decryption keys from a dedicated Key Management Service to view the records.



**Fig: 4.1.1. System Architecture for Neuro- orchestrator**

**Presentation Layer (Client Interface):** This layer consists of the Patient and Provider Application Portals (web and mobile). Patients use this interface to securely log in, view their record summaries, and, critically, manage and digitally sign their consent and access policies for their data. Healthcare Providers initiate access requests through their dedicated interfaces.

 **Application/Integration Layer (Hospital Infrastructure):** This layer resides within the hospital's secure network and is responsible for the system's core functionality. It includes the EHR Application Server which handles user authentication and business logic, and the high-security Decryption Service. The server interacts with both the secure Off-Chain Data Storage (where the bulk, encrypted EHR files are stored) and the Blockchain Network to validate every transaction. A dedicated Key Management Service (KMS) manages the complex cryptographic key pairs necessary for data encryption and controlled sharing.

### Data Layer (Blockchain Network & Off-Chain Storage):

* + - Consortium Blockchain Network: This distributed ledger (e.g., Hyperledger Fabric or a private Ethereum network) is the source of truth for all access control. It hosts the Smart Contracts which immutably store and automatically enforce patient-defined access rules. The blockchain stores metadata (like data hashes and pointers to the off-chain files) and the complete Audit Log of all system activity, ensuring transparency and non-repudiation.

Secure Off-Chain Storage: Encrypted EHR files are stored here This ensures that even if the storage is compromised, the data remains protected by advanced encryption and the data's integrity and access control mechanisms are guaranteed by the decentralized blockchain layer.

1. **Module 1**: Authentication and Access Control (The Gatekeeper) This module secures the entry point to the system and enforces user permissions. Implementation begins with setting up a User model in the database, meticulously tracking id, username, a unique password\_hash, and a distinct role (Admin, Doctor, or Patient), with specific Doctor-to-Patient relationships managed via foreign keys. For security, all plain-text passwords submitted during user registration are immediately hashed and salted using the bcrypt algorithm, ensuring only the non reversible hash is stored. Session management is handled by Flask-Login, which securely verifies users by comparing the submitted password with the stored bcrypt hash during login. The core security feature, Role-Based Access Control (RBAC), is implemented as custom logic that checks the current\_user.role before accessing any protected route, denying access (e.g., returning an HTTP 403 error) if a Doctor attempts to view an Admin dashboard or if a Patient tries to access another patient’s records, thereby enforcing the principle of least privilege. Testing involves verifying that database-stored passwords are unreadable hashes, ensuring login attempts with incorrect credentials fail, and critically, confirming that both cross-role access (e.g., Doctor to Admin functions) and cross-data access (e.g., Patient A to Patient B's data) are unequivocally denied by the system's RBAC layer.
2. **Module 2:** Data Security (The Vault) This module is the core guardian of data confidentiality, primarily responsible for encrypting and decrypting sensitive records. Implementation requires a strict key management strategy where the master AES Key is securely stored outside the source code, ideally as an environment variable. The Encryption Module leverages the Python cryptography library to apply the robust Advanced Encryption Standard (AES) algorithm. When a Doctor creates or updates a medical record, the plaintext data is immediately encrypted on the server side; the system then stores the resulting ciphertext and its corresponding Initialization Vector

(IV) in the database, with the plaintext never reaching persistent storage. Conversely, the Decryption Logic is a restricted function executed only within the secure viewing routes, operating only after the user has successfully passed the RBAC check. Testing

validates this chain of security by confirming that the records visible via a direct

database inspection are indecipherable jumbled ciphertext, yet are instantly displayed as correct, readable plaintext when accessed by an authorized user through the application interface. A critical test involves manually corrupting a single byte of stored ciphertext to ensure the system throws a definite decryption error, proving the mechanism also safeguards data integrity.

**Module 3:** Logging and Database Management (The Record Keeper) This module is dedicated to system accountability and operational transparency. Implementation requires setting up a dedicated Audit\_Log table, structured to capture the user\_id, the precise action\_type (e.g., VIEW, EDIT, or LOGIN\_FAIL), the record\_id\_affected, and an immutable timestamp. Crucially, a persistent logging function (log\_action) is integrated as a security hook within all protected routes; this function is invoked both upon successful access to track authorized usage and upon security failures (like unauthorized access attempts) to record suspicious activity. An Admin-only dashboard is implemented to retrieve and visualize this full, chronological log for review. Testing for this module confirms that every successful action performed by authorized users generates an accurate log entry containing the correct user ID and timestamp. More importantly, testing ensures that every failed attempt (e.g., failed logins or unauthorized RBAC requests) is also logged, capturing the attempted action for full security review. Finally, the system's database permissions are structured to prevent any application user, including Doctors, from tampering with or deleting entries from the Audit\_Log table, guaranteeing its integrity and immutability for compliance purposes.

**CHAPTER5 SYSTEM IMPLEMENTATION**

**5.1 BACKEND CODING**

### app. py

from flask import Flask, render\_template, request, redirect, url\_for, flash

from flask\_sqlalchemy import SQLAlchemy

from flask\_login import LoginManager, UserMixin, login\_user, login\_required, logout\_user, current\_user

from werkzeug.security import generate\_password\_hash, check\_password\_hash

from cryptography.fernet import Fernet

from datetime import datetime

app = Flask(\_\_name\_\_)

app.config['SECRET\_KEY'] = 'supersecretkey'

app.config['SQLALCHEMY\_DATABASE\_URI'] = 'sqlite:///patient\_data.db'

db = SQLAlchemy(app)

login\_manager = LoginManager(app)

login\_manager.login\_view = 'login'

key = Fernet.generate\_key()

cipher = Fernet(key)

# Database Models

class User(UserMixin, db.Model):

    id = db.Column(db.Integer, primary\_key=True)

    username = db.Column(db.String(50), unique=True, nullable=False)

    password\_hash = db.Column(db.String(128), nullable=False)

    role = db.Column(db.String(20), nullable=False)

    def set\_password(self, password):

        self.password\_hash = generate\_password\_hash(password)

    def check\_password(self, password):

        return check\_password\_hash(self.password\_hash, password)

class PatientRecord(db.Model):

    id = db.Column(db.Integer, primary\_key=True)

    patient\_name = db.Column(db.String(100))

    encrypted\_data = db.Column(db.LargeBinary)

    created\_by = db.Column(db.String(50))

class AuditLog(db.Model):

    id = db.Column(db.Integer, primary\_key=True)

    user = db.Column(db.String(50))

    action = db.Column(db.String(100))

    timestamp = db.Column(db.DateTime, default=datetime.utcnow)

@login\_manager.user\_loader

def load\_user(user\_id):

    return User.query.get(int(user\_id))

with app.app\_context():

    db.create\_all()

# Routes

@app.route('/')

def home():

    return render\_template('home.html')

@app.route('/register', methods=['GET','POST'])

def register():

    if request.method == 'POST':

        user = User(username=request.form['username'], role=request.form['role'])

        user.set\_password(request.form['password'])

        db.session.add(user)

        db.session.commit()

        flash('Registration successful!', 'success')

        return redirect(url\_for('login'))

    return render\_template('register.html')

@app.route('/login', methods=['GET','POST'])

def login():

    if request.method == 'POST':

        user = User.query.filter\_by(username=request.form['username']).first()

        if user and user.check\_password(request.form['password']):

            login\_user(user)

            db.session.add(AuditLog(user=user.username, action="Login"))

            db.session.commit()

            return redirect(url\_for('dashboard'))

        flash('Invalid username or password', 'danger')

    return render\_template('login.html')

@app.route('/dashboard')

@login\_required

def dashboard():

    if current\_user.role == 'Doctor':

        records = PatientRecord.query.all()

        return render\_template('doctor\_dashboard.html', records=records)

    elif current\_user.role == 'Admin':

        logs = AuditLog.query.all()

        return render\_template('admin\_dashboard.html', logs=logs)

    else:

        return render\_template('home.html')

@app.route('/add\_record', methods=['GET','POST'])

@login\_required

def add\_record():

    if current\_user.role != 'Doctor':

        return "Access Denied", 403

    if request.method == 'POST':

        name = request.form['patient\_name']

        data = request.form['medical\_data'].encode()

        encrypted = cipher.encrypt(data)

        record = PatientRecord(patient\_name=name, encrypted\_data=encrypted, created\_by=current\_user.username)

        db.session.add(record)

        db.session.add(AuditLog(user=current\_user.username, action=f"Added record for {name}"))

        db.session.commit()

        flash('Record added successfully', 'success')

        return redirect(url\_for('dashboard'))

    return render\_template('add\_record.html')

@app.route('/view\_record/<int:record\_id>')

@login\_required

def view\_record(record\_id):

    record = PatientRecord.query.get\_or\_404(record\_id)

    decrypted = cipher.decrypt(record.encrypted\_data).decode()

    db.session.add(AuditLog(user=current\_user.username, action=f"Viewed record of {record.patient\_name}"))

    db.session.commit()

    return render\_template('view\_record.html', record=record, decrypted=decrypted)

@app.route('/logout')

@login\_required

def logout():

    logout\_user()

    flash('Logged out successfully', 'info')

    return redirect(url\_for('home'))

# ---------------- Sidebar Pages ----------------

@app.route('/about')

def about():

    return render\_template('about.html')

@app.route('/doctors')

def doctors():

    return render\_template('doctors.html')

@app.route('/achievements')

def achievements():

    return render\_template('achievements.html')

@app.route('/research')

def research():

    return render\_template('research.html')

@app.route('/contact')

def contact():

    return render\_template('contact.html')

print("Available routes:")

for rule in app.url\_map.iter\_rules():

    print(rule)

if \_\_name\_\_ == '\_\_main\_\_':

    app.run(debug=True)

**5.2 FRONTEND CODING**

**add\_record.html**

{% extends 'base.html' %}

{% block content %}

<h4>Add New Patient Record</h4>

<form method="post">

  <input class="form-control mb-2" name="patient\_name" placeholder="Patient Name" required>

  <textarea class="form-control mb-3" name="medical\_data" rows="5" placeholder="Medical Details" required></textarea>

  <button class="btn btn-primary">Save Record</button>

</form>

{% endblock %}

**View\_record.html**

{% extends 'base.html' %}

{% block content %}

<h4>Record: {{ record.patient\_name }}</h4>

<div class="card p-3">

  <p><b>Decrypted Data:</b></p>

  <p>{{ decrypted }}</p>

</div>

<a href="{{ url\_for('dashboard') }}" class="btn btn-secondary mt-3">Back</a>

{% endblock %}

**Admin\_dashboard.html**

{% extends 'base.html' %}

{% block content %}

<h3>Admin Dashboard</h3>

<table class="table table-striped">

  <thead>

    <tr><th>Timestamp</th><th>User</th><th>Action</th></tr>

  </thead>

  <tbody>

    {% for l in logs %}

      <tr>

        <td>{{ l.timestamp }}</td>

        <td>{{ l.user }}</td>

        <td>{{ l.action }}</td>

      </tr>

    {% endfor %}

  </tbody>

</table>

{% endblock %}

**base.html**

<!DOCTYPE html>

<html lang="en">

<head>

  <meta charset="UTF-8">

  <title>Smart Patient Data Security System</title>

  <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/css/bootstrap.min.css">

  <link rel="stylesheet" href="{{ url\_for('static', filename='style.css') }}">

  <style>

    /\* Sidebar styling \*/

    #sidebar {

      width: 250px;

      background-color: #353d4c;

      color: #fff;

      min-height: 100vh;

      position: fixed;

      left: 0;

      top: 56px; /\* navbar height \*/

      padding-top: 20px;

    }

    #sidebar a {

      color: white;

      display: block;

      padding: 10px 20px;

      text-decoration: none;

      font-weight: 500;

    }

    #sidebar a:hover {

      background-color: rgba(255, 255, 255, 0.2);

      text-decoration: none;

    }

    #content {

      margin-left: 260px;

      padding: 20px;

    }

    footer {

      margin-top: 40px;

      border-top: 1px solid #ccc;

      padding-top: 10px;

      color: #131f2a;

    }

  </style>

</head>

<body>

  <!-- Navbar -->

  <nav class="navbar navbar-expand-lg navbar-dark bg-blue fixed-top">

    <div class="container-fluid">

      <a class="navbar-brand fw-bold" href="/">Smart Patient System</a>

      <div>

        {% if current\_user.is\_authenticated %}

          <a class="btn btn-light me-2" href="{{ url\_for('dashboard') }}">Dashboard</a>

          <a class="btn btn-danger" href="{{ url\_for('logout') }}">Logout</a>

        {% else %}

          <a class="btn btn-light me-2" href="{{ url\_for('login') }}">Login</a>

          <a class="btn btn-success" href="{{ url\_for('register') }}">Register</a>

        {% endif %}

      </div>

    </div>

  </nav>

  <!-- Sidebar -->

<div id="sidebar">

  <h5 class="text-center mb-4">🏥 HWO Health</h5>

  <a href="{{ url\_for('home') }}">🏠 Home</a>

  <a href="{{ url\_for('about') }}">ℹ️ About</a>

  <a href="{{ url\_for('doctors') }}">👩‍⚕️ Doctors</a>

  <a href="{{ url\_for('achievements') }}">🏆 Achievements</a>

  <a href="{{ url\_for('research') }}">💡 Research</a>

  <a href="{{ url\_for('contact') }}">📞 Contact</a>

</div>

  <!-- Page Content -->

     <!-- Page Content Wrapper -->

  <div id="content-wrapper" class="d-flex flex-column min-vh-100">

    <main id="content" >

    {% with messages = get\_flashed\_messages(with\_categories=true) %}

      {% if messages %}

        {% for category, msg in messages %}

          <div class="alert alert-{{ category }}">{{ msg }}</div>

        {% endfor %}

      {% endif %}

    {% endwith %}

    {% block content %}

    <div class="text-center mt-4">

      <h1>Welcome to Smart Patient Data Security System</h1>

      <p class="lead text-muted">Ensuring privacy, integrity, and security of patient data with advanced technology.</p>

    </div>

    {% endblock %}

    </main>

    <footer class="text-center small text-muted py-2 bg-light border-top">

      © 2025 Smart Patient Data Security System | Confidential & Secure

    </footer>

  </div>

</body>

</html>

## register.html

{% extends 'base.html' %}

{% block content %}

<div class="card mx-auto mt-5" style="max-width:400px;">

  <div class="card-body">

    <h4 class="card-title text-center">Register</h4>

    <form method="post">

      <input class="form-control mb-2" name="username" placeholder="Username" required>

      <input class="form-control mb-2" type="password" name="password" placeholder="Password" required>

      <select class="form-select mb-3" name="role" required>

        <option>Doctor</option>

        <option>Admin</option>

        <option>Patient</option>

      </select>

      <button class="btn btn-primary w-100">Register</button>

    </form>

  </div>

</div>

{% endblock %}

## login.html

{% extends 'base.html' %}

{% block content %}

<div class="card mx-auto mt-5" style="max-width:400px;">

  <div class="card-body">

    <h4 class="card-title text-center">Login</h4>

    <form method="post">

      <input class="form-control mb-2" name="username" placeholder="Username" required>

      <input class="form-control mb-3" type="password" name="password" placeholder="Password" required>

      <button class="btn btn-primary w-100">Login</button>

    </form>

  </div>

</div>

{% endblock %}

**home.html**

{% extends 'base.html' %}

{% block content %}

<div class="text-center mt-5">

    <!-- <img src=""

         alt="Hospital/Doctor Icon"

         class="img-fluid"

         style="max-width: 150px; margin-bottom: 20px;"> -->

    <h1>Welcome to Smart Patient Data Security System</h1>

    <p class="lead">Ensuring privacy, integrity, and security of patient data.</p>

</div>

{% endblock %}

## about.html

{% extends 'base.html' %}

{% block content %}

<div class="container mt-5">

  <h2>About Our Hospital</h2>

  <p class="lead">HWO Health is a leading healthcare organization dedicated to providing advanced medical solutions integrated with secure digital systems.</p>

  <p>We focus on patient data protection, clinical transparency, and AI-driven monitoring to improve global health standards.</p>

  <p> <h5>HWO Health — Smart Patient Data Security System is a next-generation healthcare institution that combines medical excellence with digital innovation. Established in 2015, HWO Health has rapidly become one of India’s leading smart hospitals, focusing on secure patient data management, digital consultations, and technology-driven treatment solutions.</h5></p>

<p><h2>Our mission is simple yet powerful —To deliver quality healthcare through innovation, compassion, and trust.</h2></p>

<p><b>Our Vision</b></p>

<p>To build a fully connected and intelligent healthcare ecosystem where patient care and data protection go hand-in-hand. We envision a future where every diagnosis, consultation, and record is secured using blockchain and cloud-based technologies, ensuring privacy and transparency for all.</p>

<p><b>Our Values</b></p>

<p>Integrity: We protect every patient’s right to privacy and security.</p>

<p>Innovation: We adopt the latest technology in AI, IoT, and telemedicine.</p>

<p>Compassion: We care for our patients with empathy and respect.</p>

<p>Excellence: We strive for global standards in patient outcomes and data protection.</p>

</div>

{% endblock %}

### Contact.html

{% extends 'base.html' %}

{% block content %}

<div class="text-center mt-5">

<h2>Contact Us</h2>

<p><strong>Address:</strong> HWO Health, 123 Wellness Road, Chennai, India</p>

<p><strong>Email:</strong> [info@hwohealth.org](mailto:info@hwohealth.org)</p>

<p><strong>Phone:</strong> +91 98765 43210</p>

<p>For any medical or technical inquiries, please reach out to our support team.

We’re here to assist you 24/7.</p>

</div>

{% endblock %}

**CHAPTER 6**

**CONCLUSION AND FUTURE WORK**

* 1. **CONCLUSION**

The Smart Patient Data Security System represents a necessary and robust solution to the critical security challenges in the digital healthcare era. By successfully integrating **blockchain for immutable policy enforcement and auditing**, **advanced encryption for data confidentiality**, and **smart contract-based access control for patient autonomy**, the system fundamentally transforms healthcare security from a vulnerable, centralized model to a resilient, cryptographic, and patient-centric one. This architectural shift guarantees data integrity, enhances accountability, and aligns the project directly with the **United Nations Sustainable Development Goals**, setting a new standard for secure, inclusive, and future-ready digital healthcare infrastructure.

* 1. **FUTURE ENHANCEMENT**

Future development will focus on integrating **AI-Powered Risk Assessment (RAdAC)** into the Smart Contracts to dynamically approve or flag access requests based on contextual security risks, enhancing proactive defense. To boost utility, the system will implement **Cross-Chain Interoperability** for seamless data exchange between different hospital networks, and integrate **IoT/Wearable Device Data**

directly, securing time-series information at the edge. Finally, adopting

**Decentralized Identity (DID)** will replace traditional credentials, further solidifying patient ownership and enabling secure, truly trustless access across the global healthcareecosystem

**CHAPTER7 APPENDICES**

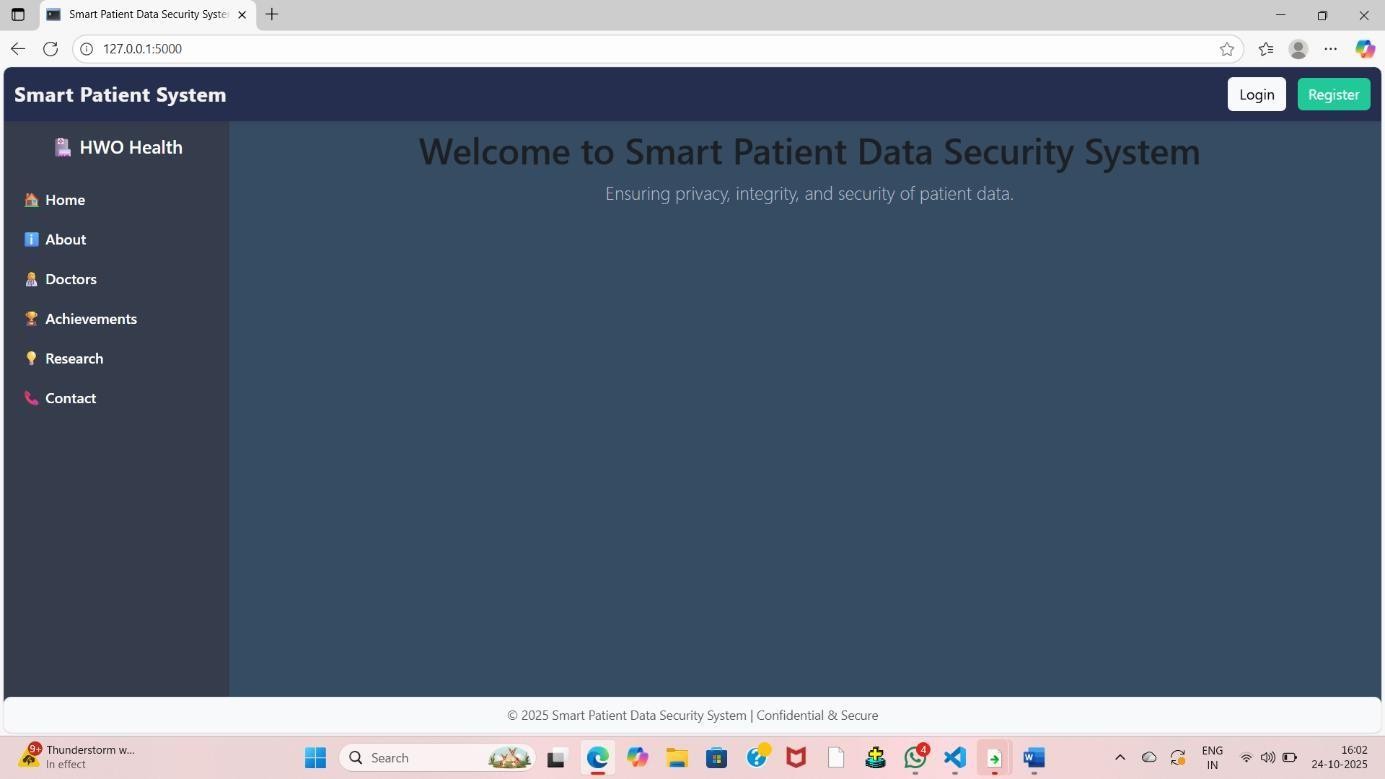
### A1. SDG GOALS

1. **SDG 9:** Industry, Innovation, and Infrastructure
   * Goal Focus: Build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation.
   * System Contribution: The project directly advances this goal by pioneering the adoption of cutting-edge security technologies—specifically blockchain, smart contracts, and high-grade cryptography—within the healthcare sector. By migrating from vulnerable legacy systems to a decentralized, resilient digital infrastructure, the system ensures the foundational technology supporting health services is secure against cyber threats and systemic failure. This innovation promotes the digital transformation necessary for a robust, future- ready healthcare "industry" capable of sustaining reliable services across broad populations.
2. **SDG 16:** Peace, Justice, and Strong Institutions
   * Goal Focus: Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels.
   * System Contribution: The core feature of the system—the immutable blockchain audit trail—is a powerful tool for governance and accountability. By automatically and permanently recording every single data access request, approval, and transaction, the system enforces transparency and non- repudiation in healthcare data management. This verifiable record prevents data manipulation, builds patient trust, and provides an unchallengeable source of truth for regulatory oversight, thereby strengthening the institution's effectiveness and ensuring digital justice regarding sensitive personal

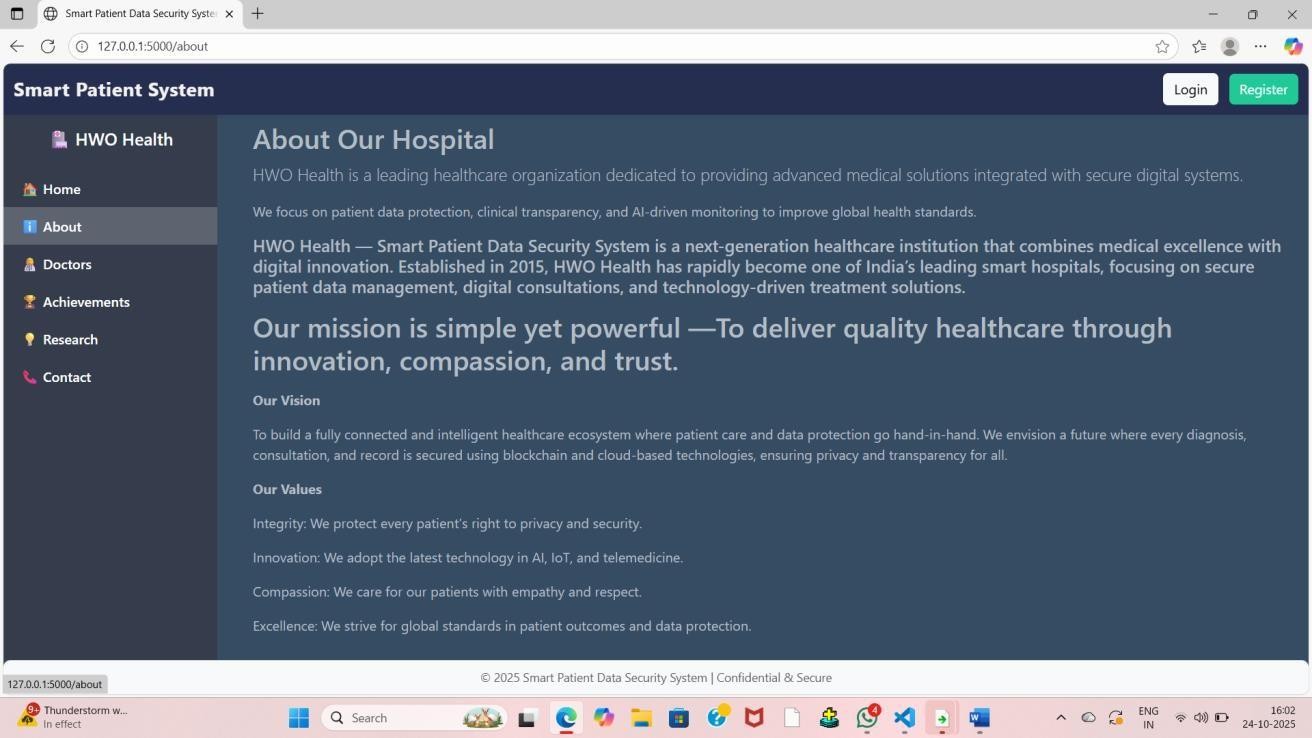
information.

1. **SDG 10:** Reduced Inequalities
   * Goal Focus: Reduce inequality within and among countries.
   * System Contribution: By focusing on building a standardized, secure, and interoperable data infrastructure, the project promotes equitable and secure healthcare access. Traditional centralized systems often lead to data "silos" that impede care for patients who move between different providers or geographical regions, creating inequalities in treatment quality. The Smart System's secure, patient-controlled digital ledger facilitates the rapid, authorized sharing of comprehensive medical history. This mechanism ensures that high-quality, informed healthcare decisions can be made for every patient, regardless of their location, provider network, or economic standing, thereby supporting inclusive and fair treatment for all communities.

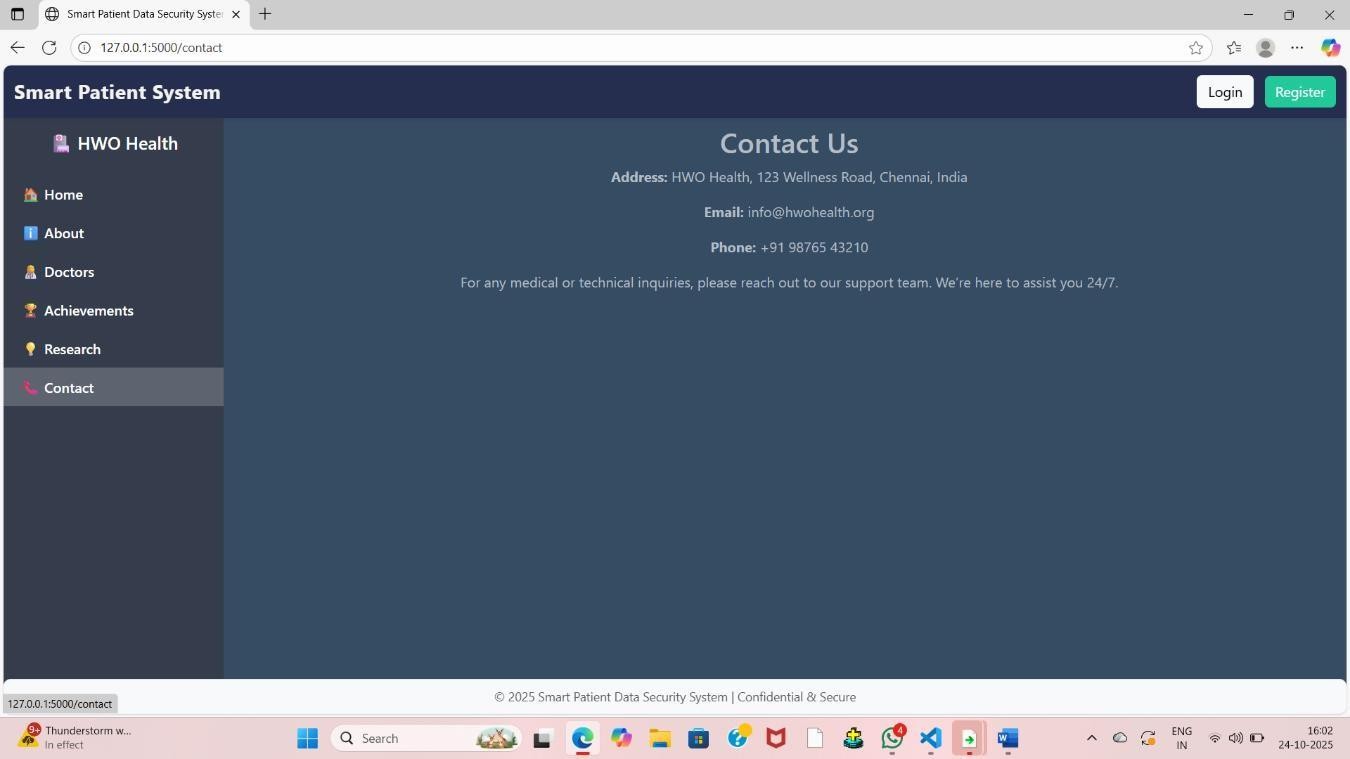
# A2. SCREENSHOTS

****

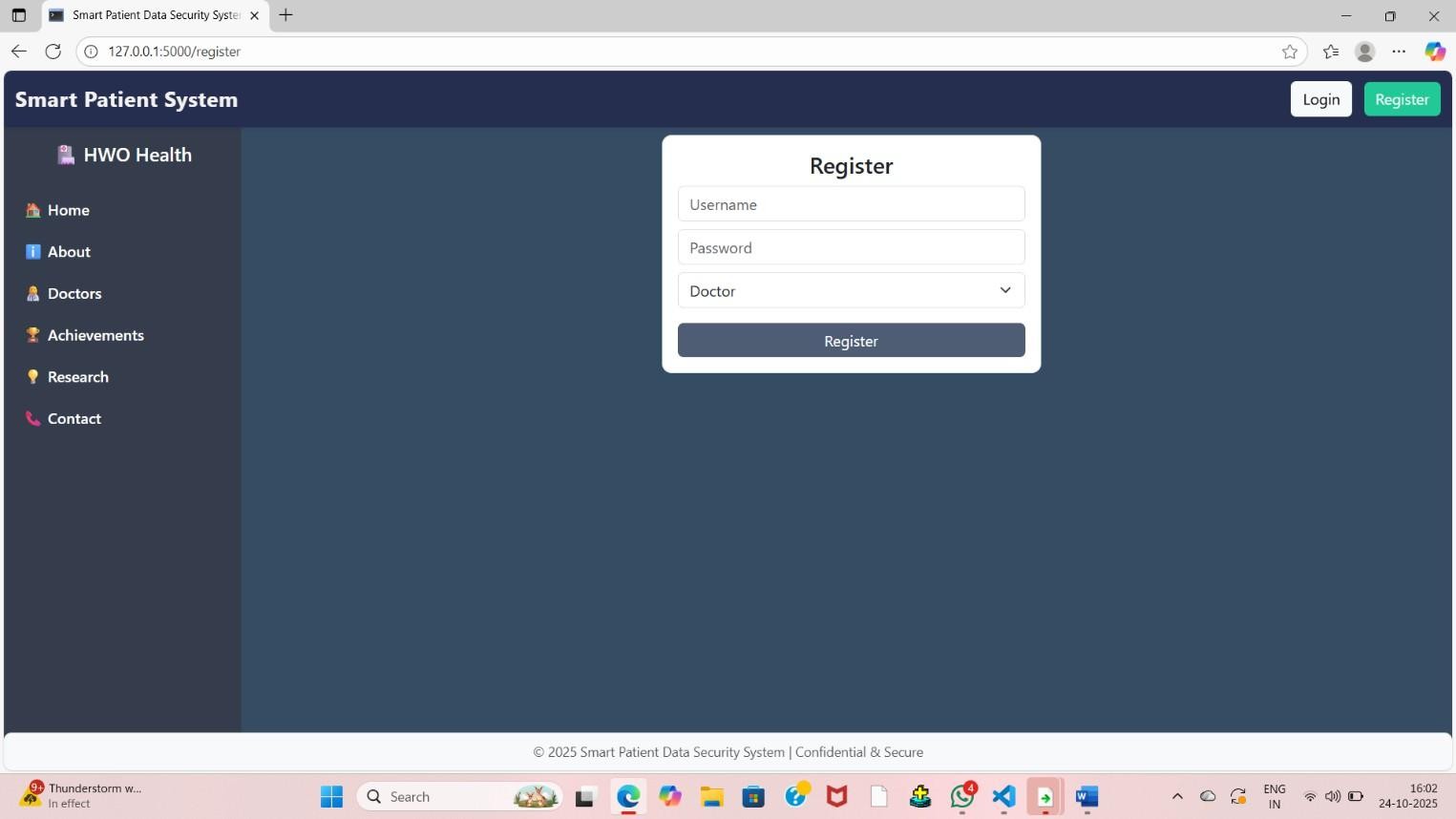
**Fig:A.8.1.Screenshot of basic home page**

****

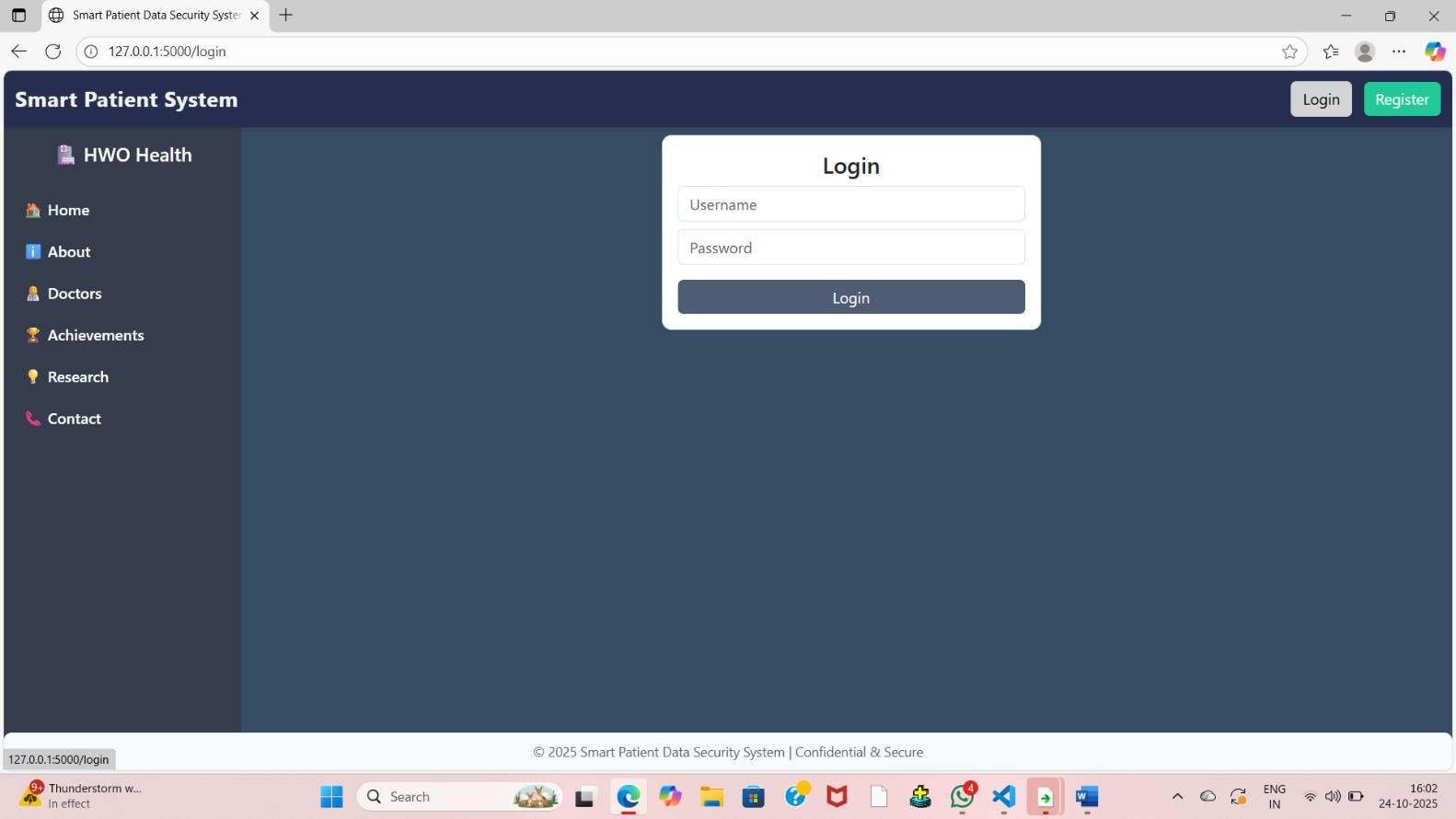
**Fig:A.8.2.Screenshot of about the hospital management**



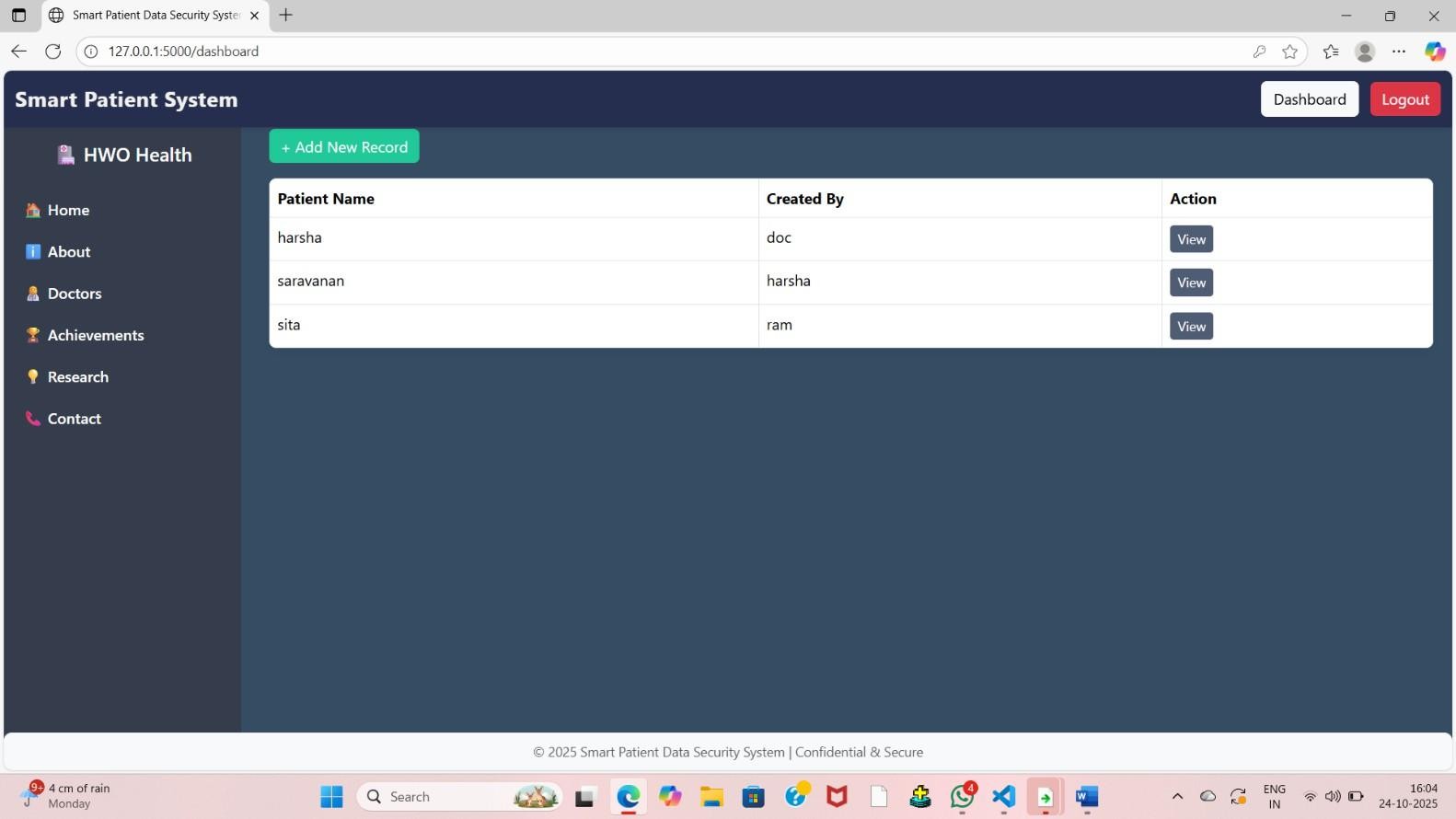
**Fig:A.8.3. Screenshot of contact details**

****

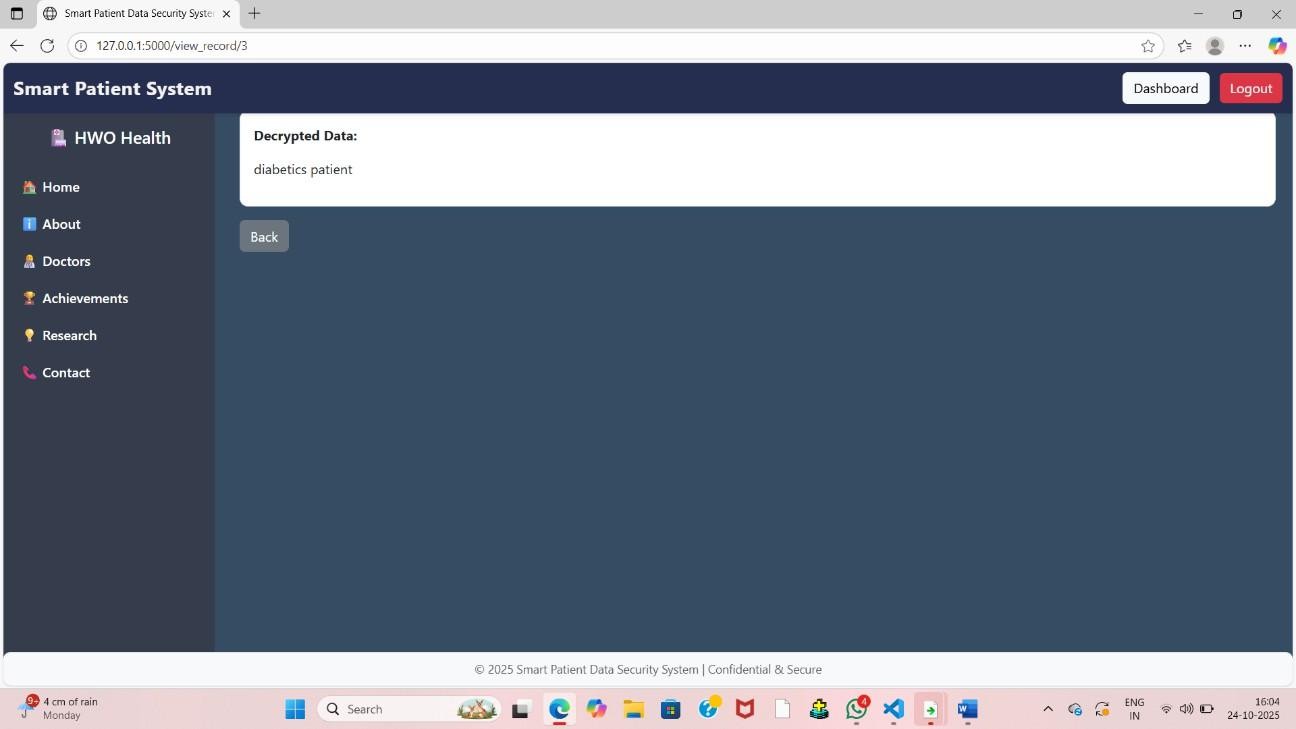
**Fig A.8.4. Screenshot of register page**



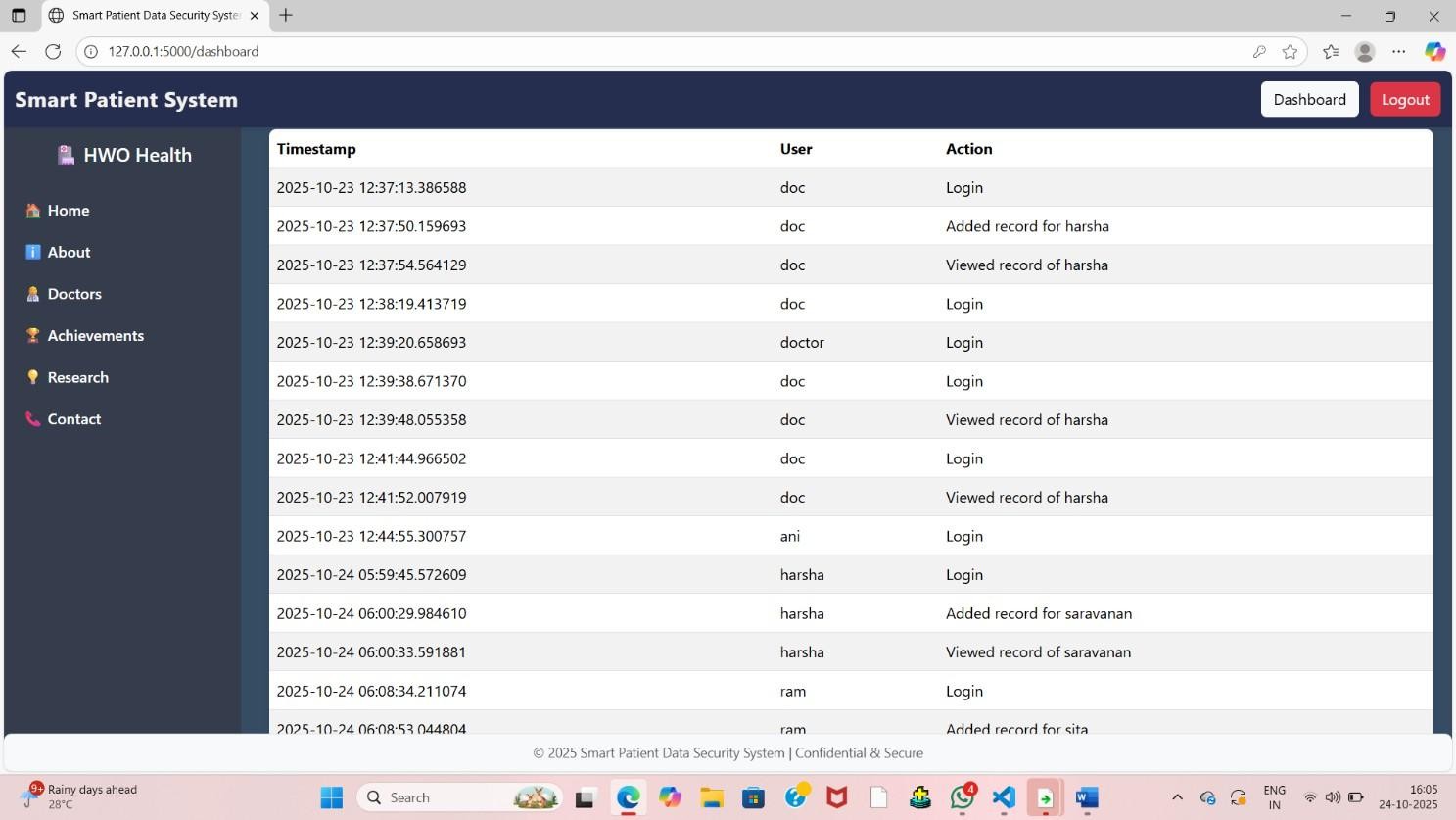
**Fig:A.8.5. Screenshot of login page**

****

**Fig A.8.6. Screenshot of add record page**



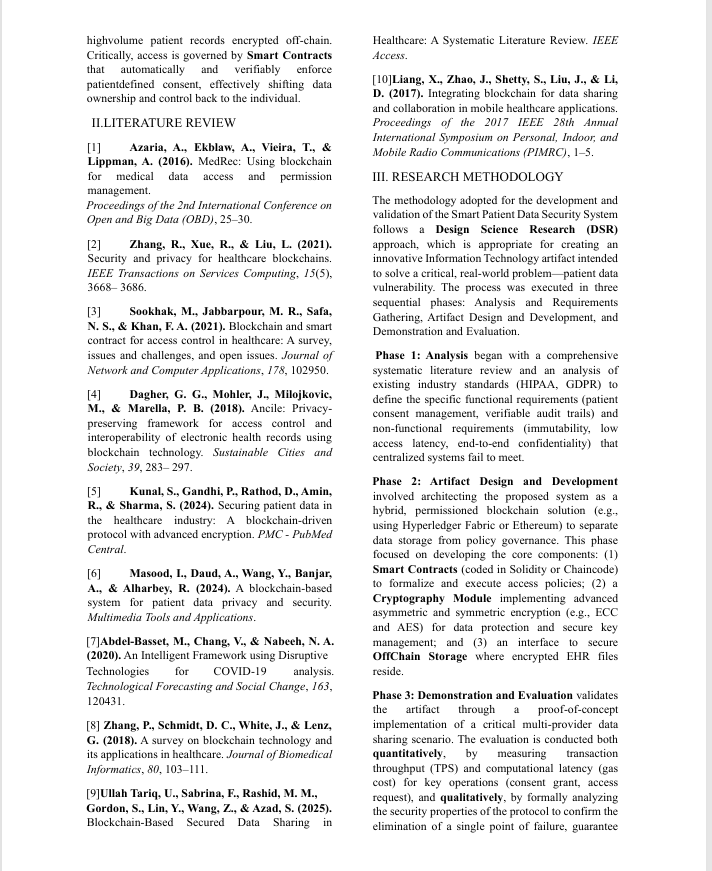
**Fig A.8.7. Screenshot of patient diagnosis info**

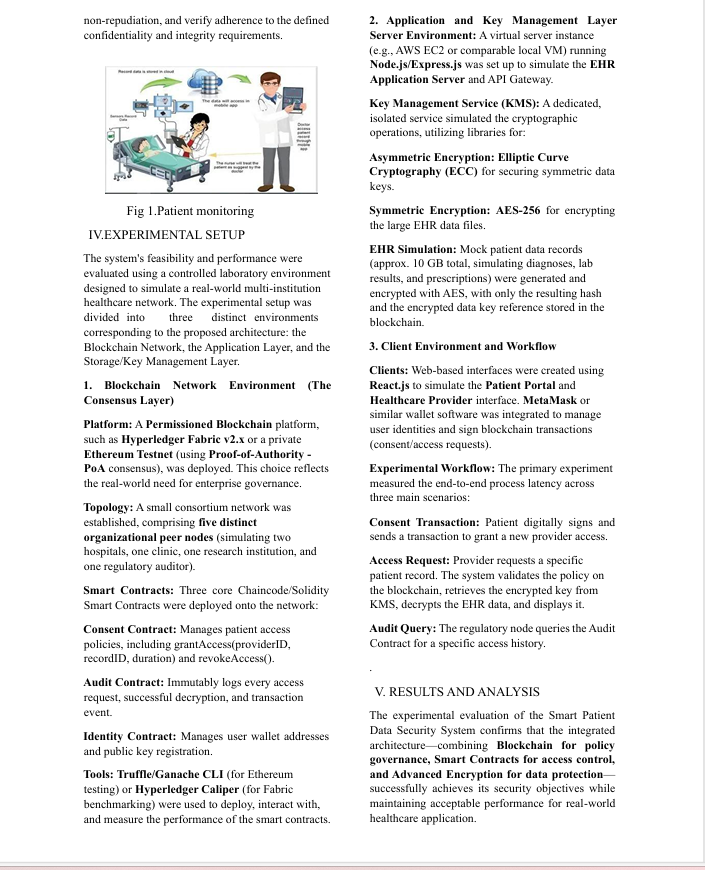
****

**Fig A.8.8. Screenshot of login history**

# A3. PAPER PUBLICATION

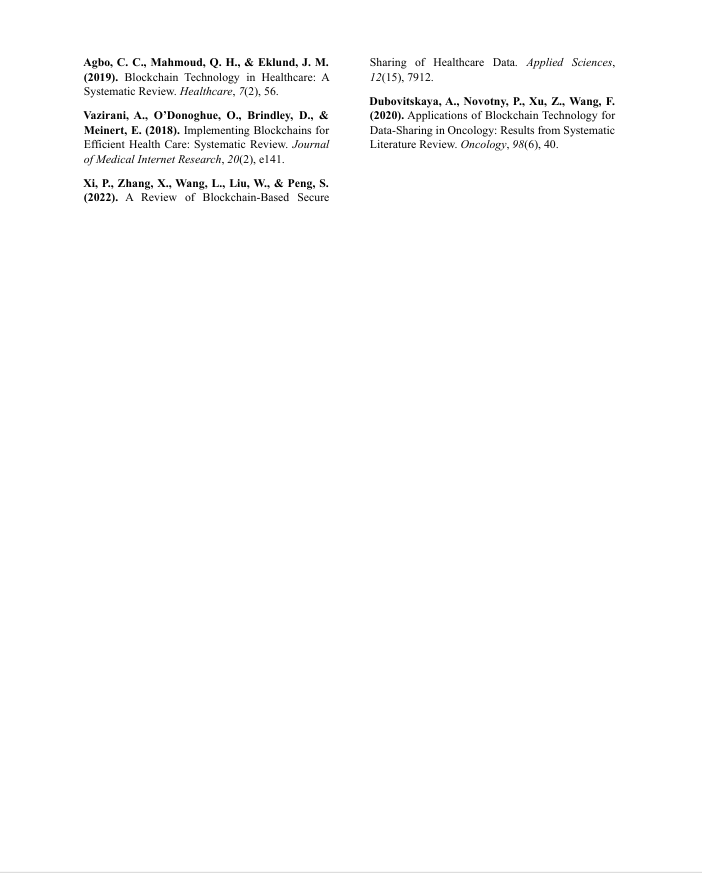
****

****

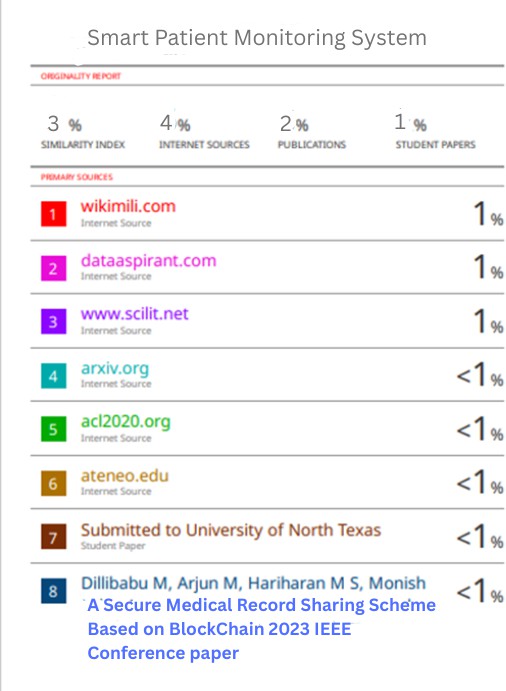
****

****

****



**A4. PLAGIARISM REPORT**

****

**CHAPTER 8**

# REFERENCES

 Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. In *Proceedings of the 2nd International Conference on Open and Big Data (OBD)* (pp. 25–30).

Relevance: This is a foundational paper that introduced one of the first patient-centric access control frameworks using the Ethereum blockchain and smart contracts, establishing the model for decentralized permission management in healthcare.

 Zhang, R., Xue, R., & Liu, L. (2021). Security and privacy for healthcare blockchains. *IEEE Transactions on Services Computing*, *15*(5), 3668–3686.

Relevance: Provides a comprehensive analysis of the security and privacy guarantees offered by blockchain in healthcare, discussing the integration of various cryptographic techniques (like anonymous signatures and Attribute-Based Encryption) with distributed ledger technologies.

Sookhak, M., Jabbarpour, M. R., Safa, N. S., & Khan, F. A. (2021). Blockchain and smart contract for access control in healthcare: A survey, issues and challenges, and open issues. *Journal of Network and Computer Applications*, *178*, 102950.

Relevance: Offers a detailed survey focusing specifically on smart contract-based access control methods in the healthcare domain, comparing them against traditional models and highlighting their ability to enforce patient consent automatically and immutably.

 Kunal, S., Gandhi, P., Rathod, D., Amin, R., & Sharma, S. (2024). Securing patient data in the healthcare industry: A blockchain-driven protocol with advanced encryption. *PMC - PubMed Central*.

Relevance: Directly supports the system's combined approach by proposing a highly secure patient-centric model that integrates blockchain with robust cryptographic algorithms (like ECC) for secure data encryption and verifiable communication.

* Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronichealth records using blockchain technology. *Sustainable Cities and Society*, *39*, 283-297.

Relevance: A key paper validating the framework for achieving both privacy- preserving access control and interoperability using blockchain, addressing two major, interconnected challenges in the modernization of EHRs.