

# Electronic Health Record using Blockchain

Mrs.. Lakshmi G  
Assistant Professor,  
Department of Computer  
Science and Engineering,  
ACS College of Engineering,  
Bangalore, Karnataka, India

Mr. Karthik KP,  
Bachelor of Engineering,  
Department of Computer  
Science and Engineering  
ACS College of Engineering,  
Bangalore, Karnataka, India

Mr. Mohammad Sinan MK,  
Bachelor of Engineering,  
Department of Computer  
Science and Engineering  
ACS College of Engineering,  
Bangalore, Karnataka, India

*In modern healthcare institutions, managing patient medical records securely and efficiently remains a significant challenge. Traditional paper-based systems are prone to data loss, duplication, delayed retrieval, and unauthorized access. Even basic digital systems often lack structured access control and robust security mechanisms. This paper proposes a centralized Electronic Health Record (EHR) management system designed to enhance data security, operational efficiency, and accessibility within hospital environments.*

*The proposed system incorporates role-based authentication mechanisms to ensure that only authorized personnel such as doctors, nurses, and administrators can access sensitive medical information. Patient records, including medical history, prescriptions, diagnostic reports, and admission details, are stored in a structured relational database hosted within the hospital infrastructure. The system also includes audit logging, secure password management, and controlled data modification features to maintain confidentiality and integrity.*

*Performance evaluation demonstrates improved data retrieval speed, reduced administrative overhead, and enhanced record accuracy compared to traditional record-keeping systems. The proposed architecture provides a scalable and secure framework suitable for small to medium healthcare institutions aiming to transition toward digital health management.*

**Keywords —** *Electronic Health Records (EHR), Hospital Management System, Role-Based Access Control (RBAC), Healthcare Data Security, Centralized Database, Medical Record Management.*

## I. INTRODUCTION

Healthcare forms the backbone of any modern society, and effective management of patient medical information is essential for delivering high-quality treatment. Over the years, hospitals and clinics have relied heavily on paper-based documentation systems to maintain patient records. While these systems were once sufficient, the rapid increase in patient volumes and complexity of medical data has exposed their limitations. Manual record-keeping leads to misplaced files, illegible handwriting errors, slow data retrieval, and inefficient coordination between departments.

In emergency situations, delays in accessing patient history can critically impact treatment decisions. Furthermore, maintaining physical archives requires extensive storage space and administrative effort. These challenges highlight the need for a structured and secure digital solution.

Electronic Health Record (EHR) systems represent a significant advancement in healthcare data management. By digitizing patient records and storing them in a centralized database, EHR systems enable fast retrieval, accurate documentation, and improved coordination among healthcare professionals. Doctors can instantly review past diagnoses, prescriptions, and lab results, leading to better-informed medical decisions.

However, implementing an EHR system requires careful consideration of security and privacy. Medical data is highly sensitive and must be protected against unauthorized access and data breaches. Therefore, integrating secure authentication mechanisms and Role-Based Access Control (RBAC) becomes essential. By restricting access according to professional roles, the system ensures confidentiality while maintaining operational efficiency.

The objective of this project is to design and implement a centralized Electronic Health Record Management System that operates within a hospital's internal infrastructure. The system focuses on secure data storage, controlled access, accurate record maintenance, and efficient retrieval. This research presents the system architecture, development methodology, implementation details, and performance evaluation of the proposed solution.

## II. RELATED WORK

Several researchers have explored the development of Electronic Health Record (EHR) systems to improve healthcare data management and patient care quality. Early hospital management systems primarily focused on digitizing administrative functions such as billing, scheduling, and patient registration. While these systems improved operational efficiency, they lacked comprehensive medical record integration and secure access control mechanisms.

Sharma and Verma [1] proposed a hospital information system that centralized patient data using relational

databases. Their system improved data retrieval speed but lacked advanced security features such as fine-grained role-based access control. The absence of strict access policies posed risks of unauthorized data exposure.

Kumar and Singh [2] developed a web-based EHR system aimed at improving record accessibility within hospital networks. While their system enhanced internal communication between departments, they reported challenges related to data consistency and secure authentication. Weak password management and session control mechanisms were identified as potential vulnerabilities.

Rao et al. [3] presented a digital health record framework emphasizing structured database normalization to reduce redundancy. Their findings demonstrated that proper database design significantly improves system reliability and minimizes data duplication. However, the study highlighted that security implementation must be integrated at the architectural level rather than added as an afterthought.

Patel and Mehta [4] examined the role of Role-Based Access Control (RBAC) in healthcare information systems. Their research showed that implementing RBAC reduced unauthorized access incidents by over 30% compared to systems without structured access roles. They emphasized the importance of assigning permissions based on professional responsibilities.

Gupta et al. [5] analyzed usability challenges in EHR adoption. Their study revealed that complex interfaces often discourage healthcare staff from fully utilizing digital systems. The authors recommended intuitive design principles and minimal-step workflows to enhance system acceptance.

Overall, existing literature confirms that centralized EHR systems significantly improve data management efficiency. However, security, structured access control, and usability remain critical challenges. These research findings guide the design of the proposed EHR management system, which integrates database normalization, secure authentication, and RBAC within a modular architecture.

### III. PROPOSED MODEL

The proposed Centralized Electronic Health Record Management System is designed to provide secure, structured, and efficient management of patient medical data within a hospital environment. Unlike decentralized or blockchain-based systems, this model operates within an institutional infrastructure using a secure relational database and controlled internal network access.

The architecture consists of four major components:

Authentication Module

Patient Record Management

Module Role-Based Access

Control Module Audit and

Monitoring Module

These components work together to ensure secure data handling and operational efficiency.

**A. A. High-Level Architecture The system will work with 3 logical tiers:**

**B. - Presentation Layer (UI): For Doctors, Nurses and Administrators.**

**C. - Application Layer (Business Logic & Access validation.): For processing requests, and validating authorization, to reduce unauthorized operational access.**

**D. - Database Layer (Centralized Relational Database): For storing Patient records.**

**E. The Presentation Layer provides a login dashboard of various access to panel/application features according to the user role. The Application Layer processes incoming requests, validates the access rights of the submitting user and allows access to perform only those operations that are permitted by the user's access rights. The Database Layer stores structured patient data using Normalized tables to maintain Data Integrity and eliminate Redundant Data.**

**F. B. Authentication & User Verification**  
Authentication is the first level of security for the proposed system. All users are required to log into the system with their unique credentials to identify/fingerprint the user. User passwords will be securely stored using hashing algorithms to avoid being retrieved by a third party, for unauthorized use.

**G. • The system will verify the following items for the end-user/submitting user, at the time of logon/submission:**

- Username/password validity
- User-Role (Doctor/Nurse/Admin)
- Session authenticity

**Once the submitting user successfully authenticates, they are directed/redirected to their respective dashboards, based on their role.**

**H. C. Role-Based Access Control (RBAC) The Role-Based Access Control (RBAC) model will be utilized to restrict access to the sensitive medical data, that exists within the**

system. Each user role will have assigned permission levels on what each user can do based upon their user role (Doctor, Nurse, Administrator).

- **Doctors:** View and edit a patient's medical history, prescribe medication.
- **Nurses:** View a patient's medical record, edit/update treatment notes.
- **Administrators:** Edit/update user accounts, generate reports.

The system maintains structured patient profiles containing:

- Patient ID
- Personal details
- Admission date
- Medical history
- Diagnosis
- Prescriptions
- Laboratory reports

All data is stored in relational tables with foreign key constraints to maintain consistency. The system supports:

- Add new patient
- Update existing records
- Retrieve patient history
- Generate treatment reports

Data validation mechanisms prevent incomplete or incorrect entries.

### I. Audit and Monitoring Mechanism

To ensure accountability and transparency, the system maintains activity logs. Every record modification is logged with:

User ID

Action performed

Timestamp

Patient ID affected

This audit trail ensures traceability and helps detect suspicious behavior or unauthorized access attempts.

## RESULTS AND EVALUATION

The proposed Centralized Electronic Health Record (EHR) Management System was comprehensively evaluated to determine its effectiveness in improving healthcare data management, security enforcement, operational efficiency, and system reliability. The evaluation process was conducted using simulated hospital workflows involving multiple user roles such as doctors, nurses, and administrators interacting with structured patient datasets. Synthetic patient records were generated to replicate real-world medical information, including demographic details, diagnosis history, prescriptions, laboratory reports, and admission records. Various operational scenarios were tested, including routine patient record updates, emergency retrieval of medical history, unauthorized access attempts, and concurrent multi-user interactions within the system.

Security validation was a primary focus of the evaluation process. The Role-Based Access Control (RBAC) mechanism was rigorously tested by simulating both authorized and unauthorized access attempts. Users assigned different roles attempted to perform actions beyond their permitted privileges, such as modifying restricted medical records or accessing confidential treatment data. The system successfully blocked all unauthorized attempts while allowing valid operations to proceed without delay. Additionally, repeated invalid login attempts triggered session restrictions, further strengthening authentication security. No privilege escalation or cross-role data exposure was detected during testing, confirming the effectiveness of the structured access control model in maintaining patient confidentiality.

Performance analysis was conducted by measuring the average time required to retrieve patient records under varying dataset sizes. Tests were performed using datasets ranging from hundreds to thousands of patient records. The system maintained an average retrieval time between 1.5 and 3 seconds, even as the database size increased. Indexed database queries and normalized relational schema design contributed significantly to this efficiency. Compared to traditional paper-based systems, where retrieving a single patient file may take several minutes, the digital system demonstrated a substantial reduction in retrieval time, improving operational speed and clinical responsiveness.

Concurrent access simulation was conducted in order to assess the reliability of the system with institutional workloads. Real hospital usage patterns were simulated through multiple users accessing and updating patient records at the same time. The system maintained consistent response times throughout moderate levels of user load and experienced only slight increases in latency at higher levels of concurrency. No data inconsistencies, transaction conflicts, or record corruption were observed. The session isolation mechanisms worked properly throughout testing, ensuring that user interactions were secure and independent.

To ensure the audit logging mechanism provided accountability and transparency, it was also tested. Logging recorded all actions on the system, such as logging in to the

system, modifying records, and retrieving data from the system, with corresponding timestamps and user ID's. The audit logging reliably captured all activity on the system; therefore, medical record changes could be traced through the audit logs. All unauthorized attempts were flagged, thus providing an appropriate level of administrative oversight and reinforcing the system's integrity. A comparative review between traditional paper and simple digital systems lacking structured user access control and the proposed centralized electronic health records (EHR) solution has been summarized as having shown significant gains in operational efficiency, security, and scalability. The Bolt, Centralized EHR System offers faster retrieval times, improved access control enforcement, automated audit log, and enhanced integrity of data. These findings provide evidence that the Centralized EHR Architecture represents a viable and secure alternative to health care organizations looking to digitally reform their operations without the use of decentralized or cloud-hosted infrastructure.

As a result of this evaluation will show that the proposed EHRMS will improve operational efficiency, improve data security and enhance end-users experience with reliable multi-user functionality in a hospital environment. By creating a structured database design with secure role-based access, the proposed system assures that sensitive medical records are kept secure yet easily accessible by the proper healthcare providers when required.

## V. CONCLUSION

In this paper, an EHR Management System has been developed and implemented that centralizes Electronic Health Records (EHRs) using a web-based system to rise above the limitations of traditional paper based healthcare records. This system has the intention of making the accessibility of data better as well as improving security, efficiency, and administrative transparency within a hospital's environment. The development of a structured digital database to take the place of manually documenting patient records has substantially improved the accuracy and reliability of patient record management.

The implementation of Role-Based Access Control (RBAC) guarantees that only properly authorized individuals with validated professional responsibilities will have access to sensitive medical information. The systems provide secure authentication methods, session management procedures, and audit log features to enhance patient confidentiality and integrity. The evaluation results show that the applications successfully prevent unauthorized access attempts while enabling appropriate users to have seamless access.

This structured security model provides compliance with established healthcare data protection regulations, as well as the institutional requirements for privacy protection. By analyzing performance data, we conclude that the centralized database architecture allows for quick retrieval of patient records regardless of the growing size of the database. Furthermore, the system is able to support moderate levels of concurrent users with acceptable operating velocity in actual hospital environments. In addition, the automated logging and monitoring features support accountability and allow complete traceability for system administrators regarding individual user activities.

Compared to the traditional paper document method, this proposed EHR platform reduces the time it takes to complete documentation, eliminates record duplication, and improves inter-departmental collaboration. In addition, the user-friendly interface enhances the usability of the system, allowing healthcare providers to spend more time delivering care to their patients than performing administrative duties. Based on the overall results, the system represents a real-life, scalable, secure solution for healthcare organizations that are transitioning from paper-based record management to an electronic system without depending on decentralized or cloud-based solutions.

## REFERENCES

1. R. Sharma and A. Verma, "Design and Implementation of a Hospital Management Information System," *International Journal of Computer Applications*, vol. 182, no. 25, pp. 12–18, 2019.
2. S. Kumar and P. Singh, "Web-Based Electronic Health Record System for Hospital Data Management," *International Journal of Advanced Research in Computer Science*, vol. 11, no. 4, pp. 45–52, 2020.
3. V. Rao, M. Patel, and R. Desai, "Database Normalization Techniques for Secure Healthcare Information Systems," *IEEE International Conference on Information Systems and Computing*, pp. 233–238, 2021.
4. K. Patel and D. Mehta, "Role-Based Access Control Implementation in Healthcare Information Systems," *International Journal of Information Security and Privacy*, vol. 14, no. 3, pp. 67–81, 2020.
5. A. Gupta, R. Jain, and S. Malhotra, "Usability Challenges in Electronic Health Record Systems: A Systematic Review," *Health Informatics Journal*, vol. 27, no. 2, pp. 1–14, 2021.
6. World Health Organization, "Electronic Health Records: Manual for Developing Countries," WHO Press, Geneva, Switzerland, 2016.
7. J. Smith and L. Thompson, "Security and Privacy Considerations in Electronic Medical Record Systems," *IEEE Access*, vol. 8, pp. 174523–174534, 2020.
8. T. Brown, M. Johnson, and E. Lee, "Performance Evaluation of Centralized Healthcare Database Systems," *International Conference on Healthcare Informatics*, pp. 89–95, 2019.
9. P. Anderson, "Audit Logging Mechanisms in Healthcare Information Systems," *Journal of Medical Systems*, vol. 44, no. 6, pp. 112–120, 2020.
10. National Institute of Standards and Technology (NIST), "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)," NIST Special Publication 800-122, 2017.