IJRDET

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 03, March 2026)

MediLocker: A DigiLocker-Based System for Secure and Hospital Independent Medical Record Management.

Dr. Sarika H. Gadekar[1], Prof. Vidya S. Chandgude[2], Khushi S. Agarwal[3], Tanuja S. Shelke[4]

[1,2]Assistant Professor, [3,4]Student, MAEER's MIT Arts Science Commerce College, Alandi, Pune, India

***Abstract* -- The rapid digitization of healthcare services has led to an exponential increase in the generation of medical data, including diagnostic reports, laboratory results, prescriptions, imaging records, and long-term treatment histories. Despite this growth, the management and accessibility of medical records remain significantly fragmented across healthcare institutions. Patients are often required to carry physical documents or store scattered digital reports on personal devices when visiting hospitals, clinics, or diagnostic centers. This manual and decentralized approach creates substantial challenges, such as loss or damage of records, lack of complete medical history during consultations, repetition of diagnostic procedures, delayed treatment decisions, and increased healthcare costs.**

In emergency medical situations, the absence of immediate access to accurate patient history—such as known allergies, chronic diseases, previous surgeries, or ongoing medications—can result in life-threatening clinical errors. Although Electronic Medical Record (EMR) and Electronic Health Record (EHR) systems have been introduced to digitize healthcare data, most existing implementations are institution-specific, lack interoperability, and offer limited patient control over data sharing. Consequently, continuity of care across multiple healthcare providers remains difficult to achieve.

This paper proposes MediLocker, a DigiLocker-based medical report and history management system designed to enable secure, hospital-independent access to verified patient medical records without requiring patients to physically or digitally transport their reports. The proposed system maintains a centralized and encrypted digital repository that stores medical documents generated by hospitals, laboratories, and diagnostic centers, all linked to a unique patient identity. Authorized healthcare providers can access relevant medical records only after obtaining explicit patient consent through a robust authentication mechanism.

MediLocker employs advanced security measures, including role-based access control, encryption of data at rest and in transit, multi-factor authentication, and comprehensive audit logging to ensure confidentiality, integrity, availability, and accountability of medical data. The system supports seamless sharing of medical history across institutions, reduces redundant diagnostic tests, accelerates clinical decision-making, and significantly enhances emergency healthcare response. By promoting a patient-centric, paperless, and interoperable healthcare ecosystem, MediLocker contributes toward improved healthcare efficiency, better patient outcomes, and compliance with modern data protection regulations such as HIPAA, GDPR, and India's Digital Personal Data Protection Act.

***Keywords--* MediLocker, DigiLocker, Medical Records, Electronic Health Records, Healthcare Information Systems, Data Security, Patient-Centric Healthcare**

I. Introduction

Modern healthcare systems are increasingly dependent on accurate, timely, and comprehensive medical information to deliver effective patient care. Advances in medical imaging, diagnostics, telemedicine, and wearable health devices have dramatically increased the volume and complexity of patient health data. However, the mechanisms used to manage and share this data have not evolved at the same pace. Medical records are typically stored in isolated information systems maintained independently by hospitals, clinics, laboratories, pharmacies, and insurance providers.

As a result, patients are often forced to act as intermediaries in the healthcare information exchange process. They are required to carry physical files, printed reports, USB drives, or mobile phone images of medical documents when visiting different healthcare facilities. This approach is not only inconvenient but also highly unreliable, particularly for elderly patients, individuals with chronic illnesses, or patients seeking emergency care.

A widely reported real-life incident involved a road accident victim who was admitted unconscious to a tertiary care hospital in a different city. Due to the absence of accessible medical history, doctors were unaware of the patient's pre-existing heart condition and ongoing medication. This lack of information delayed appropriate treatment and significantly increased medical risk. In another instance, a cancer patient undergoing treatment at multiple hospitals had to repeatedly undergo expensive diagnostic tests because prior reports were unavailable or deemed unverifiable by new healthcare providers.

The COVID-19 pandemic further exposed the limitations of fragmented healthcare data systems. During emergency transfers and hospital overloads, physicians often lacked access to patients' previous test results, vaccination status, or comorbidity information. These challenges highlighted the urgent need for a unified, secure, and patient-controlled digital health record system.

While EMR and EHR systems have improved internal hospital workflows, their lack of interoperability and patient-centric access control continues to limit their effectiveness. MediLocker addresses these challenges by leveraging DigiLocker infrastructure to provide a secure, standardized, and hospital-independent medical record management solution.

II. Literature Review (Related Work)

Numerous studies have examined the challenges associated with traditional medical record management systems. Early EMR systems focused on digitizing paper records within hospitals, improving internal efficiency but failing to support data sharing across institutions. Researchers have identified interoperability as one of the most significant limitations of existing healthcare information systems.

Recent research has explored blockchain-based medical record systems to address issues of data integrity and patient ownership. Blockchain ensures immutability and transparent access control; however, practical deployment remains challenging due to scalability issues, high computational costs, and regulatory concerns. Studies indicate that while blockchain offers strong security guarantees, it may not be suitable for large-scale national healthcare systems without significant optimization.

Personal Health Record (PHR) systems allow patients to store and manage their own medical data. While PHRs promote patient engagement, they often depend on manual uploads and lack mechanisms to verify the authenticity of uploaded medical documents. This limitation reduces their reliability in clinical settings.

Other research focuses on privacy-preserving techniques such as attribute-based encryption, role-based access control, and secure cloud storage. These methods improve data protection but do not fully resolve the issue of fragmented data across healthcare providers. The reviewed literature indicates a clear research gap for a secure, centralized, patient-controlled system that supports verified, hospital-independent access—motivating the MediLocker approach.

III. Problem Statement

The current healthcare ecosystem suffers from fragmented medical record storage, where patient data is dispersed across multiple healthcare providers without a standardized mechanism for secure sharing. Patients are required to manually manage and transport medical reports throughout their lifetime, leading to multiple systemic inefficiencies.

In rural and semi-urban regions, patients frequently lose paper-based medical records due to environmental damage, relocation, or long treatment durations. In urban areas, patients often store reports on mobile devices, which can be lost, damaged, or inaccessible during emergencies. Hospitals frequently repeat diagnostic procedures due to lack of trust in externally produced reports, increasing healthcare costs and patient discomfort.

A documented incident involved a pregnant woman admitted to an emergency ward without antenatal records. Due to missing blood group and medical history information, critical treatment decisions were delayed, placing both mother and child at risk. In another case, a kidney patient undergoing dialysis at different hospitals had inconsistent treatment due to unavailable prior reports, leading to severe complications.

These examples demonstrate that the absence of a centralized, secure, and interoperable medical record system directly impacts patient safety, healthcare efficiency, and clinical outcomes. MediLocker aims to resolve these issues by providing verified, instantly accessible, and patient-controlled medical records across institutions.

IV. Objectives

The objectives of the MediLocker system are:

1. To eliminate the need for patients to carry physical or digital medical reports.
2. To provide a secure and centralized repository for lifetime medical records.
3. To enable hospital-independent access through a unique patient identity.
4. To ensure patient-centric, consent-based access control.
5. To maintain data privacy, integrity, and confidentiality.
6. To support faster and more accurate clinical decision-making.
7. To reduce redundant diagnostic procedures and healthcare costs.
8. To improve continuity and quality of patient care.
9. To ensure compliance with legal and ethical data-protection standards.

V. Proposed System: MediLocker

A. System Overview

MediLocker is a DigiLocker-based platform that stores verified medical records in a centralized digital repository. Each patient is assigned a unique identity that links all medical documents generated throughout their lifetime.

B. System Architecture

The architecture includes a user interface layer, authentication and consent layer, application layer, secure cloud storage, and a security and audit layer. These components work together to ensure secure data access and management.

C. System Workflow

Patients register once, healthcare providers upload verified reports, and authorized doctors access records after obtaining patient consent. This workflow eliminates the need for physical documents.

D. User Modules

The system includes patient, doctor, hospital/lab, and admin modules, each with defined roles and permissions.

VI. Detailed System Architecture Analysis

The MediLocker system architecture is designed to support scalability, security, interoperability, and patient-centric control. The architecture follows a layered approach to ensure separation of concerns and ease of maintenance.

A. Presentation Layer

This layer provides user interaction through web and mobile interfaces. Patients, doctors, hospitals, and administrators interact with the system using authenticated dashboards. The interface is designed to be intuitive, enabling quick access during emergencies.

B. Application Layer

The application layer handles core business logic, including medical report management, consent handling, user role validation, and session management. This layer ensures that access requests are processed according to predefined security policies.

C. Authentication and Consent Layer

This layer manages identity verification and patient consent. Multi-factor authentication mechanisms such as OTP and biometric verification are employed. Consent tokens are generated for time-bound access, ensuring patient control over medical data.

D. Data Management Layer

Medical records are stored in encrypted form within secure cloud databases. Metadata indexing enables efficient retrieval while ensuring that raw data remains protected.

E. Security and Audit Layer

All system activities are logged for audit purposes. Encryption, intrusion detection, and anomaly monitoring mechanisms ensure compliance with healthcare data protection standards.

VII. Security And Privacy Mechanisms

Security and privacy are foundational requirements for any healthcare information system. MediLocker adopts a multi-layered security architecture designed to protect sensitive medical data against unauthorized access, data breaches, and misuse.

Encryption:

All medical records stored within MediLocker are encrypted using industry-standard encryption algorithms. Data is encrypted both at rest (within databases and cloud storage) and in transit (during data exchange between users and servers). For example, when a laboratory uploads a blood test report, the data is encrypted before storage and can only be decrypted by authorized users after consent approval.

Role-Based Access Control (RBAC): Different user roles—patients, doctors, laboratories, and administrators—are granted access strictly based on their responsibilities. A doctor may view diagnostic reports but cannot modify historical records, while a laboratory can upload reports but cannot access unrelated patient history.

Consent-Based Authentication: Patients retain full control over their medical data. Healthcare providers must request access, and patients can grant time-limited or purpose-specific consent. For instance, a patient may allow a surgeon temporary access to surgical history but restrict access to psychiatric records.

Audit Logging: Every access attempt, modification, or download is recorded in an immutable audit log. This ensures transparency and allows detection of unauthorized activities. If a breach occurs, logs enable rapid forensic investigation.

Multi-Factor Authentication (MFA): Users authenticate using multiple factors such as passwords, OTPs, or biometric verification, significantly reducing the risk of credential compromise.

VIII. Comparative Study

Feature	Traditional System	EMR/EHR System	MediLocker
Record Storage	Paper-based	Digital (Hospital-specific)	Centralized Digital Locker
Patient Control	None	Limited	Full Consent-Based Control
Interoperability	No	Limited	High (Hospital-Independent)
Emergency Access	Manual	Restricted	Instant with Authorization
Data Security	Low	Medium	High (Encryption + RBAC)
Report Carrying	Mandatory	Sometimes	Not Required

The comparison clearly indicates that MediLocker overcomes major limitations of traditional and existing digital systems.

IX. Legal And Ethical Considerations

The handling of medical information carries profound legal and ethical obligations because health records contain highly confidential and personal details. Any unauthorized access, modification, or disclosure of such data may lead to serious consequences, including violation of patient privacy, social discrimination, financial exploitation, and erosion of trust in healthcare institutions. Recognizing these risks, MediLocker is designed with a strong ethical foundation and strict adherence to prevailing legal standards governing healthcare data protection. The legal and ethical framework of MediLocker is tightly integrated with its security and privacy architecture to ensure responsible data governance.

A. Patient Autonomy and Informed Authorization

Respect for patient autonomy is a fundamental ethical principle in healthcare. MediLocker ensures that patients remain the primary decision-makers regarding the use and sharing of their medical data. Access to medical records is governed by an explicit consent-driven mechanism, where healthcare providers must obtain authorization before viewing patient information. Patients are clearly notified about who is requesting access, the specific purpose of access, and the duration for which permission is sought. This transparent authorization process reinforces informed consent practices and empowers patients to exercise control over their personal health information.

B. Protection of Confidentiality and Privacy

Safeguarding patient confidentiality is a core ethical responsibility of healthcare systems. MediLocker enforces strict confidentiality through the use of encryption technologies, role-based access restrictions, and multi-factor authentication mechanisms. These controls ensure that sensitive medical data is visible only to individuals with legitimate authorization. Even within the same healthcare institution, access is limited based on professional responsibilities, preventing unnecessary exposure of patient records. Such controlled access mechanisms significantly reduce the likelihood of data misuse and uphold ethical privacy standards.

C. Assurance of Data Integrity and Reliability

Ensuring the accuracy and reliability of medical records is both a legal obligation and an ethical necessity. MediLocker incorporates verification mechanisms to prevent unauthorized alteration of stored medical documents. Digital signatures and tamper-detection techniques are used to preserve the authenticity of records. This guarantees that healthcare professionals can depend on the integrity of the information while making diagnostic or treatment decisions, which is particularly critical during emergencies and high-risk clinical situations.

D. Accountability and Operational Transparency

Modern data protection regulations emphasize accountability in personal data handling. MediLocker addresses this requirement by maintaining comprehensive audit trails that record all data access, modifications, and sharing activities.

These logs enable traceability, facilitate investigation of suspected misuse, and support legal compliance. From an ethical standpoint, such transparency strengthens patient confidence by demonstrating responsible and auditable handling of sensitive medical information.

E. Ethical Data Usage and Harm Reduction

MediLocker is designed around the ethical principle of minimizing harm. Access to patient data is restricted to the minimum information required for clinical purposes, following the principle of least privilege. This reduces the risk of accidental disclosure or inappropriate use of medical data. Additionally, the system actively discourages non-clinical, commercial, or unauthorized exploitation of health records, thereby promoting ethical and responsible data utilization.

F. Compliance with Legal Mandates

By embedding encryption, consent management, access controls, and monitoring mechanisms into its core architecture, MediLocker supports compliance with national and international healthcare data protection laws. These safeguards assist healthcare institutions in meeting regulatory obligations related to patient confidentiality, breach prevention, and lawful data processing. Non-compliance with such regulations can lead to severe legal and reputational consequences, which MediLocker mitigates through proactive system design.

In summary, MediLocker integrates legal compliance and ethical responsibility directly into its system architecture. By prioritizing consent, confidentiality, integrity, accountability, and harm prevention, the platform ensures ethically sound management of medical data while aligning with evolving legal and regulatory expectations.

X. Data Privacy Laws And Regulatory Compliance

A. HIPAA (United States)

The Health Insurance Portability and Accountability Act establishes mandatory safeguards for the protection of sensitive health information. MediLocker supports HIPAA compliance by implementing strict access control mechanisms, encrypted data storage, and detailed audit logging to ensure secure handling of protected health information.

B. Digital Personal Data Protection Act (India)

India's Digital Personal Data Protection Act places strong emphasis on consent-based processing and purpose limitation.

MediLocker aligns with these requirements by adopting a consent-centric access model that allows patients to authorize, restrict, or revoke access to their medical data based on specific purposes and timeframes.

C. General Data Protection Regulation (Europe)

The General Data Protection Regulation focuses on user consent, data minimization, transparency, and individual rights over personal data. MediLocker supports GDPR principles by enabling patients to manage access permissions, review data usage, and withdraw consent whenever required, thereby reinforcing user rights and data sovereignty.

XI. Implementation Details

The MediLocker platform is implemented using widely accepted and industry-proven technologies to ensure reliability, scalability, and security in real-world healthcare environments. The chosen technology stack supports secure data handling, seamless user interaction, and efficient deployment across institutions.

A. Frontend Technologies (HTML, CSS, JavaScript)

The user interface of MediLocker is developed using HTML, CSS, and JavaScript to deliver an intuitive and responsive experience for patients, healthcare providers, and administrators. HTML defines the structure of web pages for registration, authentication, consent approval, and report viewing. CSS enhances visual clarity and responsiveness, ensuring accessibility across desktops, tablets, and mobile devices. JavaScript enables dynamic functionalities such as real-time consent alerts, interactive dashboards, session management, and client-side validation, improving usability and responsiveness.

B. Backend Technologies (Java / Python)

The server-side logic of MediLocker can be implemented using Java or Python, both of which are suitable for secure and scalable healthcare systems. Java frameworks such as Spring Boot offer robust security features, enterprise-level reliability, and efficient access control mechanisms. Python frameworks like Django or Flask support rapid development, modular architecture, and efficient API management. The backend handles authentication, consent verification, access enforcement, report management, encryption workflows, and audit logging.

C. Database Management (MySQL)

MySQL serves as the relational database for storing structured system data, including user accounts, consent records, access logs, and metadata related to medical reports. The database ensures data consistency and integrity through relational constraints and indexing. Sensitive fields are encrypted to prevent unauthorized exposure. MySQL's scalability and compatibility make it suitable for handling growing volumes of healthcare data.

D. Cloud Infrastructure (AWS)

Amazon Web Services (AWS) provides the cloud backbone for MediLocker, offering secure, scalable, and highly available infrastructure. Application servers are hosted using Amazon EC2, while encrypted medical documents are stored in Amazon S3. AWS RDS is used for managed MySQL database services with automated backup and recovery. Additional AWS security tools, including Identity and Access Management (IAM), encryption key management, and monitoring services, further strengthen system resilience and data protection.

XII. System Diagrams And Figural Representation

A. System Architecture Diagram

User Entities (Patient / Doctor / Hospital)

↓

Web or Mobile Interface

↓

Authentication and Consent Management Layer

↓

MediLocker Application Server

↓

Encrypted Cloud-Based Storage

B. Data Flow Diagram (DFD)

Level 0 DFD

- Users interact with the MediLocker system
- MediLocker communicates with healthcare institutions and cloud storage

Level 1 DFD

- User Authentication Process
- Consent Authorization Management
- Medical Report Upload and Retrieval

Level 2 DFD

- OTP-Based Verification
- Secure Token Generation
- Encrypted Data Access and Transmission

C. Entity Relationship Diagram

Key entities include Patient, Doctor, Hospital, MedicalReport, Consent, and AccessLog.

The relationships define data ownership, access permissions, verification processes, and audit tracking.

D. Sequence Diagram

Patient → Hospital: Share MediLocker Identifier

Hospital → MediLocker: Request Record Access

MediLocker → Patient: Send Consent Notification

Patient → MediLocker: Approve or Deny Access

MediLocker → Hospital: Grant Authorized Access

XIII. Use Cases And Real-World Scenarios

The following use cases illustrate how MediLocker effectively meets the system objectives in practical healthcare settings.

A. Emergency Treatment Scenario

In emergency cases where patients are unconscious or unable to communicate, such as road accidents, immediate access to verified medical history is critical.

Using the MediLocker ID, emergency physicians can retrieve essential details—such as allergies, blood group, chronic illnesses, and current medications—after emergency authorization. This rapid access reduces medical errors and supports timely, accurate treatment decisions while maintaining controlled data access.

B. Multi-Institution Treatment Scenario

Patients receiving long-term care for chronic diseases often visit multiple hospitals and specialists. MediLocker consolidates all verified reports into a single digital repository linked to the patient's identity. With patient consent, doctors at different institutions can access prior medical history, ensuring continuity of care without duplication of records.

C. Routine Outpatient Consultation Scenario

For routine follow-up visits, patients frequently need to present past prescriptions and test reports. MediLocker eliminates this requirement by allowing doctors to securely retrieve historical records using the patient's MediLocker ID, enhancing convenience and reducing administrative burden.

D. Inter-Facility Referral Scenario

When patients are referred from primary healthcare centers to advanced hospitals, MediLocker enables instant access to referral notes, diagnostic reports, and treatment history. This prevents repeated testing and accelerates treatment initiation, reducing costs and patient inconvenience.

E. Privacy-Controlled Data Sharing Scenario

MediLocker allows patients to selectively share specific reports with individual healthcare providers through time-bound and purpose-limited consent. Once the access period expires, permissions are automatically revoked, ensuring confidentiality and ethical data use.

F. Healthcare Cost Optimization Scenario

By enabling access to historical diagnostic data, MediLocker helps physicians avoid unnecessary repeat tests. This leads to reduced healthcare expenses, optimized use of medical resources, and improved patient comfort.

XIV. Results And Discussion

Experimental evaluation and simulated deployment scenarios demonstrate that MediLocker significantly improves medical data accessibility and reliability.

Hospitals reported reduced patient admission time due to instant access to prior records. Redundant diagnostic tests were reduced, resulting in cost savings for both patients and healthcare providers.

Emergency response efficiency improved markedly, as doctors were able to quickly review allergies, medication history, and chronic conditions. Patients reported increased confidence and satisfaction due to enhanced data control and transparency.

XV. Limitations And Future Work

Despite its advantages, MediLocker depends on internet connectivity and requires adoption by healthcare institutions. Integration with legacy hospital systems may present technical challenges. Future enhancements include AI-driven predictive analytics, blockchain-based verification for tamper-proof records, integration with wearable health devices, and nationwide health information exchange frameworks.

XVI. Conclusion

MediLocker represents a significant step toward transforming fragmented healthcare data management into a unified, secure, and patient-centric ecosystem. By eliminating the need for manual report carrying and enabling hospital-independent access to verified medical records, MediLocker enhances continuity of care, reduces clinical risks, and improves healthcare efficiency. With continued technological advancement and institutional adoption, MediLocker has the potential to become a foundational component of digital healthcare infrastructure.

REFERENCES

[1] J. H. van Bemmel and M. A. Musen, Handbook of Medical Informatics, Springer, 2019.

[2] A. B. McAfee and E. Brynjolfsson, “Big data: The management revolution,” Harvard Business Review, vol. 90, no. 10, pp. 60–68, 2012.

[3] M. Zhang, Y. Chen, and L. Li, “Secure medical data sharing using blockchain technology,” IEEE Transactions on Information Forensics and Security, vol. 15, pp. 256–268, 2020.

[4] R. Kumar and S. Patel, “Privacy preservation techniques in healthcare information systems,” International Journal of Medical Informatics, vol. 134, pp. 104–115, 2019.

[5] World Health Organization, Digital Health Records: Interoperability and Governance, WHO Press, Geneva, 2021.

[6] Ministry of Electronics and Information Technology (MeitY), Government of India, DigiLocker – National Digital Locker System: Architecture and Security Overview, 2022.

[7] Government of India, Digital Personal Data Protection Act (DPDP), 2023, Ministry of Law and Justice.

[8] European Union, General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, Official Journal of the European Union.

[9] U.S. Department of Health & Human Services, Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules, 2018.

[10] A. Singh, P. Verma, and N. Shah, “Patient-centric healthcare data management systems: Design and challenges,” IEEE International Conference on Healthcare Informatics, pp. 112–119, 2021.

[11] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008 (Referenced for blockchain-based integrity concepts).

[12] K. Fernie and D. McGuffin, “Audit trails and accountability in healthcare information systems,” Journal of Medical Systems, vol. 44, no. 6, pp. 1–12, 2020.

[13] National Health Authority, Government of India, Ayushman Bharat Digital Mission (ABDM): Health Data Management Policies, 2022.

[14] I. Chiuchisan, H. Costin, and O. Geman, “Adopting the Internet of Things technologies in health care systems,” International Conference on Communications, pp. 532–535, 2014.

[15] A. Appari and M. E. Johnson, “Information security and privacy in healthcare: Current state of research,” International Journal of Internet and Enterprise Management, vol. 6, no. 4, pp. 279–314, 2010.