International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 14, Issue 1, 2026

Medicloudcare: Scalable EHR Framework

Ms. A Kavya[1], K Amithi[2], Enti Mahita Ratna[3], Y Vyshnavi[4]

[1]Assistant Professor; Department Of Computer Science And Engineering(AI&ML) Bhoj Reddy Engineering College For Women Hyderabad India.

[2,3,4]B.Tech Students; Department Of Computer Science And Engineering(AI&ML) Bhoj Reddy Engineering College For Women Hyderabad India.

Mail Id; amithiprakash@gmail.com[2] ,vyshnaviy02@gmail.com[4] ,entimahitaratna@gmail.com[3]

Abstract

MediCloudCare is a decentralized Electronic Health Record (EHR) management system developed to enhance the security, privacy, and accessibility of healthcare data. Traditional EHR systems rely on centralized storage architectures, which are highly vulnerable to data breaches, unauthorized access, and limited interoperability among healthcare providers. To overcome these challenges, the proposed system integrates blockchain technology with the InterPlanetary File System (IPFS) to ensure secure and tamper-resistant storage of medical data. In this approach, medical records are stored in IPFS, while their corresponding cryptographic hashes are maintained on the Ethereum blockchain to ensure data integrity and transparency. The system incorporates role-based access control, enabling patients, doctors, and laboratories to interact securely while giving patients full control over their health records. Furthermore, MetaMask authentication and smart contracts are utilized to strengthen trust and enforce secure access policies. An AI-powered chatbot is also integrated to improve user interaction and accessibility. Overall, MediCloudCare presents a secure, transparent, and patient-centric solution for modern healthcare data management.

Keywords— *Blockchain, EHR, IPFS, Smart Contracts, Healthcare Security, Data Privacy, Decentralization*

INTRODUCTION

The rapid evolution of digital technologies has significantly transformed the healthcare sector, particularly through the adoption of Electronic Health Records (EHR). However, most conventional EHR systems operate on centralized infrastructures, which introduce critical challenges related to data security, privacy, and ownership. In such systems, patient information is stored in a single database, making it vulnerable to cyberattacks and unauthorized access. Moreover, centralized models limit patient control over their medical data. To address these issues, MediCloudCare proposes a decentralized healthcare data management system that combines blockchain technology and IPFS. Blockchain ensures transparency, immutability, and trust, while IPFS provides secure and distributed storage for large medical files. This integration enhances both data protection and accessibility while empowering patients with greater control over their healthcare information.

Existing System

Existing healthcare information systems predominantly rely on centralized databases to store patient records. These systems often result in fragmented data, as medical information is distributed across multiple hospitals and laboratories without proper integration. Consequently, healthcare providers face difficulties in accessing a patient's complete medical history, which can impact the quality of care. Additionally, centralized systems lack strong interoperability standards, making secure data sharing between institutions inefficient. The dependence on a single storage system also increases the risk of system failures and cyber threats, further compromising sensitive patient information.

Limitations of Existing Systems

Traditional healthcare systems face several limitations due to their centralized nature. One major issue is the high risk of data breaches, as centralized databases are prime targets for cyberattacks. Furthermore, there is limited interoperability between different healthcare providers, which restricts seamless data exchange. Patients also have minimal control over their own medical records, as data access and management are handled by institutions. Another significant drawback is the presence of a single point of failure, where any system malfunction or attack can disrupt the entire database. Additionally, these systems lack transparency, as users are often unaware of how and when their data is accessed or modified.

Proposed System

MediCloudCare introduces a decentralized architecture that leverages blockchain and IPFS to address the limitations of traditional systems. Instead of storing large medical files directly on the blockchain, the system stores them in IPFS, while only their unique cryptographic hashes are recorded on the blockchain. This approach ensures data integrity, immutability, and efficient storage management. Smart contracts are employed to manage access control dynamically, allowing patients to grant or revoke permissions to healthcare

providers as needed. This design ensures secure, transparent, and patient-driven data sharing.

LITERATURE SURVEY

Recent studies have highlighted the limitations of storing large volumes of medical data directly on blockchain networks due to high costs and scalability issues. Researchers such as Liu et al. (2020) and Guo et al. (2022) propose a hybrid architecture in which blockchain is used to store only metadata, such as cryptographic hashes, while actual data is stored off-chain using decentralized storage systems like IPFS. This approach ensures efficient storage management while maintaining data integrity and security. MediCloudCare adopts this hybrid model to achieve scalability and cost-effectiveness while ensuring secure data verification.

Smart Contract-Based Access Control

Ensuring secure and flexible access control is a critical requirement in healthcare systems. Studies by Shuaib et al. (2022) and Wang et al. (2024) emphasize the use of smart contracts to implement fine-grained access control mechanisms. These contracts allow automated enforcement of access policies, ensuring that only authorized users can access sensitive medical data. MediCloudCare incorporates this concept by using smart contracts to enable patient-controlled access, thereby improving privacy and trust in the system.

Cloud Computing in Healthcare

Cloud computing has been widely adopted in healthcare for its scalability and ability to provide real-time access to medical data. Bamiah et al. (2023) highlighted the benefits of cloud-based systems, including improved collaboration and cost efficiency. However, the study also identified security concerns such as unauthorized access and data breaches. MediCloudCare addresses these issues by integrating blockchain technology with decentralized storage, thereby enhancing security while maintaining the advantages of cloud-based systems.

REQUIREMENT ANALYSIS

Functional Requirements

The MediCloudCare system is designed with multiple functional modules to support different stakeholders in the healthcare ecosystem. The patient module enables users to register, log in securely, upload medical records, and manage access permissions by granting or revoking authorization to healthcare providers. Patients can also view their complete medical history in a structured format. The doctor module allows authorized medical professionals to access patient records upon receiving permission, upload diagnoses, and provide treatment recommendations. Additionally, the diagnostic module supports laboratories and diagnostic centers by enabling them to upload test reports and share them securely with both patients and doctors. These modules collectively ensure seamless interaction, secure data sharing, and efficient healthcare service delivery.

Non-Functional Requirements

The system is designed to meet several non-functional requirements to ensure quality and reliability. In terms of performance, MediCloudCare provides fast response times during file uploads, data retrieval, and blockchain transactions, minimizing delays for users. Security is a critical aspect, and the system ensures encrypted communication along with blockchain-based verification to protect sensitive medical data. Scalability is achieved through decentralized storage and modular architecture, allowing the system to handle increasing users and large volumes of data efficiently. The usability of the system is enhanced through a simple and intuitive user interface, enabling easy navigation for all types of users. Furthermore, the system is designed to maintain high availability with an uptime target of 99.9%, ensuring continuous access to medical records. Reliability is also emphasized, as the system consistently performs operations without failure and guarantees that data remains accessible whenever required.

Computational Resource Requirements

Hardware Requirements

The system requires standard computing resources to operate efficiently. A processor equivalent to an Intel Core i5 is recommended to handle application processing and blockchain interactions. A minimum of 8 GB RAM is required to support smooth multitasking and system performance. Additionally, at least 256 GB of storage is necessary to accommodate application files, databases, and temporary data.

Software Requirements

The software requirements define the technological framework used to develop and deploy the system. MediCloudCare operates on Windows 10 as the primary operating system. The frontend is developed using React.js along with HTML and CSS to create a responsive and interactive user interface. The backend is implemented using Node.js with the Express.js framework to handle server-side logic and API communication. MongoDB is used as the database, with Mongoose as the Object Relational Mapping (ORM) tool for schema management. The system is developed using JavaScript (ES6+) as the primary programming language. Blockchain integration is achieved using Ethereum and Solidity for smart contract development. IPFS is utilized for decentralized storage of medical records, ensuring secure and distributed data management.

Life Cycle Model

The development of MediCloudCare follows the Iterative Process Model, which enables the system

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 14, Issue 1, 2026

to be built incrementally through repeated cycles. Instead of developing the entire system in a single phase, the project is divided into smaller modules, each of which is developed, tested, and refined independently. During each iteration, all phases of the software development lifecycle—including planning, requirement analysis, design, implementation, testing, and maintenance—are executed. After each cycle, the system is evaluated, and improvements are made based on feedback and identified issues. This approach allows early detection of errors, continuous enhancement, flexibility in accommodating changes, and ultimately results in a more robust and high-quality software system.

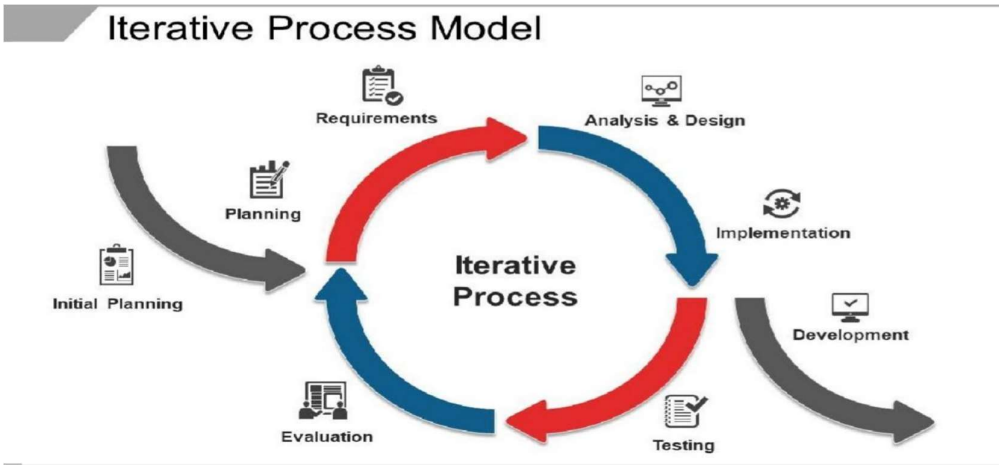


Fig 1; Iterative Process Model

System Architecture

The architecture of MediCloudCare defines the structure and interaction of its various components, including the frontend, backend, blockchain network, IPFS storage, and database. The system processes user requests in a sequential manner, starting from the user interface and passing through backend services before interacting with decentralized components. The architecture ensures modularity, scalability, and efficient request handling.

Software Architecture

The software architecture outlines how different software components interact within the system. It includes the frontend interface, backend APIs, database management system, and integration with blockchain and IPFS. Each component is designed to perform specific tasks while maintaining seamless communication with other modules.

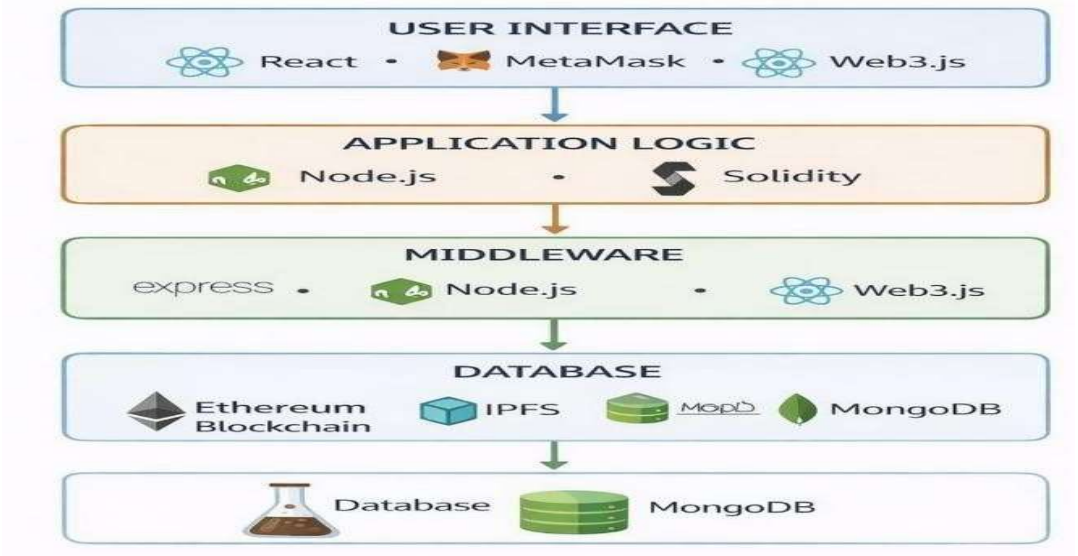


Fig 2; Software Architecture

Technical Architecture

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 14, Issue 1, 2026

The technical architecture focuses on the underlying technologies and tools used to implement the system. It includes Ethereum blockchain for storing hashes, IPFS for decentralized file storage, MongoDB for metadata storage, and MetaMask for authentication. This layered architecture ensures secure, scalable, and efficient system performance.

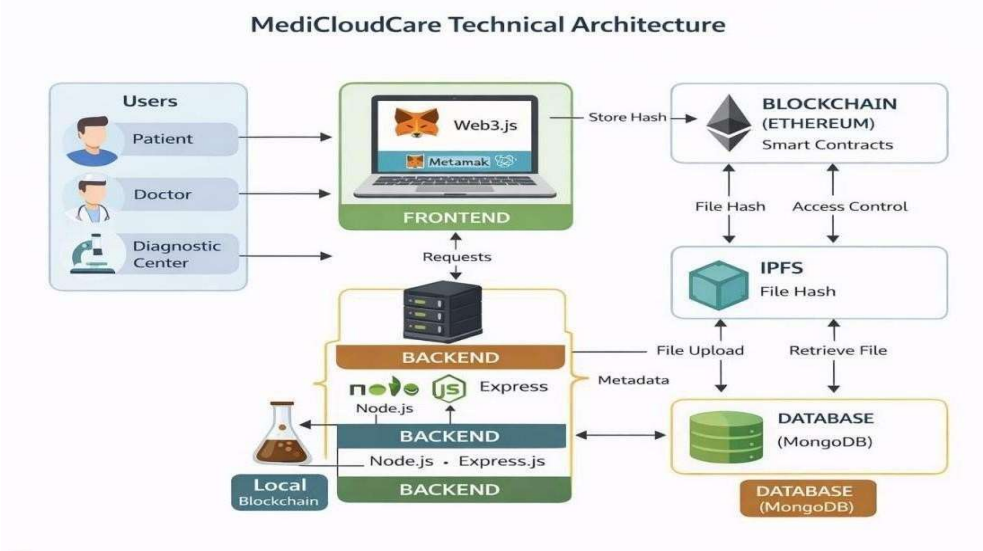


Fig 3; Technical Architecture

IMPLEMENTATION

The MediCloudCare system is implemented as a decentralized application that integrates blockchain technology and IPFS to ensure secure and transparent management of electronic health records. The implementation begins with the development of a user-friendly interface using React.js, allowing users to interact with the system efficiently. Medical data such as reports and prescriptions are collected through the interface and processed by the backend.Uploaded files are stored in IPFS, where each file generates a unique hash that acts as its identifier. This hash is then stored on the Ethereum blockchain using smart contracts, ensuring data immutability and integrity. Authentication is handled through MetaMask, enabling secure blockchain-based login and transaction signing. Role-based access control is enforced through smart contracts, ensuring that only authorized users can access specific records.MongoDB is used to store non-sensitive data such as user profiles and metadata, enabling efficient data management. The system also incorporates logging and monitoring mechanisms to track all activities and ensure transparency. Additionally, an AI-based module is integrated for report analysis and chatbot interaction, enhancing system usability and functionality.

Technologies Used

The implementation of MediCloudCare utilizes a combination of modern technologies. The frontend is developed using React.js, supported by Tailwind CSS and JavaScript for building a responsive user interface. The backend is implemented using Node.js and Express.js to handle server-side operations and API communication. Smart contracts are written in Solidity and deployed using tools such as HardHat.

MongoDB serves as the database for storing metadata and user-related information. IPFS is used for decentralized storage of medical files, ensuring secure and distributed data management. The Ethereum blockchain is used to store file hashes and maintain an immutable record of transactions. MetaMask provides wallet-based authentication and secure transaction signing. Development tools such as Ganache and Visual Studio Code are used for testing and implementation.

TESTING

Testing plays a crucial role in ensuring the reliability, security, and efficiency of the MediCloudCare system. It involves validating system functionality, performance, and data protection mechanisms across various modules, including file upload, blockchain integration, access control, and data retrieval.

Dimensions of Testing

The system is evaluated across multiple dimensions to ensure quality. Functional testing verifies that all system operations perform correctly, including login, file upload, and access management. Performance testing assesses the speed and efficiency of operations such as file uploads and blockchain transactions. Security testing ensures that authentication and data protection mechanisms prevent unauthorized access. Usability testing evaluates the ease of use and user experience of the system.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 14, Issue 1, 2026

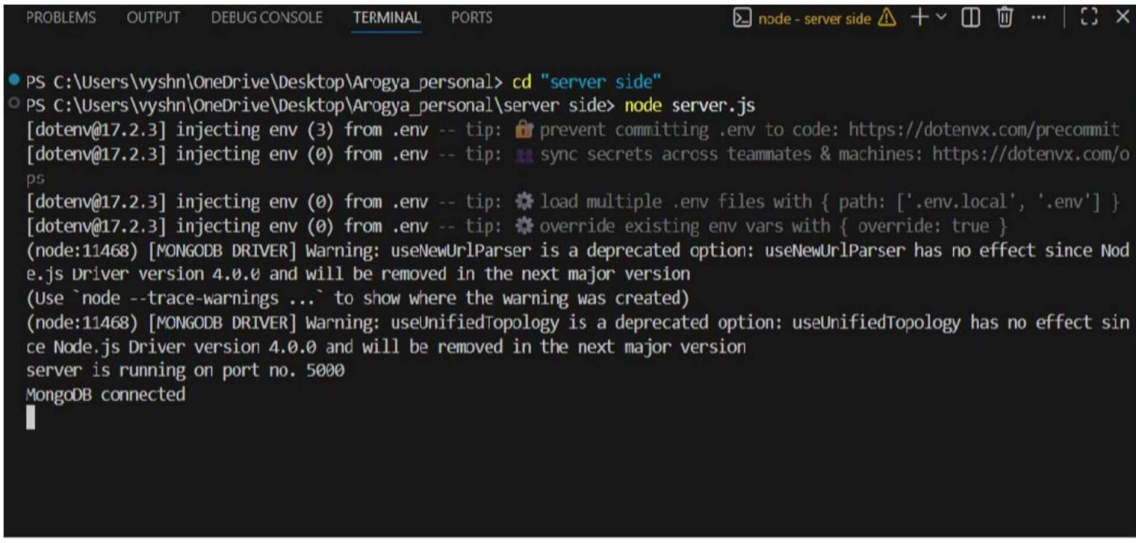
Stages of Testing

Testing is conducted in multiple stages to ensure system reliability. Unit testing focuses on individual modules such as authentication and smart contracts. Integration testing ensures that all system components work together seamlessly. System testing validates the complete end-to-end functionality of the application. Acceptance testing ensures that the system meets user requirements and expectations.

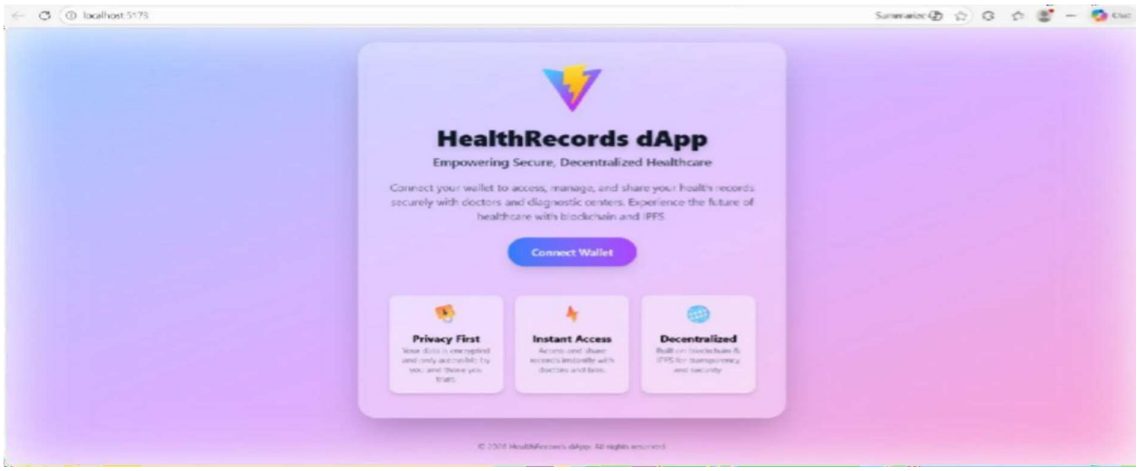
Types of Testing

Different testing approaches are used to validate system performance. Manual testing is performed to verify user interface functionality and workflows. Automated testing is used for APIs, backend services, and smart contract execution. Regression testing ensures that system updates do not affect existing functionality. Security testing validates authentication, authorization, and data protection mechanisms.

INPUT AND OUTPUT

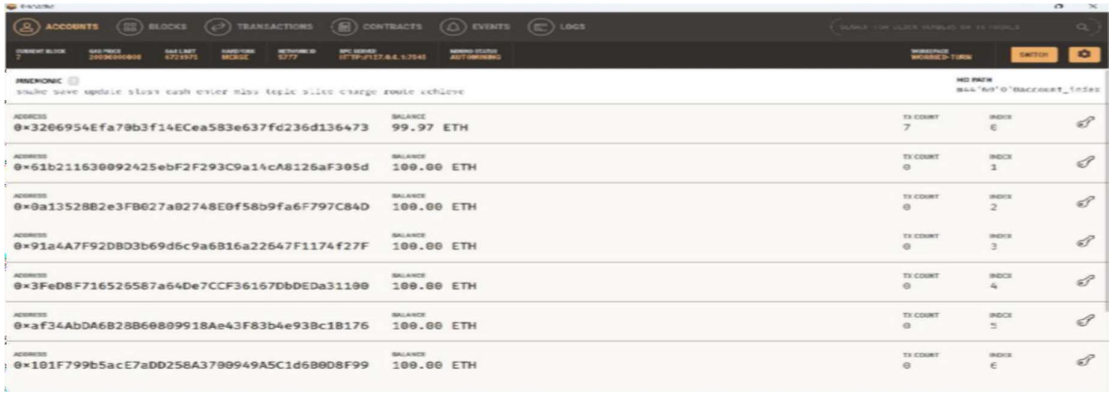


Screenshot 1: command prompt

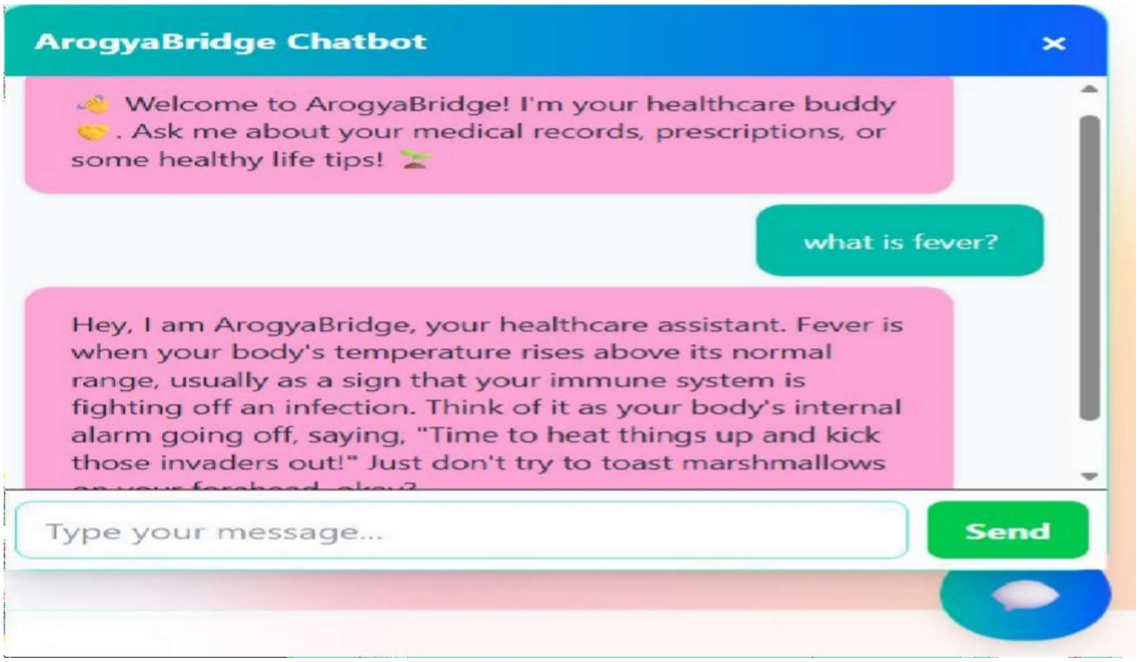


Screenshot 2: Home Page

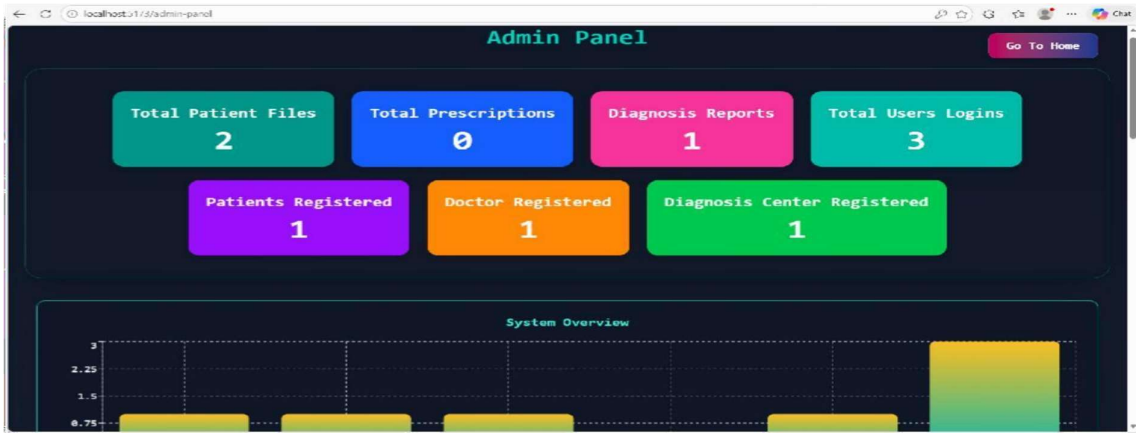
International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 14, Issue 1, 2026



Screenshot 3: Transactions



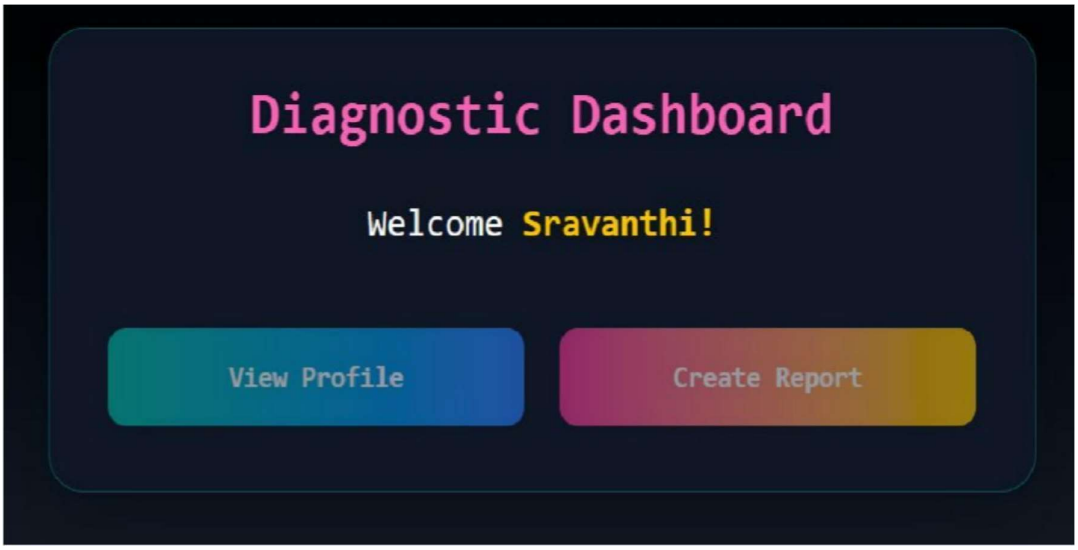
Screenshot 4: AI Assistance



Screenshot 5: Admin Panel

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 14, Issue 1, 2026

Screenshot 6: Doctor's Profile



Screenshot 7: Diagnostic Dashboard

Conclusion

The MediCloudCare system presents an effective approach to managing Electronic Health Records (EHR) through a decentralized architecture that emphasizes security, transparency, and data integrity. By integrating modern web technologies with blockchain and distributed storage, the system addresses the key limitations of conventional centralized healthcare solutions. The combination of the MERN stack with Ethereum blockchain and IPFS enables secure handling of sensitive medical data while ensuring that records remain immutable and verifiable.A significant contribution of the system is its patient-centric design, where individuals are given full control over their medical information. Through the use of smart contracts and MetaMask authentication, patients can manage access permissions, thereby enhancing privacy and trust. The use of IPFS for file storage ensures efficient and decentralized management of large medical datasets, while blockchain technology maintains a transparent and tamper-resistant audit trail

Future Scope

The MediCloudCare system can be further enhanced in several directions to improve its functionality and

real-world applicability. One potential area of improvement is interoperability with existing healthcare systems. By integrating standardized healthcare protocols and APIs, the platform can enable seamless data exchange between hospitals, clinics, and other medical institutions, thereby improving coordination and continuity of care.

Another promising extension involves the incorporation of advanced artificial intelligence techniques. Future versions of the system could include AI-based modules for disease prediction, personalized health recommendations, and automated medical report analysis, which would significantly enhance decision-making capabilities and patient support.

The integration of Internet of Things (IoT) devices and wearable health technologies also presents an important opportunity. By collecting real-time physiological data from devices such as smartwatches and fitness trackers, the system could provide continuous health monitoring and early detection of medical conditions.

In addition, the development of a dedicated mobile application would improve accessibility and user convenience, allowing patients and healthcare providers to manage records anytime and anywhere. Finally, the system can be scaled to support multi-hospital environments and large healthcare networks, enabling widespread adoption across different regions and healthcare ecosystems.

REFERENCES

[1] A. Hahnaz, U. Qamar, and A. Khalid, "Using blockchain for electronic health records," *IEEE Access*, vol. 7, pp. 147782–147795, 2019.

[2] F. A. Reen *et al.*, "Decentralized patient-centric e-health record management system using blockchain and IPFS," in *Proc. Int. Conf. Computer and Information Sciences*, 2020.

[3] A. A. Mamun, S. Azam, and C. Gritti, "Blockchain-based electronic health records management: A comprehensive review and future research direction," *IEEE Access*, vol. 10, pp. 5768–5789, 2022.

[4] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," *IEEE Access*, vol. 5, pp. 14757–14767, 2017.

[5] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Proc. Int. Conf. Open and Big Data*, 2016.

[6] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control," *Journal of Medical Systems*, vol. 40, no. 10, p. 218, 2016.

[7] A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman, "A case study for blockchain in healthcare: MedRec prototype for electronic health records and medical research data," in *Proc. IEEE Open and Big Data Conf.*, 2016.

[8] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, "FHIRChain: Applying blockchain to securely and scalably share clinical data," *Computational and Structural Biotechnology Journal*, vol. 16, pp. 267–278, 2018.

[9] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "Secure and trustable electronic medical records sharing using blockchain," in *Proc. AMIA Annual Symposium*, 2017.

[10] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in *Proc. IEEE 28th Annual Int. Symp.*, 2017.

[11] T. T. Kuo, H. E. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and healthcare applications," *Journal of the American Medical Informatics Association*, vol. 24, no. 6, pp. 1211–1220, 2017.

[12] C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, "Blockchain technology in healthcare: A systematic review," *Healthcare*, vol. 7, no. 2, p. 56, 2019.

[13] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, "MedBlock: Efficient and secure medical data sharing via blockchain," *Journal of Medical Systems*, vol. 42, no. 8, p. 136, 2018.

[14] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring," *Journal of Medical Systems*, vol. 42, no. 7, p. 130, 2018.

[15] S. Tanwar, K. Parekh, and R. Evans, "Blockchain-based electronic healthcare record system for Healthcare 4.0 applications," *Journal of Information Security and Applications*, vol. 50, p. 102407, 2020.