Journal of Artificial Intelligence and Capsule Networks (ISSN: 2582-2012)
www.irojournals.com/aicn/

Blockchain-based Electronic Health Record Management System

Sulav Shrestha[1], Sagar Panta[2]

Computer Engineering, United Technical College, Pokhara University, Bagmati, Nepal

Email: [1]Sulavs84@gmail.com, [2]pantasagar81@gmail.com

Abstract

The Blockchain-based Electronic Health Record (B-EHR) system represents a significant advancement in healthcare data management. Concerns over data confidentiality and security have become increasingly critical in the healthcare sector, given the need for immediate data accessibility. Traditional centralized systems face accessibility issues, necessitating a transformative solution, and blockchain technology emerges as a promising candidate. This research introduces a patient-controlled, blockchain-based system that efficiently manages and safeguards individuals' health-related data. By harnessing the Ethereum network and utilizing tools such as Ganache, Solidity, and web3.js, this system takes a systematic approach to overcome the limitations of centralized systems. Smart contracts, the basis of blockchain technology, serve as the backbone for storing and processing patients' data in a decentralized manner. Transactions are conducted securely through these smart contracts, ensuring patient privacy and data security. Notably, any modifications to transactions can be verified and propagated across the entire distributed network, enhancing data integrity. Complementing this system is a cryptocurrency wallet like MetaMask, providing a centrally controlled repository where records can be swiftly accessed and secured by authorized individuals, including doctors and patients. This integration significantly improves data accessibility and security within the healthcare domain. Ultimately, this research aims to leverage blockchain technology for simultaneous data retrieval, enhancing efficiency, credibility, and accessibility. It offers a robust framework for securely storing data with tailored access permissions and facilitates the safe transfer of patient medical records. In essence, it introduces a swift and secure health record system and an innovative protocol, promoting

DOI: https://doi.org/10.36548/jaicn.2023.3.006
Received: 15.08.2023, received in revised form: 12.09.2023, accepted: 24.09.2023, published: 07.10.2023

greater transparency and ownership of sensitive data in the healthcare sector through blockchain integration.

Keywords: Electronic Health Record, Ethereum, MetaMask, Blockchain, Decentralization, cryptocurrency wallet.

1. Introduction

The concept of blockchain technology was originated by Satoshi Nakamoto in 2008 with the publication of the Bitcoin whitepaper. Bitcoin, the first decentralized cryptocurrency, introduced the world to the potential of blockchain as a secure and transparent ledger. Since then, blockchain has evolved beyond cryptocurrency and found applications in various industries, including healthcare. Electronic Health Records emerged as a digital form of patient medical records, but challenges such as security vulnerabilities and lack of interoperability were faced [1]. In healthcare, Electronic Health Records (EHRs) emerged as digital versions of patient medical histories. However, traditional EHR systems faced challenges like security vulnerabilities and interoperability issues. Blockchain emerged as a potential solution to enhance EHR management. EHRs contain essential clinical and administrative data for healthcare, aiming to streamline processes and improve patient care. Blockchain addresses these issues by offering a decentralized and secure approach. It ensures data integrity through cryptographic hashing and enhances security with public-key cryptography, giving each user a unique public and private key. Blockchain resolves interoperability challenges by enabling seamless data sharing among trusted parties. It also facilitates smart contracts that automate actions based on predefined criteria, streamlining consent management, and ensuring data access under specific conditions. Integrating blockchain with EHRs enhances data security, privacy, interoperability, and patient control, revolutionizing healthcare data management [1] [4].

2. Problem Statement

Countries like Nepal encounter challenges related to security, interoperability, and patient privacy. These outdated methods lack efficiency and hinder effective healthcare delivery and coordination among providers. To address these issues, a blockchain-based health record management system is essential. Blockchain offers a decentralized, tamper-resistant, and transparent platform for secure data storage and access. It ensures privacy, consent

management, and data integrity, and mitigates the risk of fraud or unauthorized access. Implementing blockchain in Nepal can enhance healthcare delivery, and coordination, and facilitate interoperability among healthcare systems [2]. The interoperability capabilities of blockchain can facilitate the seamless sharing and exchange of health records across different healthcare organizations and systems. This would enable healthcare providers to access comprehensive and up-to-date patient information, leading to improved care coordination, accurate diagnoses, and effective treatment planning [3].

According to authors in [2], By adopting a blockchain-based health record management system, Nepal can overcome the limitations of traditional methods and empower both patients and healthcare providers with a secure, interoperable, and efficient solution. This system would enhance data privacy, promote collaboration among healthcare stakeholders, and ultimately improve healthcare outcomes for the population.

3. Objectives

The objective of blockchain-based health record management is:

1. To address interoperability issues and enable seamless data exchange among healthcare providers using distributed ledger, standardized protocols, and secure data sharing mechanisms [4] [5] [6].
2. To automate and enforce privacy policies and data access controls, securing patient health records by allowing access and interactions solely for authorized individuals in accordance with pre-established rules and conditions [7] [2].

4. Related Work

In the context of healthcare interoperability and Electronic Health Records (EHR) management, several research papers and proposals have been discussed. In reference [10], Linn and Koo suggest an approach of storing electronic medical records (EMRs) off-chain in a data lake rather than on a blockchain. While some basic principles and touch on scalability, access security, and data privacy are provided, their work still lacks a comprehensive system or detailed implementation. Notably, the research does not delve into aspects such as fault tolerance, disaster recovery, or performance. In [11], Jiang et al. introduce BlocHIE, a

Healthcare Information Exchange platform that leverages blockchain technology in a cloud environment. This platform comprises two interrelated blockchains: EMRChain for managing EMRs and PHD-Chain for personal healthcare data. The study has put forth a Proof of Work-based consensus algorithm with a modified transaction processing method, achieving a commendable throughput of 46 transactions per second. However, the scalability and performance of the platform under high-stress and crisis situations require further testing and evaluation. The author Dubovitskaya, Xu, and his colleagues [10] present a framework for securely sharing EMR data with precise access control, particularly tailored for oncology clinical systems. The Hyperledger Fabric and a PBFT consensus algorithm is utilized in the research. While emphasizing consent management, data transfer efficiency, and extended treatment period management, the scalability of the system remains unverified in real-world scenarios, necessitating further performance assessment. Regarding [4], the medical chain a case study focused on giving users ownership and control over their health records while promoting transparency among healthcare stakeholders is suggested. However, this work is primarily centered on a business plan and lacks comprehensive technical details. Notably, it introduces an emergency access backup system using an emergency bracelet for caregiver access to critical patient information. In conclusion, blockchain technology holds significant promise for transforming EHR management systems, offering decentralization, security, transparency, patient control, data integrity, and interoperability advantages. Various blockchain models like Ethereum, Hyperledger, Corda, and Tendermint have been proposed, each providing unique benefits. Nevertheless, addressing scalability, performance, and emergency access backup systems remains crucial for practical blockchain-based health record management [3] [13].

5. Proposed Work

The proposed development involves creating a web application for a Blockchain-based Electronic Health Records system using the Next.js web framework. This application will be seamlessly integrated with the Ethereum-based blockchain to ensure the utmost security of patient data through reliable transactions. Within the healthcare system, each transaction corresponds to various aspects of a patient's medical history, including hospital visits, administrative records, diagnosis reports, treatment specifics, physician's notes, laboratory results, prescriptions, X-rays, and outcomes, among others.

Through this system, patients will gain control over their data-sharing preferences, allowing them to view and grant permission to doctors selectively. The patients will have the autonomy to decide which parts of their medical history healthcare providers can access, ensuring the privacy and security of the remaining data. The decentralized nature of blockchain promotes interoperability among different healthcare institutions, enabling them to adopt a standardized system for storing health data [4] [5]. The architecture of the system adheres to multiple high-level patterns and principles. It primarily emphasizes the external components of the system that are visible to users and their interactions with one another. Figure 1 illustrates the overall architecture of the system. In this architecture, it consists of three modules (Layers).

The first module is the User Management Layer, which provides a user interface for patients and doctors to interact with the Electronic Health Record system. Through this module, users can input and retrieve data that will be stored in decentralized storage.

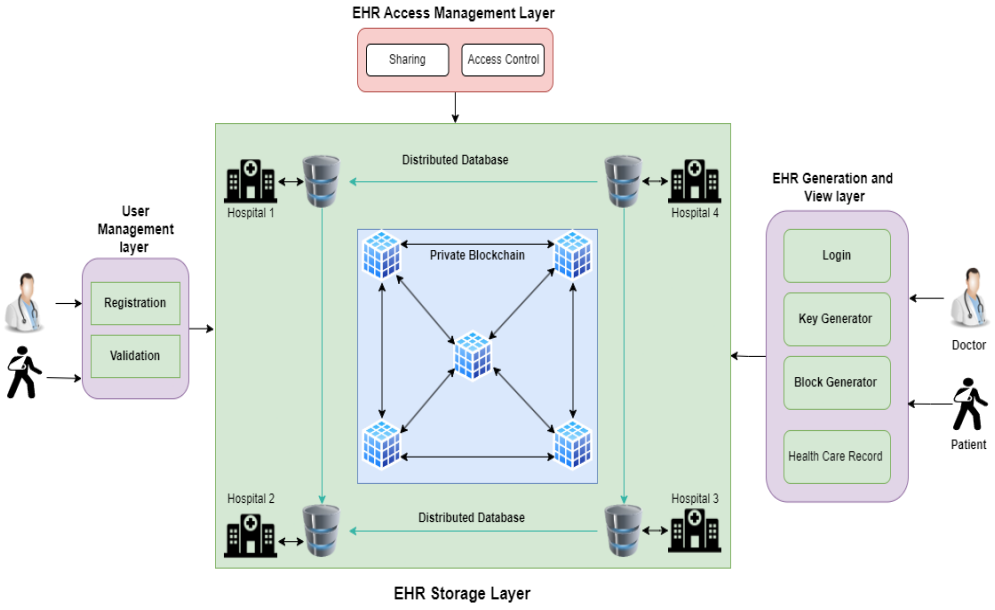

Figure 1. System Architecture

The second module is the EHR Storage Layer, which serves as the backbone of the research. In this module, data is stored in blockchains maintained by hospitals, with databases that are distributed across the network. Popular tools that have been used in this module include Next.js, Ganache, Truffle, and MetaMask. APIs are used to facilitate communication between the User Management Layer and the EHR Storage Layer, with incoming requests triggering data storage procedures in the latter.

The third module is the EHR Generation and View Layer, which provides a comprehensive and efficient means of managing patient health information in electronic format. Healthcare providers can access patient data from multiple sources through this module, which includes tools for searching, filtering, and visualizing trends and patterns in the data.

6. Flowchart

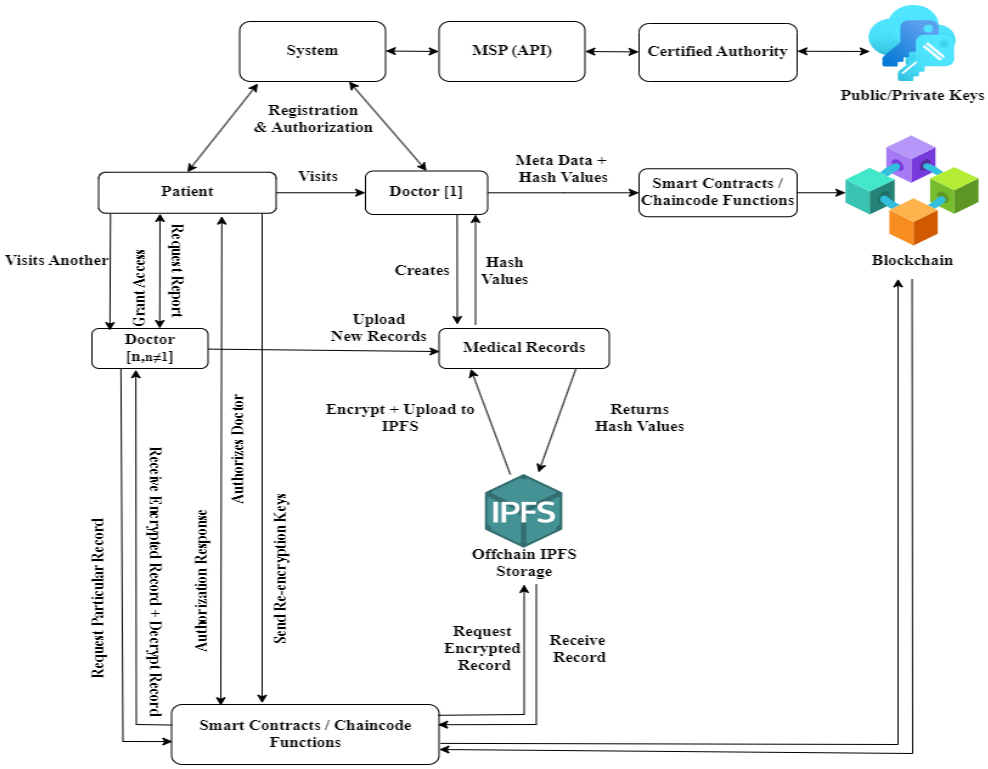

Figure 2. Flowchart of the System

The flowchart in Figure.2 illustrates the operation of the Electronic Health Record Management System, showcasing encryption, key generation, and access control processes. User registration leads to the creation of three keys: a private key (stored locally), a public key (in the database), and a symmetric key (encrypted with the public key on the server). Access is granted by providing the private key, which retrieves and decrypts the symmetric key for authorized personnel. Storing EHRs in IPFS involves encrypting medical data into PDFs, further encrypting with a symmetric key, and storing on IPFS, generating a CID (Content Identifier). This CID is recorded in the blockchain. Access requires the private key to query the blockchain for the CID and retrieve files from IPFS, decrypted using the private key. The system's stack includes database queries, file storage in IPFS, blockchain transactions, and

EHR retrieval and decryption. Key features encompass feasibility, cost-efficiency, strong security, and scalability through IPFS for file storage.

To simplify the entire flowchart of the system, the entire process is divided into distinct stages for discussion.

6.1 Smart Contract Deployment and Interaction

In the context of a blockchain-based Electronic Health Records (EHR) system, the process of creating and deploying smart contracts as shown in Figure.3 involves several key steps. Smart contracts are initially crafted in Solidity to define functions for managing health records and access permissions. These contracts are then compiled using Remix IDE, generating bytecode for the blockchain. The resulting Application Binary Interface (ABI) code is stored in JSON files, like PatientContract.json and DoctorContract.json. Truffle, a development framework, is used for further compilation and setting up the deployment environment. Once compiled, these smart contracts are deployed on the blockchain, enabling them to execute and oversee the specified functionalities [12].

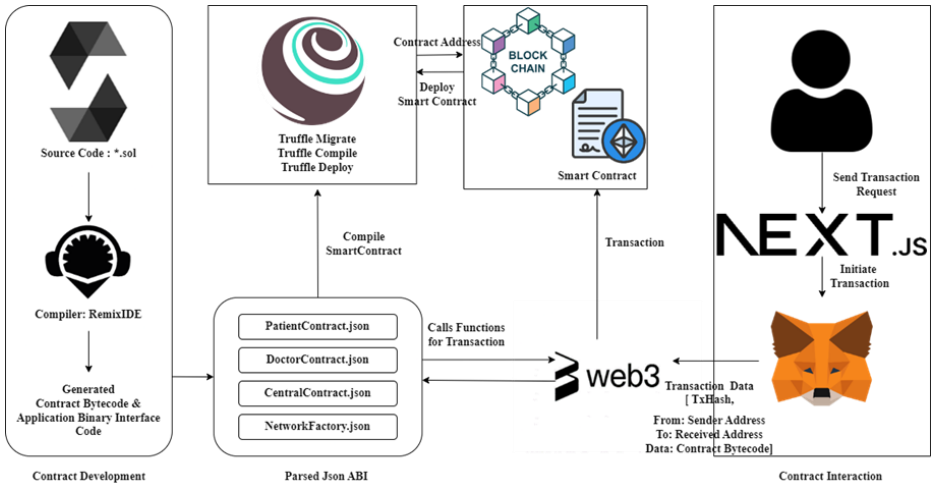

Figure 3. Smart Contract Deployment and Interaction

When a user registers in the system, three key types are generated: Private, Public, and Symmetric keys. The private key is kept highly secure and stored locally on the user's device to prevent unauthorized access. The public key is meant for open sharing, used for verifying signatures and encrypting messages, and is stored on the server, along with an encrypted version of it and the symmetric key. The symmetric key plays a dual role in both data

encryption and decryption processes. The Figure 4 shows the process involved in key generation.

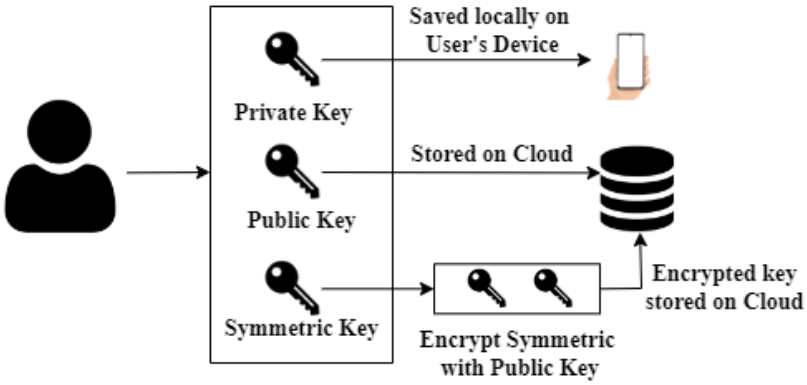

Figure 4. Key Generation Process

6.2 Storing EHR on IPFS

To store Electronic Health Records (EHR) on IPFS, authorized doctors encrypt patient data with a server-provided symmetric key before uploading it to IPFS as shown in Figure.5. A generated hash file confirms successful upload. This hash, along with other data, is later encrypted and stored on the blockchain, ensuring secure and decentralized EHR storage [3].

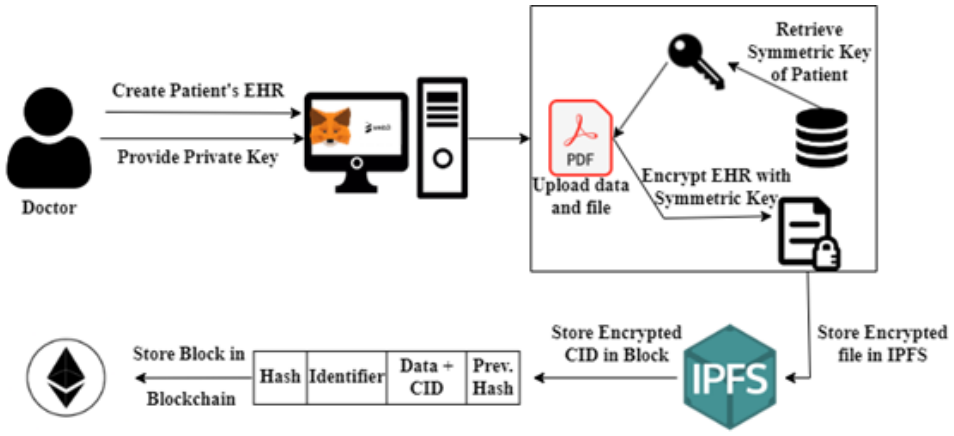

Figure 5. Process of Storing EHR on IPFS

6.3 Accessing the EHR

In healthcare data access, the user starts with a private and patient's public key, submits an EHR request, verified via blockchain, receives an encrypted CID and patient data. The CID

is used to retrieve the EHR from IPFS and get a symmetric key from the server for decryption, ensuring authorized access to the EHR [9].

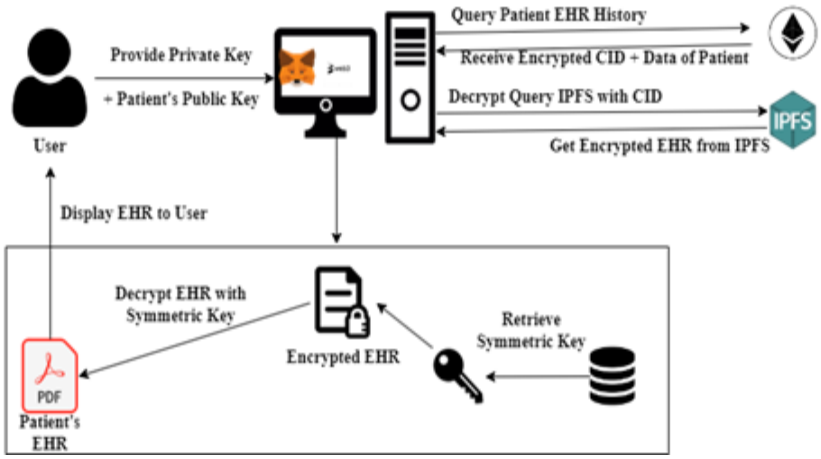

Figure 6. Accessing the EHR

7. Methods and Methodologies

In this section, a formal description of the proposed frameworks elucidates the software platform employed in its development and enumerates the advantages it offers. The subsequent section delves into comprehensive explanations of the key constituents driving the implementation of this framework, notably Ethereum and the Interplanetary File System (IPFS).

7.1 The Smart Contract

Smart contracts are sets of executable instructions on the blockchain, operating directly on the blockchain to ensure resistance to tampering. These contracts are written in the Solidity programming language, allowing programmers to define actions on the blockchain. Solidity code can be written, compiled, and deployed on the Ethereum blockchain. Python is a programming language that can implement Ethereum's Solidity language for crafting smart contract code [14].

7.2 IPFS and Security Algorithm

The Interplanetary File System (IPFS) stands out as a distributed data storage technology, operating on a peer-to-peer network. What sets it apart is its robust approach to

ensuring both secure and tamper-proof data storage, accomplished through the assignment of unique cryptographic hashes to each file. To conserve storage space and streamline data management, IPFS strictly prohibits duplicate files. This feature not only eliminates redundancy but also simplifies data handling. For security, IPFS leverages the SHA-256 algorithm, providing robust protection for stored content. IPFS doesn't merely stop at secure storage; it also excels in efficient data retrieval and safeguarding data integrity. Files within IPFS are uniquely identified by cryptographic hashes, making each one distinct and traceable. This content-based addressing, combined with a Distributed Hash Table (DHT) and a Merkle Directed Acyclic Graph (DAG) structure, ensures speedy and accurate data retrieval. Moreover, the use of cryptographic hashes for file verification prevents any unauthorized tampering with the stored data. In summary, IPFS offers a comprehensive solution for optimized storage, robust security, and efficient data retrieval. By utilizing cryptographic hash functions and content-based addressing, it ensures both data integrity and resource efficiency within its network [15] [8].

The IPFS protocol operates as follows:

1. Each file in IPFS is assigned a unique cryptographic hash.
2. The IPFS network does not allow duplicate files [8]

7.3 Software Used

7.3.1 WEB3

Web3 employs the Hypertext Transfer Protocol[i] (HTTP) connection to establish a connection with the Ethereum network through an Ethereum node. This Ethereum node can either be a local node running on the ETH wallet or a remote one. MetaMask, on the other hand, is a browser extension that facilitates Ethereum account operations and can be seamlessly integrated with websites.

7.3.2 Ganache

Ganache is a deterministic blockchain, meaning it consistently begins in the same state. This predictability is advantageous for testing smart contracts because it ensures consistent test results each time you execute them. Ganache is also known for its speed, allowing for swift deployment, and testing of smart contracts. This characteristic makes it a valuable tool for rapid development and iterative processes.

7.3.3 Truffle

Truffle is a handy tool for blockchain developers, offering a one-click setup for smart contract researches. It streamlines deployment and testing, making it a top choice for developers aiming to work on production-ready blockchain.

7.3.4 MetaMask

MetaMask is a top self-custodial wallet, renowned for its user-friendliness and security when interacting with blockchain applications. It acts as a secure gateway to access web3 technologies, simplifying user engagement. A standout feature is the generation of passwords and keys on the user's device, guaranteeing exclusive access to their accounts and data.

7.3.5 VS Code

Visual Studio Code (VS Code) is a popular, free, and open-source code editor from Microsoft. It's versatile, supporting various programming languages, and designed for modern web and cloud app development.

7.3.6 Solidity

Solidity is a high-level programming language designed for crafting self-executing smart contracts on blockchains like Ethereum. It enables seamless interaction with smart contracts for decentralized services in applications, including React.js and Next.js.

7.3.7 Languages Used

The website's front-end design is developed using HTML, Tailwind-CSS, Next.js, and React.js. The server and back-end are managed through the Solidity programming language and Python. Two essential tools, Truffle and Ganache, are employed for creating local Ethereum blockchains to construct the system. To establish the blockchain and access the system, key tools like the Ethereum virtual interface, MetaMask [wallet], Truffle, Yarn [command-line interface], Ganache, and Local Web3 are utilized.

8. Results and Discussion

This section discusses the access process to the proposed system. This research represents more than just a technological endeavor; This section discusses the access process to the proposed system, which represents an innovative and collaborative effort to revolutionize healthcare data management. The research seamlessly integrates blockchain technology into healthcare, emphasizing data security, user experience, and efficient record management. The journey of creating this blockchain-based Electronic Health Record system has been defined by dedicated effort and careful design, resulting in interfaces for Homepage, Doctor, Admin, and Patient that reflect this collaborative initiative.

8.1 Homepage

Figure 7 displays the system's homepage, accessible through user account creation. Users can access the system via this homepage, which includes five portals: Dashboard (for system administrators), Doctor, and Patient. Besides these, there's a signup form for patients and unique addresses for doctors and admins [10].

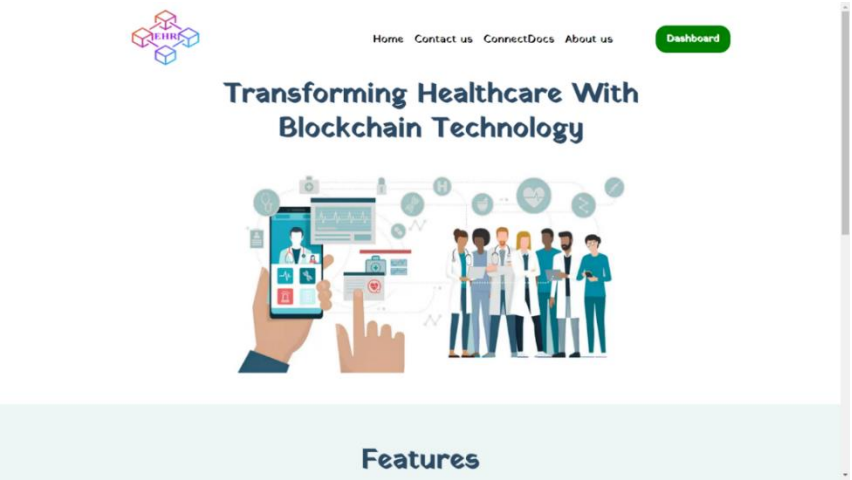

Figure 7. Homepage of the Proposed System

8.2 Patients Upload their Records

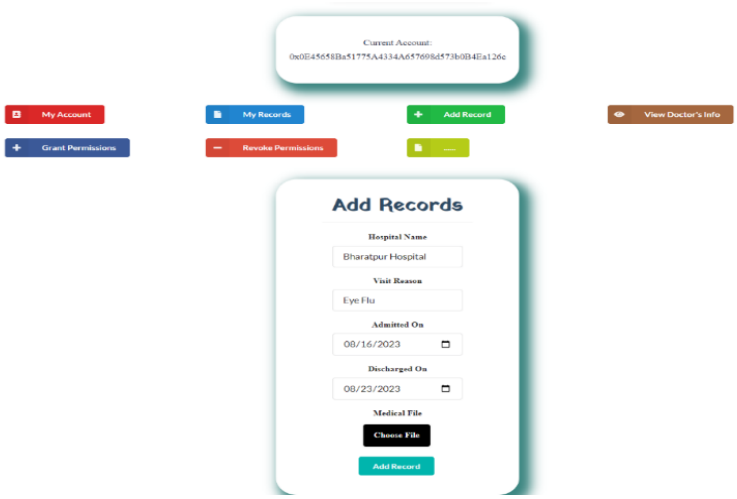

Figure 8. Patients Uploading their Records.

The above Figure 8 describes how the patients can upload or add their medical records. The patient can upload their medical file as well as include the hospital's name, he/she visited for a checkup, the reason for which he/she visited, dates of admission, and discharge [11].

8.3 Doctor Accessing Record

Figure 9 shows how doctors' access medical records: registering patients, creating encrypted blockchain records, managing permissions via smart contracts, verifying with cryptographic keys, decrypting data locally, and logging all interactions on the blockchain for transparency [12].

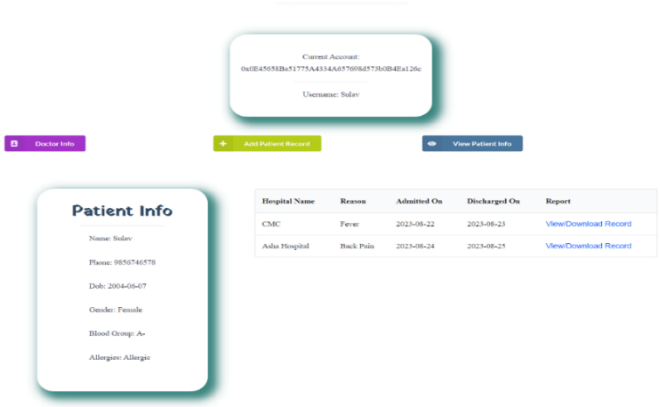

Figure 9. Doctor Accessing Records.

9. Conclusion

In summary, the proposed system Blockchain-Based Electronic Health Record Management System represents a significant leap forward in healthcare technology. By harnessing blockchain, this system revolutionized data security and patient privacy, eliminating unauthorized access. The system streamlines the sharing of Electronic Health Records across healthcare organizations, enhancing overall coordination. System smart contracts efficiently handle patient consent and regulatory compliance, reducing administrative complexities. At the conclusion of this research it's evident that the work carried out is at the forefront of healthcare technology transformation, demonstrating how blockchain can optimize healthcare, making it more efficient, secure, and patient-centered.

References

[1] Sharma, Ashutosh, Sarishma, Ravi Tomar, Naveen Chilamkurti, and Byung-Gyu Kim. "Blockchain based smart contracts for internet of medical things in e-healthcare." Electronics 9, no. 10 (2020): 1609.

[2] Watkinson-Powell, Anna, and A. Lee. "Benefits of an electronic medical records system in rural Nepal." Journal of the Nepal Medical Association 52, no. 188 (2012).

[3] Yang, Huihui, and Bian Yang. "A blockchain-based approach to the secure sharing of healthcare data." In Proceedings of the norwegian information security conference, pp. 100-111. Oslo, Norway: Nisk J, 2017.

[4] Azaria, Asaph, Ariel Ekblaw, Thiago Vieira, and Andrew Lippman. "Medrec: Using blockchain for medical data access and permission management." In 2016 2nd international conference on open and big data (OBD), pp. 25-30. IEEE, 2016.

[5] Gharat, Anurag, Pratik Aher, Punit Chaudhari, and Bhavana Alte. "A framework for secure storage and sharing of electronic health records using blockchain technology." In ITM Web of Conferences, vol. 40, p. 03037. EDP Sciences, 2021.

[6] Sheth, Alpen, and Hemang Subramanian. "Blockchain and contract theory: modeling smart contracts using insurance markets." Managerial Finance 46, no. 6 (2019): 803-814.

[7] Nishi, Farjana Khanam, Mahizebin Shams-E-Mofiz, Mohammad Monirujjaman Khan, Abdulmajeed Alsufyani, Sami Bourouis, Punit Gupta, and Dinesh Kumar Saini. "Electronic healthcare data record security using blockchain and smart contract." Journal of Sensors 2022 (2022): 1-22.

[8] Linn, Laure A., and Martha B. Koo. "Blockchain for health data and its potential use in health it and health care related research." In ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST, pp. 1-10. 2016.

[9] Akhter Md Hasib, Kazi Tamzid, Ixion Chowdhury, Saadman Sakib, Mohammad Monirujjaman Khan, Nawal Alsufyani, Abdulmajeed Alsufyani, and Sami Bourouis. "Electronic health record monitoring system and data security using blockchain technology." Security and Communication Networks 2022 (2022): 1-15.

[10] Yue, Xiao, Huiju Wang, Dawei Jin, Mingqiang Li, and Wei Jiang. "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control." Journal of medical systems 40 (2016): 1-8.

[11] Albeyatti, A. "Medicalchain whitepaper 2.1." (2018).

[12] Chaudhuri, A. B. Flowchart and algorithm basics: The art of programming. Mercury Learning and Information, 2020.

[13] Jiang, Shan, Jiannong Cao, Hanqing Wu, Yanni Yang, Mingyu Ma, and Jianfei He. "Blochie: a blockchain-based platform for healthcare information exchange." In 2018 ieee international conference on smart computing (smartcomp), pp. 49-56. IEEE, 2018.

[14] Buterin, Vitalik. "A next-generation smart contract and decentralized application platform." white paper 3, no. 37 (2014): 2-1.

Author's biography

Sulav Shrestha, born in Bharatpur, Nepal, on March 22, 2002, recently completed his bachelor's degree in computer engineering with a remarkable CGPA of 3.55, showcasing his commitment to academic excellence. His journey into technology and innovation has been influenced by figures like Krish Naik, Ganesh from Think School, Dhaval Patel, and Denis Ivy, but his greatest source of inspiration and guidance has been his brother, Rabin Shrestha. Sulav is not only a standout academic but also an adventurer who loves exploring the outdoors, from small hikes to trekking expeditions. His curiosity extends to financial planning and investment, and his treks to various places have deepened his appreciation for the natural world and its wonders.

Sagar Panta, born in Bharatpur, Nepal, on April 15, 2000, recently completed his bachelor's degree in computer engineering with a notable CGPA of 3.51, demonstrating his dedication to academic excellence. His passion for technology and the arts is fueled by YouTube influencers like Telusko, Ganesh from Think School, Easytus4u, and Denis Ivy. Beyond academics and technology, He actively engages in research projects, presenting papers that reflect his intellectual prowess and earning recognition for his dedication. Sagar's journey embodies a commitment to academic excellence, artistic expression, and technological innovation, making him a well-rounded individual who embraces both analytical and creative pursuits with enthusiasm.