© FEB 2026 | IRE Journals | Volume 9 Issue 8 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I8-1714242

Transparent and Reliable Medico-Legal Record Management Solution

S. DIVYA THARSHINI[1], B. SHANMUGA SUNDARI[2], T. SUGI[3]
[1]*PG Student, Department of CSE, PET Engineering College, Vallioor*
[2,3] *Assistant Professor, Department of CSE, PET Engineering College, Vallioor*

Abstract- ***Medico legal records contain critical information that bridges healthcare and law, including patient medical histories, treatment records, forensic reports, and legal case data, and managing these records efficiently is essential to ensure security, accuracy, and accountability. Traditional record management systems often rely on manual processes or basic digital storage solutions, which are prone to slow search times, weak encryption, limited access control, and inadequate audit ability, leading to potential data breaches, unauthorized access, and delayed decision-making. Care Chain addresses these challenges by integrating advanced technologies to provide a secure, transparent, and efficient management solution. The system utilizes. B-Tree indexing for rapid and organized data retrieval, Key-Policy Attribute-Based Encryption (KP-ABE) to restrict decryption to authorized personnel based on predefined attributes, and Role-Based Access Control (RBAC) to enforce role-specific permissions for doctors, lawyers, administrators, judges, and patients. Additionally, Block chain-based logging records all interactions with the records, including creation, modification, access, and deletion, ensuring a tamper-proof, immutable audit trail for transparency and accountability. By combining these technologies, Care Chain minimizes manual effort, accelerates search and retrieval prevents unauthorized access, and maintains data integrity.***

I. INTRODUCTION

Medical records serve a vital role in healthcare by providing a complete and accurate account of a patient's medical history, including medical conditions, diagnoses, treatments, and their outcomes. According to the American Institute for Health Management, medical records fulfill five primary purposes: supporting patient care by providing a documented basis for treatment planning, facilitating communication among physicians, nurses, and other healthcare professionals, serving as legal documentation of a patient's health and care, enabling billing and reimbursement by documenting services rendered and payments, and supporting research and quality management by monitoring and analyzing care practices[1]. The National Library of Medicine emphasizes that medical records track interactions between patients and healthcare providers, offering valuable information on diagnoses, procedures, lab tests, and other services. These records also assist in legal matters such as medical malpractice and accident-related litigation. Additionally, with the integration of information technology, healthcare can become more cost-effective and efficient: safety is improved, processes are 2 expedited, claims and reimbursements are streamlined, treatment effectiveness is monitored, outcomes are predicted, legal liability is reduced, and errors or omissions are minimized. Accurate and methodical documentation of assessments, symptoms, diagnoses, and treatments ultimately enhances quality assurance, facilitates continuity of care, and ensures that subsequent healthcare professionals can provide optimal patient care[2].

II. LITERATURE SURVEY

In 2024 Zigang Wu , Haijiang Wang the objective of this study is to design a secure and privacy-preserving medical data-sharing system that overcomes limitations of existing searchable encryption schemes in electronic health record (EHR) systems, including lack of fine-grained access policies, policy hiding, and incomplete search results. The study proposes a blockchain-aided attribute-based searchable encryption scheme that leverages an inner product predicate mechanism[9]. Fine-grained access policies with wildcards allow precise control over data access, while the inner product predicate ensures fully hidden access policies and prevents sensitive data leakage.

In 2023 Abhishek Bisht; Ashok Kumar Das the objective of this study is to design a secure, efficient, and practical scheme for sharing Personal Health Records (PHRs) in Internet of Medical Things (IoMT) environments, addressing the challenges of confidentiality, search verifiability, and forward security. The proposed approach integrates searchable symmetric encryption, blockchain

technology, and Inter-Planetary File System (IPFS) for decentralized storage. Formal security proofs are provided to validate the scheme, and extensive test-bed experiments are conducted to assess its practicality in IoMT scenarios[11].

In 2023 Sumit Kumar Rana; Arun Kumar Rana this study aims to safeguard digital evidence in legal proceedings by proposing a decentralized approach using blockchain and smart contracts to ensure integrity, transparency, and immutability[12]. The approach uses a distributed ledger with smart contracts to manage digital evidence across multiple parties, ensuring trust and accountability. Architecture design includes blockchain network setup, smart contract programming, and decentralized storage integration.

In 2022 Aysha Alnuaimi; Amna Alshehhi; Khaled Salah to design a secure and decentralized system for processing health insurance claims for prescription drugs, mitigating fraud and ensuring privacy and trustworthiness. A private Ethereum blockchain is used along with two smart contracts (registration and approval[6]. The 9 system is integrated with IPFS for off-chain storage and DApps for user access. Gateway mechanisms filter data visibility to maintain privacy[10]. System architecture, sequence diagrams, and algorithms are provided for implementation. Smart contracts for claim registration and approval; blockchain-based traceability and IPFS for decentralized storage.

In 2021 Xiang Gao; Jia Yu; Yan Chang to provide a practical approach for integrity auditing of encrypted cloud data based on keywords while preserving sensitive information privacy. The scheme enables a Third Party Auditor (TPA) to audit encrypted cloud files containing user-specified keywords without learning sensitive information.

III. EXISTING SYSTEM

The current systems for managing medico-legal records primarily rely on traditional or basic digital approaches, which have significant limitations in terms of efficiency, security, and reliability.

● Paper-Based Records In many institutions, medico-legal documents are still maintained physically in files and folders. [6]While this method is straightforward, it is highly prone to damage, loss, and deterioration over time. Searching for a specific record among hundreds or thousands of files can be extremely slow and inefficient, making timely access to critical data difficult. This method also increases the risk of human error and misplacement of important documents.

● Manual Indexing Records in traditional systems are often organized alphabetically or chronologically. This manual indexing method is not only time-consuming but also inefficient when searching for records based on multiple criteria, such as case type, patient name, or date. Updating or modifying records is cumbersome, and duplication errors are common, making it challenging to maintain data integrity.

● Basic Digital Storage Some organizations have adopted simple digital storage systems, such as spreadsheets or basic databases, to manage medico-legal records. While these systems provide easier storage and retrieval compared to paper-based methods, they lack advanced features such as secure encryption, fine-grained access control, and efficient search mechanisms[3]. These limitations leave sensitive medical and legal information vulnerable to unauthorized access and accidental data loss.

● Password-Based Protection Traditional digital systems often rely solely on basic username and password authentication for security. While passwords provide a basic level of protection, they do not prevent unauthorized access if credentials are compromised. Moreover, these systems lack advanced encryption techniques, leaving the data vulnerable to hacking, leaks, or tampering[4].

DISADVANTAGES

● Physical records are prone to damage and loss.
● Basic encryption methods are vulnerable to attacks.
● Lack of advanced indexing delays record access.
●Minimal role-based security increases unauthorized access risks.

IV. PROPOSED SYSTEM

The proposed system is designed to address the drawbacks of traditional medico-legal record management systems by combining advanced technologies to ensure security, efficiency, and organization. It focuses on faster record retrieval, robust data protection, controlled user access, and transparent auditing to enhance the overall management of sensitive medico-legal data[5].

● Efficient Search Mechanism to improve the speed and accuracy of record retrieval, the system

© FEB 2026 | IRE Journals | Volume 9 Issue 8 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I8-1714242

incorporates B-Tree indexing. B-Tree is a balanced tree data structure that organizes records hierarchically, allowing quick searching, insertion, and deletion. This approach significantly reduces the time required to locate specific records compared to manual or linear search methods, making the system highly efficient for large datasets.

● Enhanced Data Security the system employs KP-ABE (Key-Policy Attribute-Based Encryption) to protect sensitive medico-legal records. With KP-ABE, data is encrypted in such a way that only users whose attributes match the defined access policy can decrypt the records. This ensures that confidential information is accessible only to authorized personnel, preventing data breaches and unauthorized access while maintaining privacy[7].

● Controlled Access Management to manage user permissions effectively, the system integrates Role-Based Access Control (RBAC). RBAC assigns roles to users based on their job functions, such as doctors, legal officers, or administrators, and grants access permissions accordingly. This mechanism ensures that users can only access the information relevant to their responsibilities, reducing the risk of misuse or accidental exposure of confidential records.

● Transparent Audit Logging the system uses Blockchain technology to maintain immutable logs of all data interactions. Every action, including record creation, access, or modification, is recorded on the blockchain with a timestamp and user identity. This provides a transparent and tamper-proof audit trail, ensuring accountability, enhancing trust in the system, and facilitating compliance with legal and regulatory requirements[8].

ADVANTAGES

● Ensures secure storage and quick retrieval of medico-legal records.
● Easy access to verified records for legal investigations.
● Provides organized and accurate data for case proceedings.
● Enhances patient data management and compliance with legal standards.

V. SYSTEM ARCHITECTURE

The proposed system architecture provides a transparent, secure, and reliable medico-legal record management solution by integrating authentication, encryption, secure storage, and audit mechanisms, ensuring legal validity and data integrity.

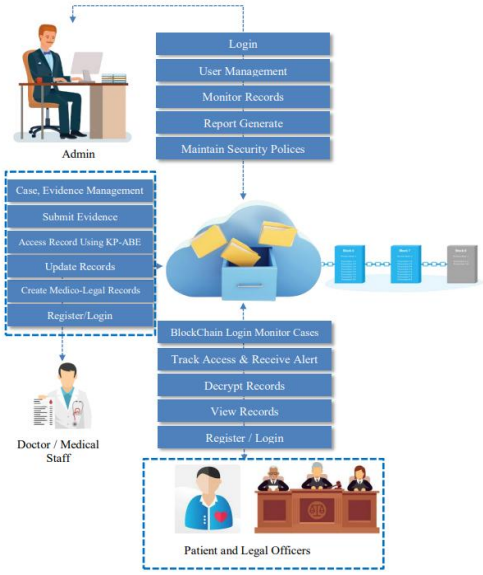

Figure 5.1: System Architecture

VI. SYSTEM IMPLEMENTATION

5.1. MFA Web Dashboard

The Web Dashboard acts as the central control panel of the system, integrating the database and blockchain infrastructure. It allows administrators, doctors, legal officers, and patients to access, manage, and monitor medico-legal records from a single interface.

5.2. End-User Module

5.2.1 Admin Module

● Login: Provides a secure login interface for the admin to access the system.
● User Management: Allows admins to add, remove, or update users, assign roles, and manage permissions.
● Monitor Records: Enables tracking of record creation, access, and modifications via blockchain audit logs.
● Generate Reports: Allows admins to generate reports on system usage, access patterns, and compliance.
● Security Enforcement: Ensures compliance with legal and medical regulations, enforcing system-wide security policies.

5.2.2 Doctor / Medical Staff Module

● Registration & Login: Doctors can register and log in securely to access the system.

© FEB 2026 | IRE Journals | Volume 9 Issue 8 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I8-1714242

● Create Records: Allows doctors to create medico-legal records such as 25 medical reports, incident logs, or forensic notes.
● Update Records: Enables modification of records within the scope of role-based permissions.
● Secure Access: Records are encrypted using KP-ABE to ensure only authorized users can view them.
● Submit Evidence: Allows doctors to securely provide patient information or case evidence for legal purposes.

5.2.3 Legal Officer Module
● Login: Provides secure access for legal officers to the system.
● View Records: Allows access to encrypted medico-legal records relevant to investigations or legal proceedings.
● Decrypt Records: Decryption is allowed only if the user's attributes match the access policies.
● Blockchain Logging: Every record accessed is logged immutably for accountability and transparency.
● Monitor Cases: Enables officers to track case-related activities and audit record usage.

5.2.4. Patient Module
● Registration & Login: Allows patients to securely register and access their accounts.
● View Records: Enables patients to view their own medico-legal records securely.
● Track Access: Lets patients see who has accessed their records and when.
● Receive Alerts: Sends notifications in case of unauthorized access attempts or suspicious activity.
● Privacy Control: Ensures patients' data privacy while keeping them informed about their records.

5.3. User Authentication Module
This module provides secure login and authentication for all users. Authentication is role-based, meaning each user can access only the functionalities allowed for their role. Multi-factor authentication (such as OTPs or email verification) can be added for enhanced security[12].

5.4. Record Creation and Storage Module
Authorized users can create, update, and store medico-legal records. Before storage, each record is encrypted using KP-ABE, which allows decryption only by users with matching attributes. Records are stored in JSON format, making them compatible with blockchain logging and ensuring structured, easy-to-query storage[14].

5.5. Search and Retrieval Module
The system uses B-Tree indexing, which allows fast and efficient search even for large datasets. Users can search records by patient name, case number, date, or type of incident.

5.6. Access Control Module Role-Based Access Control (RBAC)
Ensures that only authorized users can access or modify records based on their roles. For example, doctors can add patient data, legal officers can view case files, and administrators can manage the system.

5.7. Blockchain Logging Module
Every action performed on the system, including record creation, modification, or access, is logged on a blockchain ledger. Blockchain ensures that these logs are immutable and tamper-proof, providing full transparency and accountability[13].

5.8. Reporting and Analytics Module
This module generates reports on record access, modifications, and system usage. Analytics help administrators identify unusual access patterns, monitor compliance with data security protocols, and optimize system operations. Reports can be customized by date, user role, or record type for effective oversight.

5.9. Notification Module
The notification module sends real-time alerts to users for critical events. For example, if an unauthorized access attempt is detected, the system alerts administrators and the record owner. Notifications can be sent via email, SMS, or in-app alerts.

VII. RESULT AND DISCUSSION

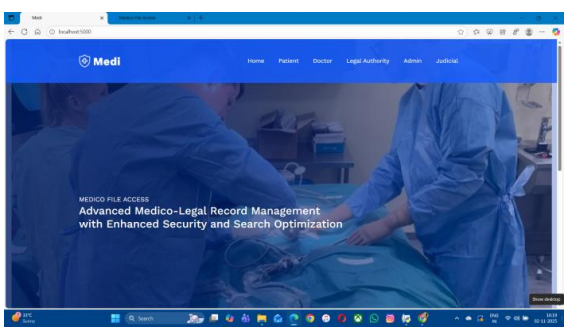

Figure 7.1: Home page

© FEB 2026 | IRE Journals | Volume 9 Issue 8 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I8-1714242

This Home page is used to define the advanced medico- legal record management with enhanced security and search optimization. This page it contain Doctor , Patient , legal authority, admin, judicial by this way we move from one page to another. And here we are using B tree indexing , RBAC , KP-ABE.

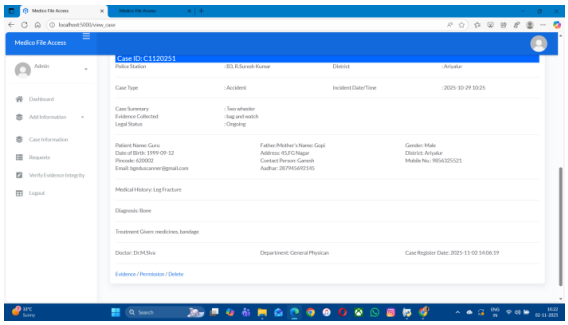

Figure 7.2: Admin Login Page

This is the admin side interface that the admin should enter their username and password for adding the case information add authority, request. And here we can add evidence and give permission to the authority.

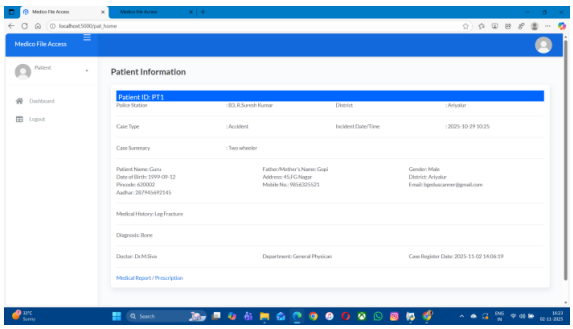

Figure 7.3: Patient Information

In this page it defines Patient Information which means the details about The concern patient . The patient they can view only their data with the help of their user id and password.

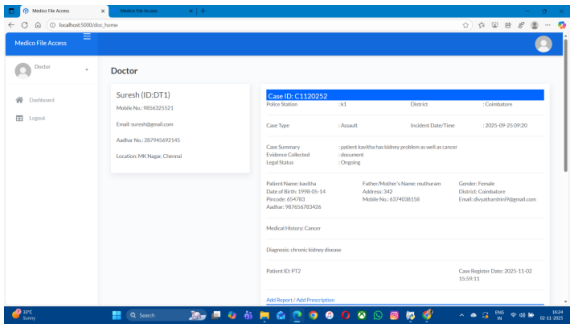

Figure 7.4: Doctor Information

This is a Authority login page it contain specific username and password. After the case is registered and the evidence can be view by particular authority.

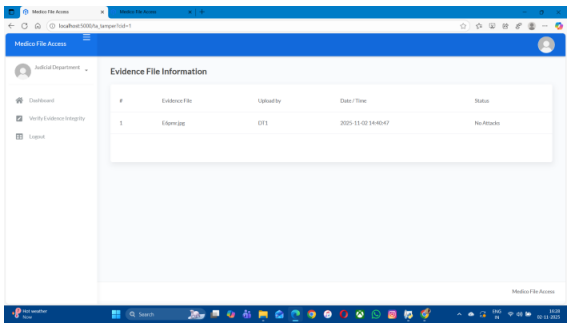

Figure 7.5: Evidence File Information

This page it used to define the of evidence file information about uploaded by, date/time , status. And it show evidence integrity.

VIII. CONCLUSION AND FUTURE ENHANCEMENT

In conclusion, this project successfully implements a project, providing a secure, transparent, and efficient solution for managing sensitive medical and legal records. By integrating KP-ABE encryption, Role-Based Access Control, and blockchain-based audit logging, the system ensures that only authorized personnel can access confidential information while maintaining a tamper-proof record of all interactions. Doctors, legal officers, administrators, and patients can securely create, view, and manage records, with real-time notifications for updates or unauthorized access attempts.[15] the limitations of traditional paper-based and basic digital systems, further enhancements can strengthen security, expand accessibility, and improve interoperability with other healthcare and legal databases. Overall , this project significantly improves transparency, security, and Efficiency in medico- legal record management solution.

- Mobile Application Development – Create a dedicated mobile app for secure access and real-time record updates by doctors, legal officers, and patients.
- Multi-Language Support – Introduce regional language interfaces to improve accessibility for users across different locations.
- Enhanced Security Measures – Strengthen encryption, implement multi-factor authentication, and enhance blockchain protocols for added data protection.

● Integration with Healthcare and Legal Systems – Enable interoperability with hospital management systems, court databases, and government healthcare portals.
● AI-Driven Analytics–Incorporate AI for predictive insights, anomaly detection in record access, and automated report generation.
● Cloud-Based Scalability – Expand cloud storage and distributed access to support large- scale adoption and remote access for authorized stakeholders.

IX. ACKNOWLEDGEMENT

I would like to express sincere gratitude to the faculty members of PET Engineering College for their continuous guidance and academic support throughout the course of this research. Special thanks are extended to the project guide for valuable suggestions and encouragement that contributed to the successful completion of the study.

REFERENCES

[1] J. Li et al., "Multiauthority attribute-based encryption for assuring data deletion", IEEE Syst. J., vol. 17, no. 2, pp. 2029-2038, Jun. 2023.
[2] S. Chen, J. Li, Y. Zhang and J. Han, "Efficient revocable attribute-based encryption with verifiable data integrity", IEEE Internet Things J., Oct. 2023.
[3] S. Xu et al., "Efficient ciphertext-policy attribute-based encryption with blackbox traceability", Inf. Sci., vol. 538, pp. 19-38, Oct. 2020.
[4] W. Chen, S. Zhu, J. Li, J. Wu, C. L. Chen and Y. Y. Deng, "Authorized shared electronic medical record system with proxy re-encryption and blockchain technology", Sensors, vol. 21, no. 22, pp. 7765-7765, 2021.
[5] K. Xue, N. Gai, J. Hong, D. S. L. Wei, P. Hong and N. Yu, "Efficient and secure attribute-based access control with identical sub-policies frequently used in cloud storage", IEEE Trans. Dependable Secure Comput., vol. 19, no. 1, pp. 635-646, Jan./Feb. 2022.
[6] T. Dillon, C. Wu, and E. Chang, “Cloud computing: Issues and challenges,” in Proc. 24th IEEE Int. Conf. Adv. Inf. Netw. Appl., Apr. 2010, pp. 27–33.
[7] D. X. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” in Proc. IEEE Symp.Security Privacy (S&P), Berkeley, CA, USA, 2000, pp. 44–55.
[8] J. Benet. “IPFS-content addressed, versioned, P2P file system.” 2014. [Online]. Available: https://arxiv.org/abs/1407.3561
[9] J. Katz and Y. Lindell, Introduction to Modern Cryptography. Boca Raton, FL, USA : CRC Press, 2020.
[10] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, “Hawk: The blockchain model of cryptography and privacy-preserving smart contracts,” 61 in Proc. IEEE Symp. Security Privacy (S&P). San Jose, CA, USA, 2016, pp. 839–858.
[11] P. C. Tang, J. S. Ash, D. W. Bates, J. M. Overhage, and D. Z. Sands, “Personal health records: Definitions, benefits, and strategies for overcoming barriers to adoption,” J. Amer. Med. Inform. Assoc., vol. 13, no. 2, pp. 121–126, Mar. 2006.
[12] B. Tellenbach, “Identity-based cryptography,” in Trends in Data Protection and Encryption Technologies. Cham, Switzerland : Springer, 2023, pp. 59– 64.
[13] A. Roehrs, C. A. da Costa, and R. da Rosa Righi, “OmniPHR: A Distributed Architecture Model to Integrate Personal Health Records,” Journal of Biomedical Informatics, vol. 71, pp. 70–81, 2017.
[14] T. H. Davenport and J. G. Harris, “Electronic Medical Records: Legal and Ethical Issues,” Health Care Management Review, vol. 30, no. 3, pp. 222–230, 2005.
[15] P. K. Sinha, “Medico-Legal Importance of Medical Records,” Indian Journal of Forensic Medicine & Toxicology, vol. 12, no. 2, pp. 45–49, 2018.