Multidisciplinary | Peer-Reviewed
Open Access | Research Journal

Article ID: IRJIST-2026-041
Volume 1 | Issue 2 | 2026

International Research Journal of Innovation in Science and Technology

BioMedLink
Health Records at Your Fingertips

Jayant Nandwalkar[1], Vaishnavi Patil[2], Yash Waykole[3], Divesh Prasad[4]

[1-4]Datta Meghe College of Engineering, Navi Mumbai, Maharashtra, India

Correspondence: [1]10jnand@gmail.com, [2]patilvaishnavi9998@gmail.com, [3]yashwaykole04@gmail.com, [4]diveshprasad31@gmail.com

Abstract

In modern healthcare systems, quick and secure access to patient medical records is very important, especially during emergency situations where the patient may be unconscious or unable to communicate properly. This paper presents BioMedLink, a fingerprint-based medical record retrieval system designed to provide fast and secure access to patient information using biometric authentication. The system captures fingerprint data, performs feature extraction, and matches the generated fingerprint template with records stored in the hospital database. If the record is unavailable locally, the system sends a secure request to a centralized healthcare hub connected with multiple hospitals. After successful authentication, patient medical details such as previous diagnoses, treatment history, and emergency-related information can be retrieved in real time. The proposed system uses SHA-256 hashing, encrypted communication, role-based access control, and audit logging to maintain data privacy and system security. The platform is developed using React, Node.js, Express, Python, and MongoDB to ensure scalability and smooth inter-hospital communication. The proposed framework helps improve accessibility of medical records, reduces retrieval delay during emergencies, and supports better coordination between healthcare institutions.

Keywords: Biometric Authentication; Fingerprint Recognition; Medical Record Retrieval; Electronic Health Records; Healthcare Interoperability; Emergency Healthcare System.

1. Introduction

Access to accurate patient medical information is very important in modern healthcare systems, especially during emergency situations where the patient may be unconscious, partially responsive, or unable to communicate properly. In many hospitals, traditional identification methods such as ID cards, manual record verification, or paper-based systems are still used, which may delay medical decision-making during critical situations [1, 19].

With the increasing adoption of digital healthcare technologies, hospitals require systems that can provide secure and quick access to patient medical history. Among different biometric technologies, fingerprint recognition is considered reliable due to its uniqueness, permanence, and ease of use [5, 16].

This paper presents BioMedLink, a fingerprint-based medical record retrieval system that enables secure and fast access to patient health records across healthcare facilities [2, 16]. The system uses biometric feature extraction techniques to generate fingerprint templates, which are further secured using SHA-256 hashing methods for safe storage and authentication [7, 13].

The proposed system follows a hub-and-spoke multi-hospital architecture where patient index information is maintained through a centralized healthcare hub, while detailed medical records remain stored within individual hospital databases. During emergency situations, authorized medical staff can scan the patient's fingerprint and retrieve medical history in real time from connected healthcare institutions [6, 19].

The main objective of the proposed framework is to improve emergency medical accessibility, reduce patient identification delays, and support

secure inter-hospital communication using biometric authentication techniques.

2. Literature Review

Over the past decade, biometric technologies have been widely studied for improving patient identification and secure medical record access in healthcare systems. Traditional healthcare identification methods based on demographic details, ID cards, QR codes, or manual verification are often time-consuming and less reliable during emergency situations [1, 19].

To overcome these limitations, several researchers proposed fingerprint-based authentication systems using feature extraction and minutiae matching techniques to improve identification accuracy and reduce false acceptance rates. Different biometric approaches using fingerprint recognition, CNN-based authentication, and feature matching methods have shown promising performance in healthcare and security applications [5, 9, 10, 16].

Blockchain-supported healthcare systems were also introduced in recent studies to improve security, transparency, and tamper resistance of medical records [4]. Although such systems improve data integrity, many of them require high computational resources and complex infrastructure, making real-time deployment difficult in smaller healthcare facilities.

Cloud-based Electronic Health Record (EHR) systems improved accessibility and centralized storage of patient information; however, issues related to interoperability, data privacy, and communication delay between hospitals still remain important challenges [3, 14, 18].

In countries such as India, Kenya, and Nigeria, biometric healthcare initiatives demonstrated improvements in patient verification and reduction of identity-related fraud. However, most of these systems mainly focused on identity authentication or insurance verification rather than real-time emergency medical record retrieval across multiple hospitals [6, 19].

Based on the reviewed literature, it is observed that limited work has focused on combining fingerprint authentication, secure inter-hospital communication, and emergency medical record retrieval within a single integrated healthcare framework. The proposed BioMedLink system attempts to address this gap by providing a secure and scalable fingerprint-based healthcare record retrieval platform for emergency medical applications.

3. Methodology

The BioMedLink system is designed using a secure multi-layer healthcare architecture that supports fingerprint-based medical record retrieval across multiple hospitals. The framework connects healthcare staff, hospital databases, and a centralized emergency communication hub through secure web-based services.

3.1. User / Client Layer

Healthcare professionals such as doctors, nurses, reception staff, and administrators can access the system through a browser-based interface. Depending on their authorized role, users can register patients, manage medical records, perform fingerprint-based patient searches, and access medical reports through a role-based dashboard.

3.2. BioMedLink Dashboard

The BioMedLink dashboard acts as the main control interface of the system. It combines different modules such as patient registration, fingerprint authentication, medical record management, emergency search, and audit monitoring into a single platform. This centralized interface helps healthcare staff perform operations more efficiently during normal as well as emergency situations.

3.3. Backend Server – Node.js and Express

The backend server is developed using Node.js and Express.js. It handles user authentication, API communication, session management, fingerprint search requests, and secure data transfer between hospitals. The backend also manages role-based access permissions to ensure that only authorized users can access sensitive patient information.

3.4. Fingerprint Processing Module – Python

Fingerprint images captured by the system are processed using biometric feature extraction techniques to generate unique fingerprint templates. These templates are secured using the SHA-256 hashing algorithm before being stored

in the database. During authentication, the captured fingerprint is converted into a feature vector and matched with stored templates for patient identification.

3.5. Emergency Hub / Inter-Hospital Communication

A centralized emergency hub is used to connect multiple hospitals using a hub-and-spoke communication model. If the patient record is not available in the local hospital database, the system sends a secure encrypted request to the central hub. The hub identifies the hospital associated with the fingerprint record and enables secure transfer of medical information between healthcare institutions in real time.

3.6. Database Layer – MongoDB

MongoDB is used for storing encrypted fingerprint templates, patient medical records, hospital details, and system activity logs. The database structure supports scalability, faster retrieval, and secure storage of patient information while maintaining interoperability between connected hospitals.

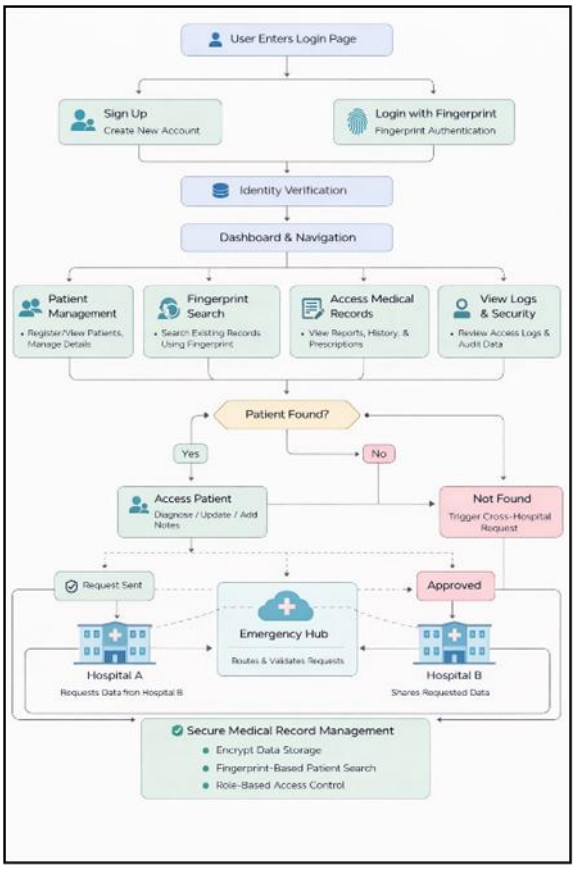

Figure 1: *Overall working flow of the BioMedLink system.*

4. Specifications

Table 1 presents the main technologies and software tools used for development of the BioMedLink system. The selected technology stack was kept lightweight and flexible to ensure easier deployment, faster system response, and smooth integration between different healthcare modules. The combination of frontend, backend, database, and biometric processing technologies also helps maintain scalability and secure communication within the proposed framework.

Table 1: *Technology Stack Used in BioMedLink*

Module	Technology / Tool	Role in the System
Frontend / User Interface	React.js	Provides responsive dashboard for hospital staff to register patients, scan fingerprints, search records and view logs.
Backend API & Server	Node.js + Express.js	Handles routing, authentication, role-based access, API communicati-on and business logic.
Fingerprint Processing Engine	Python + OpenCV + CNN	Extracts fingerprint features, generates templates and performs fingerprint matching for patient identification.
Identity Verification Module	Biometric Matching Algorithm	Matches scanned fingerprint with stor-ed templates for instant patient verificati-on.
Patient Management Module	MERN Stack Integration	Allows patient registration, profile updates, and record management.
Medical Record Access Module	Secure REST APIs	Retrieves diagnosis, prescriptions, rep-orts and emergency medical history.
Cross-Hospital Communication	Secure API + TLS Encryption	Sends and receives record requests between hospitals via Emergency Hub.
Emergency Hub	Centralized Routing Server	Validates requests and routes patient record queries across hospitals.
Security & Encryption	SHA-256 + AES	Encrypts fingerprint templates and secures data transmission.
Security & Encryption	SHA-256 + AES	Encrypts fingerprint templates and secures data transmission.
Logging & Audit Module	Winston Logger / Audit Logs	Tracks access history and system activ-ity for security and compliance.
Logging & Audit Module	Winston Logger / Audit Logs	Tracks access history and system activi-ty for security and compliance.

5. Proposed Framework

5.1. System Architecture

The proposed BioMedLink framework consists of three major layers: the client layer, server layer, and database layer. In addition to these layers, a centralized communication hub is included to support secure interaction between multiple hospitals.

The client layer is developed using React and provides separate dashboard access for administrators, doctors, and healthcare staff based on their assigned roles. Through this

interface, users can perform patient registration, fingerprint scanning, emergency patient search, and medical report access operations.

The server layer is developed using Node.js and Express.js. It manages the main application logic, user authentication, API routing, and communication between different system components. Role-Based Access Control (RBAC) is implemented using JSON Web Tokens (JWT) to ensure that only authorized users can access patient information. The server also handles secure fingerprint template processing using SHA-256 hashing techniques.

MongoDB Atlas is used as the database layer for storing fingerprint templates, patient records, emergency logs, and hospital-related information. The database structure supports secure storage, scalability, and faster retrieval of healthcare data.

The centralized emergency hub acts as the communication bridge between connected hospitals. It maintains a global fingerprint index and helps identify the hospital associated with the patient record. This architecture supports secure and efficient inter-hospital medical record sharing during emergency situations. Figure 2 shows the overall system architecture of the BioMedLink framework.

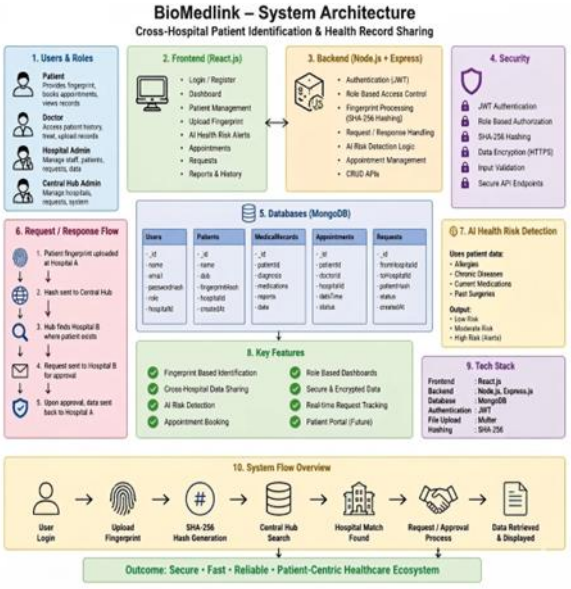

Figure 2: *System Architecture of BioMedLink*

5.2. Working

The BioMedLink system starts functioning when a patient fingerprint is captured either during registration or during emergency identification. The captured fingerprint image is processed using biometric feature extraction methods to generate a unique fingerprint template.

The generated template is then secured using the SHA-256 hashing algorithm before being stored in the database. During emergency situations where patient identity is unavailable, the scanned fingerprint is converted into a hashed template and matched through the centralized emergency hub.

The central hub compares the received fingerprint template with its indexed records and identifies the hospital associated with the patient. Once verification is completed, secure communication is established between the requesting hospital and the corresponding healthcare institution.

Medical records are then transferred securely using encrypted communication protocols such as HTTPS and TLS. This process helps healthcare professionals retrieve patient medical history quickly and supports faster medical decision-making during emergencies.

6. Results and System Demonstration

The developed BioMedLink system was tested for fingerprint-based patient identification, secure medical record retrieval, and inter-hospital communication workflow. The implementation demonstrated successful retrieval of patient information using biometric authentication with secure communication between connected system modules.

The homepage of the system provides access to patient registration, login, fingerprint scanning, and emergency medical record retrieval modules through a simplified web interface.

Figure 3: *Homepage Interface of BioMedLink*

The admin dashboard allows authorized users to manage patient information, monitor system activities, and access healthcare records based on assigned access permissions. The dashboard was designed to provide easier navigation and centralized control of different system operations.

Figure 4: *Admin Dashboard of BioMedLink*

The fingerprint scanning module captures biometric input and processes it using feature extraction techniques for patient authentication. The generated fingerprint template is securely matched with stored records for identification.

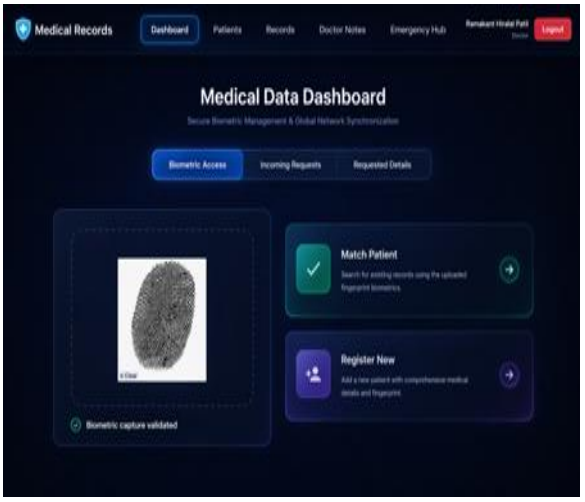

Figure 5: *Fingerprint Authentication and Scanning Module*

The centralized emergency hub enables secure matching of fingerprint records across connected hospitals. If the patient record is unavailable in the local database, the system identifies the corresponding hospital and retrieves the required medical information through encrypted communication channels.

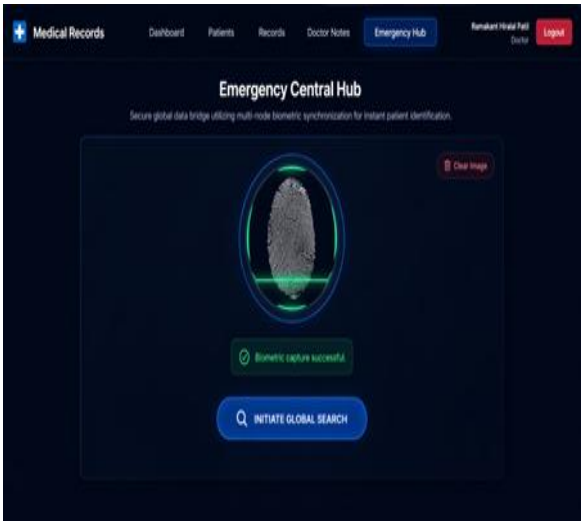

Figure 6: *Centralized Hub-Based Patient Record Matching Process*

The developed framework demonstrated improved accessibility of patient medical records and reduced manual dependency during emergency healthcare situations. The system architecture also supports scalability and secure interoperability between healthcare institutions.

7. Conclusion

The proposed BioMedLink framework presents a secure and scalable approach for biometric-based medical record retrieval in healthcare environments. The system combines fingerprint authentication, encrypted communication, and centralized inter-hospital coordination to enable faster access to patient medical information during emergency situations.

The integration of biometric feature extraction with SHA-256 secured fingerprint templates helps improve patient identification reliability while reducing dependency on manual verification methods. The hub-and-spoke architecture further supports secure interoperability between healthcare institutions by enabling controlled exchange of medical records across connected hospitals.

The developed framework demonstrates how real-time fingerprint authentication can be integrated with modern healthcare information systems to reduce retrieval delay, improve continuity of treatment, and support faster clinical decision-making during emergencies. The use of role-based access control, encrypted communication protocols, and audit monitoring mechanisms additionally strengthens healthcare data privacy and system security.

The proposed system also provides flexibility for future expansion into cloud-connected healthcare environments, centralized emergency response systems, and AI-assisted healthcare analytics platforms. With further optimization and large-scale deployment, BioMedLink can support more efficient and secure digital healthcare infrastructure for multi-hospital medical networks.

References

[1] M. Malathi, S. Shuba, M. K. Swetha, and K. Thrisha,"Secure and user-centric medical history retrieval using multi-factor biometric access," *International Journal for Multidisciplinary Research (IJFMR)*, E-ISSN: 2582-2160. [Online]. Available: https://www.ijfmr.com

[2] A. Sobur, R. K. Ray, S. Akter, M. F. Kabir, M. Y. Ahmad, M. M. Rahman, and M. Z. Hossain, "Medical image classification and enhancement using machine learning: A focus on fingerprint colorized data," *Journal of Neonatal Surgery*, vol. 14, no. 32s, 2025. [Online]. Available: https://www.jneonatalsurg.com.

[3] J. Guo, H. Mu, X. Liu, H. Ren, and C. Han,"Federated learning for biometric recognition: A survey," Artificial Intelligence Review, vol. 57, Art. no. 208, 2024. doi: 10.1007 s10462-024-10847-7.

[4] T. Takahashi, Y. Zhihao, and K. Omote,"Emergency medical access control system based on public blockchain," Journal of Medical Systems, vol. 48, Art. no. 90, 2024. doi: 10.1007/s10916-024-02102-x.

[5] M. A. Cader, J. Banks, and V. Chandran, "Fingerprint systems: Sensors, image acquisition, interoperability and challenges," Sensors, vol. 23, no. 14, Art. no. 6591, 2023. doi: 10.3390/s23146591.

[6] M. S. M. Alfatni, A. M. Ebiad, M. A. Al-Bahbouh, and L. A. Esmeda, "Electronic health file system based on fingerprint sensor technology," *Journal of Advanced Research in Applied Sciences and Engineering Technology*, 2023. [Online]. Available: https://semarakilmu.com.my.

[7] F. Castro, D. Impedovo, and G. Pirlo, "A medical image encryption scheme for secure fingerprint- based authenticated transmission," Applied Sciences, vol. 13, no. 10, Art. no. 6099, 2023. doi: 10.3390/app13106099.

[8] R. Kalaiselvan, R. Rufiney, and A. Bahari,"The fingerprint based on medical information & patient retrieval," Progress in Engineering Application and Technology, vol. 2, no. 2, pp. 590–599, 2021. [Online]. Available: https://publisher.uthm.edu.my

[9] A. Alshardan et al., "Multimodal biometric identification: Leveraging convolutional neural network (CNN) architectures and fusion techniques with fingerprint and finger vein data," PeerJ Computer Science, vol. 10, e2440, 2024. doi: 10.7717/peerj-cs.2440.

[10] A. W. H. Al-Askari and K. M. Z. Othman, "Enhancing biometric authentication in healthcare applications using convolutional neural network," Journal of Engineering Science and Technology, vol. 20, no. 4, pp. 887–900, 2025.

[11] S. Sengupta, "A secured biometric-based authentication scheme in IoT-based patient monitoring system," in Emerging Technology in Modelling and Graphics, J. Mandal and D. Bhattacharya, Eds., vol. 937, Springer, Singapore, 2020. doi: 10.1007/978-981-13-7403-6_44.

[12] L. N. G. Koralla,"Biometric data and behavior analysis," World Journal of Advanced Research and Reviews, vol. 26, no. 1, pp. 339–350, 2025. doi: 10.30574/wjarr.2025.26.1.1084.

[13] V. Nedunoori, "A comprehensive review of encryption and protection techniques for healthcare data," in Artificial Intelligence in Healthcare Information Systems—Security and Privacy Challenges, N. R. Vajjhala et al., Eds., vol. 34, Springer, Cham, 2025. doi: 10.1007/978-3-031-84404-1_8.

[14] K. Y. Yigzaw et al., "Health data security and privacy: Challenges and solutions for the future," in Healthcare Data Analytics and Management, Elsevier, 2021, pp. 281–303. doi: 10.1016/B978-0-12-823413-6.00014-8.

[15] R. H. Hamid, "Improving biometric authentication: Advanced techniques for fingerprint minutiae extraction," International Journal of Applied Sciences and Technology (MINAR), 2025.

[16] E. B. Edim and A. I. Udofot, "Biometric authentication and algorithm: A review," International Journal of Science and Research Archive, vol. 14, no. 3, pp. 960–986, 2025. doi: 10.30574/ijsra.2025-14.3.0473.

[17] M. Suman, N. Shobha, S. B. Ashoka, and J. P. K. Chinta, "Biometric fingerprint verification with Siamese neural network and transfer learning," Journal of Machine and Computing, 2025. doi: 10.53759/7669/jmc202606003.

[18] H. N. Ali and S. S. M. Al-Dabbagh, "A systematic literature review on biometric

authentication in mobile banking," F1000Research, vol. 15, p. 5, 2026. doi: 10.12688/f1000research.173855.1.

[19] V. A. Akpan and F. V. Olawale, "Development of fingerprint biometric authentication system for health information exchange," Journal of ICT Development, Applications and Research, vol. 6, no. 2, pp. 1–16, 2024. doi: 10.47524/jictdar.v6i2.6.

[20] O. O. Shoewu, O. J. Ayangbekun, M. A. Adedoyin, E. Aigbovbioise-Job, L. A. Akinyemi, and F. C. Oluwaseyi, "Design and development of health centre management system with fingerprint identification," The Pacific Journal of Science and Technology, vol. 21, no. 2, pp. 190–202, Nov. 2020. [Online]. Available: http://www.akamaiuniversity.us/PJST.htm

Publisher's Note & Copyright

IRJIST Journals remains neutral regarding jurisdictional claims in published maps and institutional affiliations; the views expressed are solely those of the authors.