iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** I **Month of publication:** January 2025

DOI: https://doi.org/10.22214/ijraset.2025.66726

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue I Jan 2025- Available at www.ijraset.com

Medi-Crypt: Patient Data Management System Using Blockchain

Dr. S Mercy[1], Lavanya Y M[2], Shreya Ganesh Hegde[3] , Bhanushree N N[4], Harshith R[5]
[1, 2, 3, 4, 5]*Department of Information Science and Engineering, Bangalore Institute of Technology, VV Puram, Bangalore*

Abstract: ***In the era of digital healthcare, safeguarding patient data has become a challenge. MediCrypt leverages blockchain technology to revolutionize the management of medical records, offering a decentralized and tamper-proof system that prioritizes security, privacy, and accessibility. By integrating robust encryption mechanisms and smart contracts, MediCrypt ensures that patient information remains confidential while enabling authorized access for healthcare providers. Alongside secure patient data management, Medi-Crypt integrates insurance features, enabling personalized health coverage and efficient claims processing. Patients can manage their policies as secure digital tokens, simplifying claim validation and payment settlements via smart contracts. The system's architecture promotes interoperability, allowing seamless data exchange across diverse platforms. Designed with scalability and user empowerment in mind, MediCrypt establishes a new benchmark for efficient and secure healthcare data management, transforming how sensitive medical information is handled and shared.***

Keywords: Blockchain, Ethereum, Smart Contract, Healthcare, Access control, Electronic Health Records (EHR), Patient-Centric, Personal health records

I. INTRODUCTION

The rapid digitization of healthcare has introduced significant advancements in patient care but also highlighted critical challenges in managing sensitive medical information and insurance workflows. Centralized databases are prone to breaches, unauthorized access, and tampering. Similarly, traditional insurance systems often suffer from inefficiencies, including fraud, delayed claims processing, and lack of transparency. Furthermore, the lack of interoperability among healthcare systems creates inefficiencies, making it difficult for providers to access and share patient records seamlessly.

Medi-Crypt is a blockchain-based platform designed to address these challenges. It provides a decentralized, tamper-proof framework for managing patient records and insurance data. Leveraging blockchain's immutable ledger, Medi-Crypt ensures data integrity while empowering patients with control over their health and insurance records. Key features include role-based access control, secure storage using IPFS, and smart contracts that automate insurance claims and settlements.

By integrating HIPAA and GDPR compliance, Medi-Crypt fosters trust among stakeholders. Its scalable architecture and interoperability with existing systems make it a transformative tool in modern healthcare and insurance ecosystems. Through MediCrypt, we aim to redefine how patient information is stored, shared, and accessed, ensuring a balance between privacy, security, and accessibility.

II. RELATED WORK

Madine et al. [1] demonstrated how blockchain can empower patients by decentralizing medical records using IPFS for secure storage and proxy re-encryption for controlled data sharing. Their work underscores improved data integrity, privacy, and patient autonomy.

Zhuang et al. [2] proposed a blockchain-based Health Information Exchange (HIE) framework to tackle privacy and security gaps in traditional healthcare systems. Through large-scale simulations, they proved its potential to securely manage large-scale medical data exchanges.

Mamun et al. [3] provided an extensive review of blockchain applications in EHR systems, discussing challenges such as scalability, legal compliance, and privacy while highlighting the need for robust real-world testing and validation.

Ramzan et al. [4] examined blockchain's integration in IoMT and healthcare supply chains, emphasizing its ability to enhance trust and transparency but pointing out challenges like data scalability and privacy.

Kumar et al. [5] introduced a blockchain architecture combining Ethereum, IPFS, and cryptographic techniques for EHR storage. Their system enhanced patient control and data privacy, providing a scalable solution for secure health data management.

©IJRASET: All Rights are Reserved

III. PROBLEM DEFINITION

The traditional healthcare system faces significant challenges in managing patient data securely and efficiently. Centralized storage of medical records is prone to breaches, unauthorized access, and data tampering, compromising patient privacy and trust. Additionally, the absence of seamless interaction between patients, doctors, and insurers creates inefficiencies in payment processing and data sharing. Patients often lack control over their own medical records, while insurers and healthcare providers face delays and uncertainties in financial settlements.

The reliance on third-party intermediaries for insurance claim processing further complicates matters, leading to delays, errors, and disputes that hinder timely and transparent settlements. These issues highlight the need for a decentralized solution that ensures data integrity, automates transactions, and fosters trust among all stakeholders in the healthcare ecosystem.

IV. OBJECTIVES

1) Enhanced Data Security: Implement blockchain technology to ensure that patient data is stored securely and is immune to unauthorized access or tampering. This objective focuses on leveraging the decentralized nature of blockchain to provide robust security for sensitive medical records.
2) Improved Data Privacy: Safeguard patient information by implementing encryption and access control mechanisms that allow only authorized users to view or modify data. This objective aims to protect patient confidentiality and maintain trust between patients and healthcare providers.
3) Interoperability Across Systems: Facilitate seamless data sharing and interoperability between different healthcare systems, ensuring that patient records can be accessed and updated by authorized personnel across various platforms. This objective addresses the need for compatibility between diverse healthcare IT systems.
4) Data Integrity and Transparency: Ensure the integrity and transparency of medical records by using blockchain's immutable ledger, which records all transactions and modifications with full traceability. This objective focuses on maintaining accurate and reliable patient information.
5) Streamlined Access to Medical Records: Develop a user-friendly interface that allows healthcare providers and patients to access medical records quickly and efficiently, improving the speed and quality of healthcare delivery. This objective aims to enhance user experience and facilitate timely medical interventions.

V. PROPOSED SYSTEM AND ARCHITECTURE

A. *System Overview*

Medi-Crypt integrates blockchain technology, decentralized storage, and a user-centric design to address inefficiencies in traditional healthcare systems. Its core features include decentralized storage on the IPFS (Inter Planetary File System), ensuring tamper-proof and scalable storage of medical records. The system leverages smart contracts to automate access control, insurance claims processing, and payment settlements, enhancing workflow efficiency. Role-Based Access Control (RBAC) gives patients full authority to manage access to their medical records, while insurance integration allows patients to purchase policies, submit claims, and track settlements. Real-time communication through web sockets facilitates seamless interaction between client applications and the blockchain backend.

B. *Key Components of Architecture*

The Medi-Crypt architecture is composed of several key components that work together to ensure secure and efficient healthcare management. The client interface is a mobile and web application that integrates with MetaMask for secure blockchain interactions. Patients, doctors, and insurers use this platform to upload records, manage permissions, and process claims. The blockchain layer, built on Ethereum, ensures decentralized and immutable transaction logging, allowing secure interactions with smart contracts. Patient records are stored off-chain on IPFS, reducing blockchain storage costs while maintaining integrity. The smart contracts automate operations like managing patient permissions and verifying claims, ensuring secure payment settlements. Encryption using AES and RSA ensures patient data confidentiality, while web sockets enable real-time synchronization between the client and blockchain.

C. *Diagrams and Explanations*

The following diagrams provide a detailed view of the interactions and data flows within the Medi-Crypt system. They are essential for understanding how the components work together to provide secure and efficient healthcare data management.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

1) Sequence Diagram

The sequence diagram in Fig. 1 shows the step-by-step interactions between the primary users—patients, doctors, and insurers—within the Medi-Crypt system.

- Patient Registration: The patient begins by using the client application to register on the platform. This registration involves connecting their MetaMask wallet, which generates a unique blockchain ID for the patient. This ID is stored on the Ethereum blockchain, ensuring secure, decentralized identity management.
- Doctor Interaction: Once registered, the patient can authorize a doctor to access their medical records. This authorization is managed through a smart contract, where the patient grants permissions to the doctor. After authorization, the doctor can securely upload or view patient records stored on IPFS, ensuring that no unauthorized access occurs.
- Insurance Claims: When the patient decides to file an insurance claim, they grant access to the insurer. The insurer can then validate the claim by verifying the transaction history stored on the blockchain and accessing the relevant encrypted medical records stored on IPFS. Smart contracts handle this interaction, ensuring that claims are processed efficiently and securely.

This diagram highlights how the blockchain technology supports secure and immutable interactions throughout the process, preventing unauthorized access or tampering with sensitive data. Blockchain provides an immutable audit trail of actions performed by patients, doctors, and insurers.

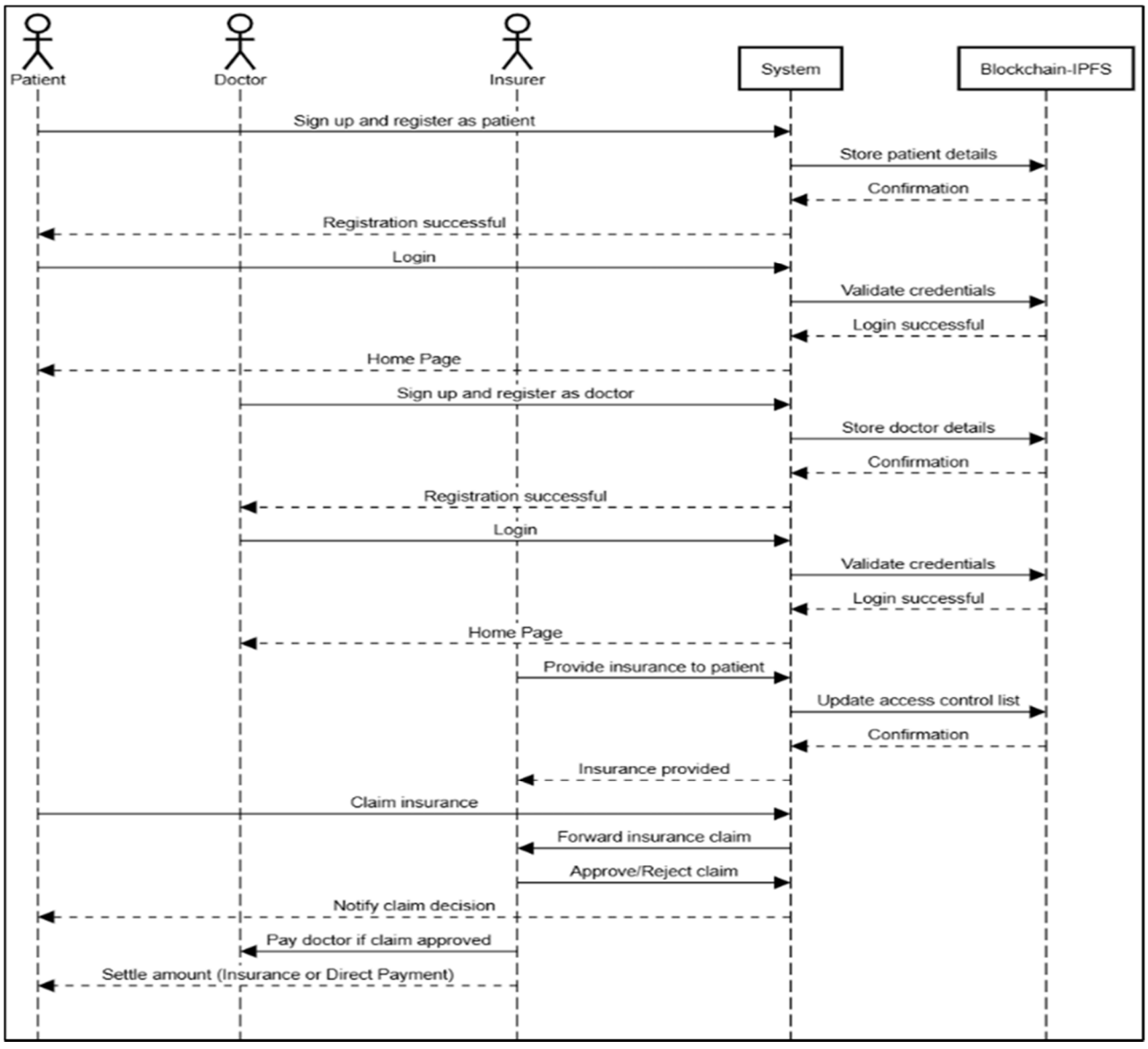


Fig. 1 Sequence Diagram

2) Use Case diagram

The use case diagram in Figure 5.2 shows the different roles within the Medi-Crypt platform and their interactions with the system. The primary roles are patients, doctors, and insurers.

- Patients: The patient can register and log in to the system, upload their medical records, view them, and manage permissions granted to doctors and insurers. They also have the ability to purchase insurance policies and file claims. The patient has control over their data, granting or revoking access as they see fit.
- Doctors: Doctors register and log in to the platform to access medical records of patients, but only those for which they have been granted authorization. They can upload diagnosis reports or medical records to IPFS, updating the patient's data in a secure and tamper-proof manner.
- Insurers: Insurers register and log in to access patient records. However, they can only view data that the patient has explicitly authorized. They can validate insurance claims using the data available to them and settle payments via smart contracts.

The use case diagram highlights the role-based access control (RBAC) mechanism in the system, which ensures that users can only perform actions within the scope of their assigned roles, preserving the security and privacy of the platform.

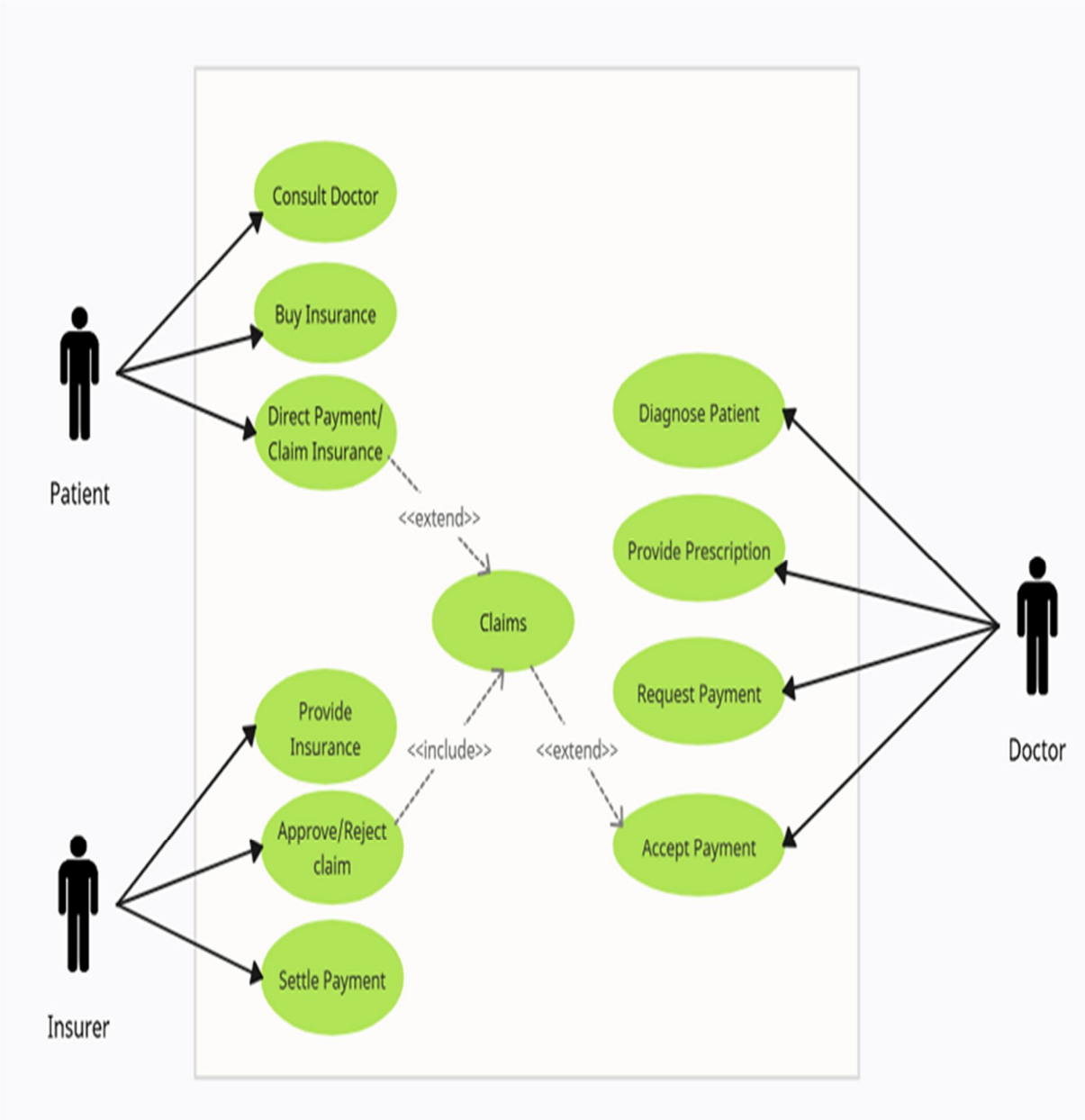


Fig. 2 Use case diagram

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue I Jan 2025- Available at www.ijraset.com

3) Data Flow Diagram

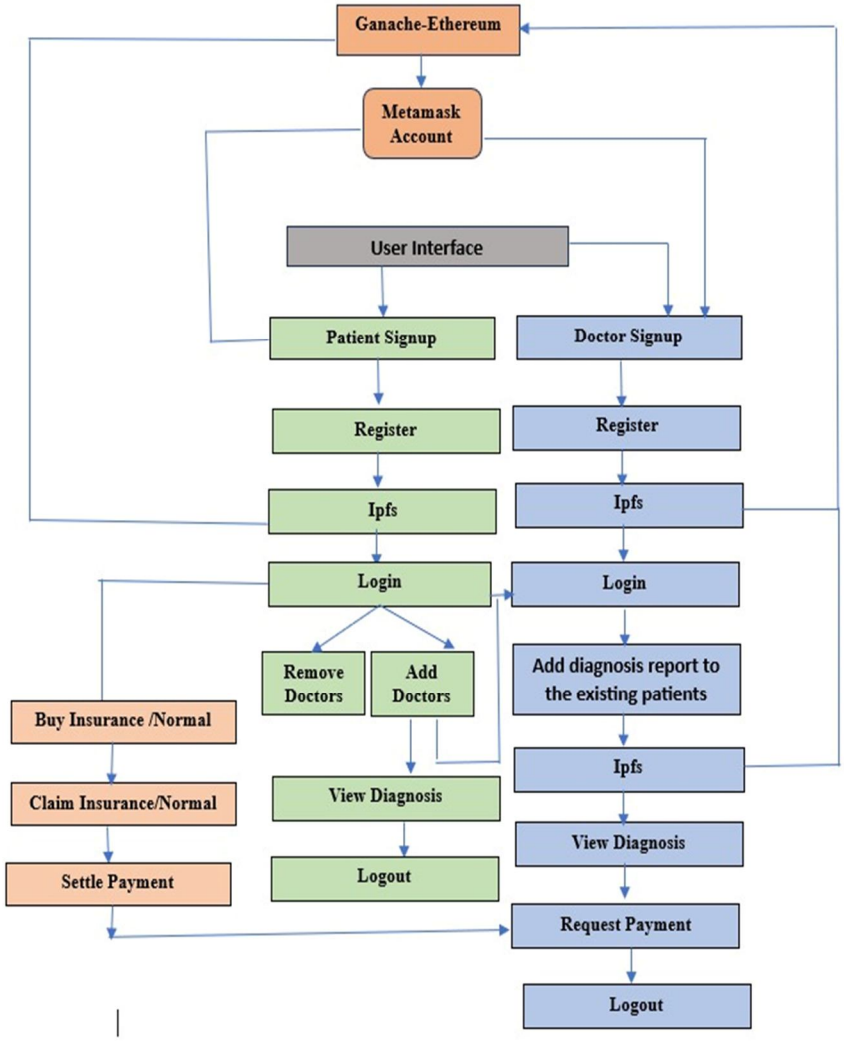


Fig. 3 Data Flow Diagram

The data flow diagram in Figure 5.3 visualizes how data moves through the system, illustrating the communication between the client interface, blockchain, and IPFS storage.

- Patient Actions: The patient interacts with the platform via the client interface to perform tasks like registration, uploading records, and granting permissions to doctors and insurers. These actions are communicated to the blockchain through the MetaMask wallet, which triggers the execution of smart contracts. For example, when a patient uploads a record, it is encrypted and stored on IPFS, while metadata (such as the file hash) is recorded on the Ethereum blockchain.
- Doctor and Insurer Actions: Doctors and insurers also interact with the platform to access data. They send requests to the blockchain, where smart contracts validate their permissions to access specific patient data. Once authorized, they can retrieve medical records from IPFS or validate claims based on the blockchain's transaction history.
- Data Storage: Encrypted medical records are stored off-chain on IPFS. While the records themselves are stored off-chain to avoid high blockchain storage costs, metadata, including a reference to the file (such as the file hash), is stored on the blockchain to maintain integrity and ensure data is verifiable. This setup leverages both on-chain and off-chain storage to balance scalability, cost, and security.

The data flow diagram emphasizes how data flows securely and efficiently between various components, maintaining the integrity of records while reducing costs through off-chain storage.

©IJRASET: All Rights are Reserved

D. Security and Privacy Features

Medi-Crypt incorporates several security and privacy measures to protect patient data. AES encryption is used to ensure the confidentiality of medical records, while RSA encryption facilitates secure key exchange during data sharing. Role-Based Access Control (RBAC) is enforced by smart contracts, restricting access to sensitive data based on user roles. The blockchain guarantees immutable audit logs, providing a transparent and secure record of actions performed on the platform.

In emergency situations, doctors can request temporary access to a patient's records, which is logged on the blockchain and requires patient approval afterward.

E. Benefits of Proposed Architecture

The architecture of Medi-Crypt offers several key benefits. Decentralization eliminates single points of failure and reduces the risk of data breaches, while blockchain transparency ensures accountability and trust by recording all transactions. Automation through smart contracts minimizes manual intervention and errors, streamlining workflows. The patient-centric design empowers patients to control access to their data, fostering trust and privacy. Finally, the system's interoperability allows seamless data sharing between healthcare providers, patients, and insurers, enhancing collaboration and efficiency across the healthcare ecosystem.

VI. IMPLEMENTATION

A. Ganache-Ethereum and MetaMask Integration

The system uses Ganache-Ethereum as a local blockchain network for deploying and testing Ethereum smart contracts. MetaMask acts as the Web3 wallet that enables users to interact with the Ethereum blockchain. MetaMask allows patients, doctors, and insurers to connect their accounts securely, facilitating decentralized authentication and transactions on the blockchain.

B. User Interface

The system's frontend is developed using React.js for an intuitive and responsive user experience. The Web3.js library bridges the gap between the Ethereum blockchain and the frontend application, allowing seamless interaction with smart contracts. The user interface allows patients and doctors to perform tasks like registration, login, and managing permissions while ensuring accessibility and usability.

C. Patient Signup and Login

Patients can sign up through the user interface by providing details such as name, email, and age. Their data is stored securely using Ethereum smart contracts, and files like medical records are uploaded to IPFS (Inter Planetary File System). Patients can then log in using their MetaMask accounts to access the system. Once logged in, patients have complete control over their medical data and permissions.

D. Doctor Signup and Diagnosis Management

Doctors can register and log in similarly to patients. After gaining access permissions from patients, doctors can upload diagnosis reports to IPFS. The IPFS hash of the uploaded file is stored on the blockchain for traceability and immutability. Doctors can also request payments for their services and verify insurance claims made by patients.

E. Data Storage with IPFS

The system integrates IPFS to store medical reports and other large files in a decentralized manner. Instead of storing files directly on the blockchain, IPFS provides a secure and efficient solution. The file hash is stored on the Ethereum blockchain, ensuring that data remains immutable, tamper-proof, and accessible only to authorized users.

F. Access Management

Patients have full control over access permissions. They can add or remove doctors from their access list using Ethereum smart contracts. This ensures that only authorized doctors can view and upload diagnosis reports. Patients can also view the list of doctors who have access to their data and revoke permissions at any time, ensuring patient-centric control.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue I Jan 2025- Available at www.ijraset.com

G. Insurance Management

Patients can buy insurance policies through the system and store policy details on the blockchain. If medical expenses arise, patients can claim insurance, and doctors can validate the claim by uploading diagnosis reports. Smart contracts automate the verification process, reducing delays and ensuring transparency. Payments can be settled either through insurance or directly between patients and doctors using Ethereum transactions.

H. Payment Settlement

The system facilitates seamless payment settlement through Ethereum-based transactions. Patients can settle payments for medical services or insurance claims directly with doctors and insurers via their MetaMask accounts. Smart contracts ensure that the transactions are secure, transparent, and immutable, eliminating intermediaries.

I. Data Transparency and Security

By leveraging blockchain technology, the system ensures that all data is immutable and fully traceable. Any action, such as uploading reports, granting permissions, or making payments, is recorded on the blockchain, enhancing transparency. IPFS ensures that sensitive medical records remain secure and accessible only to authorized stakeholders.

J. Scalability

The system's architecture is designed to be scalable and maintainable. The use of React.js for the frontend ensures a responsive user experience, while the modular structure allows for easy updates and feature additions. To address scalability concerns related to blockchain transactions, the system leverages Ethereum's public network for secure transactions and IPFS for decentralized file storage, reducing the load on the blockchain itself. Additionally, the platform's decentralized storage architecture allows for efficient scaling of data storage as the number of users and medical records grows, without compromising performance. The modular design of the system makes it adaptable to handle larger volumes of data and users, ensuring that the system remains performant and reliable as it scales.

This implementation successfully combines blockchain, decentralized storage, and modern web development tools to create a secure, patient-centric healthcare management system. It empowers patients with full control over their medical data, streamlines doctor-patient interactions, and automates insurance claims and payment processes, ensuring transparency, data integrity, and efficiency.

VII. RESULTS AND DISCUSSION

The implementation of the Medi-Crypt system has successfully demonstrated the ability to provide secure, decentralized management of healthcare records and insurance workflows. The following outlines the key results and discusses the outcomes, challenges, and improvements made during the development of the system.

A. Results

The following are the results of the Medi-Crypt system, showcasing key pages and dashboards in the user interface. Each screenshot highlights the functionality and design of the platform, ensuring an intuitive and responsive user experience. The images below illustrate the various stages of interaction for patients, doctors, and insurers.

The home page (Fig. 4) serves as the gateway to the platform, providing users with an overview of its features and easy access to services such as patient records, doctor management, and insurance claims. The layout ensures clear navigation for new users and quick access for registered users.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



Fig. 4 Home page of Medi-Crypt

The login page (Fig. 5) allows users to authenticate using their MetaMask wallet, providing a secure and straightforward entry point. This page enables different roles—patients, doctors, and insurers—to log in and access the appropriate features. The user interface is simple and designed for ease of use while maintaining secure access control.

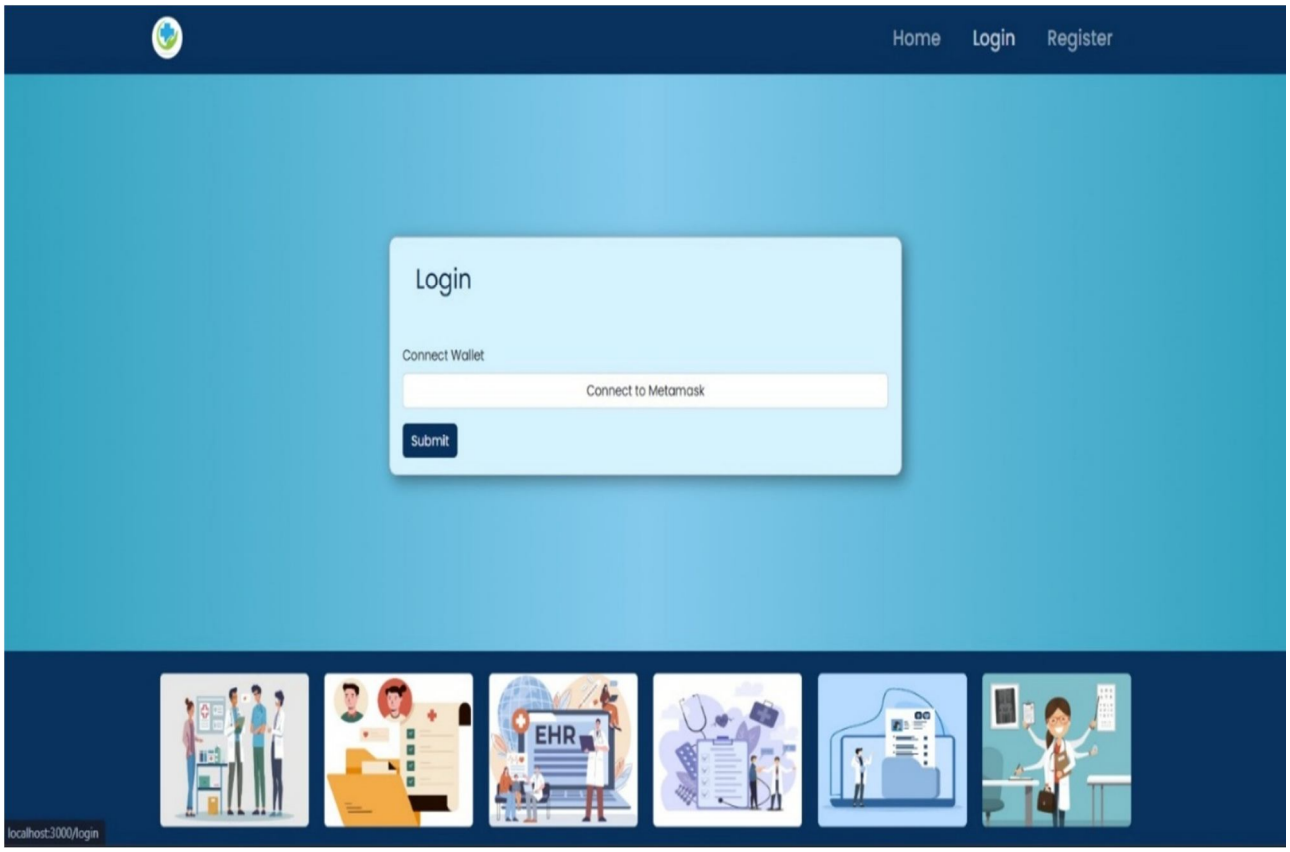


Fig 5. Login Page

The registration page (Fig. 6) enables new users to create an account by submitting essential information such as name, email, and age. Additionally, patients can upload their medical records during registration. Once the details are entered, users are prompted to authenticate using MetaMask, ensuring secure sign-up for all stakeholders.

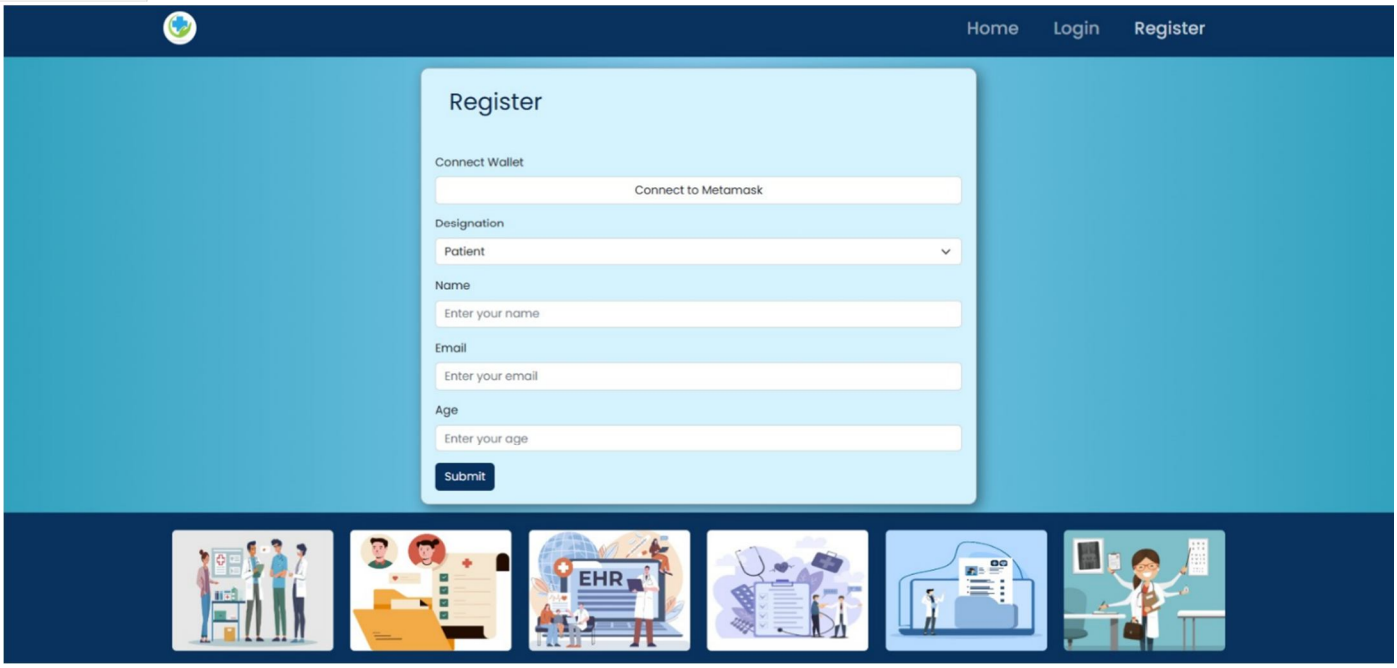


Fig. 6 Registration Page

On the register page for various designations (Fig. 7), users can select their role, such as Patient, Doctor, or Insurer. Depending on the selection, the system tailors the registration process, presenting specific options and features relevant to each role. This ensures a user-centric design, offering streamlined registration for each type of user.

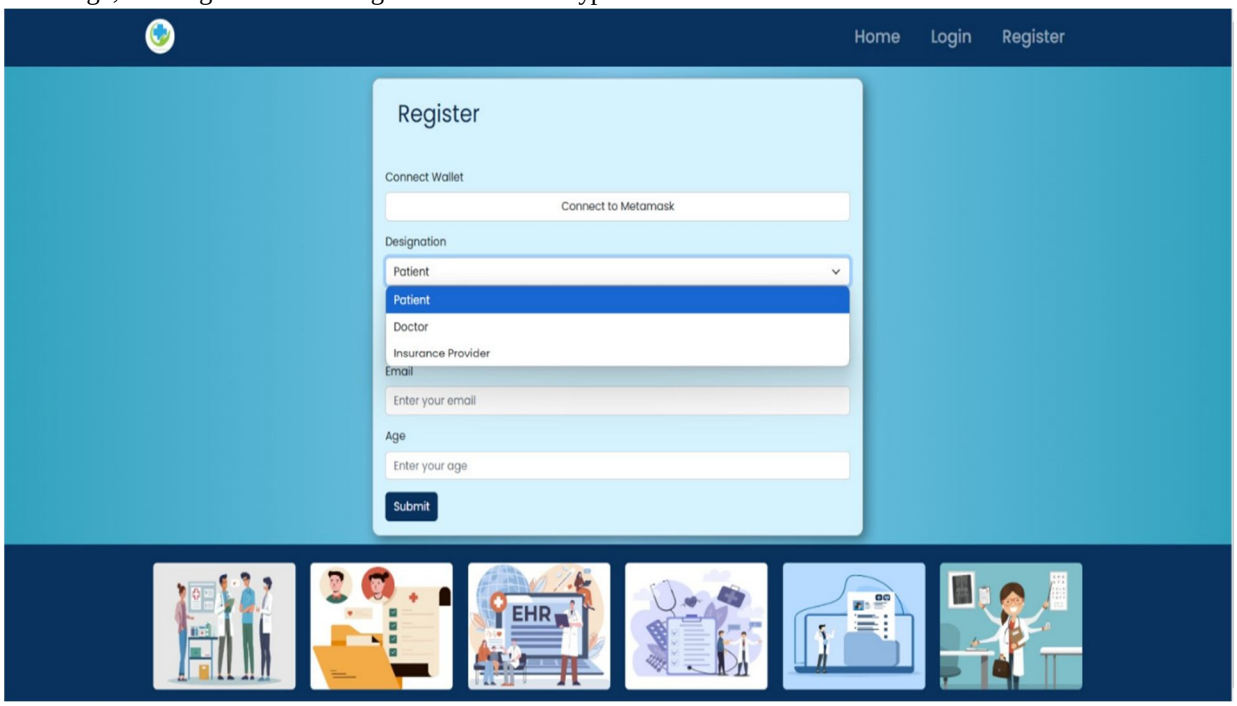


Fig. 7 Registration Page for various designations

The patient's dashboard (Fig. 8) acts as the central hub for managing medical records, viewing diagnosis reports, and granting or revoking access to doctors and insurers. Patients can interact with their data easily, with options to manage permissions for healthcare professionals and insurers, as well as track their insurance claims.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

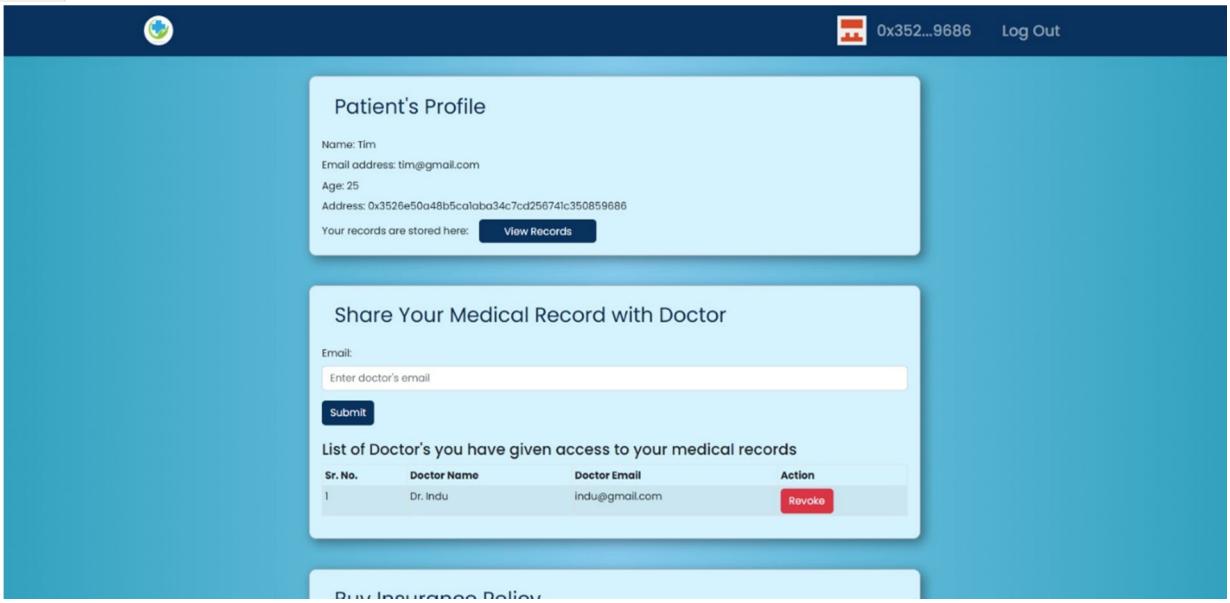


Fig. 8 Patient Dashboard

The doctor's dashboard (Fig. 9) allows doctors to access patient records with permission, upload diagnosis reports, and manage treatment plans. Doctors can also request payments and validate insurance claims, ensuring they have full control over their services while adhering to the patient's preferences.

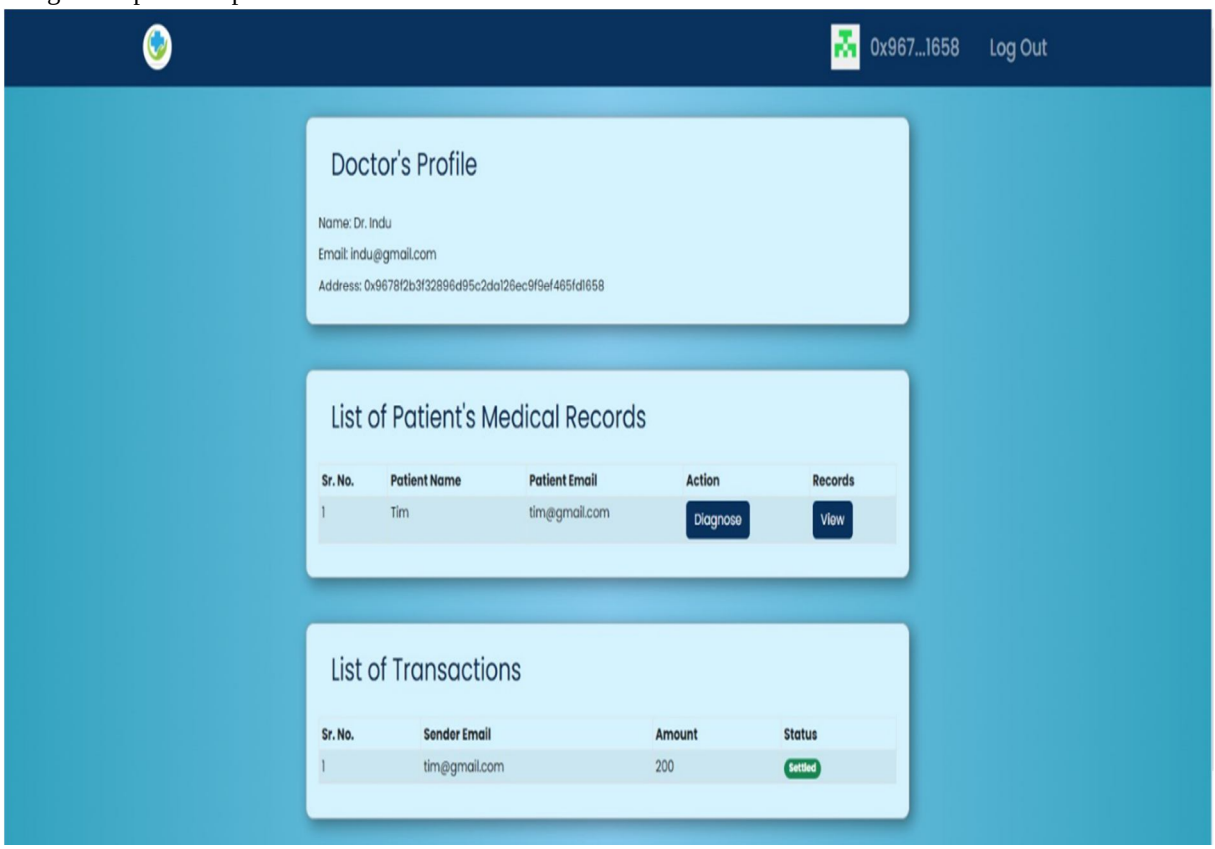


Fig. 9 Doctor Dashboard

The insurer profile (Fig. 10) provides insurers with the ability to view authorized patient data, validate insurance claims, and process payments. This interface ensures that insurers can quickly access the necessary information to verify claims and settle payments, facilitating efficient workflows for all involved parties.

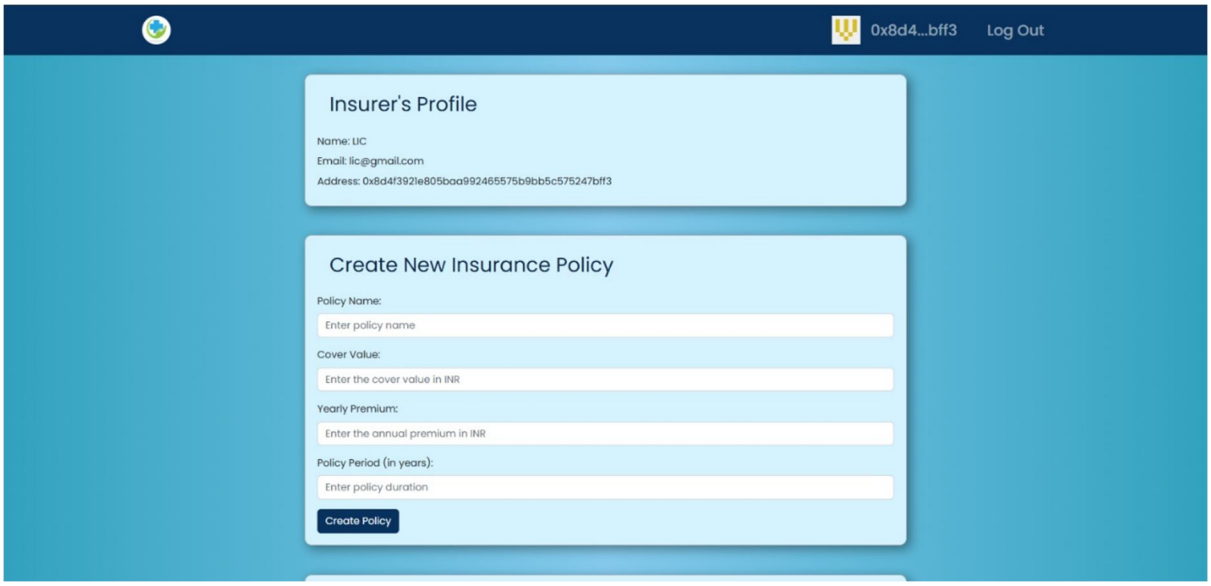


Fig. 10 Insurer Profile

These pages demonstrate the functionality and design of the Medi-Crypt system, ensuring that the platform remains secure, transparent, and user-friendly for all participants.

B. Discussion

The Medi-Crypt system has shown that blockchain and decentralized storage can provide a more secure, transparent, and efficient solution for managing healthcare records. Below are the key takeaways and challenges faced during the development:

1) Security and Privacy:

- Strengths: By leveraging blockchain for secure transactions and IPFS for decentralized storage, the Medi-Crypt system ensures the integrity of medical records while maintaining patient privacy. The use of AES and RSA encryption methods provides a strong layer of security, preventing unauthorized access to sensitive data.
- Challenges: Although the encryption mechanisms used are strong, it is essential to ensure that users handle their private keys and credentials with care. If a user's private key is compromised, their medical records could potentially be exposed, undermining the system's security.

2) Decentralization and Immutability:

- Strengths: The decentralized nature of the system, enabled by blockchain and IPFS, eliminates the risks associated with centralized databases, such as single points of failure and data breaches. All interactions are immutable, meaning once a record is stored, it cannot be altered, providing transparency and accountability.
- Challenges: While decentralization offers significant advantages, it also introduces complexity in terms of scalability and transaction costs. Ethereum's high gas fees during network congestion could make frequent interactions costly, although this can be mitigated by using layer-2 solutions or private blockchains for internal transactions.

3) Automation with Smart Contracts:

- Strengths: Smart contracts automate key processes, reducing human error and the potential for fraud. The insurance claim validation and payment settlement processes, for example, were automated successfully, streamlining operations and improving trust among stakeholders.
- Challenges: While automation is beneficial, it also requires careful testing to ensure that all edge cases are handled properly. The logic within the smart contracts must be thoroughly verified to avoid vulnerabilities that could be exploited.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

4) User Experience:

- Strengths: The platform's user interface was designed to be intuitive and accessible, allowing users with varying levels of technical expertise to interact with the system seamlessly. The integration with Metamask provided a secure and straightforward method of authentication and blockchain interaction.
- Challenges: One of the challenges faced was ensuring the smooth integration between the client interface and the blockchain backend. The blockchain's slow transaction speeds and the need for users to confirm transactions via Metamask sometimes led to delays, which could affect the user experience. However, these issues were mitigated by using proper asynchronous handling and providing users with clear feedback during transaction processing.

VIII. FUTURE ENHANCEMENTS

The future of MediCrypt lies in transforming healthcare into a secure, transparent, and patient-centric digital ecosystem. By leveraging blockchain technology, MediCrypt empowers patients to seamlessly share medical records with global healthcare providers, enabling accurate and timely diagnosis. Its ability to safeguard data integrity and facilitate role-based access positions it as a cornerstone for modern healthcare, ensuring trust and efficiency across stakeholders.

Medi Crypt's smart contracts can revolutionize the insurance landscape by automating claim processes, reducing paperwork, and enabling quicker settlements. Beyond clinical care, the platform holds immense potential for advancing medical research and innovation. By granting researchers access to anonymized, verified patient data, MediCrypt can drive breakthroughs in clinical trials and healthcare technologies on a global scale. Its scalability and integration with emerging technologies like AI and IoT enhance real-time health monitoring and personalized healthcare delivery.

As the demand for secure digital health solutions grows, Medi Crypt's ability to adapt and expand into global healthcare networks ensures its relevance for the future. It has the potential to streamline cross-border data sharing, support collaborative medical research, and foster trust among insurers, patients, and healthcare providers. MediCrypt stands poised to create a connected and efficient ecosystem, driving improved patient outcomes and reshaping the future of healthcare.

IX. CONCLUSION

The MediCrypt project provides a secure and efficient solution for patient data management using blockchain technology. Its decentralized and immutable nature ensures medical data is secure, tamper-proof, and accessible only to authorized individuals. Patients maintain control over their records by granting or revoking access to doctors as needed, ensuring transparency while safeguarding privacy.

Key features include patients' ability to add or remove doctors from their access list and doctors securely uploading diagnosis reports upon access. The system also streamlines administrative processes like insurance claims and payment settlements, improving efficiency and collaboration between patients and healthcare providers.

By enhancing data security, patient control, and interoperability, MediCrypt empowers patients and simplifies healthcare workflows. Its scalable design ensures efficient medical record management, setting a strong foundation for a more secure and patient-centred digital healthcare system.

X. ACKNOWLEDGEMENT

We convey our sincere thanks to Rajya Vokkaligara Sangha, Bangalore and our guide Dr. S Mercy, Associate Professor, Department of Information Science and Engineering, Bangalore Institute of Technology, without whose direction, this would not have been possible. We also express our gratitude to our team members whose participation and coordination resulted in successful completion of the paper.

REFERENCES

[1] M. M. Madine, A. A. Battah, I. Yaqoob, K. Salah, R. Jayaraman, Y. Al-Hammadi, S. Pesic, and S. Ellahham, "Blockchain for Giving Patients Control Over Their Medical Records," IEEE Access, vol. 8, pp. 193102–193115, 2020

[2] Y. Zhuang, L. R. Sheets, Y.-W. Chen, Z.-Y. Shae, J. J. P. Tsai, and C.-R. Shyu, "A Patient-Centric Health Information Exchange Framework Using Blockchain Technology," IEEE J. Biomed. Health Informat., vol. 24, no. 8, pp. 2169–2176, Aug. 2020

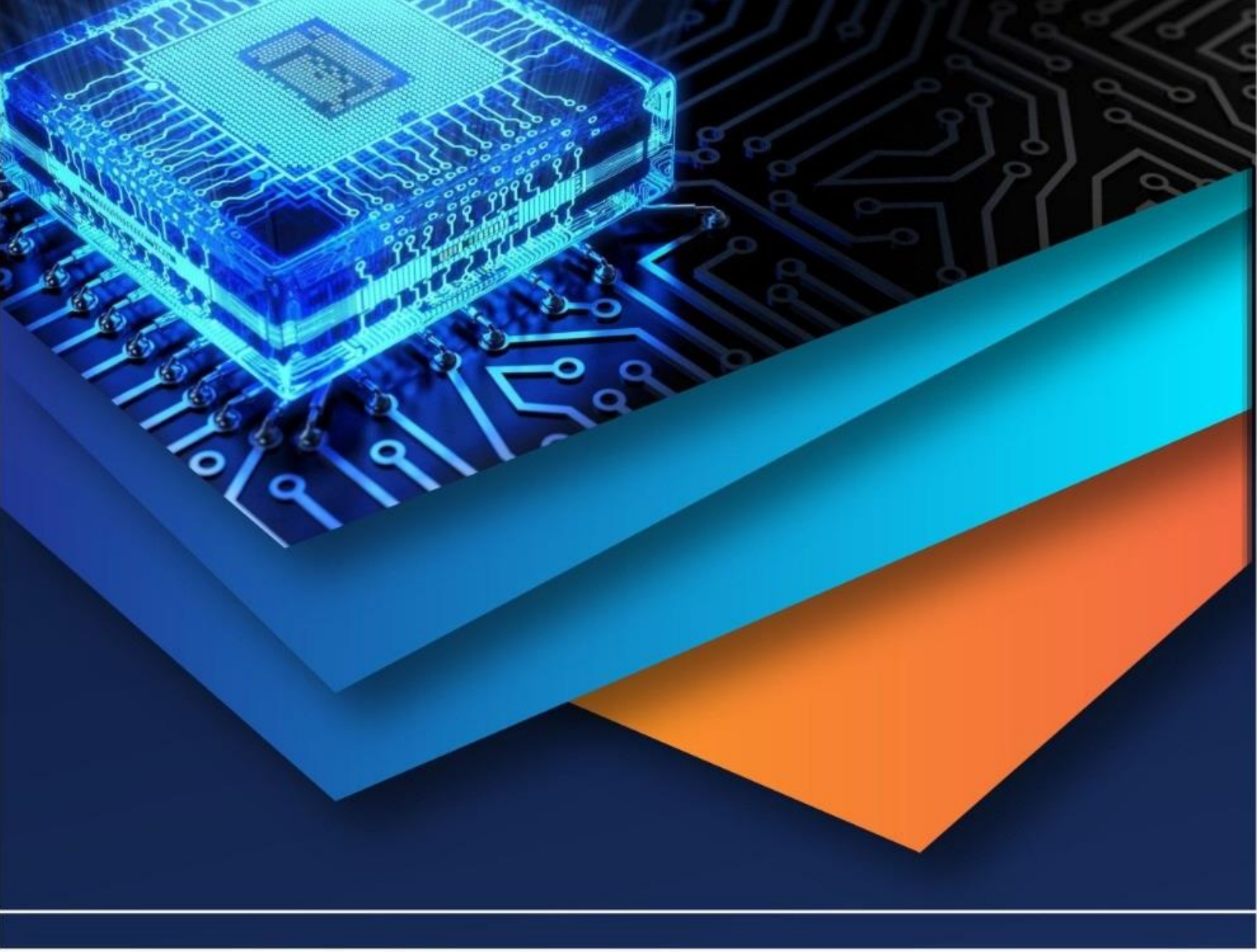
[3] A. A. Mamun, S. Azam, and C. Gritti, "Blockchain-Based Electronic Health Records Management: A Comprehensive Review and Future Research Direction," IEEE Access, vol. 10, pp. 11929–11955, 2022

[4] S. Ramzan, A. Aqdus, V. Ravi, D. Koundal, R. Amin, and M. A. Al Ghamdi, "Healthcare Applications Using Blockchain Technology: Motivations and Challenges," IEEE Trans. Eng. Manage., vol. 69, no. 3, pp. 1114–1131, Jul. 2022

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

[5] A. Kumar, R. Kumar, and S. S. Sodhi, "A Novel Privacy Preserving Blockchain Based Secure Storage Framework for Electronic Health Records," J. Inf. Optim. Sci., vol. 43, no. 3, pp. 549–570, 2022
[6] S. Barbaria, M. C. Mont, E. Ghadafi, H. Mahjoubi, and H. B. Rahmouni, "Leveraging Patient Information Sharing Using Blockchain-based Distributed Networks," IEEE Access, vol. 10, pp. 106334–106351, Sep. 2022.
[7] S. Abbate, P. Centobelli, R. Cerchione, E. Oropallo, and E. Riccio, "Blockchain Technology for Embracing Healthcare 4.0," IEEE Trans. Eng. Manage., vol. 70, no. 8, pp. 2998–3009, Aug. 2023.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)