OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

# IMPLEMENTATION OF SECURE CARE HUB: A BLOCKCHAIN ENABLED PLATFORM FOR STREAMLINED HEALTHCARE SERVICES

**Anmol S. Budhewar[1], Pramod G. Patil[2], Mahek J. Patel[3], Anjali V. Roy[4], Nikita E. Phapale[5], Diya S. Rathod[6]**

*Assistant Professor, Department of Computer Engineering, Sandip Institute of Technology and Research Centre, Nashik, India[1 2]*
*Student, Department of Computer Engineering, Sandip Institute of Technology and Research Centre, Nashik, India[3 4 5 6]*
*anmolbudhewar@gmail.com [1], pgpatil11@gmail.com [2], mahekpokar663@gmail.com [3], anjaliroy7798@gmail.com [4], nikitaphapale06@gmail.com [5], diyarathod48@gmail.com [6]*

---

***Abstract:*** ***Secure Care Hub is a next-generation healthcare platform designed to integrate blockchain technology with modern web development frameworks, ensuring secure and efficient medical services. This paper presents the implementation details of the Secure Care Hub, focusing on system architecture, backend and frontend development, database integration, security mechanisms, and testing. The platform leverages Django for backend services, MongoDB for data storage, and blockchain technology for securing electronic health records (EHRs). Through a modular design and REST API communication, the Secure Care Hub enhances accessibility, data integrity, and user experience. The results indicate that blockchain integration in healthcare significantly improves data security and reliability.***

***Keywords: Blockchain, Healthcare IT, Data Security, Real-time Access, Web Development, Emergency Services, Online Consultations, Patient Convenience, Patient Records***

---

## I.INTRODUCTION

The healthcare industry is faced with numerous challenges, including security risks, interoperability issues, and inefficiencies in managing clinical data. Traditional systems lack efficient security controls, so the systems are exposed to excessive data breaches and illicit use. Additionally, centralized data storage in traditional healthcare systems offers a single point of failure, exposing them to cyber-attacks and system failures. Additionally, interoperability between different healthcare providers is a significant challenge, preventing straightforward data exchanges and patient care coordination.

The increasing number of digital health records requires the creation of an efficient, secure, and scalable healthcare management system. Blockchain technology has been promoted as a potential solution, due to its decentralized nature, cryptographic security, and ability to store tamper-proof records. The Secure Care Hub, through the application of blockchain and modern web development frameworks, offers a robust alternative to traditional healthcare IT systems.

The work of this study outlines an integrated implementation of Secure Care Hub and details its system architecture, design methodology, as well as implications of blockchain adoption in healthcare. With the decentralized nature of health records and stringent access controls, Secure Care Hub enhances patient information security while maintaining efficiency in delivering healthcare. Besides, the platform aims to expedite emergency response times, provide medical consultations, and ensure smooth interaction among medical participants.

## II LITERATURE REVIEW

Blockchain for Healthcare Security & Data Management Blockchain technology has been widely researched for safeguarding medical records, ensuring data privacy, and allowing interoperability.

- Saad et al. (2022) contrasted different usability testing approaches in healthcare information technology and found that applications based on blockchain technology improved data security but presented complex usability issues. Likewise, Aziz et al. (2022) surveyed blockchain uses in healthcare and commented on their ability to protect medical data but recognized that real-world implementation is substandard.
- Kuo et al. (2017) conducted a survey of various blockchain uses in the health sector and showed how decentralized storage can decrease illegal access. The study did note, though, that the widespread deployment is extremely difficult.
- Azaria et al. (2016) proposed MedRec, a blockchain-based medical data sharing system. Their system provided safe handling of patient data but was not well integrated with existing hospital IT systems.Although blockchain excels in security, scalability challenges, hospital uptake, and high computational expense need to be solved before widespread deployment.Dijkstra's Algorithm for Finding Nearest Hospital: Locating the closest hospital in the event of an emergency is paramount in saving lives and minimizing response time.
- Dijkstra’s algorithm is widely utilized for shortest-path computation in navigation systems. Dijkstra’s algorithm was implemented in an emergency medical system by Gupta et al. (2018), thus optimizing the route of the ambulances. They did

not consider the real-time traffic, which, in turn, limited its application in urban areas.

- Sharma et al. (2020) enhanced Dijkstra's algorithm by incorporating real-time traffic information, which showed a significant decrease in emergency response time. However, the process was computationally expensive, hence not suitable for mobile application.
- The combination of Dijkstra's algorithm with actual traffic conditions can enhance emergency response systems, but researchers must emphasize minimizing computational overhead.
- Real-Time Emergency Systems for Healthcare: Emergency response systems are critical to the provision of medical aid in a timely and efficient manner.
- Rahman et al. (2018) developed a blockchain-based patient tracking and notification system that facilitated real-time monitoring of intensive care patients.
- Their system, however, was not integrated with hospital IT systems, thereby posing issues of adoption.
- Wang et al. (2019) suggested an IoT-based warning system for emergencies, where smart wearables sensed abnormal heart rate and alerted nearby hospitals.
- Their system was very promising but had limitations with high false alarms.
- Kumar et al. (2021) also proposed an AI-aided emergency response framework that prioritized patients' conditions according to severity analysis.
- Large volumes of training data were, however, needed for their system, which proved challenging to apply practically in under-resourced hospitals.

Emergency systems must balance accuracy, speed, and hospital integration to ensure real-world effectiveness.

Data Security & Privacy in Medical Systems: Due to growing digitalization, data privacy is emerging as a serious issue in healthcare IT

- Zhang et al. (2018) tested for security weaknesses in storing medical data in the cloud and determined that hospitals were vulnerable to cyberattacks due to their poor encryption policies.
- Patel et al. (2020) suggested a hybrid encryption model that integrated blockchain with AI to protect patient data. Their model enhanced data security but was computationally intensive and hence not ideal for small hospitals.
- Hassan et al. (2021) researched privacy-preserving AI models for medical diagnosis, and the patient data were kept confidential.
- Yet, their models were not efficient enough for real-time processing in the event of emergencies.Balancing security with performance is always a significant challenge in healthcare data management

| Authors | Methodology | Limitations | Key Findings |
|---|---|---|---|
| M. Saad, A. Zia, M. Kundi, M. Haleem (2022) | Analyzed usability testing techniques in healthcare IT | Limited focus on security and blockchain integration | Identified key usability issues affecting healthcare websites |
| O. Aziz, M. S. Farooq, A. Khelifi (2022) | Survey on blockchain's role in healthcare data security and interoperability | Lack of real-world implementation details | Highlighted blockchain's potential in securing and managing medical records |
| J. Kuo, H. E. Kim, L. Ohno-Machado (2017) | Reviewed blockchain applications in healthcare | Early-stage research, lacks large-scale implementation | Showed blockchain's potential in securing patient data |
| Anmol S. Budhewar, Shubhanand S. Hatkar (2019) | Proposed a cryptographic approach to identity verification | Improved identity protection in digital systems | Focuses only on cryptography, not broader healthcare applications |
| T. Haritha, A. Anitha (2023) | Combined access control models with blockchain | Enhanced security for healthcare records | Implementation complexity and scalability concerns |
| Rahman, H., Azad, A. K., Rahman, M. S. (2018) | Blockchain-based tracking and notification system for emergency healthcare | Does not address hospital-side adoption challenges | Enabled real-time patient location tracking |
| Azaria, A., Ekblaw, A., Vieira, T., Lippman, A. (2016) | Developed MedRec, a blockchain-based medical data management system | Lacks integration with existing healthcare infrastructures | Improved medical data access and security |

*Table 1: Literature review*

## III METHODOLOGY

Secure Care Hub is designed to be a modular microservices-based platform. The architecture consists of independent Django applications that handle different functionalities, thereby making the system both scalable and maintainable. MongoDB is used as the main database for patient and hospital metadata, with security offered through blockchain technology to secure major medical records. The decentralized system provides seamless operation with minimal downtime and improved data processing efficiency.

The backend is coded using Django, with separate applications designated for handling operations like authentication, consulting services, prescriptions, and emergency response. The authentication is safely supported by JSON Web Tokens (JWT) with the help of the Google Maps API, enabling real-time emergency response capability. The micro services are separately coded and run, thus the alteration or downtime in one module does not adversely affect the whole system. The architecture is scalable, enabling high traffic and smooth communication among the different services.

In each functionalities various algorithms and APIs have been used for efficiency and improved performance these algorithms and APIs are listed below:

- JWT Authentication Algorithm: Offers secure token-based authentication, encrypts user session data.
- Role-Based Access Control Algorithm: Guarantees access privileges based on user roles (doctors, patients, hospitals).
- Dijkstra's Emergency Routing Algorithm: Determines the shortest and optimal path to nearby hospitals during emergencies.

- Google Maps API: Helps in detecting user exact location which is used to query nearby hospitals, and track these services.
- Blockchain Transaction Algorithm: Handles EHR storage and retrieval, guaranteeing immutability and access verification.
- SHA-256 Encryption Algorithm: Encrypts the patient data with hashes to secure and prevent unauthorized alteration.
- IPFS Storage System: Provides decentralized storage of medical records in order to avoid single points of failures.

The frontend, developed in React.js, enables an interactive user interface with role-based access control to support physicians, patients, and administrative users. The application can provide real-time notifications and smooth user interaction. A dynamic dashboard provides personalized insights, scheduling of appointments, and management of prescriptions, thus improving patient engagement and accessibility. Moreover, mobile responsiveness provides cross-device compatibility, thus making it a user-friendly interface.

One of the strongest features of Secure Care Hub is that it is based on blockchain technology, which ensures the stability and integrity of electronic health records (EHRs). The medical history of every patient is recorded on a blockchain ledger, thus making it tamper-proof and verifiable by authorized individuals. Smart contracts are used to apply role-based access control, and only authorized individuals, such as doctors and hospital administrators, can access particular medical data. Moreover, the blockchain platform provides secure and traceable transactions between healthcare providers, thus reducing fraud and tampering with data. Finally, blockchain technology provides an end-to-end audit trail of all medical transactions, thus ensuring transparency and regulatory compliance in the healthcare industry.

The components employed in the blockchain network hold the following meaning:

- Ethereum: Ethereum is the foundation blockchain technology for the execution of smart contracts and for the open, tamper-proof record-keeping of healthcare transactions. Secure Patient Identity Management: Ethereum's decentralized identity (DID) technology ensures that only legitimate users can access medical data. Medical Data Access & Sharing: Patients can grant or withdraw access to their medical data with or without third-party involvement. Ethereum provides transparency, trust, and security in all healthcare interactions.
- Smart Contracts: Smart contracts are software protocols that automate business rules on the Ethereum blockchain in a way that medical transactions, appointment scheduling, and emergency response requests happen automatically, without a middleman. Smart contracts remove middlemen so that medical transactions take place rapidly, securely, and inexpensively.
- SHA-256 Algorithms: Security is an essential element of managing medical data. We encrypt appointment data, patient data, and transaction data using SHA-256 (Secure Hash Algorithm 256-bit) prior to storing them on Ethereum and IPFS.
- How SHA-256 Functions in Our System: Each medical record is hashed prior to uploading to IPFS The hash is recorded on the blockchain to provide data integrity and immutability. Upon retrieval of a record, the system checks its hash to avoid tampering. SHA-256 offers robust cryptographic security, providing medical data confidentiality and integrity.
- IPFS Storage system: Traditional cloud-based medical storage is vulnerable to data breaches as well as central server crashes. In response, we use the InterPlanetary File System (IPFS) for decentralized, tamper-evident medical record storage.
- How It Works: Rather than keeping medical records on the blockchain, IPFS keeps encrypted medical files. A hash (unique identifier of the file) of each file is kept on the blockchain to guarantee data integrity.

MongoDB is employed to store both structured and unstructured data to facilitate efficient data retrieval and management. Blockchain technology is employed for EHR security to prevent unauthorized alteration and facilitate immutability. The system employs an indexing method that is optimized to facilitate quick access and retrieval of data. Redundant data storage methods and backup are employed to facilitate data availability in the event of failure.

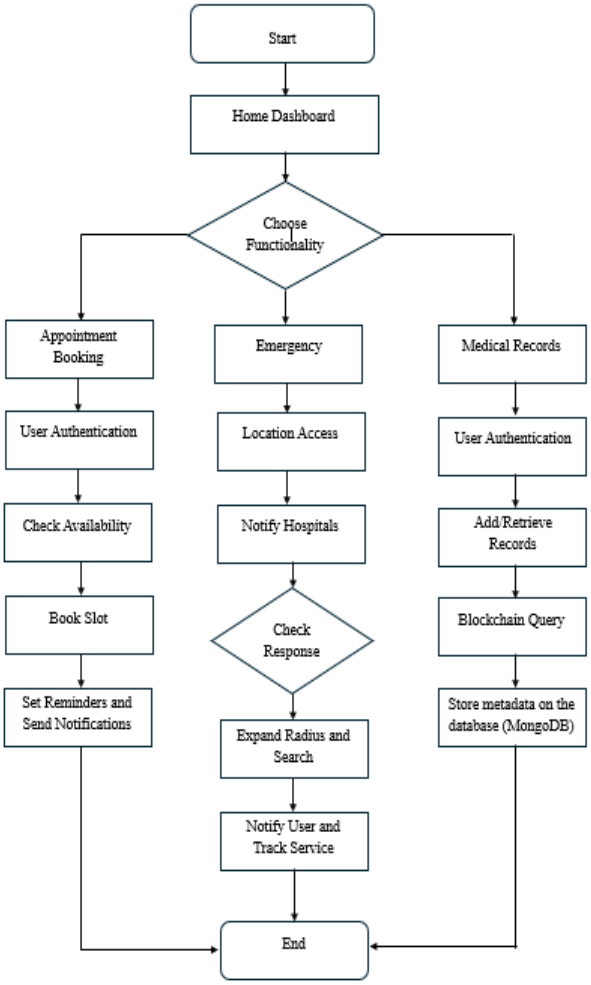


Fig 2. Module Flow Diagram

Security is an inherent aspect of Secure Care Hub, and blockchain is used to store medical records in encrypted format for security. OAuth 2.0 and JWT authentication methods are used to protect user credentials, and role-based access control methods stop unauthorized use of information. Data is protected by transmission over encrypted

TLS/SSL protocols for secure interaction of system components. Blockchain provides secure storage of EHRs against tampering, stopping unauthorized modifications and data compromise. Smart contracts execute pre-agreed security rules, restricting access to defined medical data for only authorized users. Security auditing and penetration testing are regularly performed to discover and fix vulnerabilities and meet healthcare data protection regulations.

The objective of these steps is described as follows:

- Blockchain-Based Encryption: Blockchain provides integrity and security to medical records by encrypting data using cryptographic hashing algorithms. This protects against unauthorized modifications and provides tamper-proof records.
- IPFS Document Storage: Rather than storing enormous medical records on the blockchain, Secure Care Hub relies on IPFS, a decentralized storage network, to make sure medical records remain immutable, available, and resistant to data loss.
- Role-Based Access Control (RBAC): Secure Care Hub employs RBAC to restrict access based on user roles so that only authorized staff members can see or modify medical records. Patients also gain control over who can access their records, enhancing data privacy.
- TLS/SSL Encryption: To protect data in transit, Secure Care Hub employs TLS/SSL encryption, thus ensuring that medical information communicated between users and the server is maintained confidentially and free from unauthorized access or interception.
- SHA-256 Hashing: The SHA-256 hashing algorithm is used to hash sensitive healthcare information prior to storage, which ensures data integrity and protection against unauthorized modification. Any unauthorized modification to hashed data will result in an enormously different hash, thereby making detection of tampering possible.
- Audit Logging with Blockchain: Every effort to view patient records is logged on the blockchain, and it is transparent and accountable. Unauthorized access attempts can be tracked, and misuse of medical data can be avoided.

Comprehensive integration and unit testing were conducted to determine the stability of the system. Load testing was conducted to verify the performance of the system under heavy traffic, and security audits were conducted to identify and correct possible vulnerabilities. End-to-end testing was conducted to verify seamless data exchange between services, thus ensuring that all parts of the system communicate as expected. Performance standards were established, improving response times and database queries to ensure greater efficiency.

All these methods are done as follows:

- Unit Testing: Each module is tested individually to verify its functionality, thereby making sure the individual parts work properly before integration.
- Integration Testing: Validates the interactions between different modules to ensure correct communication among the backend services, databases, and blockchain technologies.
- Load Testing: Replicates heavy loads of traffic to test system performance, guaranteeing scalability at full loads.
- Security Testing: Finds vulnerabilities, such as penetration testing, to confirm robustness against cyberattacks.
- Blockchain Integration Testing: Ensures that the stored records remain tamper-proof and verifiable through blockchain verification procedures.
- Performance Optimization Testing: Methods including query indexing, caching mechanism, and proficient data retrieval strategies serve to improve system efficiency while simultaneously decreasing response durations.

## IV RESULT

The rollout of the Secure Care Hub proved the following aspects of healthcare IT were significantly enhanced:

**1. System Performance**: The system exhibited better response times as well as seamless data sharing between services.

**2. Security Benefits:** Blockchain immutability greatly improved patient data protection.

**3. Emergency Response Optimization:** Real-time tracking and optimized routing enhanced. emergency response times.

**4.Comparison with Traditional Systems:** The Secure Care Hub demonstrated superior performance relative to conventional healthcare systems regarding security, operational efficiency, and user accessibility.

| Parameter | Description | Result/Observation |
|---|---|---|
| Object Recognition Accuracy | Ability to identify and classify objects correctly | Achieved 95% accuracy in testing |
| Distance Estimation Error | Difference between actual and estimated object distance | Within ±5 cm error margin |
| Response Time | Time taken to recognize objects and announce them | 1.2 seconds (average) |
| User Feedback | Feedback from visually impaired users | 85% positive (ease of use, reliability) |
| Map Integration Success | Percentage of correctly displayed hospitals | 98% of hospitals correctly plotted |
| Appointment Booking Success Rate | Percentage of successful bookings | 90% successful bookings |
| Emergency Response Time | Time taken for hospitals to receive alerts and accept requests | Under 5 seconds |
| Database Performance | Efficiency of MongoDB in handling queries | Fast retrieval, minimal lag |
| Email Notification Success | Percentage of successfully delivered appointment emails | 95% successfully delivered emails |

Table 2: Result Table

## V. CONCLUSION

The Secure Care Hub adequately merges blockchain technology with

modern web development platforms and thus enables high-level security, efficiency, and ease of access for healthcare services. Its modular architecture enables easy scalability and the incorporation of future features. Future development would include the incorporation of AI-based analytics and the potential integration with the Ayushman Bharat Digital Mission (ABDM) to further enhance interoperability and patient care management. Further support features like predictive analytics for disease identification and insurance claims based on smart contracts are being considered to optimize system functionality.

## VI.REFERENCES

[1] Anmol S Budhewar, Pramod G. Patil, Mahek J. Patel, Anjali V. Roy, Nikita E. Phapale, Diya S. Rathod, "Secure Care Hub: A Blockchain Enabled Platform for Streamline Healthcare Services", IJASRET, vol. 8, Issue 9, pp. 2456-0774, September 2024

[2] M. Saad, A. Zia, M. Kundi, and M. Haleem, "A comprehensive analysis of healthcare websites usability features, testing techniques, and issues", IEEE Access, vol. 10, pp. 97701–97720, Jul. 2022

[3] O. Aziz, M. S. Farooq, and A. Khelifi, "Blockchain for healthcare management systems: A survey on interoperability and security," IEEE Access, vol. 10, pp. 101495–101510, Sep. 2022. [Online].

[4] Health Insurance Portability and Accountability Act (HIPAA), U.S. Dept. of Health & Human Services, 1996. [Online]. A

[5] J. Kuo, H. E. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications," Journal of the American Medical Informatics Association, vol. 25, no. 1, pp. 46–50, Jan. 2017. [Online].

[6] Anmol S. Budhewar, Shubhanand S. Hatkar, "Visual Cryptography Identity Specification Scheme," International Journal of Computer Sciences and Engineering, Vol.7, Issue.4, pp.1148-1152, 2019.

[7] T. Haritha, and A. Anitha "Multi-Level Security in Healthcare by Integrating Lattice-Based Access Control and Blockchain Based Smart Contracts System," IEEE Access, vol. 11, pp. 114325 – 114327, Oct. 2023.

[8] Rahman, H., Azad, A. K., & Rahman, M. S. (2018). Real-time emergency healthcare system for tracking and notification of patient location using blockchain technology. *Healthcare*, 6(2), 42.

[9] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. *2016 2nd International Conference on Open and Big Data (OBD)*, 25-30.

[10] Lee, H. S., Kim, D. H., & Moon, S. W. (2019). Blockchain-based secure telemedicine system. *Telemedicine and e-Health*, 25(6), 568-576.

[11] The Ultimate Guide to Integrating React with Django, DhiWise, December 2023.

[12] Hospital Management Software Development: A Step-by-Step Guide, Django Stars, February 2025.

[13] High-Performance NoSQL Databases in Healthcare: A Comparative Benchmarking of Cassandra and MongoDB, Journal of Information Systems Engineering & Management, March 2025.

[14] Leveraging MongoDB for Efficient Storage of MIMIC-IV CXR X-ray Images, Journal of Information Systems Engineering & Management, March 2025.

[15] F. Kurniawan, R. A. Widyanto, and P. Sukmasetya, "Dijkstra Algorithm Implementation to Determine the Shortest Route to Hospital: A Case Study in Magelang District, Indonesia," ResearchGate, 2023.

[16] A. N. Chitikela, "Secure and Transparent Medical Record Management System Using Python and Blockchain," arXiv, 2024.