International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 07, NCIRTAI - 2026

Blockchain - Based Secure Medical Data Management

Ms.V.HEMA[1], Mrs.P.Rohini[2], Mrs.C.KOWSALYA[3]
[1]Student, Department of CSE, Chendhuran College of Engineering & Technology, Pudukkottai.
[2]Assistant Professor & Head , Department of CSE, Chendhuran College of Engineering & Technology, Pudukkottai.
[3]Assistant Professor, Department of CSE, Chendhuran College of Engineering & Technology, Pudukkottai.
Email id: vhema4201@gmail.com[1], rohini.ccet@gmail.com[2], queenbbe9722@gmail.com[3]

ABSTRACT **- In the modern healthcare ecosystem, ensuring the security of patient medical data while enabling timely and controlled access for authorized healthcare professionals is a critical challenge. Traditional healthcare record management systems often suffer from inadequate access control, lack of transparency, and vulnerability to data breaches, resulting in compromised patient privacy and data integrity. To address these issues, this project proposes a Blockchain-based secure Medical Data Management that provides a patient-centric, consent-driven, and highly secure digital healthcare solution. The proposed system is built on a role-based architecture involving Admin, Doctor, and Patient modules. Patients retain full ownership and control over their medical records, while doctors can access patient records only after obtaining explicit, time-bound consent from the patient. Administrators oversee user verification, access approvals, and system-level security monitoring. Medical reports uploaded by doctors are securely encrypted before storage, ensuring data confidentiality and integrity at rest. Instead of exposing direct file URLs, the system uses secure, time-limited access tokens to prevent unauthorized downloads, link sharing, and misuse of sensitive medical data. To further enhance security, the system integrates OTP-based verification for critical operations such as record access approvals and sensitive data viewing. Patients receive real-time notifications and OTPs, allowing them to explicitly approve or deny doctor access requests. All access events are recorded through audit logging and tamper-detection mechanisms, ensuring traceability, accountability, and compliance with security standards. Additional functionalities such as appointment management, emergency access handling, real-time notifications, and administrative dashboards with analytics improve system usability and operational efficiency. The application is developed using the MERN stack (MongoDB, Express.js, React.js, Node.js), providing a scalable and robust architecture suitable for real-world healthcare environments. Overall, the proposed system ensures confidentiality, integrity, availability, and patient-controlled access to medical data, making it a secure, scalable, and trustworthy solution for modern digital healthcare record management.**

Keywords--- **MERN Stack, Secure Access Tokens, Tamper Detection, Role-Based Access Control (RBAC), Electronic Health Records (EHR)**

I. INTRODUCTION

Healthcare is one of the most critical sectors where data accuracy, privacy, and security play a vital role. Medical records contain highly sensitive information such as patient identity details, medical history, diagnostic reports, prescriptions, and treatment plans. In recent years, healthcare institutions have rapidly shifted from manual paper-based record systems to digital healthcare record management systems in order to improve efficiency, accessibility, and quality of patient care.

However, this digital transformation has also introduced serious challenges related to data security, privacy, and unauthorized access. Many existing systems store patient records in centralized databases with limited security controls, making them vulnerable to cyberattacks, data leaks, and misuse by insiders. Once compromised, patient data can be altered, stolen, or misused without the patient's knowledge.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 07, NCIRTAI - 2026

Hence, there is an urgent need for a secure and patient-controlled healthcare record management system that ensures confidentiality, integrity, and transparency of medical data.

II. BACKGROUND OF THE STUDY

Traditionally, medical records were maintained as physical files within hospitals or clinics. These records were difficult to share across institutions and prone to loss, damage, and duplication. With the advancement of information technology, electronic health record (EHR) systems were introduced to digitize patient data and allow faster access by healthcare professionals.

Although EHR systems improved efficiency, they introduced new security concerns. Most existing digital systems follow a centralized access model, where administrators or doctors can access patient records without explicit patient approval. Patients have minimal control over who views their data, how long it is accessed, or for what purpose.

Furthermore, many systems lack proper audit mechanisms to track record access and modifications. This results in reduced transparency and accountability, increasing the risk of unauthorized data usage. These limitations highlight the importance of designing a secure, transparent, and consent-driven healthcare record system.

III. PROBLEM STATEMENT

Existing healthcare record management systems do not provide sufficient security and patient control over medical data. Medical records are often stored in centralized databases without strong encryption and without proper consent mechanisms. Patients are unable to track or restrict access to their records, leading to privacy violations and data misuse. There is a lack of transparency in record access, and systems fail to provide tamper-proof audit trails. These issues demand a secure healthcare record management solution that ensures confidentiality, integrity, availability, and patient ownership of medical data. The system introduces a patient-centric approach where patients have complete ownership and control over their medical data.

IV. EXISTING SYSTEM

In the existing healthcare system, patient medical records are mostly maintained either in physical form or in centralized digital databases managed by hospitals or healthcare organizations. These systems allow doctors and administrators to access patient data directly without explicit approval from the patient in many cases.

Most existing systems rely on centralized storage models where all data is stored in a single location. Access control is often limited to role-based permissions, but lacks fine-grained control and real-time consent from patients.

The conventional healthcare record management system follows a centralized architecture in which patient data is collected during clinical visits and subsequently recorded or updated by healthcare professionals. These medical records are stored in a centralized database system, enabling authorized doctors and administrative staff to retrieve and modify patient information as required. Access control mechanisms in such systems are typically coarse-grained and institution-centric, allowing healthcare providers continuous access without dynamic or patient-driven authorization. Consequently, patients have limited or no control over their medical data once it is stored. Furthermore, the system lacks transparency and fine-grained auditing capabilities, preventing patients from monitoring access patterns, including who accessed their data, when it was accessed, and for what purpose. This absence of patient-centric control and visibility introduces significant risks related to data privacy, unauthorized access, and potential misuse of sensitive healthcare information.

V. PROPOSED SYSTEM

The proposed system introduces that focuses on security, transparency, and patient consent. In this system, medical records are encrypted before storage and can only be accessed by authorized users with patient approval. The system follows a patient-centric model where patients are the owners of their medical data and can control who accesses it and for how long.

VI. SYSTEM ARCHITECTURE

The Secure Healthcare Record Management System follows a client–server architecture. The system consists of three major layers:

1. Presentation Layer (Frontend)
2. Application Layer (Backend)
3. Data & Security Layer

Each layer is responsible for a specific set of operations and communicates securely with other layers.The Presentation Layer (frontend) serves as the user interface through which patients, doctors, and administrators interact with the system via

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 07, NCIRTAI - 2026

web-based dashboards. User requests generated from this layer are forwarded to the Application Layer (backend), where all core business logic, authentication, and authorization processes are executed. The backend validates user identity using secure mechanisms such as JWT-based authentication and enforces role-based and consent-driven access control policies.

Once validated, the system processes requests such as uploading, accessing, or modifying medical records. Sensitive data is encrypted before being transmitted to the Data & Security Layer, which ensures secure storage and management of healthcare information. This layer includes a MongoDB database for storing user data, medical records metadata, consent details, and audit logs, along with encrypted storage systems and blockchain-based logging for tamper-proof record tracking.

Additionally, the system incorporates secure view mechanisms using time-limited tokens, ensuring that medical records are accessed only by authorized users for a limited duration. All interactions, including access requests and approvals, are recorded through audit logs and blockchain logs to maintain transparency, accountability, and data integrity across the system.

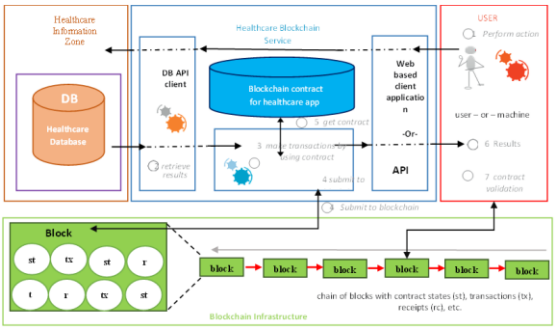

Fig 1. System architecture

A.PATIENT DASHBOARD

The patient dashboard serves as a secure and user-centric interface designed to empower patients with full control over their medical data. Through this system, patients can seamlessly access and review their medical records in a secure environment. Additionally, the platform enables patients to grant or revoke consent to healthcare providers, thereby ensuring that data sharing remains strictly under patient authorization. A key feature of the dashboard is its transparency mechanism, which allows patients to monitor and track all access events related to their records. This auditability enhances trust and accountability within the healthcare ecosystem. Furthermore, the system provides real-time notifications and alerts to keep patients informed about important activities and updates.To strengthen data privacy, the platform implements a secure access mechanism wherein medical reports are made available exclusively through time-limited view tokens. This approach minimizes the risk of unauthorized access and ensures that sensitive health information remains protected at all times.

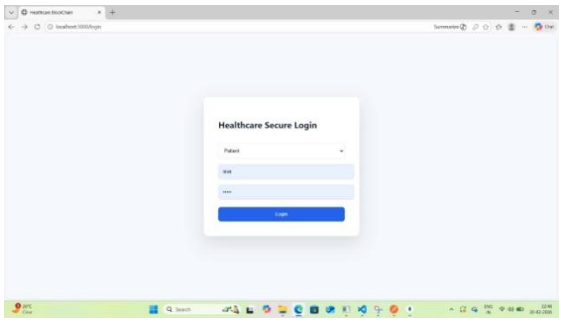

Fig 2. Patient Login

B.DOCTOR DASHBOARD

The doctor dashboard is designed to provide healthcare professionals with a secure and efficient interface for managing patient-related information and clinical workflows. Through this platform, doctors can upload medical reports in an encrypted format, ensuring that sensitive patient data is protected both during transmission and storage. Access to patient records is governed by a strict consent-based model, wherein doctors are permitted to view medical information only after explicit authorization has been granted by the patient. This approach reinforces patient-centric data ownership and aligns with privacy-preserving healthcare practices. In addition to record management, the dashboard supports appointment scheduling and management, enabling doctors to efficiently organize and track their clinical engagements. Furthermore, medical reports can be accessed through secure, time-limited tokens, ensuring that data visibility is restricted and safeguarded against unauthorized access.

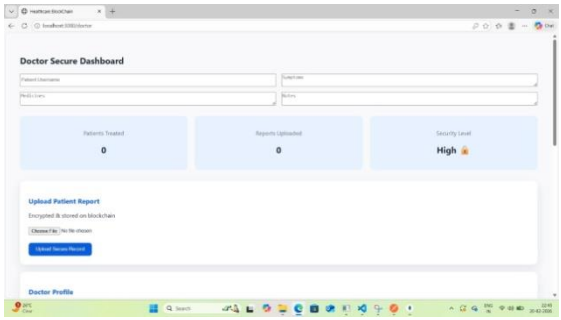

Fig 3. Doctor Accesss

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 07, NCIRTAI - 2026

C. ADMIN DASHBOARD

The admin dashboard provides a centralized interface for system administrators to manage and oversee platform operations. It enables administrators to verify and authenticate doctors, ensuring that only authorized professionals access the system. Additionally, the dashboard supports continuous monitoring of system activities to maintain operational integrity.A key feature includes access to audit logs and blockchain logs, which enhances transparency and traceability of all actions within the system. The platform also facilitates efficient handling of emergency alerts, allowing administrators to respond promptly to critical situations.

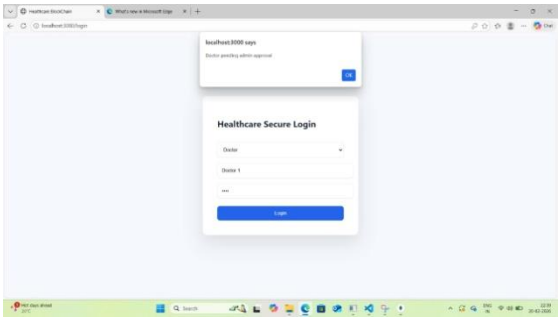

Fig 4. Admin Approval

VII. BLOCKCHAIN TECHNOLOGY

Blockchain is a decentralized and tamper-resistant digital ledger used in the proposed system to securely record all critical activities, such as patient consent, data access, and transaction logs. Each event is stored as an immutable block, ensuring that records cannot be altered or deleted. This provides transparency, traceability, and enhanced security, allowing all stakeholders to verify actions without compromising sensitive medical data. To enhance security, transparency, and data integrity, the proposed system incorporates blockchain technology as a core component of its architecture. Blockchain is utilized to maintain an immutable and tamper-resistant record of all critical system activities, including data access events, consent approvals, and transaction logs. Each access request and authorization is recorded as a transaction on the blockchain, ensuring that all interactions with patient data are transparent and verifiable. This decentralized logging mechanism prevents unauthorized modifications and provides a reliable audit trail for compliance and accountability. Furthermore, the integration of blockchain strengthens trust among stakeholders by enabling secure verification of data integrity without exposing sensitive medical information. By combining blockchain with encryption and token-based access control, the system ensures a highly secure, traceable, and trustworthy healthcare record management environment.

VIII. IPFS (InterPlanetary File System)

IPFS is a decentralized storage protocol used in the proposed system to store encrypted medical records across a distributed network. Files are identified and accessed using unique content-based hashes instead of centralized URLs, ensuring data integrity, high availability, and resistance to tampering while eliminating single points of failure. The system utilizes IPFS (InterPlanetary File System) as a decentralized storage solution for managing medical records. Encrypted patient data is stored across a distributed network, eliminating reliance on centralized servers and enhancing system resilience.

IPFS provides several key advantages, including distributed storage, which improves data availability, and tamper-resistant architecture, which ensures data integrity. Additionally, the decentralized nature of IPFS significantly reduces the risk of data loss and single-point failures. To further strengthen security, only encrypted medical files are uploaded to IPFS, ensuring that sensitive information remains protected even within the distributed environment.

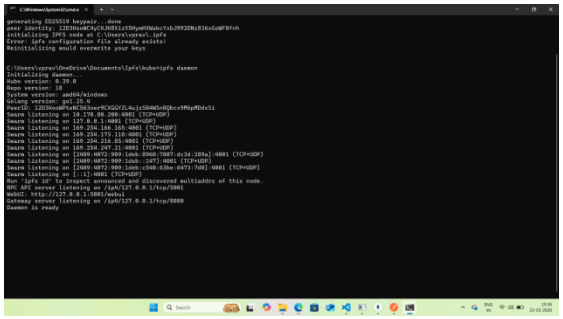

Fig 4. Approve Security

A.OUTCOME OF THIS DEVICE

The system ensures high levels of data security and privacy by encrypting medical records and storing them on IPFS, while access is controlled via secure, time-limited tokens to prevent unauthorized downloads or tampering. Patients retain full control over their records, granting or revoking doctor access in real time with OTP-based verification for sensitive operations. Transparency and accountability are achieved through blockchain-based audit logging, which records all access and consent events in an immutable, tamper-resistant ledger. The platform also enhances operational efficiency through role-specific dashboards for patients, doctors, and administrators, supporting appointment management, emergency alerts, and real-time

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 07, NCIRTAI - 2026

notifications. Built on the MERN stack, the system provides a scalable and reliable architecture suitable for modern healthcare environments. Overall, the project establishes a secure, transparent, and efficient framework for managing healthcare records while maintaining patient control and trust.

Test Case ID	Test Description	Expected Result	Status
TC01	Patient registration	Patient account created successfully	Pass
TC02	Patient login	User authenticated and dashboard displayed	Pass
TC03	Doctor login with OTP	Login allowed only after OTP verification	Pass
TC04	Admin verifies doctor	Doctor account approved successfully	Pass
TC05	Doctor uploads medical report	File encrypted and stored securely	Pass
TC06	Patient grants consent	Consent activated for specified time	Pass

Table 1.1 RESULT

IX.CONCLUSION AND FUTURE ENHANCEMENT

The Blockchain-Based Secure Medical Data Management has been successfully designed and implemented to address the critical challenges of medical data security, privacy, and controlled access in modern healthcare systems. Traditional healthcare record systems often suffer from issues such as unauthorized access, data tampering, lack of patient control, and poor transparency. This project effectively overcomes these limitations by introducing strong security mechanisms and patient-centric access control.The system ensures that all medical records are encrypted before storage, thereby protecting sensitive health information from unauthorized access. Role-based authentication combined with OTP verification for doctors strengthens system security and prevents identity misuse. The admin verification module further enhances trust by allowing only verified doctors to access patient records. One of the major achievements of this project is the implementation of patient consent-based access control. Patients retain full ownership of their medical data and can grant or revoke access to doctors for a limited time. Secure view tokens ensure that medical reports can be accessed only through authorized, time-bound, and single-use links. Audit logging provides transparency by maintaining a detailed record of all sensitive actions performed within the system.Overall, the system successfully demonstrates a secure, scalable, and user-friendly healthcare record management solution that prioritizes patient privacy while enabling efficient doctor-patient interaction.

X. REFERENCES

[1] A. Kumari, S. Tanwar, S. Tyagi, and N. Kumar, ‘‘Fog computing for 2242
healthcare 4.0 environment: Opportunities and challenges,’’ Comput. 2243
Electr. Eng., vol. 72, pp. 1–13, Nov. 2018. 2244
[2] P. Campanella, E. Lovato, C. Marone, L. Fallacara, A. Mancuso, 2245
W. Ricciardi, and M. L. Specchia, ‘‘The impact of electronic health 2246
records on healthcare quality: A systematic review and meta-analysis,’’ 2247
Eur. J. Public Health, vol. 26, no. 1, pp. 60–64, Feb. 2016. 2248
[3] S. Tanwar, K. Parekh, and R. Evans, ‘‘Blockchain-based electronic health- 2249
care record system for healthcare 4.0 applications,’’ J. Inf. Secur. Appl., 2250
vol. 50, Feb. 2020, Art. no. 102407. 2251
[4] I. Mistry, S. Tanwar, S. Tyagi, and N. Kumar, ‘‘Blockchain for 5G- 2252
enabled IoT for industrial automation: A systematic review, solutions, 2253
and challenges,’’ Mech. Syst. Signal Process., vol. 135, Jan. 2020, 2254
Art. no. 106382. 2255
[5] S. Tanwar, K. Parekh, and R. Evans, ‘‘Blockchain-based electronic health- 2256
care record system for healthcare 4.0 applications,’’ J. Inf. Secur. Appl., 2257
vol. 50, Feb. 2020, Art. no. 102407. 2258
[6] P. Tagde, S. Tagde, T. Bhattacharya, P. Tagde, H. Chopra, R. Akter, 2259
D. Kaushik, and M. Rahman, ‘‘Blockchain and artificial intelligence 2260
technology in e-health,’’ Environ. Sci. Pollut. Res., vol. 28, no. 38, 2261
pp. 52810–52831, Oct. 2021. 2262
[7] J. Vora et al., ‘‘Ensuring privacy and security in e-health records,’’ in Proc. 2263
Int. Conf. Comput. Inf. Telecommun. Syst. (CITS), Jul. 2018, pp. 1–5. 2264
[8] S. Tanwar, K. Parekh, and R. Evans, ‘‘Blockchain-based electronic health- 2265
care record system for healthcare 4.0 applications,’’ J. Inf. Secur. Appl., 2266
vol. 50, Feb. 2020, Art. no. 102407. 2267
[9] T. Kubo, A. Yanasan, T. Herbosa, N. Buddh, F. Fernando, and R. Kayano, 2268
‘‘Health data collection before, during and after emergencies and 2269

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 07, NCIRTAI - 2026

disasters—The result of the Kobe expert meeting,'' Int. J. Environ. Res. 2270
Public Health, vol. 16, no. 5, p. 893, Mar. 2019. 2271
[10] J. M. Puaschunder, ''The potential for artificial intelligence in health- 2272
care,'' Future Healthcare J., vol. 6, no. 2, p. 94, 2019.