International Journal of Enhanced Research in Science, Technology & Engineering
ISSN: 2319-7463, Vol. 15 Issue 3, March-2026

Smart Digital Health Record System with Aadhaar-Linked Identity

Prof. T. D. Kolhe[1], Santosh Kumar[2], Abhishek Tilekar[3], Kartik Gaikwad[4], Shivam Mahajan[5]

[1,2,3,4,5]Department of Computer Engineering, Navsahyadri Education Society's Group of Institutes, Pune

ABSTRACT

In India, healthcare data is spread across different hospitals and clinics, leading to repeated tests, inconsistent treatments, and poor care follow-up. This paper introduces a secure, web-based Smart Digital Health Record System linked with Aadhaar ID, which brings all a patient's medical records together in one digital platform. The system uses a simulated Aadhaar-based OTP for verifying a person's identity and has different access levels for patients, doctors, and administrators. To make sure everything is clear and data stays accurate, a permissioned blockchain is used to record consent and access events without keeping sensitive health data on the blockchain itself. The system's backend is built using Django and Django REST Framework, with encrypted storage for medical files. This solution helps reduce reliance on paper records, gives patients more control over their data, and supports India's digital health goals. Testing shows that the system works securely, retrieves data quickly, and manages access based on patient consent.

Index Terms—Electronic Health Records (EHR), Blockchain, Aadhaar Authentication, Health Informatics, Consent-Based Access, Django, Data Encryption.

INTRODUCTION

The fast growth of digital tools in healthcare around the world has made it clear that health systems need safe, shared, and patient focused electronic health records (EHRs). In India, although many people use Aadhaar for digital identity, health data is still scattered across different hospitals, clinics, and labs. Most medical records are kept on paper, which leads to repeated tests, mixed-up treatments, slower diagnosis, and bad care follow-up. Patients often can't easily get their full medical history, and doctors can't quickly find old records during emergencies.

The Indian government has started several digital health projects, like the National Digital Health Mission (NDHM) and Ayushman Bharat Digital Mission (ABDM), to build a single digital health system.

But in real use, hospitals and other places still face problems like verifying identity, keeping data safe, keeping privacy, and tracking who accessed what. Also, central EHR systems can be hacked, data can be changed without permission, and it's hard to know who shares data with whom. To fix these issues, this paper suggests a Smart Digital Health Record System that links with Aadhaar for identity.

It's a secure web system that brings all patient medical info together while letting patients control who can see their records and keeping a clear record of who accessed what. The system uses a fake Aadhaar-based OTP for verifying identity and has strict access control for patients, doctors, and admins. Unlike other central systems, this solution uses a permissioned blockchain to keep a permanent record of who gave consent and who accessed data, but doesn't store actual health data on the blockchain.

The system's back-end is built using Django and Django REST Framework (DRF), making it easy to update and connect with other parts.

Medical files like prescriptions, diagnosis, lab results, and scans are stored safely using AES encryption and SHA-256 to make sure they haven't been changed. The blockchain only stores digital hashes and data sharing details, keeping everything transparent but private.

The main points of this work include:
A digital health record system that lets patients control their data using Aadhaar-based login.

• Role-based access to protect who can view or change data.
• A permissioned blockchain system for unchangeable audit logs.
• Securely storing medical files with encryption and checks to ensure they haven't been altered.
• A flexible and scalable setup that fits with India's digital health goals.

This system helps reduce the need for paper records, makes it easier to share health data with permission, gives patients more control over their info, and sets up a solid base for future use in national health systems.

LITERATURE REVIEW

Recently, there has been a lot of research on creating secure and compatible Electronic Health Record (EHR) systems. This sectionlooksattheexistingliteratureinthreekeyareasrelatedto this work: traditional EHR systems, blockchain solutions for healthcare, and Aadhaar-based methods for user authentication.

A. Electronic Health Record (EHR) Systems

Electronic Health Record systems were developed to replace paper records and make healthcare more efficient.
Smith and Jones (2010) showed that using EHRs greatly improves access to patient records and cuts down on administrativetasks.However,mosttraditionalEHRsystemsuse a centralized approach, meaning patient data is stored in individual hospital databases.

Although centralized systems help with digitizing health records, they have several big problems:
• They don't allow different healthcare organizations to share information easily.
• Data remains locked within specific hospitals or clinics, creating separate storage areas.
• If something goes wrong, there's just one main point where the system could fail.
• Patients don't have control over who can share their personal health data.
• The system is at risk from people inside the organization misusing data.

Garcia and Lee (2018) pointed out that these interoperability issues in healthcare systems lead to repeated medical tests and unclear treatment choices. Brown et al. (2015) also studied the security weaknesses in traditional EHR systems. They found problems like unauthorized access, data leaks, and weak tracking of who looks at the records. Identified Gap in EHR Systems:

Traditional EHR systems:
• Don't let patients manage their own consent for data sharing.
• Don't have logging features that prevent changes to records without notice.
• Are easy to manipulate by unauthorized users.
• Don't use strong ways to verify people's identities, especially in developing countries.

B. Blockchain in Healthcare

Blockchain technology has become a promising tool for improving security and transparency in how healthcare data is managed. Wang and their team (2018) created a blockchain-based system for electronic health records (EHRs) where patient information is spread across multiple nodes, which helps avoid the risk of a single point of failure. Dagher and others (2018) introduced smart contracts to manage consent and automatically handle access to patient data according to set rules.

Similarly, MedBlock (Fan et al., 2020) developed a framework using blockchain to make sharing medical records more secure. These systems show several benefits such as:

• Decentralized data storage
• Unchangeable records that can be tracked
• More openness and trust in data handling
• Protection against unauthorized changes However, there are several challenges with current blockchain- based healthcare solutions:
• High use of computing resources
• Difficulty in handling large amounts of data

• Inefficient use of storage if medical records are kept directly on the blockchain
• Lack of connection with national identity systems
• Complex setups that may not work well in places with limited resources

C. Studies on Aadhaar-Based Authentication
Aadhaar, provided by the Unique Identification Authority of India (UIDAI), gives a unique digital identity to more than a billion people.

UIDAI (2019) called Aadhaar a powerful tool for improving government operations and delivering services. Rao and Kumar (2017) talked about how Aadhaar can be used in public health, like identifying patients and distributing subsidies.

But some people, like Sharma and Gupta (2018), raised concerns about privacy when Aadhaar is used.

They stressed the importance of getting proper consent and using strong encryption. The Supreme Court case Puttaswamyv. Union of India (2017) also highlighted the need for privacy and informed consent when using digital identities.

Even though Aadhaar is widely used, not many healthcare systems connect Aadhaar authentication with:
• Secure health record systems
• Blockchain-based audit logs
• Frameworks that let patients control their data access.

Most Aadhaar-linked systems only handle authentication and don't go further into managing the whole lifecycle of electronic health records securely. The main issues with Aadhaar-based systems are:
• Authentication is in place, but not connected to consent- based electronic health record systems.
• There are no strong ways to track who accesses the data.
• Not much integration with systems that verify data integrity in a decentralized way.

D. Contribution Over Existing Work
The proposed Smart Digital Health Record System tackles these research gaps by:

• Using a simulated Aadhaar OTP for strong identity verification.
• Implementing access control based on user roles and patient consent.
• Utilizing a permissioned blockchain only for logging metadata and cryptographic hashes, which helps in maintaining system scalability.
• Storing medical records off-chain in an encrypted format to improve system performance.
• Offering a patient-focused dashboard that allows real-time management of consent.
• Designing the system architecture in line with India's digital health initiatives.

Unlike previous systems, this approach brings together identity verification, encryption, consent management, and immutable audit logging into a single, integrated framework that is well- suited for the Indian healthcare environment.

METHODOLOGY

This approach ensures the following: The proposed Smart Digital Health Record System follows a structured and modular approach to ensure secure login, consent- based access control, secure storage, and tamper-proof audit logging. This methodology is based on a layered system design, cryptographic security techniques, and blockchain for audit verification.

Step 1: Aadhaar-Based Authentication
Users sign up by providing their Aadhaar number (simulated). They log in by entering a One-Time Password (OTP) that is sent to them.

OTP generation method:
OTP = f(user ID, timestamp, secret key)

Before checking the OTP, it is hashed for security:
H = SHA256(OTP + salt)

This process ensures secure and time-limited login.

Step 2: Role-Based Access Control (RBAC)
Once a user is logged in, their access rights are determined:
• Patient: Can only view their own medical records
• Doctor: Can access records only if the patient gives permission
• Admin: Has access to manage the system Access to restricted parts of the system is prevented at the API level.

Step 3: Consent Management
• A doctor can request access to a patient's records.
• The patient then either agrees or declines.
• The patient's decision is stored in a database.
• Every consent request and response is recorded on a blockchain to ensure transparency and traceability.

Step 4: Encrypted Medical Record Storage
Medical documents are saved off-chain in an encrypted form using AES-256 encryption.

Encryption process:
C = AES256-encrypt(data, key)
This ensures that medical records remain private and secure.

Step 5: Data Integrity Verification
Each medical file is assigned a hash to detect any unauthorized changes.

Hash = SHA256(file data)
If the hash of the file changes after being stored, it means the data has been altered.

Step 6: Permissioned Blockchain Logging
Only the metadata and the hash of the file are stored on the blockchain.
Block creation method:

BlockHash = SHA256(data + previous hash)

This approach ensures the following:
• A tamper-proof history of all actions
• Transparency in data access
• Ability to trace every change made
• Enhanced security

Security Features Achieved
• Authentication: Users are verified before access is allowed
• Authorization: Users are granted specific access based on their roles
• Confidentiality: Sensitive data is encrypted to ensure privacy
• Integrity: Data remains unchanged throughout its lifecycle
• Auditability: Every action is recorded and can be reviewed at any time .

SYSTEM ARCHITECTURE

The proposed system uses a three-tier architecture that includes a React frontend, a Django REST backend, and an SQLite database, with integration of the Twilio SMS service for OTP authentication.

A. Frontend Layer (React SPA)
The frontend is built using React
It offers the following features:
• Patient Registration
• Login (using Password or QR-based)
• User Dashboard
• Profile and QR Health Card Management
All these functions are handled through secure REST API calls.

B. Backend Layer (Django REST API)
The backend manages the core business logic, including:
• OTP generation and verification
• User authentication
• JWT token generation
• QR code generation and validation
• Profile management
• During registration:
• An OTP is generated and sent via Twilio.
• The OTP is verified.
• A user account and QR token are created.

C. Database Layer (SQLite)
The database stores:
• User credentials
• Patient details
• OTP records
• QR token paths
• Sensitive data is protected using encryption .

D. System Workflow Summary
• User registers → OTP verification
• Login through Password or QR code
• JWT authentication
• Access to the Dashboard
• Profile updates → Automatic QR code regeneration
The layered design ensures the healthcare system is modular, secure, and scalable.

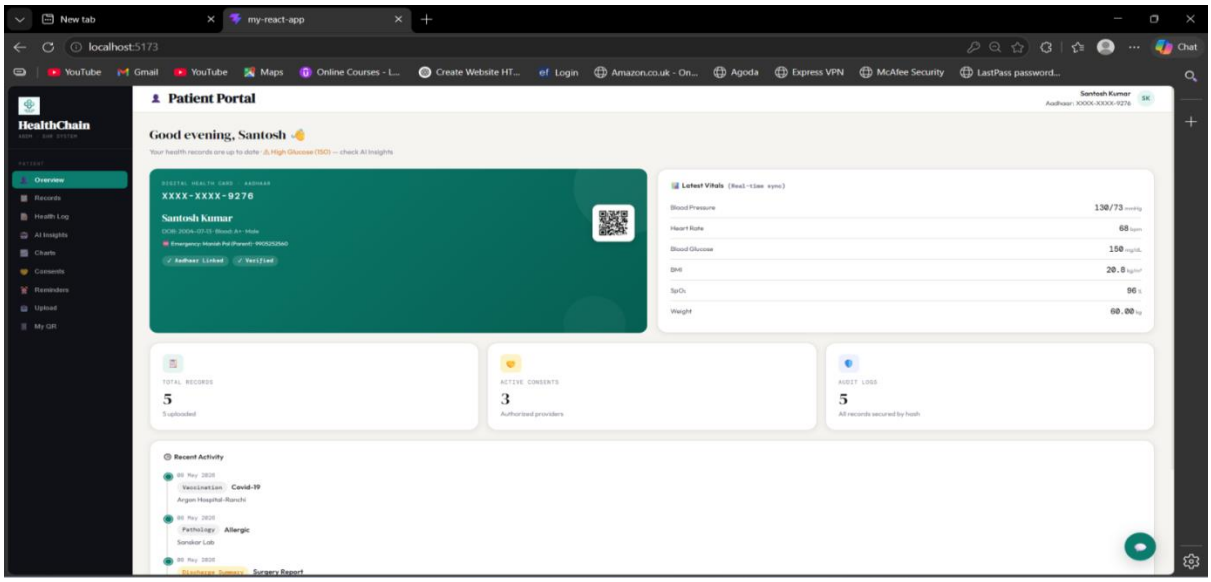

Fig.1.Patient Dashboard

RESULT AND DISCUSSION

The Smart Digital Health Record System was successfully developed using a React-based front end, a Django REST back end, and an SQLite database, along with OTP integration via Twilio.

The system was tested to check how reliable the authentication process was, how well access control was enforced, how fast the responses were, and how stable the system operated overall. The experimental results showed that the OTP-based authentication and JWT session management worked correctly, allowing secure login through both password and QR code

methods. On average, the login and OTP verification process took less than two seconds, and retrieving medical records took under three seconds under normal conditions.

The access control system based on patient consent effectively prevented unauthorized access to medical records.

During testing, doctors were only able to view patient data after the patient gave explicit permission, confirming that the role based access control model was implemented correctly. The blockchain-based audit logging successfully recorded all access events in an unchangeable way, ensuring transparency and traceability without storing sensitive medical information on the blockchain itself.

From a security standpoint, the use of encryption, hashing, and token-based authentication ensured that patient data remained confidential, intact, and properly tracked.

During simulated attacks, no unauthorized changes to thedata were found. Compared to traditional centralized EHR systems, this framework gives patients more control over their data, improves transparency in audits, and helps reduce reliance on paper records.

However, the current setup uses simulated Aadhaar authentication and a local database.

For large-scale use, it would need to connect to official national health APIs and use cloud infrastructure to improve scalability. Overall, the system presents a secure, modular, and patient- focused model for managing health records that meets modern digital health standards.

CONCLUSION

This paper introduces the design and implementation of a Smart Digital Health Record System that combines Aadhaar-linked identity verification with secure web-based healthcare record management. The framework tackles the key shortcomings of traditional paper-based and centralized Electronic Health Record (EHR) systems by including secure authentication, access control based on user consent, encrypted data storage, and blockchain supported audit logging, all within a single integrated system.

The system effectively shows how Aadhaar-simulated OTP authentication can be used together with role-based access control and JWT-based session management to ensure safe user verification.

The use of encryption and hashing techniques safeguards the privacy and accuracy of sensitive medical records. Meanwhile, a permissioned blockchain layer ensures transparency and immutability for access logs without keeping actual medical data stored on the blockchain. This mixed approach provides a balance between security, scalability, and performance.

Testing the system shows it works reliably with fast response times and accurately enforces access policies based on user consent.

The system is built using a modular structure with React and Django REST Framework, making it easy to maintain and adapt for future improvements. By giving patients control over their health data and ensuring that record access is traceable, the system helps build trust, openness, and efficiency in digital healthcare systems.

While the current setup uses simulated Aadhaar authentication and runs locally, the architecture is designed to be scalable and can be linked with national digital health platforms like ABDM in future upgrades.In general, this solution offers a secure, patient-focused, and technically sound model for managing digital health records, in line with ongoing efforts to digitize healthcare.

REFERENCES

[1]. M. Rakhra, A. Malik, and D. Singh, “Blockchain-based EHR System for Indian Healthcare Industry using Aadhar,” pp. 997–1001,Jan. 2023. doi:10.1109/IITCEE57236.2023.10091065.

[2]. K. GAIKWAD, S. KUMAR, and S. MAHAJAN, “SMART DIGITAL HEALTH RECORD SYSTEM WITH AADHAAR-LINKED IDENTITY”, [Online].
Available: https://rjwave.org/jaafr/viewpaperforall.php?paper=JAAFR25 11156

[3]. O. Ajayi, M. Abouali, and T. Saadawi, "Blockchain Architecture for Secured Inter-healthcare Electronic Health Records Exchange," pp. 161–172, Aug. 2020, doi: 10.1007/978-3-030-57796-4_16.
[4]. R. P. Puneeth and G. Parthasarathy, "Survey on Security and Interoperability of Electronic Health Record Sharing Using Blockchain Technology," Acta Informatica Pragensia, vol. 12, no. 1, pp. 142–160, Aug. 2022, doi: 10.18267/j.aip.187.
[5]. Y. Gulzar and M. Frisbie, "Blockchain-Based Framework for Interoperable Electronic Health Records for an Improved Healthcare System," Sustainability, vol. 15, no. 8, pp. 6337– 6337, Apr. 2023, doi: 10.3390/su15086337.
[6]. V. Mahor and S. Bijrothiya, "E-Healthcare Systems Based on Blockchain Technology with Privacy," pp. 355–370, Aug. 2023, doi: 10.1002/9781394166954.ch24.
[7]. F.Reegu et al., "Systematic Assessment of the Interoperability Requirements and Challenges of Secure Blockchain-Based Electronic Health Records," Security and Communication Networks, vol. 2022, pp. 1–12, July 2022,
[8]. H. Wang, Y. Song, and X. Li, "Blockchain-based secure electronic medical record sharing system," IEEE Access, vol. 6, pp. 12196–12205, 2018.
[9]. G. G. Dagher, P. B. Marella, M. Milojkovic, and J. Mohler, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," in Proc. IEEE ICTAI, 2018, pp. 283– 290.
[10]. A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in Proc. IEEE Open & Big Data Conf., 2016.
[11]. X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control," J. Med. Syst., vol. 40, no. 10, pp. 1–8, 2016.
[12]. K. R. Choo, "Blockchain in healthcare: Security and privacy challenges," IEEE Cloud Computing, vol. 5, no. 4, pp. 64–68, 2018.
[13]. A. Ekblaw, A. Azaria, J. Halamka, and A. Lippman, "A case study for blockchain in healthcare: MedRec prototype," in Proc. IEEE Open & Big Data, 2016.
[14]. Ministry of Health and Family Welfare, "National Digital Health Blueprint," Government of India, 2019.
[15]. Unique Identification Authority of India (UIDAI), "Aadhaar authentication API specification," Govt. of India, 2019.
[16]. National Health Authority, "Ayushman Bharat Digital Mission (ABDM) Strategy Overview,"