Journal of Digital Assets and Monetary Research

Volume 1, Issue 1

Research Article

Date of Submission: 20 February 2026
Date of Acceptance: 09 March 2026
Date of Publication: 13 March 2026

Secure Electronic Health Records Using Blockchain Technology

Akshay Kumar Aluri*
Independent Researcher, India

***Corresponding Author:** Akshay Kumar Aluri, Independent Researcher, India.

Citation: Akshay, A. (2026). Secure Electronic Health Records Using Blockchain Technology. *J Digi Assets Monetary Res*. 1(1), 01-12.

Abstract
Blockchain technology presents significant opportunities for improving data security, privacy, and user control across various sectors, including healthcare. Traditional Electronic Health Record (EHR) systems often struggle with unauthorized access, limited interoperability, and a lack of patient control over sensitive data. This project proposes a blockchain-based EHR system to overcome these challenges by placing the patient at the center of data management. The proposed system allows patients to upload, manage, and share their medical records while granting or revoking access as needed. It employs Solidity smart contracts for secure access control, MetaMask for authentication, Ganache and Truffle for testing, and off-chain storage using IPFS via Pinata. The front end is developed in ReactJS to ensure a seamless and intuitive experience. By storing only critical metadata on-chain and maintaining full records off-chain, the system addresses scalability and efficiency issues. This solution enhances privacy, ensures secure sharing, and empowers patients with ownership of their healthcare data.

Keywords: Blockchain Technology, Electronic Health Records (EHR), Solidity Smart Contracts, InterPlanetary File System (IPFS), Data Privacy and Security, Patient-Centric Data Management, Decentralized Storage, Access Control, Interoperability, and Medical Data Sovereignty.

Introduction
Electronic Health Records (EHRs) are digital versions of a patient's medical history, replacing traditional paper-based systems. They store critical healthcare data such as personal information, medical history, test results, diagnoses, prescriptions, allergies, vaccinations, and physician notes. Hospitals and clinics use EHRs to streamline patient care, improve efficiency, and enhance accessibility.

One of the key advantages of EHRs is their ability to facilitate better communication between healthcare providers, ensuring faster decision-making and reducing medical errors. Physicians can review allergy lists before prescribing medication, and automated alerts can prevent harmful drug interactions. Additionally, EHRs save time by eliminating manual paperwork, allowing healthcare professionals to focus more on patient care.

Despite these benefits, conventional EHR systems face significant challenges, particularly in data security, patient autonomy, and interoperability. Cyberattacks and data breaches make

sensitive medical information vulnerable, while patients often lack control over who can access their records. Furthermore, different healthcare institutions use incompatible EHR systems, making seamless data exchange difficult. Blockchain technology presents an innovative solution by offering enhanced security, transparency, and patient control over medical records. Using decentralized networks, cryptographic protection, and smart contracts, blockchain-based EHRs empower patients to manage access permissions while ensuring secure data storage.

This project proposes a blockchain-integrated EHR system, utilizing MetaMask, IPFS (via Pinata), Solidity smart contracts, Truffle, and Ganache to develop a secure, privacy-focused, and patient-centric medical record management framework. The system aims to give patients full control over their health information while improving security, efficiency, and interoperability.

Importance of Electronic Health Records:
Electronic Health Records (EHRs) enhance healthcare by providing instant access to patient data, reducing errors, and improving coordination. They streamline processes, ensuring efficiency for doctors and patients. However, security risks and lack of patient control remain challenges. Blockchain integration can offer enhanced security, transparency, and patient autonomy in medical data management.

Why Block Chain:
Blockchain is a powerful technology, but it is not needed for every system. It is best used in situations where security, transparency, and trust are very important.

- Patient Autonomy & Control
  Smart contracts let patients manage who accesses their data, granting or revoking permissions in real time. This enhances privacy and gives individuals ownership of their medical history.
- Improved Interoperability & Data Sharing
  Blockchain facilitates seamless exchange between disparate systems while maintaining data consistency. Authorized providers can access reliable, standardized records across institutions.
- Efficiency & Reduced Errors
  With real-time access to accurate health data, blockchain minimizes medical errors and redundant diagnostics. This streamlines care delivery and reduces administrative overhead.
- Decentralized & Scalable System
  Built with tools like MetaMask, IPFS, and Solidity, blockchain EHRs scale efficiently across networks. They ensure resilient, vendor-neutral data storage and retrieval.
- Transparency & Trust
  Every transaction and data change is permanently logged, creating an auditable trail. This transparency builds trust between patients, providers, and institutions
- Decentralized Storage & Security
  Blockchain disperses data across multiple nodes, eliminating centralized weak points. This architecture drastically reduces the risk of data breaches.
- Cost Reduction & Efficiency
  Automated workflows and elimination of third-party intermediaries lower operating costs. Blockchain accelerates verification, billing, and access processes with fewer manual steps.

- Future-Proofing Healthcare Data
  Blockchain supports integration with AI, IoT, and advanced analytics for dynamic healthcare ecosystems. Its scalability ensures readiness for growing data complexity.

- Fraud Prevention & Authenticity
  Immutable recordkeeping thwarts data falsification and billing fraud. Patients and insurers gain confidence in the authenticity of healthcare transactions.

Blockchain Integration with Secure EHR

Each time a significant action happens—like a doctor updating a record, a patient sharing data, or a lab uploading results—a new block is created. Here's how that process works:

Data Event Initiation

A trigger occurs (e.g. a blood test result is uploaded to the EHR system).
This creates a transaction request to record this new data securely. The request is broadcast to all nodes (computers) in the blockchain network.
Nodes validate the request using a consensus algorithm (like Proof of Work or Proof of Authority, depending on the setup).

Transaction Verification

The request is broadcast to all nodes (computers) in the blockchain network.
Nodes validate the request using a consensus algorithm (like Proof of Work or Proof of Authority, depending on the setup).

- A cryptographic hash of the previous block (chaining them together)
- Timestamp
- New health data
- A digital signature for authenticity
- The new block is appended to the chain in a linear, chronological order.
- Now, it becomes an immutable part of the EHR record.

Block Formation

Once verified, the data is bundled into a block. Each block contains:
Block Addition

What Are the Blocks in EHR Blockchain?

Block Type	Description
Reports	Upload and retrieval of records
Test Result Block	Contains lab reports, medical imaging results
Prescription Block	Logs medication prescribed or changed
Access Log Block	Tracks who accessed or requested the EHR data
Consent Block	Stores patient approvals for data sharing

Each of these is hashed and linked to the previous one, creating a transparent, traceable timeline of a patient's health journey.

How It Works

A block contains:

1. Transaction data
   - Timestamp
   - Previous block's hash
   - A nonce (initially set to 0)

2. The miner:
    - Hashes the block with the current nonce
    - Checks if the resulting hash meets the difficulty target
    - If not, increments the nonce and tries again
3. Once a valid hash is found:
    - The block is added to the blockchain
    - The nonce used is stored in the block as proof of work

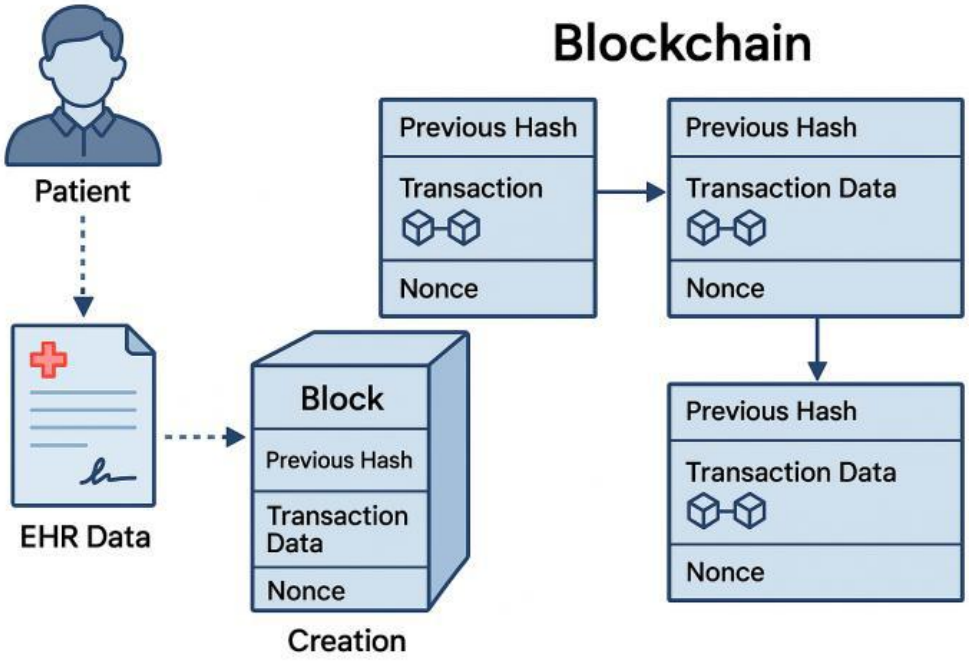

Fig.1 Blockchain Integration

Problem statement:

The healthcare system faces critical challenges in managing Electronic Health Records (EHRs), including data security vulnerabilities, interoperability issues, and restricted patient access. Data breaches expose millions of medical records, compromising privacy and trust. The lack of compatibility between different EHR systems prevents seamless data exchange, hindering healthcare efficiency. Additionally, patients have minimal control over their records, as hospitals and healthcare providers primarily manage access.

Model performance:

The proposed blockchain-based EHR system will be evaluated based on the following metrics:

- Security & Privacy Ensuring data encryption and tamper-proof records using blockchain and IPFS.
- Preventing unauthorized access with smart contract-based permission control.
- Interoperability & Efficiency Seamless data exchange between hospitals using standardized blockchain protocols.
- Optimized retrieval speed for medical records using decentralized storage solutions.
- Patient Control & Accessibility Patients can grant/revoke access via smart contracts, enhancing autonomy.
- User-friendly interface with MetaMask authentication for secure access.
- Scalability & Performance Optimization Utilizing off-chain storage techniques to efficiently handle large medical files.
- Minimizing transaction costs and processing time for medical record update.

System Analysis

Existing System

Current Electronic Health Record (EHR) systems face many challenges. They store medical data like patient history and lab results, but are often insecure, with over 173 million records breached globally. Different hospitals use different EHR systems, making it hard to share data due to no common standards. Patients struggle to access their own records, as hospitals control them, creating unfair access. Storing large files like X-rays slows systems down, and data can be easily tampered with or duplicated. Paper-based records, used earlier, were unorganized, insecure, and caused delays. Existing EHR systems, though better, are not user-friendly and lack reliability, as shown in studies like one from Finland. These issues reduce trust and efficiency in India's healthcare, affecting millions. Current solutions don't fully address security, sharing, or patient access, pushing the need for a better, secure system like blockchain.

Disadvantages:

- Less secure
- Unable to store large files
- Difficulty in retrieving data
- Less capability of data sharing

Proposed System

Healthcare system struggles with Electronic Health Records (EHRs) due to data breaches, poor sharing, and limited patient access. The proposed system uses blockchain technology, specifically Ethereum, to create a secure, decentralized platform for EHRs. It stores basic patient data and IPFS hashes on the blockchain, while large files like X-rays are kept off-chain on IPFS for faster performance. Role-based access ensures only authorized users, like doctors and patients, can view or update records, improving privacy and trust. Smart contracts manage tasks like adding, viewing, or deleting records securely. This framework aims to enhance security, data sharing, and patient control, making healthcare more efficient and reliable.

Advantages

- High secure
- Efficient in Data Sharing
- Able to store large files
- Patient Ownership
- Easy to use

Modules Implementation

Proposed System Architecture

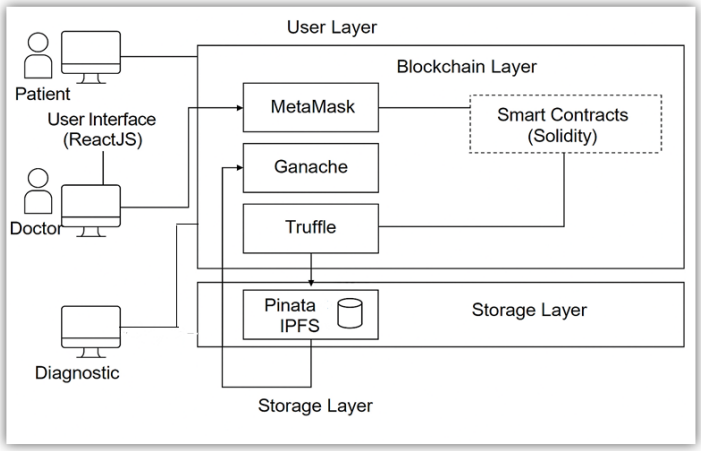

Fig.2 Proposed System Architecture

To save money and overcome scalability constraints, sensitive or bulk data—such as papers and big files—is kept off-chain using systems like Swarm and IPFS.

Web Interface with Centralized Storage

The system has an easy-to-use web interface for data presentation and query. Performance is enhanced by centralized storage, which serves as a temporary or cache layer for data that is frequently accessed.

Blockchain On-Chain Storage

On-chain storage of critical data (such as hashes, metadata, or transaction records) guarantees security, transparency, and immutability. Smart contracts make it easier to communicate, carry out, and automate preset rules (such access control or data validation).

Decentralized Off-Chain Storage

To safely connect off-chain data to the on-chain layer, the blockchain keeps track of data references, such as cryptographic hashes.

- Data transfer: The smooth transition between off-chain, on-chain, and centralized layers.
- Save Data: Storage activities across layers can be triggered by users or smart contracts.
- Interaction: Access requests and audits are mediated via smart contracts.

Data Flow & Interaction

Work Flow for Electronic Health Records

The workflow for a blockchain-based decentralized application developed with React.js, Truffle, MetaMask, Ganache, and Node.js is thoroughly described in this article. The entire lifecycle—from development to deployment and user interaction—is covered by the workflow.

Development Phase

Writing Solidity smart contracts, which specify the Dapp's rules and business logic, is the first step in the development process. These contracts are compiled, tested, and deployed using the Truffle development framework. In this stage:

- .sol files are used to write and store smart contracts.
- Truffle is used to compile contracts into bytecode and ABIs.

- JavaScript is used to write thorough tests that confirm the functionality of the contract.
- For preliminary testing, contracts are posted to a local blockchain (Ganache).

Local Testing Environment

With the help of Ganache, a local Ethereum blockchain simulation tool, developers can effectively test and debug smart contracts. Without having to wait for network confirmations, it offers instant transaction mining. The development process is streamlined by allowing developers to engage with their contracts using pre-funded test accounts instead of actual cryptocurrency.

Ganache helps developers find and fix problems fast by providing comprehensive transaction logs and error reporting. Additionally, it makes it possible to simulate various network conditions, such fluctuating gas costs and block times, guaranteeing that contracts function as best they can in actual situations.

Ganache speeds up contract deployment and improves workflow efficiency by connecting easily with development frameworks like Truffle and Hardhat. Both novice and seasoned blockchain developers Favor it because of its intuitive UI and adaptable settings. Before deploying to the Ethereum main net, developers can use Ganache to confirm gas usage estimates and enhance contract functionality, guaranteeing safe and economical transactions.

Frontend Integration

For blockchain applications, the React.js frontend serves as the user interface, facilitating smooth communication with decentralized networks and smart contracts. For blockchain connection, it makes use of Web3.js or Ethers.js libraries, guaranteeing effective data retrieval and contract execution. By enabling users to safely authenticate, sign transactions, and access their assets, the MetaMask integration streamlines wallet administration.

Because of the frontend's responsive user interface elements, user interactions run well on all devices. Transparency and usability are improved by real-time data display, which guarantees users receive changes from the blockchain instantly. Direct communication with deployed contracts is made possible by its connection to smart contract ABIs for method calls. Secure transaction signing is made possible by MetaMask, while scalability and dependability are guaranteed by Alchemy. Decentralized application development is streamlined by this design, which also offers consumers a secure experience.

Wallet Integration

As a safe wallet and entry point to decentralized networks, MetaMask is a crucial tool for communicating with Ethereum-based apps. It oversees user accounts and private keys, guaranteeing secure transaction execution and authentication. Users can safely sign transactions with MetaMask, which guards against unwanted access. It facilitates smooth main net and test net connectivity by supporting different Ethereum networks. Estimates of gas fees help consumers maximize their spending by bringing clarity to transaction costs. Transaction confirmation dialogs further improve security by confirming information prior to execution. MetaMask streamlines blockchain interactions with its intuitive UI and strong security features, increasing the usability and accessibility of decentralized applications.

Blockchain Interaction

A number of crucial procedures are involved in blockchain activities to guarantee smooth communication with decentralized networks. Users can access stored information by reading

data straight from smart contracts. Signed transactions are necessary for writing data, guaranteeing security and authenticity. In accordance with predetermined conditions, contract events are tracked to initiate particular actions. Managing transaction receipts documents crucial information and verifies effective execution. Efficiency is maximized by controlling gas prices and transaction speeds, which guarantees that transactions are completed within reasonable timeframes and at a reasonable cost. Decentralized apps are built on these operations.

Deployment Process

Blockchain technology guarantees smooth communication with decentralized apps. Users can access stored information by reading data straight from smart contracts. Signed transactions are necessary for data writing, guaranteeing authenticity and security. Real-time updates and automation based on preset triggers are made possible by listening for contract events. Transaction receipts provide crucial information for verification and attest to successful execution. Controlling gas prices ensures seamless processing by maximizing cost effectiveness and transaction speed. These functions serve as the foundation for blockchain-based apps, allowing users and smart contracts to communicate securely and openly.

User Interaction Flow

When using a decentralized application (Dapp), the user experience runs smoothly from beginning to end. Users start the engagement by accessing the Dapp via a web browser. To ensure wallet connectivity, the frontend first verifies MetaMask availability. After detection, users choose an account for blockchain transactions and connect their wallet. After that, the Dapp retrieves and shows pertinent blockchain data. Transactions are started by users using the user interface, which causes MetaMask to ask for confirmation. The transaction is broadcast to the network for execution after approval. Once finished, the frontend instantaneously reflects the transaction outcome by updating with the most recent blockchain state.

Methods	Tool	Purpose
Smart Contract	Truffle	Compile, test, and deploy contracts.
Local Testing	Ganache	Simulate Ethereum blockchain (no gas fees).
Wallet Integration	MetaMask	Securely manage keys and sign transactions.
Frontend	React.js	Build interactive UI.
Blockchain Interaction	web3.js	Connect frontend to Ethereum.
Storing	Pinata	IPFS tool to store records

Secure Blockchain Integration for Electronic Health Records

Blockchain Integration

EHRs can be stored in a decentralized manner thanks to blockchain technology, particularly Ethereum. In order to maintain integrity, immutability, and traceability, smart contracts oversee user registration, EHR construction, access restriction, and data sharing. In healthcare applications, this technology improves authenticity and secrecy.

Attribute-Based Encryption (ABE)

Instead of using particular keys, attribute-based encryption (ABE) safeguards data access based on user qualities. By enabling encryption policies linked to attributes, Ciphertext-Policy Attribute-Based Encryption (CP-ABE) provides fine-grained control over patient record access.

CP-ABE in Blockchain

- Encryption: Data is encrypted using attribute-defined policies (e.g., "only doctors").
- Decryption: Authorized users with matching attributes can
- Advantages: Fine-grained access control enhances security; only authorized parties can retrieve sensitive patient data.

CP-ABE Encryption & Decryption

Before storing patient data on the blockchain, it is encrypted using CP-ABE. Authorized users with private keys matching the encryption policy can decrypt the information, ensuring confidentiality and secure data sharing within healthcare systems.

Registration Process

Doctor Registration: Doctor must register by entering their name, email address, specialization, and password. They can check patient records and consult with doctors after successfully registering, among other healthcare-specific features.

Patient Registration: In order to register, patients must provide their name, email address, age, gender, and password. Interaction with medical specialists and tailored healthcare management are made possible by this method.

Diagnostician Registration: By providing information such their name, email address, area of expertise, and password, diagnosticians can register. They can access patient evaluations, test result submissions, and diagnostic reports after successfully registering.

Authentication Mechanism

Login credentials: Doctors, patients, and diagnosticians safely enter their password and registered email address.

Session Management: To preserve user access, the system creates a session after authentication. Unauthorized access is avoided and a seamless interaction experience is guaranteed with secure session management.

EHR Management Using Blockchain

Blockchain technology and encryption are used to securely manage Electronic Health Records (EHRs) in order to protect the privacy and integrity of data. With patient consent, doctors can create, edit, and view EHRs, preventing unwanted access.

Creation of EHR

- In order to record medical illnesses, symptoms, and treatments, doctors create new EHR entries. And in the same way patient can also create new EHR by uploading of past records.
- Every entry is protected by CP-ABE encryption, which guarantees that patient data may only be decrypted and accessed by authorized individuals who possess particular characteristics.

Storing EHRs on Blockchain

- EHRs are safely stored on a blockchain. The blockchain's structure is made up of blocks that hold encrypted EHR data, guaranteeing unchangeable and tamper-proof records.

- The encrypted data is appended to a new blockchain block when a physician produces an EHR entry. The blockchain's integrity is preserved because this block is connected to the one before it.

Viewing EHRs

- Encrypted EHRs are safely accessible to patients. They can view their medical records while guaranteeing the privacy of the information.
- Relevant EHR data can be decrypted and accessed by authorized healthcare providers for therapeutic purposes. Only users with the required credentials can decrypt the data thanks to CP-ABE's control over this access.

Activity SummaryKey Features

Prescription Writing

Treatment plans that are directly connected to patient EHRs can be added and updated by doctors. This guarantees that all prescription drugs and medical treatments are kept safe and within easy reach. To keep a precise and current record of the patient's medical history, any modifications or additions to the treatment plans are added as new blocks to the blockchain.

The Activity Summary module provides an overview of a patient's healthcare activities in the blockchain-based EHR system. It displays key statistics and visualizations for prescriptions, uploaded EHR records, and diagnostic reports, making it easy for users (patients and healthcare providers) to understand activity patterns. Purpose: Summarizes patient-related data from blockchain contracts (Prescription, UploadEHR, Diagnostic Upload) for quick insights.

- **Statistics:** Shows total counts, mean and standard deviation of time between records, most frequent diagnostic report type, and activity scores for each category.
- **Visualizations:** Includes a bar chart for record counts, a line chart for activity scores, and a doughnut chart for diagnostic report distribution.
- **Data Retrieval:** Fetches records using Web3 and patient's HH number or wallet address from Ethereum blockchain contracts.

Results

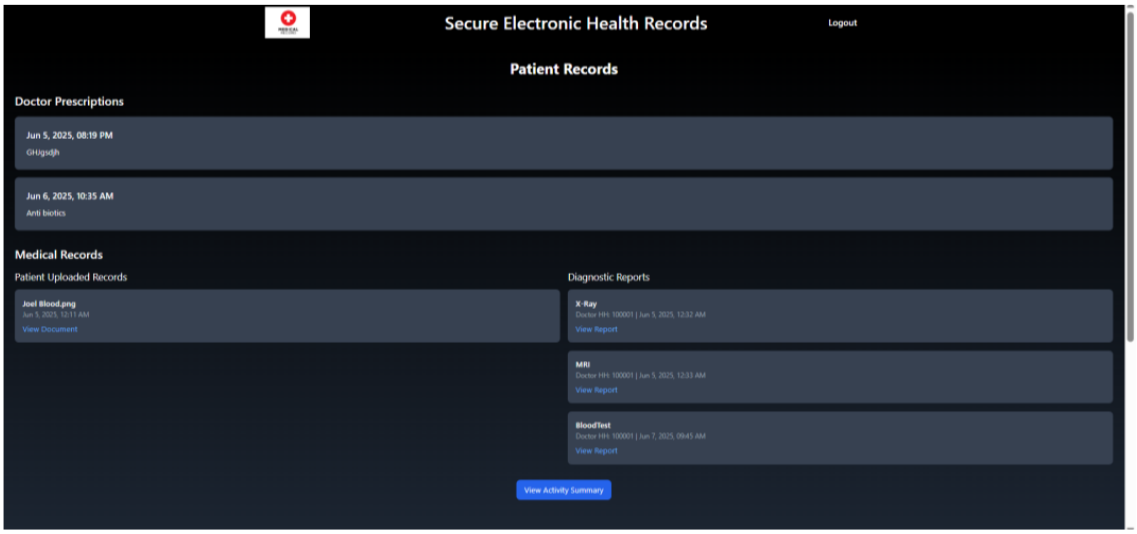

Fig.3 View Records: The View Records feature allows patients and doctors to securely access previously uploaded medical records via IPFS. It ensures quick, authorized retrieval of data using cryptographic hashes and access controls.

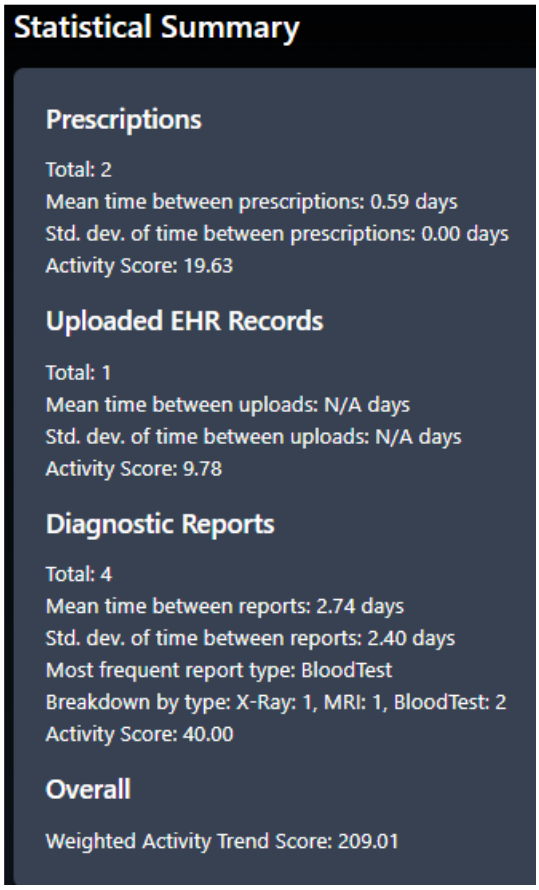

Fig.4 Statistical Summary: Provides patients overview of their health reports. It helps users easily track and understand key medical data over time.

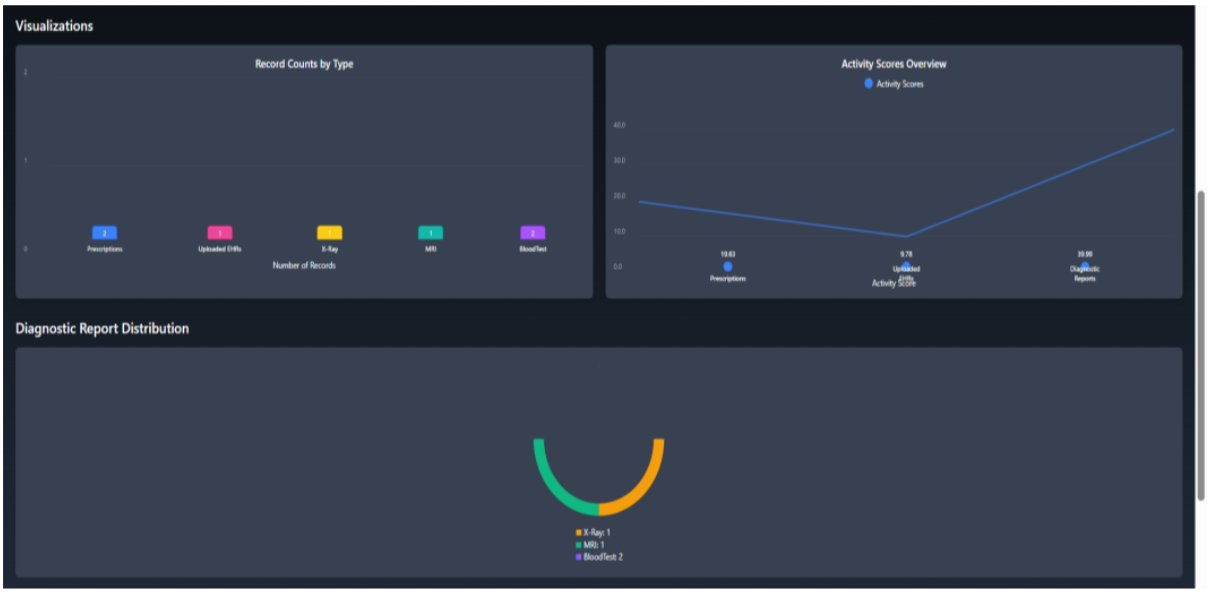

Fig.5 Visualization: Provides patients with a visual overview of their health trends using bar charts, line charts, and doughnut charts.

Conclusion And Future Scope

Conclusion

The proposed blockchain-based EHR system ensures secure, efficient, and patient-centric health data management. By leveraging smart contracts and off-chain storage, it empowers patients with full control over their records while maintaining data integrity and privacy. The use of decentralized technologies eliminates unauthorized access, enhances data sharing between stakeholders, and supports interoperability across platforms. This scalable solution addresses key shortcomings of traditional systems, making healthcare records more transparent, trustworthy, and adaptable to future advancements in digital healthcare infrastructure [1-10].

Future Scope

The system's future scope includes integration with IoMT devices to enable real-time updates of patient data from wearable and monitoring technologies. It also envisions AI-powered medical insights for predictive analytics and personalized treatment recommendations, enhancing clinical decision-making. Additionally, expanding cross-hospital data sharing aims to improve interoperability, allowing seamless access to patient records across various healthcare institutions and improving continuity of care.

References

1. D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems," IEEE Access, vol. 7, pp. 66792–66806, 2019.
2. M. Zarour et al., "Evaluating the impact of blockchain models for secure and trustworthy electronic healthcare records," IEEE Access, vol. 8, pp. 157959–157973, 2020.
3. L. Ismail, H. Materwala, and S. Zeadally, "Lightweight Blockchain for Healthcare," IEEE Access, vol. 7, pp. 149935–149951, 2019.
4. L. Tan, K. Yu, N. Shi, C. Yang, W. Wei, and H. Lu, "Towards Secure and Privacy-Preserving Data Sharing for COVID-19 Medical Records: A Blockchain-Empowered Approach," IEEE Trans Netw Sci Eng, vol. 9, no. 1, pp. 271–281, 2022.
5. X. Liu, Z. Wang, C. Jin, F. Li, and G. Li, "A Blockchain-Based Medical Data Sharing and Protection Scheme," IEEE Access, vol. 7, pp. 118943–118953, 2019.
6. Shahnaz, U. Qamar, and A. Khalid, "Using Blockchain for Electronic Health Records," IEEE Access, vol. 7, pp. 147782–147795, 2019.
7. R. Akkaoui, X. Hei, and W. Cheng, "EdgeMediChain: A Hybrid Edge Blockchain-Based Framework for Health Data Exchange," IEEE Access, vol. 8, pp. 113467–113486, 2020.
8. Z. Bao, D. He, H. Wang, M. Luo, and C. Peng, "A Group Signature Scheme With Selective Linkability and Traceability for Blockchain-Based Data Sharing Systems in E-Health Services," IEEE Internet Things J, vol. 10, no. 23, pp. 21115–21128, Dec. 2023.
9. F. Li, K. Liu, L. Zhang, S. Huang, and Q. Wu, "EHRChain: A Blockchain-Based EHR System Using Attribute-Based and Homomorphic Cryptosystem," IEEE Trans Serv Comput, vol. 15, no. 5, pp. 2755–2765, 2022.
10. X. Lu and X. Cheng, "A Secure and Lightweight Data Sharing Scheme for Internet of Medical Things," IEEE Access, vol. 8,