

Blockchain-Based Secure Medical Record Sharing with Access Control

Gulrez Shabbir Sarankar¹, Shakila Siddavatam²

¹Master's Student, Department of Computer Science, Abeda Inamdar Senior college, India

²Head of Department, Department of Computer Science, Abeda Inamdar Senior college, India

Abstract:

Healthcare's move into the digital world means patient data is piling up faster than ever. The old way—storing everything in one central spot—just isn't safe. People can break in, mess with data, or snoop around where they shouldn't. That puts patients at serious risk. So, here's what this research brings to the table: a blockchain-powered system that locks down access to medical records. It tracks who's looking and who's not, and makes sure nothing gets changed without leaving a trail. Instead of keeping everything in a single database, this setup uses blockchain to spread out the responsibility. Access logs and permissions sit on the blockchain, making them nearly impossible to alter or fake. Testing happens in Ganache, which is just a handy local platform for building and checking smart contracts. Whenever a doctor adds or updates a record, the system creates a unique cryptographic hash and saves it on the blockchain. The real data stays elsewhere, referenced by this hash—so nobody can peek at private info by browsing the blockchain itself. It's like locking up the details in a vault, only handing out the key to people meant to see it. Patients and doctors need that hash to prove they're allowed in. No hash? No access. Smart contracts handle the permissions automatically—no middlemen needed, no delays, and no confusion about who's supposed to do what. Lots of other systems are all about storing data, but this one focuses on keeping access locked tight and giving control back to the patient. Patients stay in charge of their medical info. Blockchain adds transparency, cuts down on sneaky edits, and keeps a permanent, tamper-proof record of every change. Bottom line: this model ramps up security, keeps private data truly private, and helps everyone trust the healthcare system a bit more. With blockchain, cryptographic hashing, and smart contracts working together, it's a solid solution for keeping healthcare data safe and accessible only to the right people.

Keywords: Blockchain, Smart HealthCare, Data Security, Electronic Health Records (EHR), Cryptographic Hashing, Access Control, Smart Contracts, Ganache, Decentralized Systems, Patient Data Privacy

1. Introduction

Healthcare has gone digital fast, and Electronic Health Records (EHRs) became the norm. Doctors and hospitals can now pull up your medical history, diagnostic reports, prescriptions, and even scans with just a few clicks. It's efficient, sure—but honestly, all this data floating around online has its own problems. Security and privacy are big concerns. Healthcare systems usually keep everything on centralized servers, which makes them sitting ducks for hackers, data leaks, and outages. One mess-up and patient info is exposed.

A lot of researchers started looking at blockchain as a fix for this. Since blockchain doesn't rely on one single spot, and its records can't be altered, it gives solid protection and transparency. Azaria[1] and colleagues created MedRec a system where patients control who sees their records via smart contracts. Then Xia's[3] team pushed things further with MeDShare, letting providers share medical data safely while keeping privacy intact. Kuo's[2] work showed how blockchain boosts security, makes systems talk to each other better, and keeps patients in charge of their data.

But, let's be honest blockchain in healthcare isn't perfect yet. Most setups are hard to scale, don't let you access info in real time, and often aren't user-friendly. The tech is still kinda clunky, especially since not many have figured out how to blend blockchain with modern web tools, so both patients and doctors end up frustrated.

This research tackles that head-on. We're pitching a Secure Medical Record Sharing System that uses blockchain for security and combines it with full-stack web tech. The idea? Put cryptographic hashes on the blockchain, keep your actual records safe in the cloud, and control who sees what with smart contracts. This means patients can say "yes" or "no" to record access anytime.

1.1. Problem Statement:

Even though Electronic Health Records (EHRs) are pretty much everywhere now, most healthcare systems still stick to centralized setups. That means they're prone to data breaches, unauthorized access, and the dreaded single point of failure. Studies like MedRec[1] and MeDShare[3] show that blockchain can make healthcare data more secure and easier to share, but these early attempts run into real world problems—scalability, usability, and getting hospitals on board aren't quite nailed down yet. On top of that, patients don't really have much power over their own records, and sharing info securely across different providers is still a mess[2].

We really need a solution that's secure, decentralized, and puts patients in control. It should protect data, give users real authority over who sees what, and make sharing transparent. This research jumps in with a blockchain-based medical record sharing system, combining smart contract access control, secure cloud storage, and a web interface that's actually easy to use. It hands patients the keys to their own medical data, letting them manage and share their records without the usual headaches.

1.2. Secondary Data:

This research draws on existing work—scholarly articles, conference papers, and technical reports—centered on how blockchain fits into healthcare. I relied on studies like MedRec [1], which explores using blockchain for medical data access control, MeDShare [3], which looks at sharing data securely across cloud systems, and work by Kuo et al[2], who dig into blockchain's potential for boosting interoperability and security in healthcare.

I also pulled information from blockchain whitepapers, cryptographic security frameworks, and established models for healthcare data management. After digging into these sources, I found some clear problems: scalability issues, patients not having enough control, and systems just being hard to use. With these insights in hand, I focused on developing a medical record sharing system that's more secure, efficient, and puts patients at the center.

1.3. Proposed Solution:

This research introduces a blockchain-based system for managing healthcare data, designed to keep patient information safe and make sure only the right people can access it. The team built the system using Ganache, which lets them deploy and test blockchain apps on their own machines.[1]

Here's how it works: When a doctor uploads patient info, the system creates a cryptographic hash and saves it to the blockchain. The patient data itself stays off-chain. If anyone tries to change that data, the hash won't match anymore, so it's easy to spot tampering.[3]

To control who sees what, the system uses a hash-based access system. Only people with permission—like patients or doctors the patient has approved—can unlock the data with the right hash key. This setup keeps information private and locked down.[2][4].

Smart contracts handle who can do what automatically. Patients get the power to grant or remove access themselves. It's all managed right on the blockchain, so there's no need for a third party to step in or keep track of permissions.[6]

What sets this apart from other systems is the focus on secure access and hands-on control, not just dumping records into storage. Only verified users can get to sensitive records. Overall, this approach makes healthcare data safer, more trustworthy, and easier to manage.[5]

2. Literature Review

Researchers have been digging into how blockchain can strengthen healthcare systems—especially when it comes to keeping medical records secure, private, and easy to share.

Take MedRec[1], for example. Azaria and his team rolled out this early blockchain-based platform and let patients decide who gets access to their records through smart contracts. It boosted transparency and security, sure, but then they ran into trouble with scaling things up and making it work in real hospitals.

Then you've got Kuo's[2] work. He looked at how blockchain fits into biomedical and healthcare applications, pointing out that it makes data more secure, easier to work with, and less tied to one central hub. He argued it helps break away from those big, centralized systems—but stopped short of showing all the nuts and bolts of putting it into practice.

Xia[3] introduced MeDShare, a framework built to share medical data among cloud service providers, securely and without depending on a single authority. The system makes sure data stays trustworthy, but it's mostly about sharing—and doesn't handle user interaction or access control as smoothly as you'd hope.

Zhang's[4] research expands on the use of blockchain for things like data sharing, patient monitoring, and supply chain tracking in healthcare. It paints a wide picture, but skips out on the gritty details of managing secure access.

Looking across all these studies, it's clear that blockchain brings solid perks—security, transparency, decentralization. But the current systems aren't perfect. They struggle with scaling, don't always give patients enough control, lack slick modern interfaces, and still aren't fully looped into today's web tech.

That's why this new solution steps in, blending blockchain with cloud storage, smart contract-driven access control, and a web-based interface. The goal is pretty simple: make medical record sharing safer, easier, and actually usable for everyone.

3. Methodology (Development Process)

3.1. Design of Research:

We took a design-based approach to build a secure medical record sharing system with blockchain and access controls. The setup uses a full-stack architecture: React.js runs the frontend, FastAPI handles backend services, MySQL manages the data, and blockchain keeps everything secure and transparent.

We looked at systems like MedRec[1] and MeDShare [3], and pushed things further by adding cloud storage and smart contract-driven access control. That way, the system handles more users, works smoothly, and keeps data safe. To make sure it fits real healthcare use, we checked security, access control efficiency, and how easy it is for people to interact with.

3.2. Technical Research:

1. **Technology Analysis:** We looked at a bunch of frontend, backend, and blockchain tools—like React.js, FastAPI, MySQL, and Ethereum—to figure out which ones make sense for building a secure medical record-sharing system.
2. **Performance and Scalability:** Once we had our shortlist, we tested each technology for speed and scalability. We wanted to be sure the system stays fast and can handle more users and medical records without a hitch.
3. **Data Security and integrity:** To keep medical records safe and untouchable, we used advanced cryptography and blockchain hashing. This stops tampering and keeps the data solid.
4. **Access control mechanism:** For access control, we set up smart contracts so patients can easily let others view their records or take that access away whenever they want. This keeps data private and sharing secure.

5. **Efficient System architecture:** We built the system on a hybrid architecture, mixing blockchain with cloud storage. This combo gives us reliable data handling, quick processing, and smooth connections between the frontend, backend, database, and blockchain—all working together seamlessly.

3.3. Architecture of the System:

This system runs on a mix of technologies: the frontend's built with React.js, the backend uses FastAPI, and everything connects to a MySQL database. Medical files live in cloud storage, but their hashes get recorded on the blockchain for security. Smart contracts handle who gets access, making sure data sharing stays safe and straightforward.

4. Design And Implementation:

4.1. System Architecture:

Frontend (Clint side): The frontend's built with React.js, so it feels modern and easy to use. Patients and doctors can sign up, log in, upload records, ask for access, or check out shared data. Everything's pretty interactive, and the frontend talks to the backend using REST APIs.

Backend (Server Side): Python FastAPI runs the backend. It handles the heavy lifting—authenticating users, managing medical records, setting who gets access, and processing those API calls. It keeps everything secure between the app, the database, and the blockchain.

Database (MySQL): All the structured info—user data, patient record details, who has permission—is kept in MySQL. It's fast, reliable, and scales well if things get busy.

Blockchain (Ethereum): Blockchain's there to keep things trustworthy. Each medical record's cryptographic hash lands on Ethereum, so nobody can tamper with the data. Smart contracts control who can access what, and patients themselves manage permissions.

Cloud Storage (AWS S3): Actual medical files go up to AWS S3 for safekeeping. Only their hashes end up on the blockchain; that way, storage is efficient and costs stay low.

System Workflow:

1. The authenticated doctor uploads the patient's medical record through the system.
2. The record is securely stored in cloud storage, and its cryptographic hash is generated.
3. The hash is stored on the blockchain to ensure data integrity.
4. The patient can securely access their medical records through the system interface.
5. Access to records is controlled using smart contracts, ensuring only authorized users can view the data.

• System Architecture Diagram:

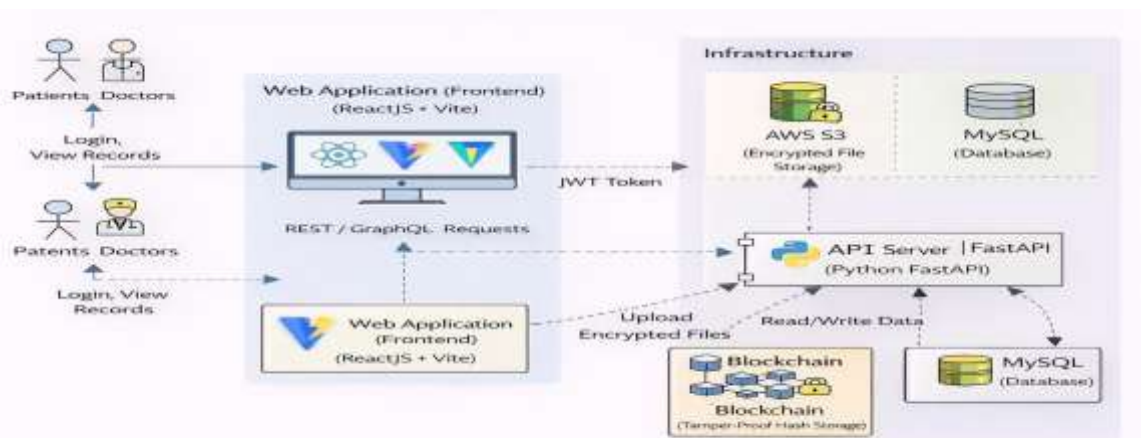


Figure 1: System Architecture of Smart HealthCare Medical Record

4.2. Technology Used:

The system brings together modern web tools and blockchain to make managing medical records both secure and efficient. On the front end, it runs on React. FastAPI takes care of the backend and keeps everything connected. MySQL organizes the structured data, while Ethereum's blockchain uses cryptographic hashing to protect data integrity. Smart contracts lock down access control so only the right people can get in. For the medical files themselves, the system stores them on AWS S3, so it can handle lots of users and keep things running quickly.

Table 1: Technology Stack for Smart HealthCare System

Component	Technology Used
Frontend	React.js, Tailwind CSS, HTML, JavaScript
Backend	Python, FastAPI
Database	MySQL
Authentication	JWT (JSON Web Token)
API Communication	REST APIs
Blockchain	Ethereum(Ganache-Local Blockchain), Web3.py
Smart Contracts	Solidity
Cloud Storage	AWS S3
Security	Cryptography (Fernet Encryption)

4.3. User Interface (UI) Screenshots

The Smart Healthcare Record Management System makes life easier for patients, doctors, and administrators. Its interface feels clean and simple—nothing complicated or cluttered. Navigation is smooth, and everything just works the way you'd expect.

Built with modern web tech, the system adjusts to any device. So whether you're on a desktop, tablet, or smartphone, the experience stays consistent. Features like uploading records, asking for access, or checking patient info are right up front. The whole setup is designed to keep things simple, clear, and quick. It delivers an easy, efficient experience, no matter who's using it.

The system provides multiple role-based interfaces to ensure smooth interaction between patients, doctors, and administrators:

- **Home Page:** The homepage is accessible to all users and provides an overview of the system along with options to register or log in.
- **Admin Login:** A secure login interface for administrators to access system controls and manage platform activities.
- **Admin Dashboard:** Allows the admin to monitor system performance, manage users, and oversee overall operations.
- **User Directory:** Displays a list of registered users (patients and doctors) with their details and status.
- **Doctor Approval:** Enables the admin to verify and approve registered doctors before granting system access.
- **Patient & Doctor Registration:** Allows new users to create accounts by providing necessary details.
- **Patient & Doctor Login:** A unified login interface for patients and doctors to securely access their accounts.
- **Doctor Add Medical Record:** Enables doctors to upload medical records such as prescriptions, reports, and diagnoses.

- **Patient Dashboard:** Allows patients to view their medical history, access shared records, and manage permissions.
- **User Profile:** Displays personal information and account details, allowing users to update their profile.

5. UI Screenshots:

The following figures show the Smart HealthCare Using Blockchain.

Figure 2: Home Page

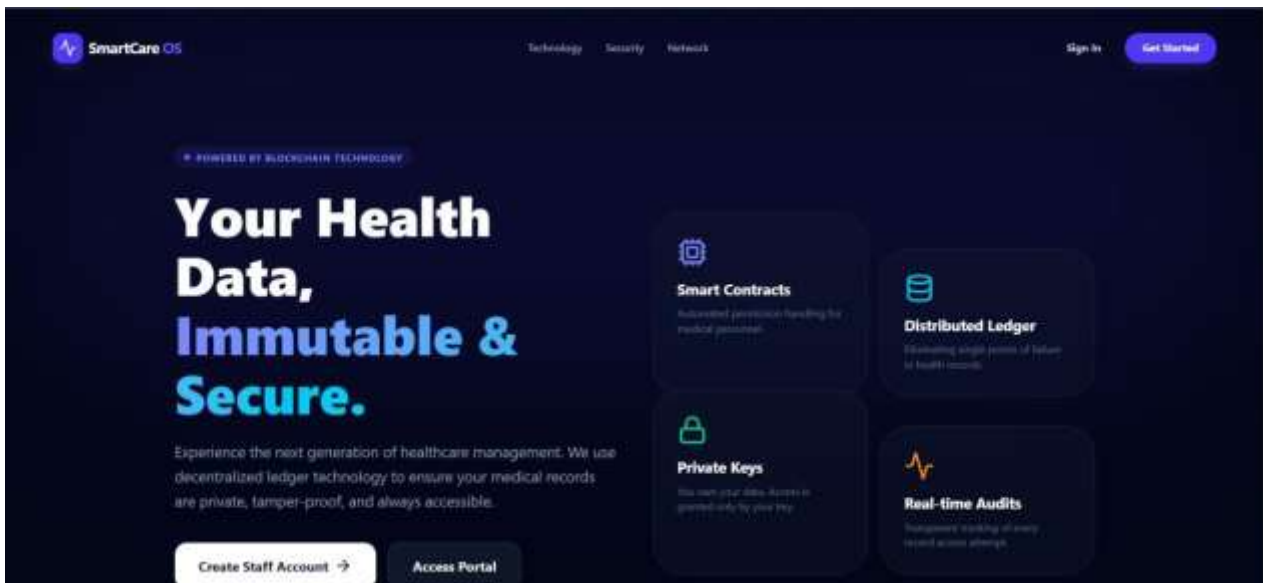


Figure 3: Admin Login:

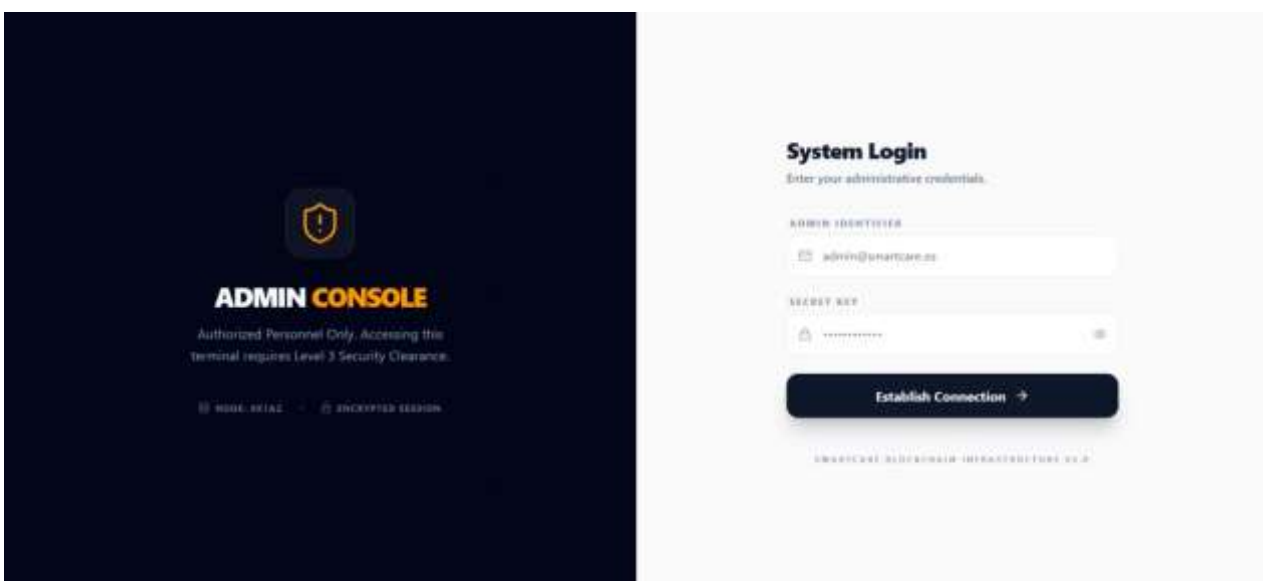


Figure 4: Admin Dashboard

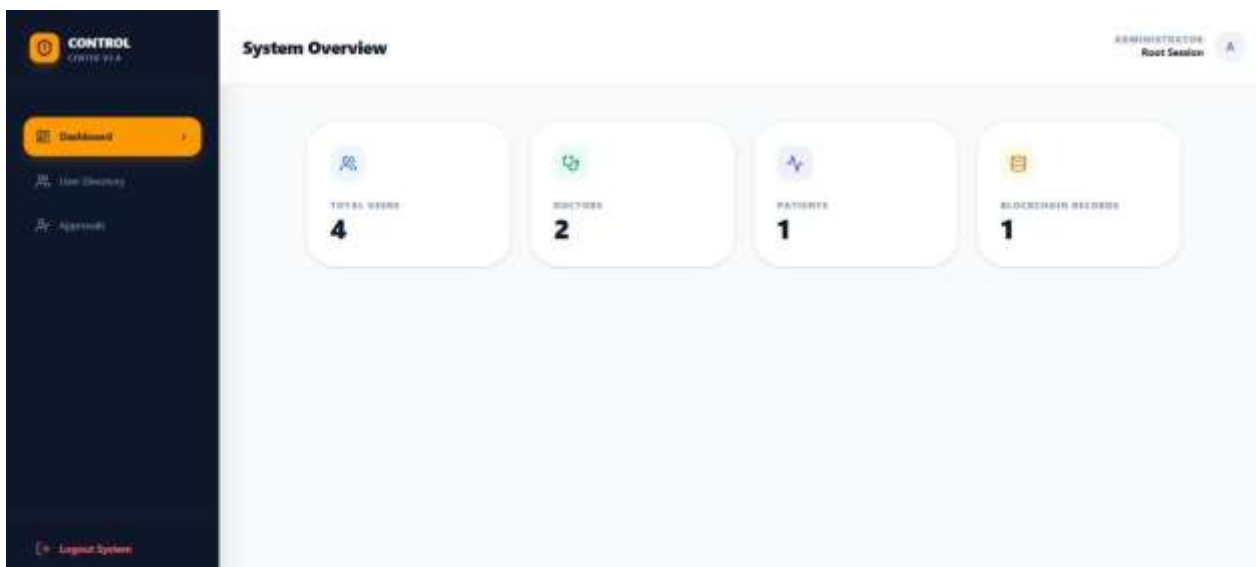


Figure 5: User Directory

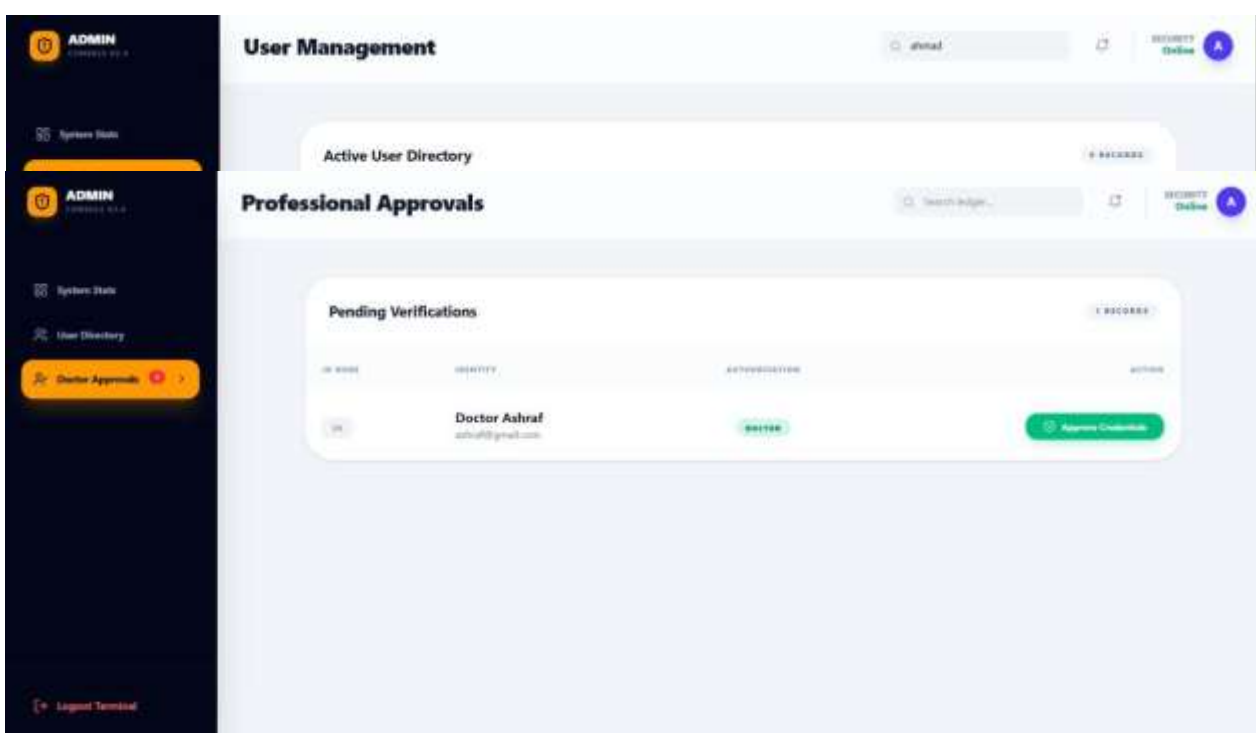


Figure 6: Doctors Approval

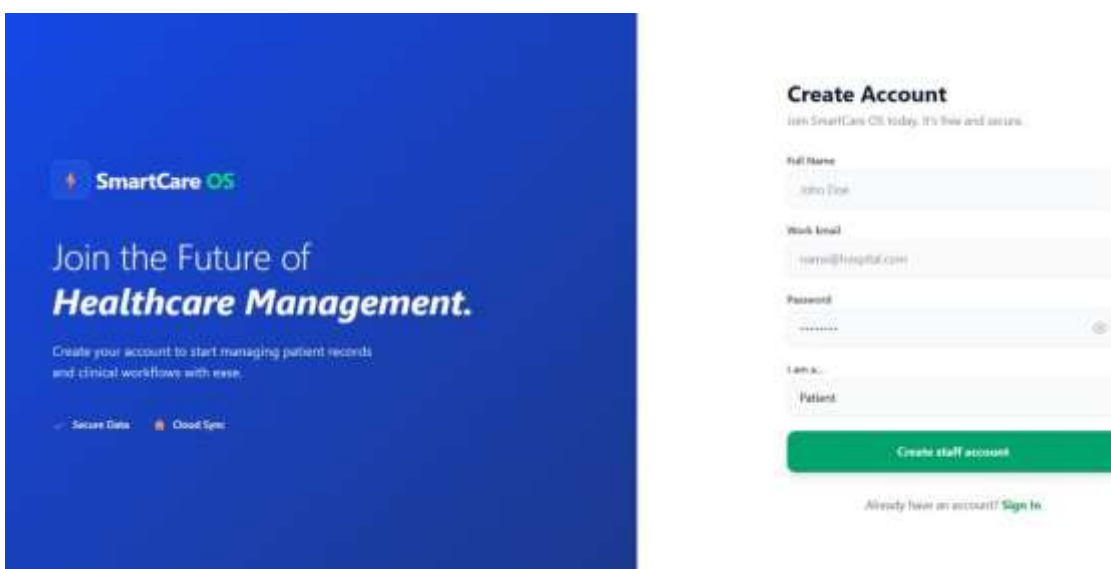


Figure 7: Patient & Doctor Register:

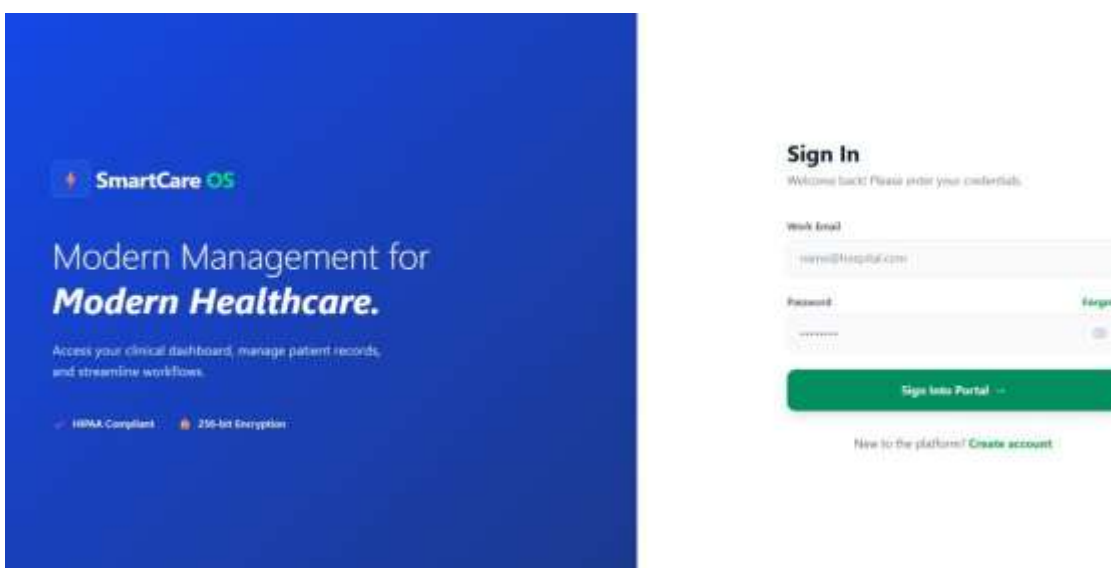
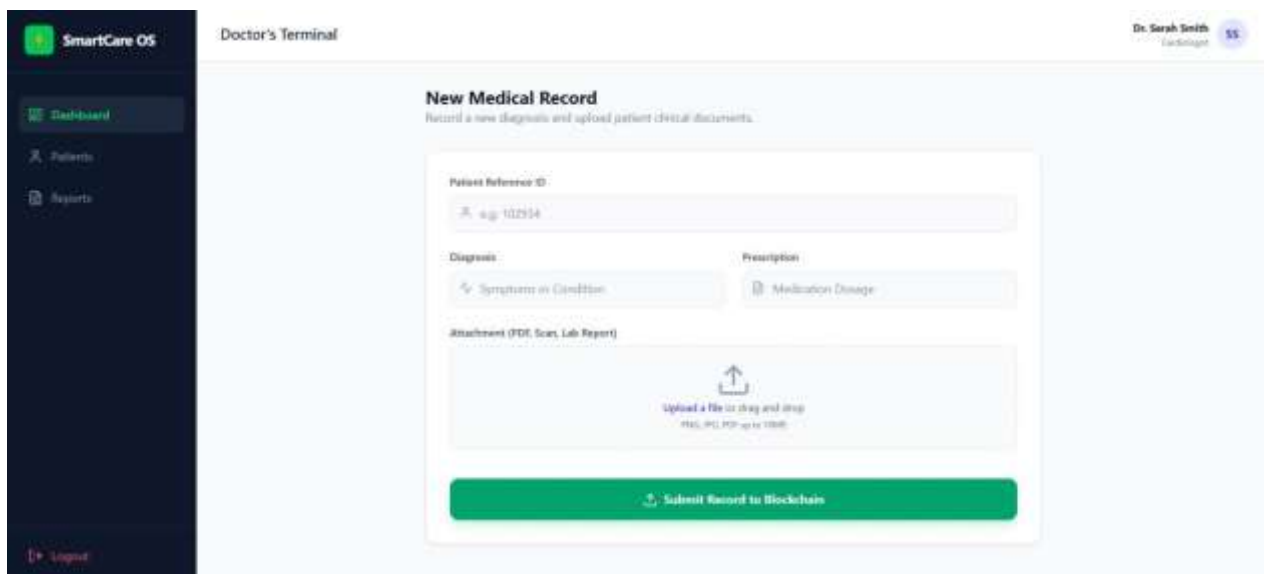
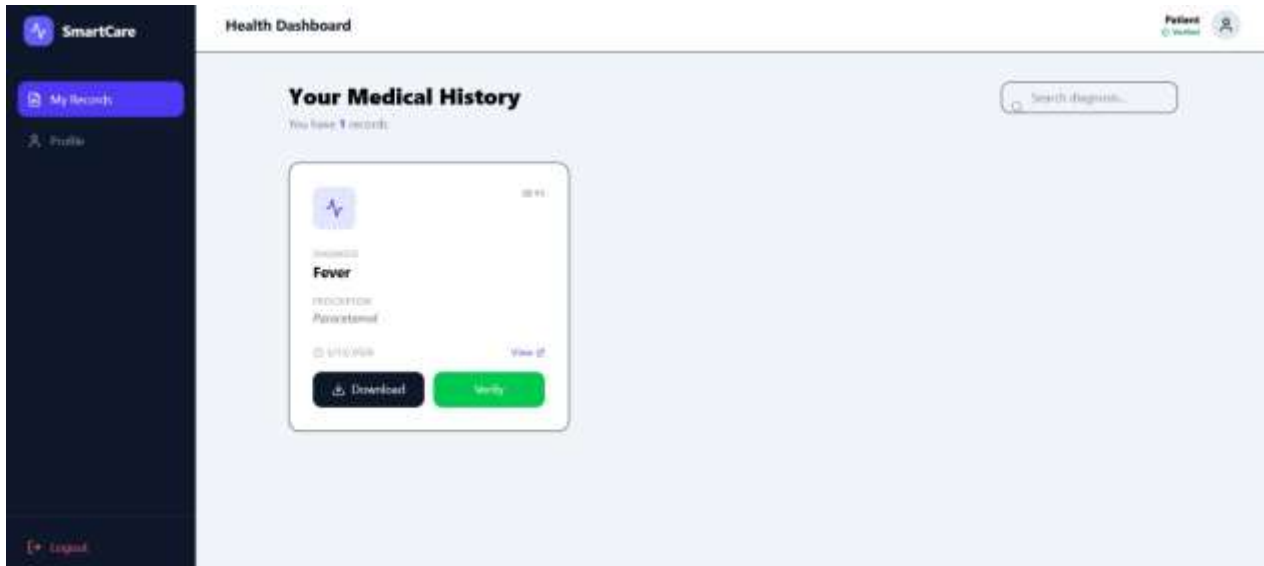


Figure 8: Patient & Doctor Login

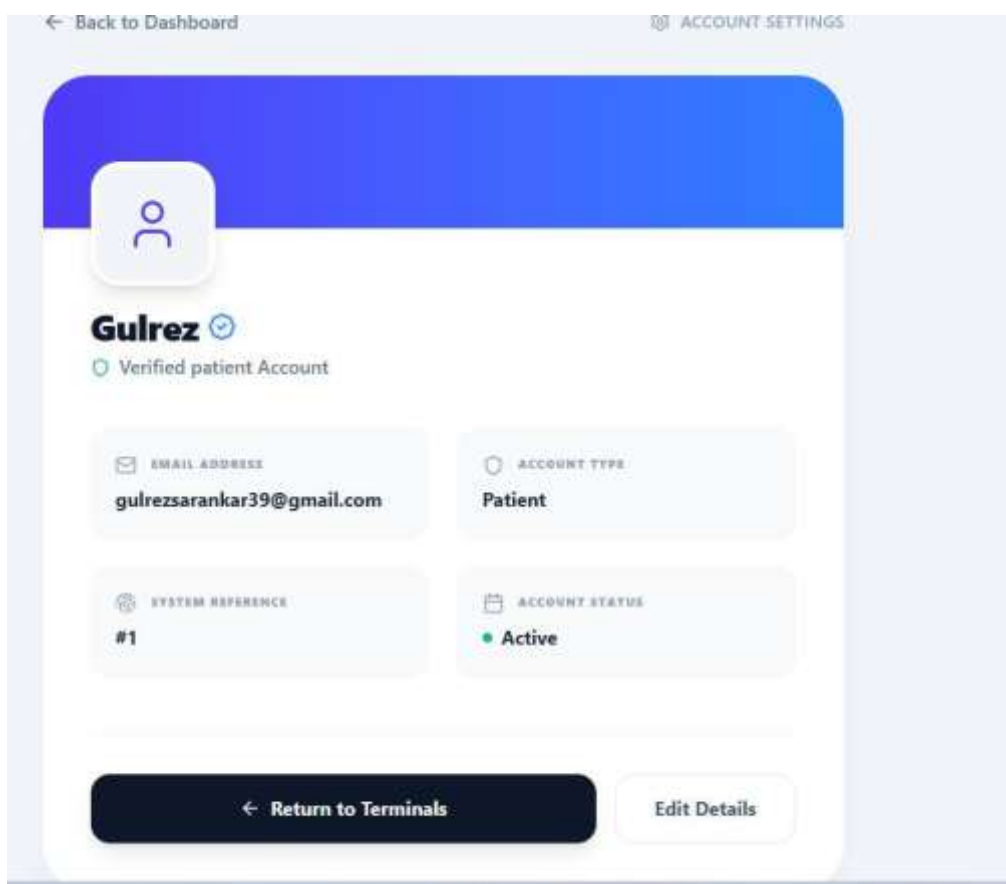
Figure 9: Doctor Add Medical Record

The screenshot shows the 'Doctor's Terminal' interface for 'SmartCare OS'. The user is 'Dr. Sarah Smith, Cardiologist'. The main section is titled 'New Medical Record' with the instruction 'Record a new diagnosis and upload patient clinical documents.' The form includes a 'Patient Reference ID' field (e.g., 102934), a 'Diagnosis' field (e.g., Symptoms on Condition), a 'Prescription' field (e.g., Medication Dosage), and an 'Attachment (PDF, Scan, Lab Report)' section with an upload icon and text 'Upload a file to drag and drop (PNG, JPG, PDF up to 10MB)'. A green button at the bottom says 'Submit Record to Blockchain'.

Figure 10: Patient Dashboard

The screenshot shows the 'Patient Dashboard' interface for 'SmartCare'. The user is 'Patient'. The main section is titled 'Your Medical History' with the text 'You have 1 records'. A search bar is labeled 'Search diagnosis...'. A card displays a medical record for 'Fever' with a 'Prescription' of 'Paracetamol'. The card also shows a date '10/10/2024' and a 'View' link. At the bottom of the card are 'Download' and 'Verify' buttons. The left sidebar has 'My Records' and 'Profile' links, and a 'Logout' button at the bottom.

Figure 11: User Profile



6. Discussion

6.1.Strengths of the System

- **Secure Data Sharing:** The blockchain keeps medical records safe. Nobody can mess with them or change anything behind your back.
- **Patient-Centric Control:** Patients get to call the shots. You decide who sees your data and when, thanks to smart contracts that put you in control.
- **Data Integrity:** With cryptographic hashing, if someone tries to alter your medical records, the system catches it right away.
- **Secure Data Sharing:** Doctors and patients can share medical records securely and quickly, without worrying about leaks or delays.
- **Transparency & Traceability:** All transactions are recorded on the blockchain, providing a clear audit trail of data access.
- **Scalability:** Every single transaction gets logged on the blockchain, so you always know who accessed your data and when.
- **User-Friendly Interface:** Using both blockchain and cloud storage means the system can handle tons of data without slowing down.
- **Reliability:** The interface is straightforward—anyone from patients to doctors to admins can figure it out without a headache.

6.2.Challenges and Limitations

- **Scalability Issue:** Scalability's a real problem. Blockchain can drag its feet when transactions start piling up, especially with big chunks of medical data flying around.
- **High Implementation Cost:** It's not cheap, either. Setting up blockchain tech and cloud storage can push development and operational costs pretty high.
- **Technical Complexity:** You need a tech team that knows their stuff. Integrating blockchain, smart contracts, and web tools isn't exactly beginner-friendly.
- **Latency in Transaction:** Transactions aren't instant. Compared to traditional centralized systems, blockchain can slow things down a bit—just enough to be noticeable.
- **Data Privacy Concern:** Data privacy sounds solid on paper, but if you mess up access controls, you could still let sensitive info slip out.
- **User Adaption:** Getting people onboard is another hurdle. Doctors, nurses, and patients might need proper training before they're comfortable using the system.
- **Dependence on Internet Connectivity:** Getting people onboard is another hurdle. Doctors, nurses, and patients might need proper training before they're comfortable using the system.

6.3.Future Scope:

- Looking ahead, there's a lot we can do.
- Linking up with national healthcare systems would let us share medical data securely on a larger scale.
- Smart contracts can get smarter too—more flexible, more automated when it comes to controlling who sees what. Building handy mobile apps would make everything easier for users to access.
- And bringing AI into the mix? That would give us sharper healthcare insights and help people make better decisions.

8. References:

References

1. Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A., "MedRec: Using Blockchain for Medical Data Access and Permission Management," IEEE Conference on Open and Big Data, 2016.
2. Kuo, T. T., Kim, H. E., & Ohno-Machado, L., "Blockchain Distributed Ledger Technologies for Biomedical and Health Care Applications," Journal of the American Medical Informatics Association, 2017.
3. Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M., "MeDShare: Trust-Less Medical Data Sharing among Cloud Service Providers via Blockchain," IEEE Access, 2017.
4. Zhang, P., White, J., Schmidt, D. C., & Lenz, G., "Blockchain Technology Use Cases in Healthcare," IEEE International Conference on Healthcare Informatics, 2018.
5. Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
6. Buterin, V., "A Next-Generation Smart Contract and Decentralized Application Platform (Ethereum Whitepaper)," 2014.
7. Antonopoulos, A. M., "Mastering Bitcoin: Programming the Open Blockchain," O'Reilly Media, 2017.
8. Dubovitskaya, A., et al., "Secure and Trustable Electronic Medical Records Sharing using Blockchain," AMIA Annual Symposium Proceedings, 2017.