International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 01 January 2026
Page No: 291-297
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0040

Secure Electronic Health Records for Personalized Patient Care

Sushil Kumar[1], Prof. Suchitra Saravanan[2], Pradeep H[3], Vidyashree K R[4], Srushti G S[5]
[1,3,4,5]Student, Dept. of Computer Science and Engineering, AMC Engineering College, Bengaluru, India
[2]Professor, Dept. of Computer Science and Engineering, AMC Engineering College, Bengaluru, India
Emails: *sushildudhani@gmail.com[1], suchitrasaravanan97@gmail.com[2], pradeepputtu4045@gmail.com[3], rudreshvidyashree@gmail.com[4], srushtigowda2511@gmail.com[5]*

Abstract

With the ever-changing landscape of healthcare today, there is a growing demand for effective, safe and patient-oriented approaches to managing health information. This project presents a secure electronic health record (EHR) solution that enhances the way that both patients and providers manage their health records. It centralises health data; supports the patient in controlling their own record; and contains advanced security features to eliminate data silos, increase the ability of patients to control what is shared with their providers and improve communication among providers. By using cloud computing, encryption, and access control the solution promotes patient engagement in their care, allows for better access to health information by patients and providers, and facilitates better clinical decision-making.

Keywords: *Electronic Health Records (EHR), Personalized patient care, Data security, Encryption, Patient Privacy, Access Control, Health Informatics*

1. Introduction

There is an urgent need for an effective electronic solution to bridge the gaps caused by current systems of healthcare communication that prevent the establishment of patient relationships with healthcare professionals through the barriers created by today's electronic storage of health records and the reduced access to one's health records; it will streamline and enhance the tracking and sharing of health information, provide immediate access to health information for patients, and facilitate the active participation of patients in their healthcare by ensuring a safe and secure means to manage their health data. Secure Electronic Health Records for Personalized Patient Care is a unique application designed to meet the above needs. The goal of this project is to establish a user-friendly, secure electronic bridge for communication and management of health information between patients and physicians. By using an electronic bridge, patients can participate more actively in their healthcare, and physicians can manage their patients' health information more efficiently.

2. Problem and Objectives

Our project seeks to improve healthcare outcomes through better Health Record Management and more personalised care using a safe, easy to use online platform that connects patients with physicians on one platform. We seek to fill the gaps that exist in today’s health information systems by emphasising patient privacy & data sharing, along with streamlining referrals and enabling better, more comprehensive patient-care. The objectives of our project are:

Secure and User-Friendly Digital Platform: Create a secure and user-friendly application for medical records management and healthcare provider-patient interactions, establishing fundamental security protections and a stable architecture.

Protected Patient Data Access: Establish an opt-in/opt-out model (permitted by both patient and physician) for the sharing of patient information between patients and physicians to allow patients to determine who has access to their medical history.

Robust Data Management for Medical Professionals: Develop/application tools (software) that will allow healthcare professionals to input, manage, and obtain complete and accurate patient data without creating interruptions to their work flow

Empower and Control Patients: Allow patients to determine who access their private health information

(PHI), gain patient consent prior to the sharing of their PHI, and develop a trust in the health care system through connectedness and transparency.

Decrease Administrative Burden: Automate all recordkeeping, appointment scheduling, and communication processes to provide medical professionals more time to care for patients through fewer distractions while providing a greater level of patient engagement and accountability.

- Once developed, our intention is to provide an application that will help connect users with providers regarding the management of their medical records. We will establish basic security protocols and into the foundation of the application's stability in order to facilitate ease of use for all users of the application.
- The ability for patients to access data that they own, while still protecting their sensitive private information, is a major focus of this research project. Therefore, this research project intends to provide patients with limited access to their data by only providing a summary of the patient’s history after being granted access (via opt-in).
- To provide robust data management for medical professionals. The objective of this proposal is to provide medical professionals with easy-to-use software applications that allow them to access, modify, and retrieve complex patient information (i.e., medical history, up-to-date health status, and patient treatment plans), which they can do with the highest level of security. Medical professionals will be able to accurately obtain patient data and be minimally disrupted while performing their professional duties.
- Objective to increase patient Empowerment and Control Over Their Data: One goal of this project is to allow users more control over who gets access to their private health information (PHI). By acquiring patient consent before distributing any PATIENT information, we will engender trust, facilitate transparency, and encourage effective decision-making concerning a patient's healthcare.
- Reduce the administrative stress on healthcare providers' office staff by using technology to automate these functions: record-keeping, assigning appointments, and corresponding with patients. As a result, the healthcare provider can devote more of his/her time to patient care.

3. Related Work

Strengthening Data for Secure Electronic Health Record System

The system uses a hybrid encryption model that combines AES-256-GCM for symmetric data encryption and public-key cryptography for secure key exchange. Each patient record is encrypted at the field level to ensure confidentiality and authenticity. This approach is based on key privacy principles [1]. and attribute-based hybrid encryption techniques. These methods include extra protection through key rotation and layered key management.

Building a Privacy-Aware Network for Data Sharing

A privacy-preserving interoperability layer allows secure data exchange between hospitals and patients while following HIPAA and GDPR rules. Data transfers use end-to-end encryption and identity verification to remove data silos and prevent unauthorized access. The framework is based on secure sharing methods in and anonymization techniques that rely on differential privacy [7].

Ensuring Transparency with Blockchain-Based Auditing

All data transactions are recorded on a blockchain-enabled audit ledger to ensure transparency and integrity. Each action, such as record creation, modification, or sharing, is timestamped, hashed, and digitally signed. This setup guarantees traceability and secure record management, as shown in [4].

Enforcing smart Access Control Policies

The system uses a combination of Attribute-Based Encryption (ABE) and Role-Based Access Control (RBAC) to control access. Only authorized users with the appropriate roles or attributes can decrypt certain data. This detailed access model enhances security and scalability based on the methods outlined in [8].

Empowering Patients through a Controlled Cloud Platform

The patient-centric cloud setup lets individuals manage their own Data Encryption Keys (DEKs) and sharing permissions. Patients can grant, restrict, or revoke access at any time, which ensures complete data ownership and trust. This model follows patient-controlled frameworks mentioned in [5].

Bridging Communication with an Interactive Health Portal

A secure communication interface connects doctors and patients through encrypted channels for consultations, notifications, and report sharing. Patients can access their records and manage follow-ups, which promotes transparency and engagement. This integrated design matches personal health record concepts and blockchain-backed verification discussed in [9].

4. Proposed Method

To address the issues of fragmented records, limited patient access, and poor communication in healthcare, this study suggests a secure, cloud-based Electronic Health Record (EHR) system. The approach ensures data privacy, accuracy, and accessibility. It also gives patients more control and lightens the load for healthcare providers. It combines encryption, access control, and blockchain-based auditing to form a dependable and unified healthcare platform [10].

User Registration and Login Security:

The system starts with the registration of patients, doctors, and administrators. It verifies these users through unique credentials and multi-factor authentication to ensure that only authorized individuals can access it. Role-based registration assigns specific privileges, creating a secure foundation for sharing information. This method supports Bellare et al. [1], who highlighted the importance of key privacy and identity protection through strong cryptographic authentication.

Encryption and Secure Data Storage:

All sensitive patient data, such as medical reports, test results, and treatment histories, is encrypted using the AES-256-GCM algorithm before being stored in the system's database. The encryption keys are managed securely to prevent unauthorized decryption or misuse. This setup follows the encryption and data privacy framework outlined by Jin et al. [2]. It ensures confidentiality and protection of electronic health information in cloud-based healthcare environments.

Blockchain-Inspired Audit and Traceability:

To maintain integrity and transparency, every user activity, such as data access, modification, and sharing, is recorded in a tamper-proof audit log. Each transaction is time-stamped, hashed, and cryptographically verified. This makes the system resistant to manipulation. This process follows Liu et al. [3], who showed how blockchain-based auditing can prevent unauthorized access and data breaches in distributed medical systems.

Attribute-Based Access Control(ABAC):

The system uses Ciphertext-Policy Attribute-Based Encryption (CP-ABE) to control access at a detailed level. Users can only see or decrypt information related to their assigned attributes or roles. For example, only a certified doctor can access certain medical records connected to their patients. This detailed control mechanism follows the work of Zhang et al. [4], who suggested ABE as an effective method for keeping electronic medical records private in healthcare clouds.

Cloud-Based Architecture and Scalability:

The platform runs in a secure cloud environment. This setup allows for scalability, reliability, and access across institutions. Encrypted data transmission through HTTPS/TLS protocols ensures safe remote access. Automated backup and recovery keep data available. This design follows Li et al. [5], who proposed a patient-focused and detailed access model for securely managing personal health records in multi-owner cloud environments.

Patient Access and Communication:

The system has a secure communication module that connects patients and healthcare providers with notifications and updates. Patients can view, manage, and share their medical records, choosing who can access their information. This encourages transparency and shared decision-making, as noted by Detmeretal. [6], who pointed out that personal health records are useful for patient-centred car.

5. Methodology

This application called "Secure Electronic Health Records. For Personalized Patient Care" Will be designed systematically, taking into consideration the important step and phases of development. Beginning with gathering requirement from stakeholders, constructing the design, with particular emphasis on a design for scalable and secure architecture, continuing to iterative system development which would include introducing security mechanism throughout and lastly, extensive testing and quality assurance would be conducted where applicable, along with methodical deployment approaches, and ongoing maintenance of the solution develop.

5.1 System Architecture

The system is designed for complex application security for patients (Figure 1).

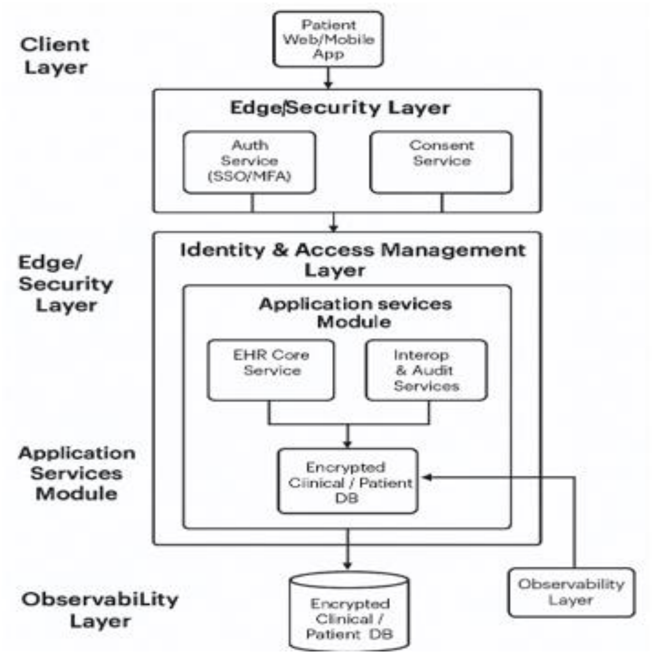

Figure 1 System Architecture for Secure Electronic Base Health Records for Personalized Patient Care

5.2 Requirements:

The Secure EHR system is meant to provide safe, reliable, and accessible healthcare data management for patients, doctors, and administrators. It requires strong authentication through SSO and MFA, consent-based data sharing, and full encryption of data in transit and at rest. The system must follow healthcare privacy standards like HIPAA or GDPR, maintain high availability, and support scalability for large user loads. Additionally, it should include audit logging, backup mechanisms, and observability tools to ensure data integrity, accountability, and ongoing monitoring.

5.3 System design:

This architecture employs a layered approach to ensure both secure and modular capabilities. The Client Layer provides secure ways to interact with web/mobile applications. Next, the Edge/Security Layer manages all aspects of authentication, consent verification, and secure/encrypted communications. The Identity and Access Management Layer is responsible for controlling user authorizations and enforcing Patient Consent-related policies. The Application Services Module manages electronic health record (EHR) data, supports electronic health record (EHR) interoperability and auditing of the EHR database, and all of these components are stored in a secure/encrypted database. Lastly, the Observability Layer provides tracking, logging, and reporting of system compliance to maintain system reliability/performance.

5.4 System development:

The implementation of a Modular Architecture in developing revolutionary digital health records allows for flexibility and scalability via Microservices Architecture. Leveraging Multiple Technologies such as Node.js, React, and Encrypted Database technologies provides safe and efficient operation. The use of CI/CD pipelines during development (e.g. using Continuous Integration to deploy applications into production) ensures key management, automates testing, and scans for vulnerabilities as they arise. Regular Backups, Compliance Checks, and Continuous Monitoring contribute to an increase in Data Security and Reliability. Ultimately, the Modelled Architecture will provide all the benefits associated with a Modular, Secure, and Monitored Model of Electronic Health Records (EHR) and will allow Healthcare Professionals to use this Model in their Daily Operations.

5.5 Flowchart

As depicted in Figure 2, The Monument Recognition and Historical Information Retrieval System identify monuments through image input and provides users with summarized historical information. The flow chart provides an overview of the process it uses to operate in real time.

User Authentication and Access:

The process starts when a user, either a patient or a doctor, logs in through the front end. Once the system verifies the user's credentials, it generates a secure JWT token and saves it in local storage to keep the session active.

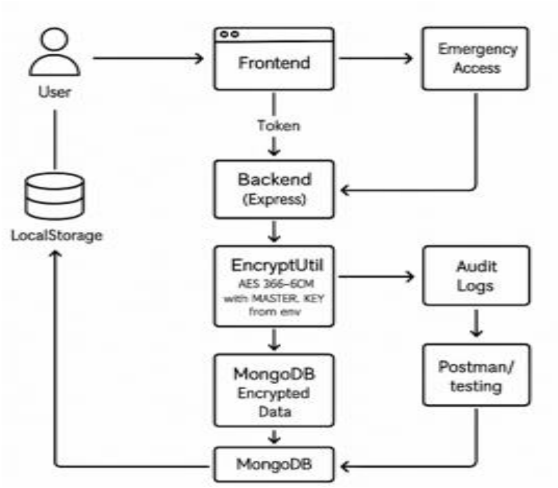

Figure 2 Process Flow for Personalized Patient Care

Frontend Request Handling:

After logging in, the frontend (web or mobile) sends encrypted requests and the stored token to the backend server. This means only signed-in users can communicate with the backend.

Backend Processing (Express server):

The backend is built with Express.js. It processes requests and checks the token. It also manages tasks like retrieving, modifying, or inserting medical information. This layer connects all parts of the system.

Data Encryption Utility (Encrypt util):

Prior to storing or transmitting any health care information, that information is encrypted using the Encrypt Util module with AES-256-GCM encryption technology. To protect against unauthorized access, a single master key for the Encrypt Util module is stored securely in environment variables, so only those who possess the key can access patient data.

Secure Storage in MongoDB:

The medical records are encrypted and stored in MongoDB. This ensures the security of all patient information. Authorized personnel can decrypt this information when they need to access or change it.

Audit Logging and Emergency Access:

All actions undertaken during the data modification process, consultations, or emergency overrides, have been recorded in audit logs as an additional layer of accountability to enable transparent activity tracking and in compliance with regulatory standards. Clinicians can use the emergency access option to quickly acquire patient data, but all uses of the emergency access tool are documented as well to provide for ongoing accountability of clinicians using these tools.

Verification and Testing:

To ensure the API responses are accurate and to ensure that all data processing workflows (i.e., encryption, decryption, authentication) run successfully, ongoing validation of the system will continue through Postman. Finally, through the frontend of the system, decrypted data will be securely presented to users.

Secure Authentication and Access Control:

- The system uses JWT (JSON Web Token) for secure user authentication.
- Achieved strong data confidentiality and integrity by using AES 256 GCM encrypted file storage, bcrypt-based password hashing, and JWT-based authentication for all protected endpoints.
- Role-based access control (RBAC) allows doctors to update records, while patients can only view their own data and Unauthorized login attempts are blocked to protect the system's integrity.
- Validated reliability and emergency workflows through end-to-end tests and sample scenarios. This demonstrated correct handling of routine operations, such as

treatments and file uploads/downloads, along with privacy-preserving emergency access.

Encryption Health Record Storage:

- All health records are encrypted using the AES-256-GCM algorithm before storage.
- Encrypted data in MongoDB includes fields like data, IV, and tag for security verification.
- Encryption ensures that even if the database is compromised, patient data stays unreadable.
- The system maintains data confidentiality and integrity during storage and Secure key management prevents unauthorized decryption or access.

Secure Retrieval and Decryption:

- Only authenticated and token-verified users can view decrypted health data.
- Data decryption happens automatically after the token is successfully validated and Unauthorized users or expired tokens will be denied access.
- The system ensures end-to-end encryption, keeping data safe from upload to retrieval.
- Decryption and viewing are strictly limited to legitimate users.

Overall System Performance:

- The system ensures secure data flow across all modules.
- Encrypted data storage and controlled decryption protect against breaches.
- Unauthorized users get “Invalid Token” or “401 Unauthorized” responses.
- The model achieves confidentiality, integrity, and accessibility (CIA) in data handling.
- The system shows strong performance, reliability, and protection of healthcare data.

Conclusion

The “secure electric health records for personalized patient care” initiative tackles a pivotal and enduring challenge in the present-day healthcare ecosystem the need for a genuinely effective, security-conscious, and patient-enable digital ecosystem in healthcare information management.as described throughout this report, existing systems are fundamentally flawed due to fragmentation, limited availability, and an acute lack of patient control over their sensitive medical data. We envision this application to be a strong digital bridge to supporting these widespread challenges. By providing a centralized. user friendly platform, both health care providers can manage patient records easily and patients can view private information about their own health statues. the central innovations is it clear commitment to patient data ownership-particularly through a consent-driven process for safe sharing of information during critical referrals. safe sharing of inf during critical referrals. Safe sharing will ensure that private, personal health data will only be shared after obtaining explicit patient consent- establishing a new standard for privacy and trust in digital health interactions. In conclusion, this project will transform patient care and establish a culture of collaboration, transparency, and security for patients. the intro of the strong security measures, along with a commitment to patient control will reduce risks associated with data breaching and non-compliance, while enhancing patient-physician communication.by increasing efficiency, reducing administrative efforts and providing better access to full health records, the “secure electronic health records for personalized patient care” app will result in better and more informed medical decision-make improved health outcomes for patients, and a dramatic shift to system of healthcare that is personalized, responsive and trustworthy and will change the future of digital health management

Future Work

- While the current system demonstrates promising results, future work may involve:
- Multi-factor login using OTP or fingerprint can be added to improve the system's security
- The system can be moved to a cloud platform for quicker, safer, and simpler access from anywhere.
- The system can connect with wearable devices like smartwatches to record patient health data automatically.
- The Shadow Mode AI watches clinician decisions and alerts them if actions stray from best practices, improving patient safety and

supporting evidence-based medicine with real-time warnings.

References

[1]. M. Bellare, A. Boldyreva, A. Desai, and D. Pointcheval, “Key-Privacy in Public-Key Encryption,” Springer, 2001.

[2]. H. Jin, Y. Luo, P. Li, and J. Mathew, “A Review of Secure and Privacy-Preserving Medical Data Sharing,” IEEE Access, 2019.

[3]. G. Liu, H. Xie, W. Wang, and H. Huang, “A Secure and Efficient Electronic Medical Record Data Sharing Scheme Based on Blockchain and Proxy Re-Encryption,” Journal of Cloud Computing, 2024.

[4]. S. Zhang, F. Guo, C. Jing, and C. Wu, “Electronic Medical Record Privacy Protection Scheme Based on Attribute Encryption Technology,” IEEE IAEAC, 2024.

[5]. M. Li, S. Yu, K. Ren, and W. Lou, “Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings,” SecureComm 2010, 2010.

[6]. D. Detmer, M. Bloomrosen, B. Raymond, and P. Tang, “Integrated Personal Health Records: Transformative Tools for Consumer-Centric Care,” BMC Med. Inform. Decis. Mak., vol. 8, p. 45, 2008

[7]. C. Dong et al., “A Survey of Natural Language Generation,” ACM Comput Surv, vol. 55, no. 8, Aug. 2022, doi: 10.1145/3554727.

[8]. S. De Capitani di Vimercati et al., “Fine-Grained Access Control for Outsourced Data,” ACM CCS, 2007.

[9]. C. Phuong et al., “Policy-Hiding Attribute-Based Encryption Schemes,” Information Sciences, 2020.

[10]. A. Bethencourt and B. Waters, “Ciphertext-Policy Attribute-Based Encryption,” IEEE Symp. on Security and Privacy, 2007.