International Journal of
Information Technology & Computer Engineering

ISSN 2347-3657

Volume 14, Issue 1, 2026

Mediblock

A Hima Bindu[1],Vaka Thanmayee Sai[2],Pendam Varshitha[3],Are Vennela[4]

[1]Assistant Professor; Department Of Computer Science And Engineering, Bhoj Reddy Engineering College For Women, Hyderabad, India

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

Mailid;bindu.avmm@gmail.com[1],thanmayeesaivaka@gmail.com[2],varshithapendam@gmail.com[3],vennelaare932@gmail.com[4]

Abstract:

Healthcare information systems often rely on centralized storage models that expose sensitive patient data to security risks and limited interoperability. This paper presents MediBlock, a decentralized framework designed to enhance healthcare data management through the integration of blockchain and cloud technologies. The system ensures secure storage, traceable insurers. Smart contracts regulate permisiions and maintain transparency trough immutable audit trails. The proposed architecture improves trust, privacy, and efficiency in handling medical records. By enabling distributed access and encryption-based protection, MediBlock contributes toward reliable healthcare information exchange while supporting scalability and integration wit existing infrastructures.

Keywords: *Blockchain, healthcare data security, cloud computing, decentralized storage, smart contracts.*

Introduction

The rapid digitization of healthcare services has significantly increased dependence on electronic data storage and sharing systems. Medical records, diagnostic reports, and treatment histories are frequently maintained in centralized databases, which raises concerns regarding data breaches, unauthorized access, and limited interoperability among institutions. These limitations affect the reliability, transparency, and efficiency of healthcare information management and reduce patient trust in digital infrastructures.

In addition, the expansion od telemedicine and remote monitoring platforms has increased the volume and frequency of healthcare data exchange. this trend requires dependable infrastructures capable of supporting timely access to medical information while preserving regulatory compliance, data consistency, and operational reliability across distributed environments.Recent advancements in distributed technologies offer promising solutions to these challenges. Blockchain technology provides decentralized and tamper-resistant data management, ensuring integrity and traceability of records, while cloud computing delivers scalable storage and accessible services. The integration of these tecnologies creates oppurtunities to enhance security, accessibility, and accountability in healthcare systems.This paper presents MediBlock, a framework designed to enable secure healthcare data mangaement by combining blockchain and cloud-based infrastructure. The proposed system allows controlled data sharing among patients, medical professionals, and insurance entities while maintaining transparency through permisiion tracking and encrypted storage. By addressing existing system limitations, MediBlock aims to improve operational efficiency and support trustworthy healthcare data exchange.

Literature Survey

Recent research has exploded the use of blockchain technology to address security and privacy challenges in healthcare data management. Hölbl et al. examined multiple blockchain-based healthcare solutions and highlighted their ability to provide data integrity, decentralization, and improved access control compared to traditional centralized storage systems. Their review emphasized the role of distributed ledgers in ensuring transparency and trust among healthcare stakeholders.

Saha et al. discussed privacy concerns associated with medical data sharing and proposed blockchain- driven healthcare frameworks tht incorporate sryptographic mechanisms to protect patient confidentiality. Their study indicated that decentralized verification and smart contract automation can strengthen authentication and reduce the risks of unauthorized access. However, scalability and integration challenges remain key limitations in practical deployment. In addition, Bamiah et al. analyzed the adoption of cloud computing within healthcare infrastructures and demonstrated its effectiveness in handling large-scale medical data storage and processing requirements. Their findings sowed that cloud platforms enable flexible resource allocation and cost-efficient system maintenance but may introduce security concerns if used independently without additional protection mechanisms.

These studies collectively suggest that combining blockchain with cloud computing can address the weakness of standalone approaches. While blockchain ensures integrity and traceability, cloud platforms provide scalability and accessibility. Motivated by these observations, the proposed MediBlock framework integrates both technologies to create a secure nd efficient healthcare data management environment.

Further investigations in the domain of healthcare information systems have emphasized the importance of interoperability and patient -centricc control over medical data. Several reserachers have exploded permission-based data sharing models where patients maintain authority over access to their records. These approaches promote transparency and accountability but often rely on centralized identity managemnt, which introduces potential vulnerabilities. Integrating decentralized authentication menchanisms has therefore become an active area of exploration to strengthen system resilience.

Another tream of research focuses on the use of smart contracts to automate administrative processes such as consent management, insurance verification, and clinical data exchange. Automation through programmable contracts reduces manual intervention and minimizes processing delays. However, existing implementations frequently encounter limitations related to healthcare environments. These factors highlight the need for hybrid solutons capable of balancing automation with operational efficiency.

In response to these observations, the MediBlock framework extends research by introducing a unified architecture that combines blockchain-based auditing with cloud-enabled data management. By incorporating role-based modules for adminstrators healthcare personnel, patients, and insurers, the system aims to enhance collaboration, ensure data protection, and provide efficient healthcare information exhange within a scalable digital environment.

Methodology

The MediBlock framework adopts a hybrid architectural approach that combines blochchain-based verification with cloud-enabled storage to address security and scalability challenges in healthcare data mangement. The system architecture is designed to decentralized record validation while maintaining efficient access to large medical datasets. Patient records are encrypted and stored within cloud repositories, while blockchain ledgers maintain immutable references and access logs. This seperation ensures that sensitive data remain scalable and accessible while preserving integrity through distributed verification. Access permissions are regulated through programmable mechanisms that allow authorized stakeholders to retrieve or update information under predefined conditions.

The framework incorporates role-oriented interaction layers representing administartive authorities, healthcare professionals, patients, researchers, and insurance entities. Each layer communicates through secured interfaces that enforce authentication and authorization protocols. This modular design supports collaborative data exchange while minimizing exposure to unauthorized manipulation. The methodological integration of distributed trust mechanisms with centralized processing resources establishes a balanced infrastructure for reliable healthcare information management.

Implementation and Experimental Setup

The implementation of the MediBlock framework utilizes a web-oriented environment supported by standard computing resources. Frontend interaction is facilitated through browser- based intrfaces, while backend processing components manage record vlidation, encryption, and communication between system modules.

The development environment incorporates commonly adopted programming and database technologies to simulate practical deployment conditions. A cloud service platform provides scalable storage support, and system execution is conducted on a general-purpose operating environment to ensure accessibility and reproducibility.

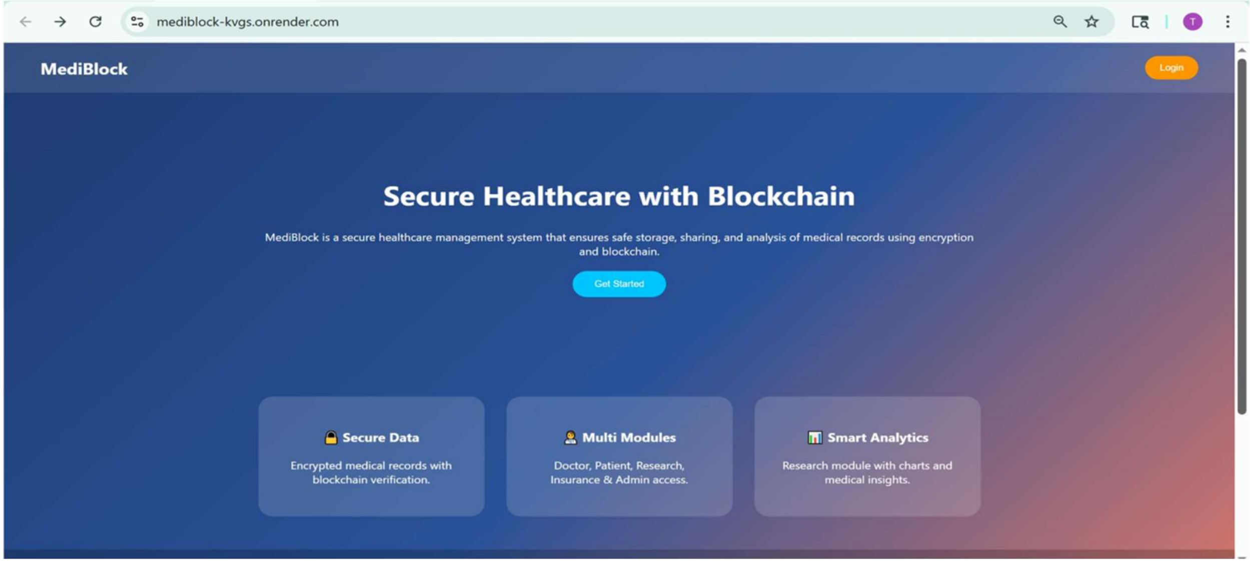
User interaction scenarios include medical record updates, access authorization, and insurance verfiaction workflows. Interface prototyoes illustrated in the project documentation demonstrate navigation structures for medical staff dashboards and patient record monitoring panels. These expaerimental configurations allow observation of system responsiveness, usability, and operational consistemcy under representative usage conditions.

Toensure secure system operation, authenticatin and role-based authorization mechanisms are incorporated during implementation. Each stakeholder category interacts with the platform through validated access channels that enforce identity verfication before permitting record viewing or modification.

The experimental setup also considers data consistency and transaction traceability. Blockchain entries generated during record updates are monitored to verify immutability and chronological ordering, ensuring that modifications remain auditable throughout system execution. Concurrent access scenarios were simulated to observe system staboloty under multi-user interaction, allowing assessment of synchronization efficiency and response behavior during routine healthcare workflows.

Furthermore, usability aspects were examined through interface interaction observations involving navigation between record modules, appointment views, and claim verification screens illustrated in the project material. The results indicate that the structural layout supports intuitive user engagement while maintaining syatem functionality, hightlighting the practicality of deplying the framework within institutional healthcare settings.

Output



Secure Healthcare with Blockchain

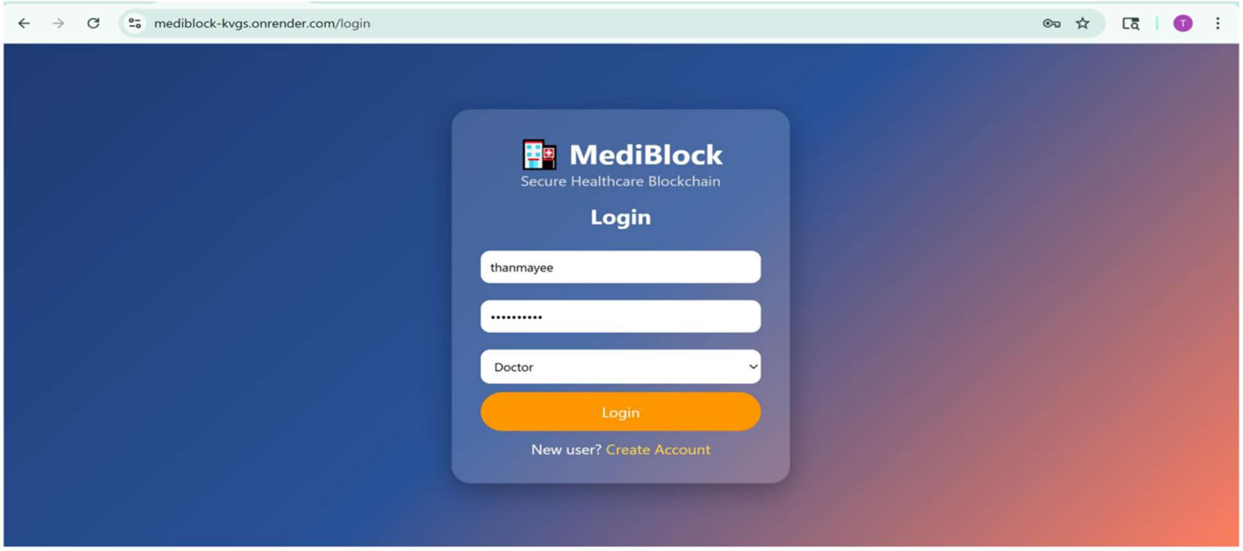
MediBlock is a secure healthcare management system that ensures safe storage, sharing, and analysis of medical records using encryption and blockchain.

🔒 Secure Data
Encrypted medical records with blockchain verification.

Multi Modules
Doctor, Patient, Research, Insurance & Admin access.

📊 Smart Analytics
Research module with charts and medical insights.

Home Page


mediblock-kvgs.onrender.com/login
MediBlock
Secure Healthcare Blockchain
Login

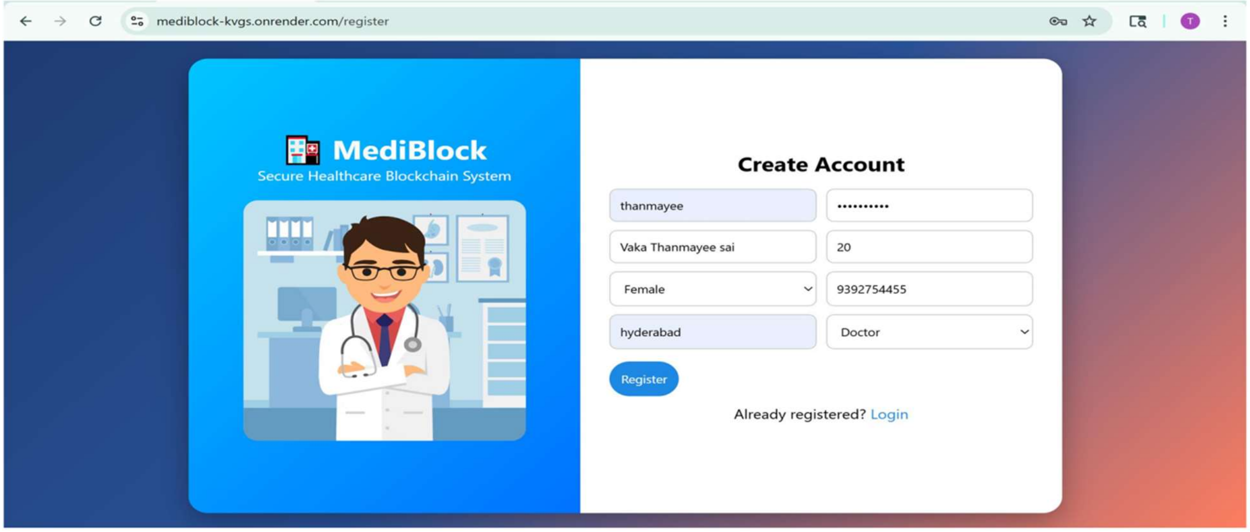
thanmayee

••••••••••

Doctor

Login
New user? Create Account

Login Page


mediblock-kvgs.onrender.com/register

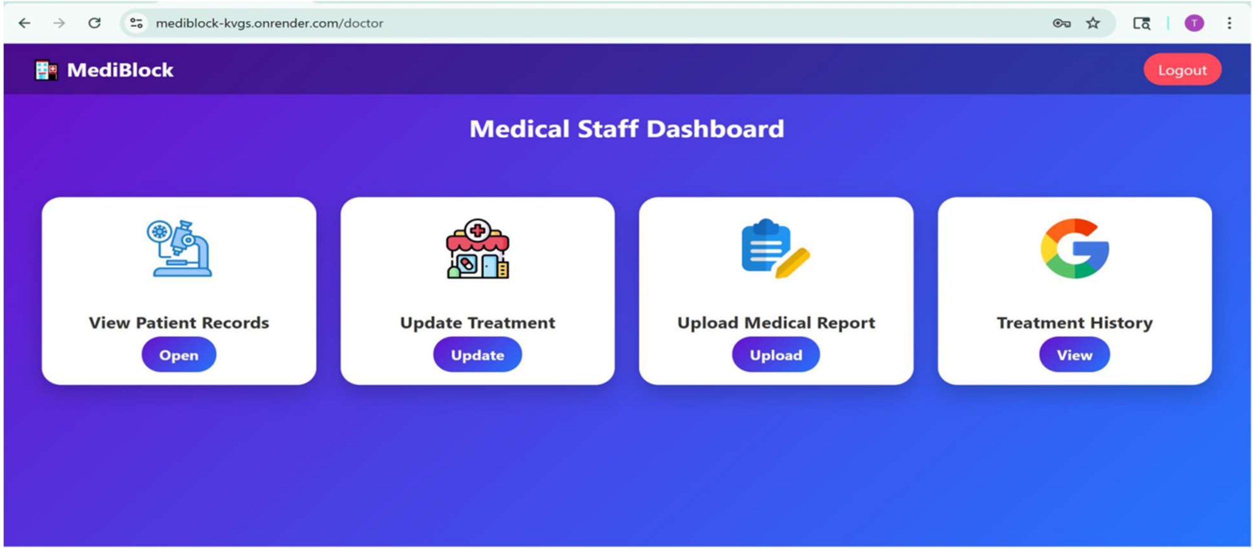
MediBlock
Secure Healthcare Blockchain System

Create Account

thanmayee | ••••••••••
Vaka Thanmayee sai | 20
Female | 9392754455
hyderabad | Doctor

Already registered? Login

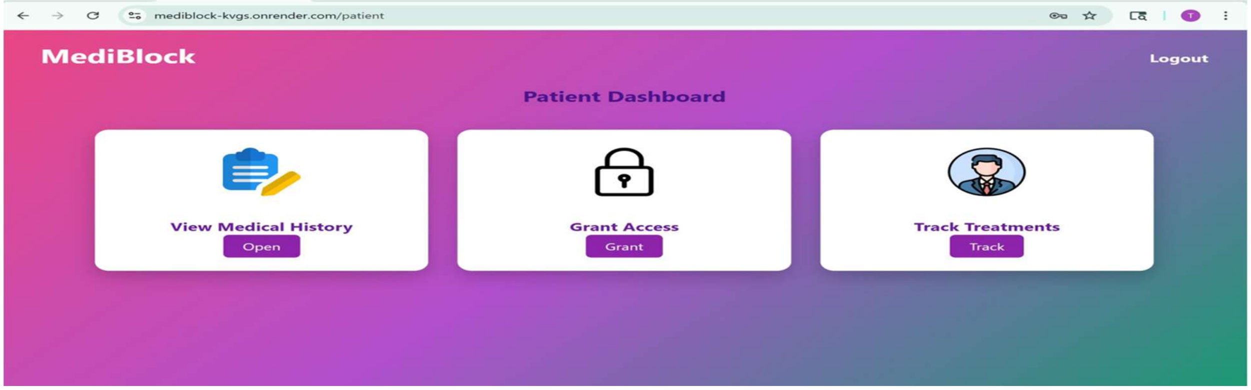
Registration Page


mediblock-kvgs.onrender.com/doctor

MediBlock

Medical Staff Dashboard

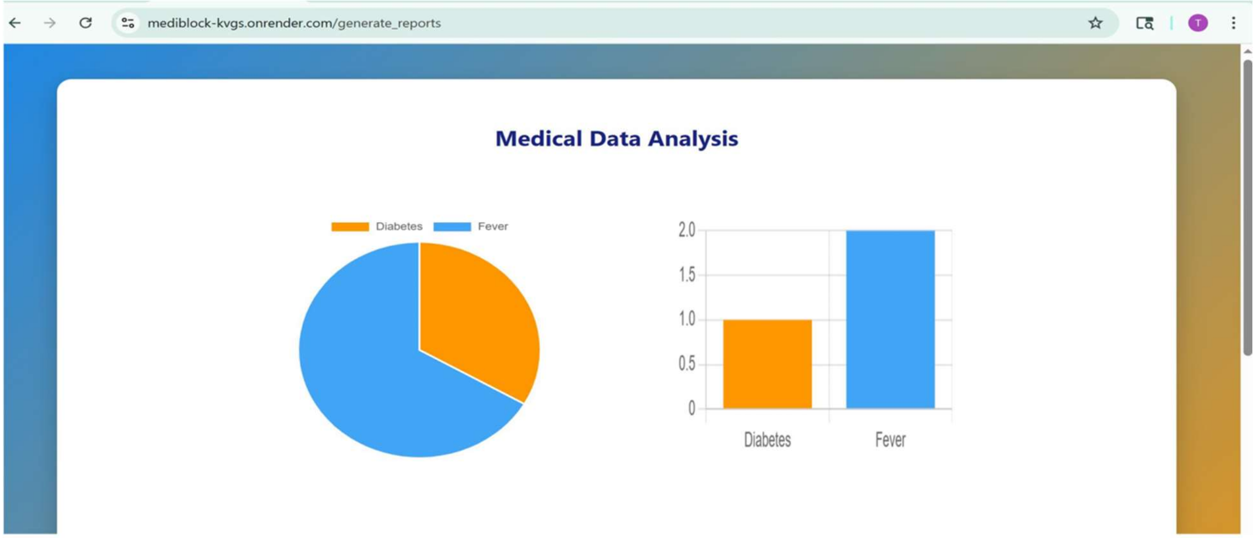
Medical Staff Dashboard


mediblock-kvgs.onrender.com/patient

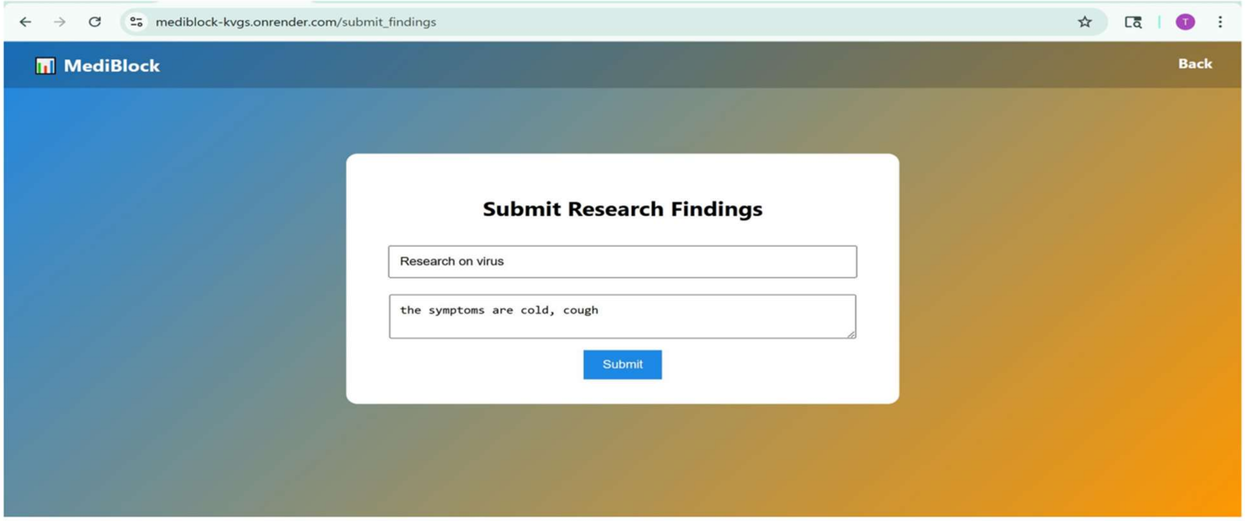
MediBlock

Patient Dashboard

Patient_Dashboard



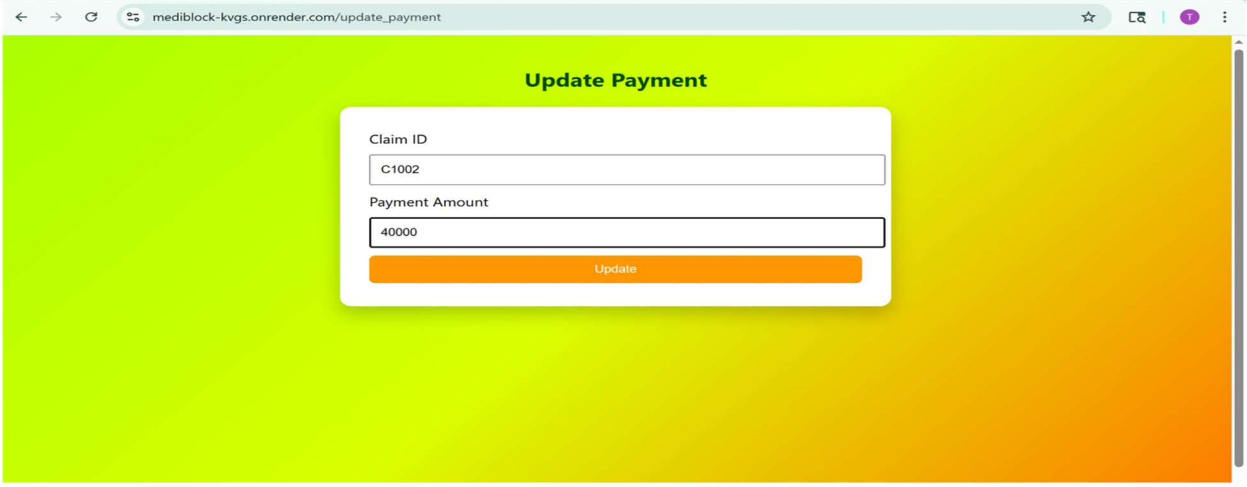
Generate_Reports



Research on virus

the symptoms are cold, cough

Submit_Findings



Claim ID: C1002

Payment Amount: 40000

Update_Payment

6 Conclusion

This paper presented MediBlock, a decentralized framework designed to enhance healthcare data management through the integration of blockchain technology and cloud-based storage infrastructure. The proposed approach addresses critical limitations of conventional centralized systems by improving transparency, strengthening security mechanisms, and enabling controlled data sharing among healthcare stakeholders. By incorporating encrypted storage, permission-based access, and traceable transaction logging, the framework promotes data integrity and user trust while supporting scalable information handling.

Implementation observations demonstrate that the modular architecture facilitates collaboration between administrative authorities, medical professionals, patients, researchers, and insurance providers without compromising confidentiality. Although distributed verification introduces computational overhead and latency considerations, the system shows strong potential for secure and efficient healthcare record management. Future work may focus on performance optimization, interoperability enhancement , and integration with advanced analytical tools to further extend system capabilities within evolving digital healthcare environments.

.

References

1. Y. Sowjanya, S. Gopalakrishnan and R. D. Kumar, "Internet of Things in Health Care: Motivation and Challenges: A Survey," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 2024, pp. 1-7, doi: 10.1109/ICCCNT61001.2024.10725769.

2 .S. Kondapalli, M. Dudala, K. K. Kumar, K. Spurthi, K. S. Kumar and R. D. Kumar, "Deep Learning Convolutional Nets: Intelligent System for Paddy Leaf Disease Diagnosis," 2025 2nd International Conference on Software, Systems and Information Technology (SSITCON), Tumkur, India, 2025, pp. 1-8, doi: 10.1109/SSITCON66133.2025.11341943.

3. AbdelSalam, F.M., et al.: Blockchain Revolutionizing Healthcare Industry: A Systematic Review. Healthcare Applications Study(2024).

4 . Mehrtak, M., et al.: Security Challenges and Solutions in Healthcare Cloud Computing.
Journal of Healthcare Engineering (2023).

5. Haleem, A., Javaid, M., Singh, R.:Blockchain Technology Applications in Healthcare: A Review.
Materials Today: Proceedings(2023).

6. Ghosh, P.K., et al.: Blockchain Application in Healthcare Systems: A Review.
Systems Journal(2023).

7.Mamun, A., Azam, S., Gritti, C.:Blockchain-Based Electronic Health Records Management: view A Comprehensive Review and
Future Research Direction
IEEE Access, vol.10,pp.5768-5789(2022).

8 . Pang, Z., Yao, Y., Li, Q., Zhang, X., Zhang, J.: Electronic Health Records Sharing Model Based on Blockchain With PBFT Consensus Algorithm.
IEEE Access, vol. 10, pp.87803-87815(2022)

9. Vojja, L., Kumar, R.D., Sivaprasad, P.V.S., Satyanarayana, A. (2025). Encryption with Identity Based Approach for Versatile Encrypted Data Sharing in Public Cloud. In: Farhaoui, Y., Herawan, T., Lucky Imoize, A., Allaoui, A.E. (eds) Intersection of Artificial Intelligence, Data Science, and Cutting-Edge Technologies: From Concepts to Applications in Smart Environment. ICAISE 2024. Lecture Notes in Networks and Systems, vol 1397. Springer, Cham. https://doi.org/10.1007/978-3-031-90921-4_81