Blockchain-Based Electronic Health Record System

Tambong, Justine Rhey M.[1], Somontina, Rovic James[2], Balon, Enrico JR.[3], Agustin, Vivien A.[4], Fernandez, Ronald B.[5]

[1,2,3]Bachelor of Science in Information Technology, Jesus Reigns Christian College, Malate, Manila Philippines

[4,5]La Consolacion University Philippines

DOI: https://doi.org/10.51244/IJRSI.2026.1305000262

Received: 20 May 2026; Accepted: 25 May 2026; Published: 12 June 2026

ABSTRACT

This study presents the design and development of a Blockchain-Based Electronic Health Record (EHR) System aimed at addressing the limitations of traditional paper-based and centralized digital record systems used in small clinics. Conventional health record management faces critical challenges including data vulnerability, unauthorized access, lack of interoperability, and inefficient record retrieval. The proposed system integrates blockchain technology with a secure web-based platform to ensure data immutability, encrypted storage, and patient-controlled access permissions. Developed using Agile methodology and the Iterative Design and Development (IDD) model, the system features a multi-layered architecture combining PostgreSQL for encrypted data storage, Solidity-based smart contracts on the Stellar Soroban blockchain for automated access control and audit trail logging, and a secure web-based platform for patient and provider interaction. Built in partnership with Herbosa Metro Doctors, the prototype was tested using simulated patient data in compliance with the Data Privacy Act of 2012 (Republic Act No. 10173). Results demonstrate that blockchain integration provides a secure, transparent, and tamper-proof approach to managing patient health information, offering a viable solution for small healthcare institutions seeking to transition from manual record-keeping to a modern, secure digital system.

INTRODUCTION

Background of the Study

In the age of digital transformation, data has become one of the most powerful resources in every field, especially in healthcare, where information accuracy and security are vital to saving lives. Electronic Health Records (EHRs) have replaced traditional paper-based systems to promote efficiency, speed, and accessibility of patient data among hospitals and healthcare professionals. However, as more hospitals migrate to digital systems, data protection has become increasingly challenging. According to Ullah [3], centralized databases used in conventional EHR systems remain highly susceptible to data breaches and corruption due to their dependence on a single controlling server. Such vulnerabilities not only compromise patient confidentiality but also undermine trust between patients and healthcare providers. The challenge now extends beyond digitalization; it revolves around ensuring that every record stored online remains accurate, private, and tamper-proof, regardless of where it is accessed.

Despite the benefits of EHRs, their limitations continue to threaten the reliability of digital healthcare management. Many hospitals still rely on centralized databases that are vulnerable to hacking, unauthorized modification, or system crashes, leading to irreversible data loss. Agbeyangi, Oki, and Mgidi [4] noted that weak access control and insufficient transparency in traditional EHRs prevent patients from tracking who accesses their data, increasing the risk of medical identity theft. This issue is evident at the study's partner clinic, Herbosa Metro Doctors in Tondo, where existing health record management practices still rely on general paper templates and face significant challenges in ensuring data privacy and controlled access in compliance with the Data Privacy Act.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

Furthermore, Saraswat [5] discussed that the lack of interoperability between different hospital systems hinders the seamless exchange of patient information, causing medical errors, delays, and duplicate testing. These weaknesses do not only affect clinical operations but also damage patient confidence in digital healthcare. When records are altered or lost, both the patient and the healthcare provider bear the consequences financially, medically, and ethically. There is a clear gap in ensuring that medical records can be safely accessed and verified without relying on a single, vulnerable point of control.

Statement of the Problem

The increasing demand for efficient and secure health record management has highlighted the limitations of paper-based systems still used by many small clinics. Manual recording often leads to challenges in data organization, retrieval, accuracy, and privacy, especially as patient volumes continue to grow. This study addresses the lack of a secure and organized system for managing patient health records by proposing the development of a blockchain-based Electronic Health Record (EHR) prototype.

Specific Problem

Specifically, this study seeks to address the following problems:

1. The clinic does not have a standardized system for recording patient information and currently depends on general paper templates available on the market. This makes it harder to maintain consistent, organized, and retrievable patient records as the number of patients grows over time.

2. The clinic lacks an integrated system for efficiently accessing and sharing patient records among healthcare personnel, resulting in delays and difficulty in coordinating patient information when needed.

3. Paper-based records do not have a way to track or limit who can view a patient's file, making it difficult to ensure that personal health information remains private and only accessible to authorized personnel.

Objectives of the Study

The main objective of this study is to design and develop a blockchain-based Electronic Health Record (EHR) system that enhances the security, accessibility, and management of patient health information. The system aims to integrate blockchain technology with digital health record management to enable secure storage, efficient sharing, and controlled access to patient data among authorized healthcare personnel. By ensuring data integrity, privacy, and transparency, the proposed system seeks to improve the overall efficiency of healthcare record handling and support reliable clinical decision-making.

Specific Objectives

Specifically, the study seeks to

1. To develop a blockchain-based Electronic Health Record (EHR) system that ensures secure and reliable storage of patient health information by utilizing blockchain features such as data immutability, encryption, and decentralized record management.

2. To enhance the accessibility and efficient sharing of patient records among authorized healthcare personnel through a digital platform that supports timely retrieval, seamless data exchange, and improved coordination in healthcare services.

3. To provide a secure access control mechanism that protects patient data and ensures that only authorized users can view or modify patient records, incorporating features such as authentication, permission control, and activity tracking to maintain privacy and accountability.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

Scope and Limitations

This study focuses on the design and development of a Blockchain-Based Electronic Health Record (EHR) prototype system intended to provide a more organized, secure, and reliable way of managing patient records in a clinic setting. The system uses blockchain technology to ensure that patient information is stored in a way that cannot be altered or accessed without proper authorization. Core features include blockchain-based data storage, secure record sharing among authorized clinic staff, a patient health history tracker, and a dashboard for viewing and managing patient information. The study is conducted within a controlled environment using simulated patient data, as direct access to actual clinic records is restricted under Republic Act No. 10173, or the Data Privacy Act of 2012. The proposed system is developed as a working prototype in partnership with Herbosa Metro Doctors, which currently manages patient information through general paper templates available on the market, with no standardized recording system in place.

The study is limited to the software-based design and functionality testing of the system and does not cover actual deployment within the clinic's operations. The prototype will not be integrated with any external healthcare platforms, government health databases, or third-party systems. The artificial intelligence component, if included, will only perform basic record classification and will not carry out any form of medical diagnosis or health prediction. System performance may also vary depending on network conditions and hardware availability during testing. Future developments may explore actual clinic deployment, broader system integration, and enhanced features once the necessary technical and legal requirements are met.

Significance of the Study

This study is important as it aims to address the limitations of traditional health record systems by introducing a Blockchain-Based Electronic Health Record (EHR) System that ensures secure, transparent, and tamper-proof medical data management. By utilizing blockchain technology, the study seeks to enhance the reliability, accessibility, and privacy of patient information while minimizing risks of unauthorized access and data loss. This innovation not only improves record-keeping efficiency but also builds greater trust between healthcare providers and patients through verifiable and decentralized data handling. The relevance of this study can be observed through the advantages it brings to various groups:

Healthcare Institutions. Hospitals and clinics gain a secure and unified platform for storing and managing medical records. The blockchain integration ensures data integrity and reduces administrative delays caused by fragmented or lost patient information.

Medical Professionals. Doctors, nurses, and staff can easily access accurate, up-to-date records that support faster diagnosis and better treatment planning. The system minimizes duplication and human error while improving workflow efficiency.

Patients. Individuals benefit from improved protection and transparency of their medical information, ensuring that only authorized medical personnel can view or update their records. This fosters patient trust and promotes responsible data management.

Researchers and Developers. The study provides a foundation for future innovations in digital health and secure data systems. It encourages the development of more advanced,

blockchain-based healthcare solutions that combine technology, security, and efficiency.

REVIEW OF RELATED LITERATURE AND STUDIES

This literature presents insights on blockchain technology in healthcare systems, with a particular focus on electronic health records (EHR), data security, interoperability, and decentralized system architectures. It explores how blockchain can address long-standing challenges in healthcare information management, including data fragmentation, lack of transparency, inefficient record sharing, and privacy concerns. Furthermore, it highlights both international and Philippine-based studies that demonstrate the relevance of blockchain

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

technology in improving healthcare delivery, strengthening data protection, and enabling more efficient and reliable health information systems.

In a related study, Nakamoto (2008) introduced blockchain as a decentralized peer-to-peer electronic system designed to eliminate the need for trusted third parties by distributing data across a network of nodes. The study explained that blockchain operates using cryptographic hashing, where each block contains a timestamp and a reference to the previous block, forming a continuous and immutable chain of records. This structure ensures that once data is recorded, it cannot be altered without affecting all subsequent blocks, thereby making the system highly resistant to tampering. Although initially developed for financial transactions, Nakamoto emphasized that the core principles of decentralization, transparency, and immutability can be applied to other sectors such as healthcare, where maintaining accurate, secure, and trustworthy patient records is critically important for clinical decision-making and long-term patient care.

Similarly, Zheng et al. (2017) conducted a comprehensive analysis of blockchain architecture and its underlying consensus mechanisms, explaining how distributed ledger technology maintains consistency across multiple nodes without relying on centralized authority. The study examined various consensus algorithms, including Proof of Work, Proof of Stake, and Byzantine Fault Tolerance, each offering different trade-offs in terms of computational efficiency, scalability, and level of security. The researchers emphasized that selecting an appropriate consensus mechanism is essential when applying blockchain in healthcare environments, as electronic health record systems require both high data integrity and fast processing speeds. Their findings demonstrated that blockchain-based systems can provide secure, synchronized, and tamper-resistant data storage while still supporting real-time access to patient information, which is crucial in clinical settings where timely decision-making can directly affect patient outcomes.

In the same way, Ullah (2025) examined the vulnerabilities associated with centralized healthcare database systems, highlighting their susceptibility to cyberattacks, ransomware incidents, and large-scale data breaches. The study revealed that millions of patient records have been compromised globally, resulting in significant financial losses and serious risks to patient privacy and safety. Ullah argued that traditional security approaches, such as firewalls and basic access control mechanisms, are no longer sufficient to defend against increasingly sophisticated cyber threats. Instead, the research emphasized the need for a fundamental shift toward decentralized architectures, such as blockchain, which distribute data across multiple nodes and eliminate single points of failure. This approach significantly enhances system resilience, reduces the likelihood of large-scale breaches, and ensures that sensitive medical information remains protected against unauthorized access and manipulation.

Correspondingly, Agbeyangi, Oki, and Mgidi (2024) investigated access control mechanisms in conventional electronic health record systems, revealing significant limitations in how these systems manage and monitor data access. Their study found that many existing EHR platforms lack transparency regarding who accesses patient information, when the access occurs, and for what purpose. Weak authentication protocols and insufficient audit trails were identified as major contributors to unauthorized access and data misuse. The researchers proposed the implementation of blockchain-based permission systems, where every data access request is recorded on an immutable ledger. This ensures that all activities are traceable and verifiable, thereby improving accountability and enabling both patients and healthcare providers to monitor how sensitive information is used. Such systems also support compliance with data protection regulations by providing a clear and auditable record of all interactions with patient data.

In another study, Saraswat (2023) analyzed the persistent interoperability challenges faced by modern healthcare systems, particularly those arising from fragmented databases, incompatible data formats, and proprietary software systems. The research highlighted that these issues prevent seamless information exchange between healthcare institutions, often resulting in duplicated medical tests, delays in diagnosis, and increased healthcare costs. Saraswat emphasized that a lack of standardized data exchange protocols continues to hinder the efficient flow of information across different providers. The study proposed that blockchain technology can address these challenges by offering a unified and standardized platform for storing and sharing patient data. By maintaining a consistent and synchronized ledger across all participating entities, blockchain can enable seamless interoperability while ensuring that data remains accurate, secure, and accessible to authorized users.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

Likewise, Kuo, Kim, and Ohno-Machado (2017) explored blockchain-based solutions for improving healthcare interoperability, proposing distributed frameworks that enable secure and efficient data sharing across multiple institutions. Their research demonstrated that blockchain systems can maintain separate institutional databases while providing a unified access layer through the use of cryptographic keys and smart contracts. This approach allows authorized users to access relevant patient information without requiring centralized intermediaries, thereby preserving institutional autonomy while improving coordination and collaboration. The study concluded that blockchain technology has the potential to significantly enhance the efficiency of health information exchange, reduce administrative burdens, and improve the overall quality of patient care.

Additionally, Szabo (1997) introduced the concept of smart contracts as self-executing digital agreements that automatically enforce predefined conditions between parties. Although originally conceptualized prior to the development of blockchain, smart contracts became fully functional with the emergence of distributed ledger technology. In healthcare applications, smart contracts enable automated permission management, allowing patients to grant, modify, or revoke access to their medical records based on specific conditions. For example, a patient may grant temporary access to a healthcare provider for a specific period, after which the system automatically revokes access. This capability enhances patient autonomy, ensures secure data sharing, and eliminates the need for manual intervention in managing permissions.

Similarly, Christidis and Devetsikiotis (2016) examined the implementation of smart contracts within blockchain systems, highlighting their ability to automate complex workflows and reduce reliance on manual processes. Their study demonstrated that smart contracts can improve system efficiency by minimizing human error, reducing processing delays, and ensuring consistent enforcement of rules. In healthcare environments, this translates to more reliable management of patient data, where access permissions, data validation, and transaction processing are handled automatically through secure and transparent code. The researchers emphasized that this level of automation is particularly beneficial in large-scale healthcare systems, where manual processes can be time-consuming and prone to inconsistencies.

Furthermore, Guo, Li, Nejad, and Shen (2023) investigated the integration of edge computing with blockchain technology in healthcare systems, demonstrating that processing data closer to its source can significantly reduce latency and improve system performance. Their study showed that edge computing allows data to be processed locally before being transmitted to the blockchain, thereby reducing the time required for data validation and storage. This approach is particularly valuable in time-sensitive medical scenarios, such as emergency care and remote patient monitoring, where delays in accessing critical information can have serious consequences. By combining edge computing with blockchain, healthcare systems can achieve both high performance and strong data security.

Supporting this, Shi et al. (2016) analyzed edge computing frameworks within the Internet of Things (IoT), explaining how decentralized data processing can enhance system efficiency and reduce dependence on centralized cloud infrastructure. The study demonstrated that edge nodes can perform preliminary tasks such as data validation, encryption, and filtering before sending information to the blockchain network. This not only improves system performance but also ensures that only relevant and verified data is stored on the blockchain. In healthcare settings, where numerous connected devices generate large volumes of data, this approach helps maintain efficiency while ensuring data integrity and security.

Moreover, Haber and Stornetta (1991) introduced cryptographic timestamping techniques that form the foundation of blockchain's immutability. Their research demonstrated how linking data records through cryptographic hashes creates a secure and tamper-evident chain, where any attempt to alter historical data can be easily detected. This principle is essential in healthcare applications, as it ensures that patient records remain accurate and unaltered throughout their lifecycle. Maintaining data integrity is critical for ensuring patient safety, supporting clinical decision-making, and preventing medical errors.

Merkle (1988) further advanced this field by developing the Merkle tree data structure, which enables efficient verification of large datasets through hierarchical hashing. This technique allows blockchain systems to confirm the existence and integrity of specific records without revealing the entire dataset, thereby enhancing both security and privacy. In electronic health record systems, Merkle trees enable healthcare providers to verify the

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

authenticity of patient data quickly and securely, while ensuring that sensitive information remains protected from unauthorized access.

In the Philippine context, De Guzman and Santos (2020) examined the current state of healthcare digitalization, revealing that a significant number of healthcare institutions still rely on paper-based or hybrid record-keeping systems. Their study identified key challenges such as limited technological infrastructure, budget constraints, and lack of technical expertise as major barriers to full digital adoption. The researchers emphasized that transitioning to secure and scalable digital systems, such as blockchain-based EHRs, could significantly improve data management, reduce inefficiencies, and enhance the overall quality of healthcare services in the country.

Similarly, Reyes (2023) analyzed the fragmented nature of health information systems in the Philippines, noting that the lack of standardization prevents effective data sharing between healthcare providers. The study found that even in digitized facilities, incompatible data formats often require manual transcription when patients move between institutions, leading to inefficiencies and potential data errors. Reyes suggested that blockchain technology could provide a unified platform that enables seamless and standardized data exchange, improving coordination and reducing administrative burdens.

Castillo and Domingo (2024) investigated compliance challenges related to the Philippine Data Privacy Act, revealing that many healthcare institutions struggle to implement adequate data protection measures. Their findings showed that insufficient access controls and weak encryption mechanisms are common causes of data breaches. The researchers recommended adopting blockchain-based systems that integrate security features directly into the system architecture, ensuring that data protection is built into the design rather than relying solely on external safeguards.

In line with this, Pascual (2023) emphasized the importance of patient rights in controlling access to their medical information, noting that existing systems often lack the technical capability to enforce these rights effectively. The study highlighted that blockchain-based systems provide transparent and auditable mechanisms for managing data access, allowing patients to monitor and control how their information is used. This approach aligns with legal requirements and promotes greater trust in digital healthcare systems.

Aquino and Cruz (2024) examined the rapid expansion of telemedicine services in the Philippines, particularly following the COVID-19 pandemic. Their research identified secure access to patient records as a major challenge in remote healthcare delivery, as many systems are unable to retrieve complete patient histories from different institutions. The study suggested that blockchain-based EHR systems could address this issue by providing authorized healthcare providers with secure and unified access to patient data, improving diagnostic accuracy and treatment outcomes.

Mendoza (2023) further explored telemedicine adoption in rural areas, highlighting concerns about data security and trust among patients. The study found that many individuals are hesitant to use digital healthcare services due to fears of data misuse and unauthorized access. Blockchain technology was proposed as a solution to enhance transparency and build trust, as it allows patients to verify how their data is accessed and ensures that all interactions are securely recorded.

Dela Cruz, Garcia, and Hernandez (2024) conducted a study on blockchain awareness among healthcare administrators in the Philippines, revealing that while knowledge of the technology remains limited, there is strong interest in its potential applications. The researchers emphasized the need for targeted educational initiatives and training programs to build technical capacity and support the adoption of blockchain-based systems in healthcare institutions.

Ramos and Villegas (2023) explored blockchain implementations in other government sectors, such as land registration and education, highlighting successful pilot projects that demonstrate the technology’s potential. Their study suggested that lessons learned from these implementations can inform the development of blockchain-based healthcare systems, particularly in terms of infrastructure requirements, regulatory frameworks, and implementation strategies.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

Santos, Lopez, and Bautista (2024) investigated mobile health application usage across different demographic groups in the Philippines, finding widespread adoption but limited understanding of data security practices. The study recommended the development of user-friendly systems that incorporate educational features to help users understand how their data is protected, thereby improving trust and encouraging adoption of digital health technologies.

Lastly, Torres (2023) examined digital literacy in medical education, noting that current curricula provide limited exposure to emerging technologies such as blockchain. The study emphasized the importance of integrating these concepts into healthcare training programs to prepare future professionals for working with advanced health information systems. Without adequate training, the adoption of innovative technologies like blockchain may face resistance from healthcare workers who are unfamiliar with these systems.

METHODOLOGY

Research Design

This study employs a developmental research methodology to design, develop, and evaluate a Blockchain-Based Electronic Health Record (EHR) System in response to several critical challenges. First, data security concerns arise from the increasing vulnerability of centralized health records to breaches and unauthorized access. Second, data integrity issues emerge due to the risk of unauthorized modification or tampering of patient records. Third, accessibility limitations are evident in small clinics that rely on inefficient manual record-keeping systems, which hinder timely data retrieval. Finally, privacy challenges persist because patients often lack control over access to their records and the availability of transparent audit trails.

The system integrates blockchain technology for decentralized and immutable data storage, smart contracts for automated access control, and a secure authentication mechanism for verifying users. A digital interface enables healthcare professionals to access and manage patient records efficiently while ensuring that all transactions are recorded transparently and securely.

The study employs simulated and publicly available healthcare record structures, incorporating standardized electronic health data formats inspired by interoperability frameworks such as FHIR and HL7, to evaluate system functionality and performance. The datasets utilized encompass several categories: patient profiles containing demographic information for approximately 100 synthetic individuals, including name, age, gender, address, and contact details; medical history entries documenting diagnoses, treatment plans, surgical procedures, and clinical notes; medication records specifying prescribed drugs, dosages, and administration schedules; allergy information detailing drug sensitivities and adverse reactions; laboratory results comprising diagnostic test findings and imaging reports; access permission logs recording data access events and authorization grants; and audit trails providing timestamps and actor identification for all blockchain transactions.

These datasets are evaluated to ensure compatibility with real-world healthcare scenarios, particularly in terms of patient record structure, access permissions, and data security requirements. Through iterative testing, the system is refined to ensure that blockchain transactions remain efficient, secure, and scalable under different usage conditions typical in healthcare environments.

The Software Development Life Cycle (SDLC) for this study uses Agile Methodology, which is well-suited for the development of complex systems that require continuous refinement and evaluation. Agile emphasizes flexibility, collaboration, and iterative improvement, making it appropriate for integrating blockchain components such as smart contracts, decentralized databases, and secure authentication systems.

Its iterative stages, including requirement analysis, sprint planning, incremental development, testing, and feedback integration, allow continuous enhancement of system security, performance, and usability. For example, smart contract logic, user authentication protocols, and data retrieval processes are refined after each development cycle to ensure system reliability and efficiency.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

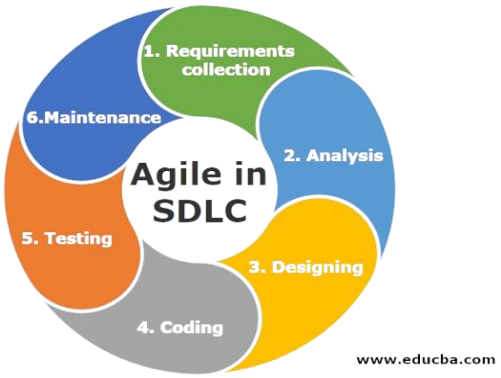


Figure 3.1 Agile Methodology

By integrating Agile principles with developmental research methodology, this study ensures a structured yet adaptive development process. The resulting system architecture prioritizes data security, interoperability, and efficient access control while maintaining scalability for potential future expansion in healthcare environments.

This study also adopts the Iterative Design and Development (IDD) model, which emphasizes continuous refinement through repeated cycles of development and evaluation. This approach ensures that system improvements are based on actual testing results and identified limitations during each iteration, allowing gradual enhancement of both system performance and security features.

The phases of the IDD model used in this study are as follows:

Requirements Collection. In this initial phase, we identify the functional and technical requirements of the system by conducting an extensive literature review and analyzing existing Electronic Health Record (EHR) systems. We evaluate various blockchain applications in healthcare to determine the necessary features for our prototype, specifically focusing on secure data storage, robust user authentication, and the mechanisms required for cross-platform interoperability.

Analysis. After gathering the requirements, we examine them to assess the overall feasibility of the system and define our final technical specifications. During this phase, we identify potential risks and evaluate the most effective blockchain network structure. We carefully analyze smart contract design requirements and data storage models, while prioritizing security considerations such as advanced encryption standards and strict access control policies.

Design. Moving into the structural phase, we develop the architectural framework of the system, which includes configuring the blockchain network and the supporting database structure. We design the user interface and map out the smart contract workflows that govern the system logic. Our focus here is defining exactly how patient records will be stored, accessed, and shared to ensure a seamless and secure experience within the decentralized environment.

Coding and Implementation. In this active phase, we implement the smart contracts that automate access control and we construct the decentralized ledger system. We also integrate the cryptographic authentication mechanisms and develop the web-based interface, ensuring that the backend blockchain logic connects seamlessly with the frontend used by healthcare providers. This is the stage where we translate our theoretical models into a functional software prototype, allowing us to identify and resolve technical challenges as they arise during development.

Testing. Evaluating the system's functionality, security, and performance through unit testing, integration testing, and simulation of healthcare scenarios. This phase ensures that data transactions are secure, access control mechanisms function correctly, and blockchain records remain immutable and consistent.

Deployment and Feedback. Implementing the prototype in a controlled environment and gathering feedback from simulated healthcare users. Performance results and user feedback are analyzed to identify areas for improvement, which are then incorporated into the next iteration of development.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

Each phase is repeated multiple times throughout the study to ensure continuous improvement of the system. This cyclical development process ensures that the Blockchain-Based Electronic Health Record System is secure, efficient, and adaptable to real-world healthcare requirements.

Through developmental research supported by the IDD framework and Agile methodology, this study aims to produce a secure, scalable, and interoperable Electronic Health Record system that enhances data integrity, improves accessibility, and strengthens patient data privacy. The resulting system directly supports the study's objectives of secure data storage, efficient record sharing, and robust access control for healthcare environments.

This study employs a dual-framework approach that combines the Iterative Design and Development (IDD) model with Agile methodology. These two frameworks serve distinct but complementary roles: IDD structures the macro-level research progression across clearly defined developmental phases, while Agile governs the micro-level execution within each phase through time-boxed sprints. The integration is justified on three grounds.

First, developmental research requires a structured phase sequence from requirements collection and analysis through design, implementation, testing, and deployment to satisfy academic documentation standards and ensure systematic progression toward a functional prototype. The IDD model provides this structure, ensuring that each phase produces documented, evaluable outputs aligned with the study's objectives.

Second, the technical complexity of integrating blockchain smart contracts, decentralized IPFS storage, cryptographic authentication, and a web-based dashboard made a purely linear development approach impractical. Agile's iterative sprint cycles allowed the team to identify and resolve integration issues incrementally for example, refining smart contract access logic after testing revealed permission edge cases without having to restart entire IDD phases.

Third, the bounded academic timeline of a capstone project required a method that allowed parallel progress across design and implementation tasks. Agile sprint planning enabled concurrent work on the frontend interface and backend smart contract logic within the same IDD phase, reducing idle time and improving overall development velocity.

The final system brings together several pieces: a permissioned blockchain layer with Solidity smart contracts for tamper-proof audit trails, smart contracts that automate access management, a Node.js/Express backend to handle application logic, a PostgreSQL database that stores encrypted synthetic patient data off-chain, and a React/Tailwind web interface where patients and clinicians interact.

However, it does not include live deployment in a real clinic, integration with outside healthcare platforms, or formal security auditing. Even with these limits, the iterative prototyping and controlled testing allow us to show that a decentralized, patient centered approach to managing health data is feasible within the scope of a capstone project.

Sprint-to-Phase Mapping

The development was carried out across six two-week sprints, each aligned with a specific IDD phase as shown below:

Sprint	Duration	IDD Phase	Deliverables
Sprint 1	Weeks 1–2	Requirements Collection	Finalized functional requirements, synthetic dataset schema, stakeholder interview notes with Herbosa Metro Doctors
Sprint 2	Weeks 3–4	Analysis	Feasibility assessment, risk register, blockchain network selection (Stellar Soroban), smart contract logic outline

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

Sprint 3	Weeks 5–6	Design	System architecture diagram, database schema (PostgreSQL), UI wireframes, smart contract workflow diagrams
Sprint 4	Weeks 7–8	Coding & Implementation (Phase 1)	Backend API (Node.js/Express), PostgreSQL integration, AES-256/SHA-256 encryption modules
Sprint 5	Weeks 9–10	Coding & Implementation (Phase 2)	Solidity smart contracts (Record Registry, Access Manager, Audit Trail) deployed to Stellar testnet; React/Tailwind frontend
Sprint 6	Weeks 11–12	Testing & Deployment	171 automated test cases executed (authentication, RBAC, tamper detection, patient management); prototype deployment in controlled environment; feedback integration

Each sprint concluded with a review session in which test results and identified deficiencies were used to refine the subsequent sprint's scope consistent with both Agile retrospective practices and IDD's principle of iterative improvement based on evaluation outcomes. For example, authentication rate-limiting logic (HTTP 429 enforcement) was identified as a gap during Sprint 4's review and implemented in Sprint 5. Similarly, the tamper-detection verification procedure using SHA-256 hash comparison was refined in Sprint 6 after initial hash storage inconsistencies were detected in Sprint 5 testing.

This concrete alignment between sprint cycles and IDD phases ensures that the dual-framework approach is not merely theoretical but is directly reflected in the system's development timeline and deliverables.

Proposed System Architecture

The proposed Blockchain Based Electronic Health Record System uses a multi layered architecture that combines distributed ledger technology with a conventional database to achieve both security and performance. The architecture follows a hybrid approach where sensitive medical data is encrypted and stored in PostgreSQL while cryptographic hashes and transaction metadata are recorded on the blockchain. This ensures data integrity without compromising system performance.

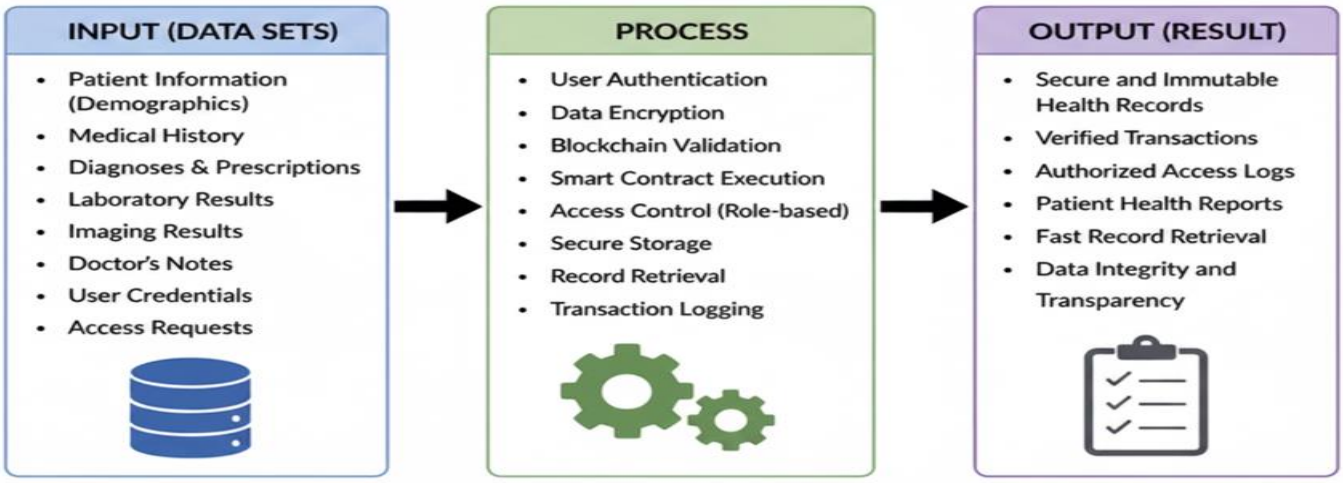


Figure 3.2 Proposed System Architecture IPO Diagram

The architecture of the Blockchain-Based Electronic Health Record (EHR) System is designed to be decentralized, modular, and capable of real-time secure data storage, cryptographic verification, and record monitoring.

The Data Acquisition and Interface Module serves as the input layer of the system. It consists of the patient and healthcare provider portals, document scanners, and digital input terminals. The system captures sensitive medical information, laboratory results, and patient identity credentials. Digital records acquired at this stage

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

include the raw patient health dataset and the authorization credential dataset. These datasets are transmitted to the Blockchain and Storage Management Module for encryption and decentralized processing.

The Decentralized Storage and Management Module functions as the process layer that handles all data communication between the front-end and the backend infrastructure. Implemented using the InterPlanetary File System (IPFS) and a supporting database, this module receives, encrypts, and distributes medical files. The process flow begins when raw files are received; they are hashed and stored across the IPFS network to ensure data redundancy. The system generates unique Content Identifiers (CIDs) which are then sent to the blockchain ledger for indexing. This module acts as a decentralized repository containing encrypted file blocks, metadata with timestamps, and retrieval hashes.

The Blockchain and Smart Contract Module operates as the specialized security process within the system. It runs within a decentralized network environment and communicates directly with the shared IPFS storage.

The Blockchain Module uses self-executing smart contracts to manage access control and record immutability in real time. The process flow begins when the module retrieves access requests from authorized providers, which are then validated against the patient's permission settings stored on the ledger. The smart contract performs a cryptographic check to ensure the integrity of the medical record. Results, including transaction hashes, block height confirmations, and access logs, are written back to the blockchain. This module operates as the "Single Source of Truth," ensuring all data remains tamper-proof and synchronized across all nodes.

The Monitoring and Verification Module serves as the primary output layer of the system, responsible for presenting complex blockchain data in a comprehensible and accessible format. It functions as the interface between the decentralized ledger and the end user, retrieving data through a Web3-enabled API and rendering it on a web-based dashboard. The dashboard is developed using React and Tailwind CSS, providing a responsive experience for users who need to verify the authenticity of records and monitor health updates over time. The results presented through this module include a real-time record update feed, access history summaries, cryptographic verification status, and historical patient data reports.

The System Administration and Security Module operates as the control and oversight component of the system, providing authorized personnel with the tools necessary to maintain network health and data privacy. Built on a secure administrative interface, it enables users to monitor node synchronization, manage user role registrations, and perform routine maintenance tasks on the smart contract protocols. By combining automated blockchain consensus with human oversight, this module ensures the system remains compliant with the Data Privacy Act and that its security outputs are accurate, allowing for administrative intervention whenever security updates or protocol adjustments are required.

Hardware Requirements

The hardware components form the physical foundation of the Blockchain-Based Electronic Health Record (EHR) System, collectively responsible for blockchain processing, data storage, system execution, and secure communication between nodes. Each component was selected based on its ability to support decentralized computation, database operations, and secure handling of sensitive patient records.

The primary computing device serves as the core development and processing unit of the system. A machine equipped with at least an Intel Core i5 or AMD Ryzen 5 processor, 16 GB of RAM, and 50 GB of available storage is required to efficiently handle blockchain node operations, backend services, and database processes. This specification ensures smooth execution of multiple services simultaneously, including smart contract deployment, API handling, and database transactions. A solid-state drive (SSD) is strongly recommended to enhance system responsiveness, particularly in terms of faster blockchain synchronization, reduced latency in database queries, and improved development performance.

For deployment purposes, a cloud-based virtual machine is utilized to host the prototype system and simulate a distributed blockchain environment. A minimum configuration of 4 CPU cores, 8 GB of RAM, and 20 GB of storage is sufficient to support the blockchain network, backend API services, and database operations during

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

testing and demonstration. This setup ensures stable execution of transactions, secure storage of patient records, and reliable system performance under controlled conditions.

End-user devices such as desktop computers, laptops, tablets, or smartphones are used to access the system through a web-based interface. These devices require no specialized hardware specifications beyond a modern web browser and stable internet connection. This ensures accessibility for healthcare professionals across different platforms while maintaining system usability and convenience in clinical environments.

The hardware configuration is directly aligned with the system's core objectives by providing the high-performance processing units and cloud servers necessary to maintain a secure, decentralized, and tamper-resistant blockchain ledger. These hardware components support the continuous operation of blockchain nodes that validate and record data changes across the network, ensuring the total immutability and integrity of all patient health records. To facilitate efficient access and sharing among authorized healthcare personnel, the system utilizes stable cloud infrastructure and high-speed network connectivity to allow seamless, simultaneous communication without compromising system performance.

Furthermore, the hardware enables the reliable execution of smart contracts which automatically regulate user authentication and enforce strict permission-based access control. This robust physical framework guarantees that sensitive patient data remains protected against unauthorized access while maintaining full synchronization across the distributed network at all times.

Software Requirements

The software components provide the intelligence and decentralized logic for the Blockchain-Based Electronic Health Record (EHR) System. These components handle data encryption, blockchain consensus, decentralized storage management, and secure user interface presentation. The selection of each software component was based on its cryptographic stability, community support, and compatibility with the distributed hardware stack.

The software stack of the Blockchain-Based EHR System is composed of carefully selected tools and frameworks that collectively support decentralized data acquisition, smart contract-driven security, and immutable monitoring. Each component was chosen for its compatibility with the system architecture and its direct contribution to the project's security objectives.

Solidity serves as the primary programming language for smart contract development, selected for its specialized capability in defining self-executing logic and permission-based rules on the blockchain. Node.js and the Express framework are used to build the backend services that facilitate communication between the patient interface, the IPFS storage module, and the blockchain ledger handling incoming medical records, managing cryptographic keys, and delivering verified results to the frontend. PostgreSQL functions as a supporting data repository for application-level metadata and user account management, while the InterPlanetary File System (IPFS) serves as the decentralized storage layer for large-scale medical documents and images. This combination is well-suited for managing both lightweight transaction hashes on-chain and large, encrypted medical files off-chain.

Remix IDE and Hardhat provide the environment for smart contract development, compilation, and testing, allowing researchers to simulate blockchain transactions, visualize gas consumption, and refine contract security through iterative cycles. Web3.js or Ethers.js is used to bridge the web interface with the blockchain network, enabling the application to sign transactions and query the ledger for patient history. AES-256 and SHA-256 libraries handle all data encryption and hashing tasks prior to transmission, ensuring that no sensitive health information is visible in plain text.

On the frontend, React.js, JavaScript, and Tailwind CSS are used to develop the secure monitoring dashboard, which retrieves verified data from the blockchain and presents it through authorized record displays, audit trail logs, and system health indicators. Git and GitHub manage version control throughout the development process. Postman is used to test and validate user authentication and transaction signing prior to system deployment.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

The software configuration is directly aligned with the system's three core objectives. To support secure and reliable storage of patient information, the IPFS integration ensures that records are stored in a decentralized environment without a single point of failure, while the database is structured to maintain metadata with strict integrity. To support efficient access and sharing among authorized personnel, the system follows a fully automated processing pipeline in which Smart Contracts query the blockchain for permission sets, validate the requester's cryptographic signature, and release the corresponding decryption keys without manual intervention. To support the objective of secure access control and auditability, the monitoring dashboard communicates with the blockchain via Web3 APIs to display real-time access logs and record updates. The administrative interface further allows authorized personnel to review node synchronization and manage decentralized identity (DID) registrations, ensuring that all health data from record creation to final verification remains traceable, immutable, and accessible only to authorized stakeholders.

Methods and Tools

This section presents the methods and tools utilized in the development of the Blockchain-Based Electronic Health Record (EHR) System. The methods and tools employed in this study are organized into two principal categories: the procedural approaches that guided the system's design, development, and evaluation, and the specific technologies and infrastructure used to implement both the decentralized ledger and the software interface components. The former encompasses the systematic steps followed by the proponents in building and validating the system, while the latter covers the blockchain protocols, smart contract languages, encryption frameworks, and hardware devices that made its technical realization possible. Together, these elements form the operational and technical foundation of the study, and each is discussed in detail in the succeeding subsections.

Methods

The development of the Blockchain-Based Electronic Health Record (EHR) System followed a structured and iterative process that emphasized decentralized security, data integrity, and seamless accessibility. The proponents began by conceptualizing the system architecture and identifying its core functionalities: the blockchain ledger for immutability, IPFS for decentralized storage, and smart contracts for automated access control. The design and coding of the decentralized prototype were then carried out, followed by the integration of cryptographic libraries, smart contract logic, and the backend infrastructure. Each stage underwent rigorous evaluation to ensure secure communication between nodes and the absolute accuracy of record-sharing permissions.

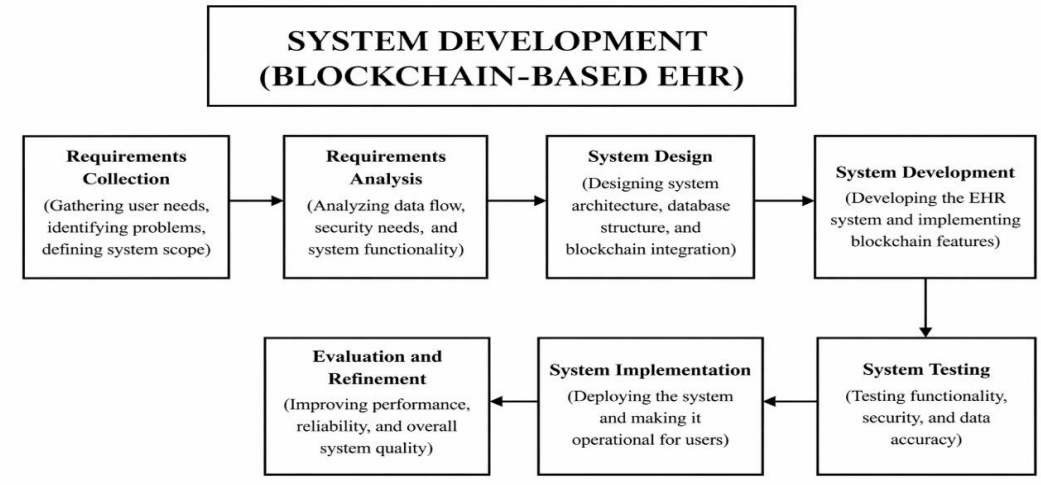


Figure 3.4.1 System Development Workflow.

The diagram illustrates the overall development process of the Blockchain-Based EHR System. It begins with decentralized system planning and cryptographic design, followed by the implementation of the blockchain network and the user-facing software. To achieve the first objective of providing secure and reliable storage for

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

patient health information, the proponents established a peer-to-peer network where each node maintains a synchronized copy of the ledger. By integrating the InterPlanetary File System (IPFS), the system ensures that large medical datasets are not stored on a single central server but are instead distributed across a decentralized network, effectively eliminating single points of failure and protecting the data from unauthorized tampering or hardware loss.

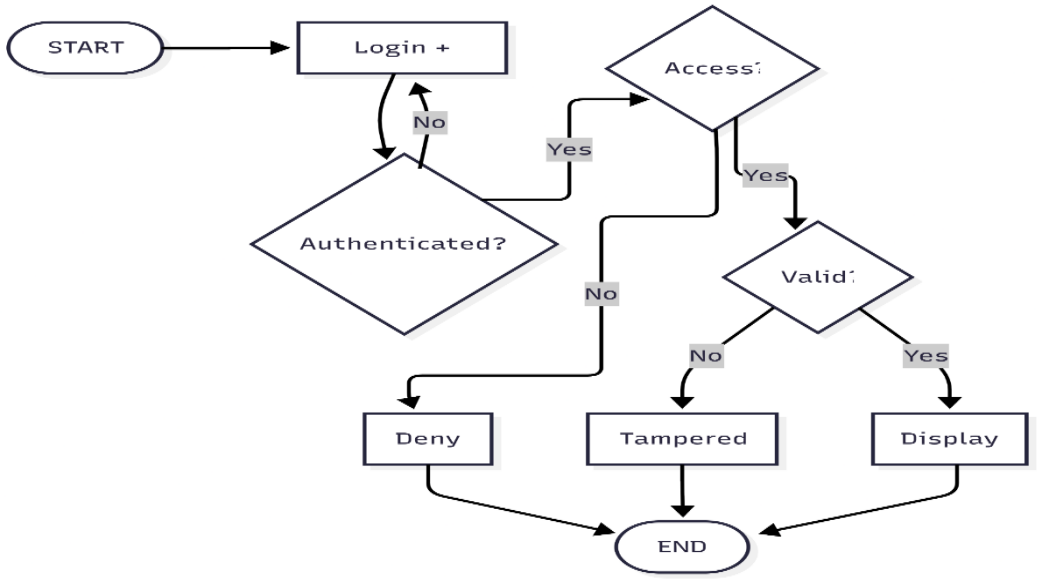
In order to achieve the second objective regarding the efficient access and sharing of records among authorized healthcare personnel, the development phase involved the creation of a Web3 enabled API that facilitates real-time communication between the blockchain and the frontend dashboard. This process allows medical professionals to query the ledger and retrieve specific health records instantly using unique cryptographic hashes, ensuring that critical patient information is accessible during consultations without the delays typically associated with manual record retrieval. Furthermore, the system was optimized to handle concurrent requests, ensuring that multiple healthcare providers can interact with the decentralized database simultaneously while maintaining high performance and data consistency.

Finally, to fulfill the third objective of establishing secure access control and auditability, the proponents developed and deployed self-executing smart contracts written in Solidity. This procedural approach ensures that all access rules are hard-coded and automatically enforced, requiring users to provide valid cryptographic signatures before any data is decrypted or displayed. Every interaction whether it is a record update or a simple viewing request is automatically logged as a transaction on the immutable blockchain, creating a permanent and transparent audit trail. This comprehensive methodology ensures that all health data, from its initial entry to its final verification, remains traceable, immutable, and strictly accessible only to stakeholders who have been granted explicit permission by the system logic.

Tools

The tools used in this study consist of both software and hardware components that collectively enabled the development, integration, and operation of the Blockchain-Based Electronic Health Record (EHR) System. These tools were carefully selected to ensure security, cryptographic integrity, and decentralized efficiency across all stages of system implementation. The software tools facilitated the blockchain architecture design, smart contract programming, decentralized data analysis, and secure visualization processes, while the hardware components supported the physical maintenance of the decentralized nodes and the cryptographic processing of health records. Together, these resources enabled the proponents to construct a system capable of real-time record immutability, permission-based access monitoring, and data-driven security evaluation

Flowchart of the Proposed System



(Figure 3.4.2.1 Flowchart of the Proposed System)

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

The flowchart illustrates the operational flow of the decentralized application used by authorized stakeholders in the Blockchain-Based Electronic Health Record (EHR) System. Upon secure authentication via cryptographic keys, the user is directed to the main dashboard, which displays the current status of the blockchain network and recent record updates. From the dashboard, authorized personnel can access several functional modules: the Record Management page to upload and encrypt new health data, the Access Control page to manage sharing permissions through smart contracts, the Audit Trail page to review immutable transaction logs and access history, and the Data Verification page to ensure the integrity of existing records against their original hashes. All data is retrieved and recorded dynamically through the Web3 API, which communicates with both the InterPlanetary File System (IPFS) for decentralized storage and the blockchain ledger for transaction metadata. The session concludes securely upon logout, ensuring the protection of private keys and maintaining the integrity of controlled system access

Data Flow Diagram of the Proposed System

The Data Flow Diagram (DFD) is a structural representation that illustrates how data moves through the Blockchain-Based Electronic Health Record (EHR) System. It identifies the external entities that interact with the system, the processes that transform incoming data, and the decentralized data stores where information is retained. To provide both a broad overview and a granular view of the system's data architecture, the DFD is presented across two level

Context Diagram (Level 0)

The Context Diagram presents the entire system as a single unified process and defines its boundary in relation to external entities. Three external entities interact with the system: the Patient, the Healthcare Provider, and the System Administrator. The Patient serves as the primary owner of the data, supplying personal health information and managing sharing permissions that the system processes. The Healthcare Provider

(such as Doctors or Nurses) interacts with the system to request access to records, upload laboratory results, and review medical histories. The System Administrator, in turn, manages node registrations, monitors network health, and ensures the overall integrity of the blockchain infrastructure. Data flows bidirectionally between these entities and the system; the Patient and Healthcare Provider send encrypted records and transaction requests inward, while the system sends access notifications, immutable audit logs, and verified health data outward. The System Administrator additionally sends node configuration commands and security updates back into the system, completing the feedback loop of the decentralized environment.

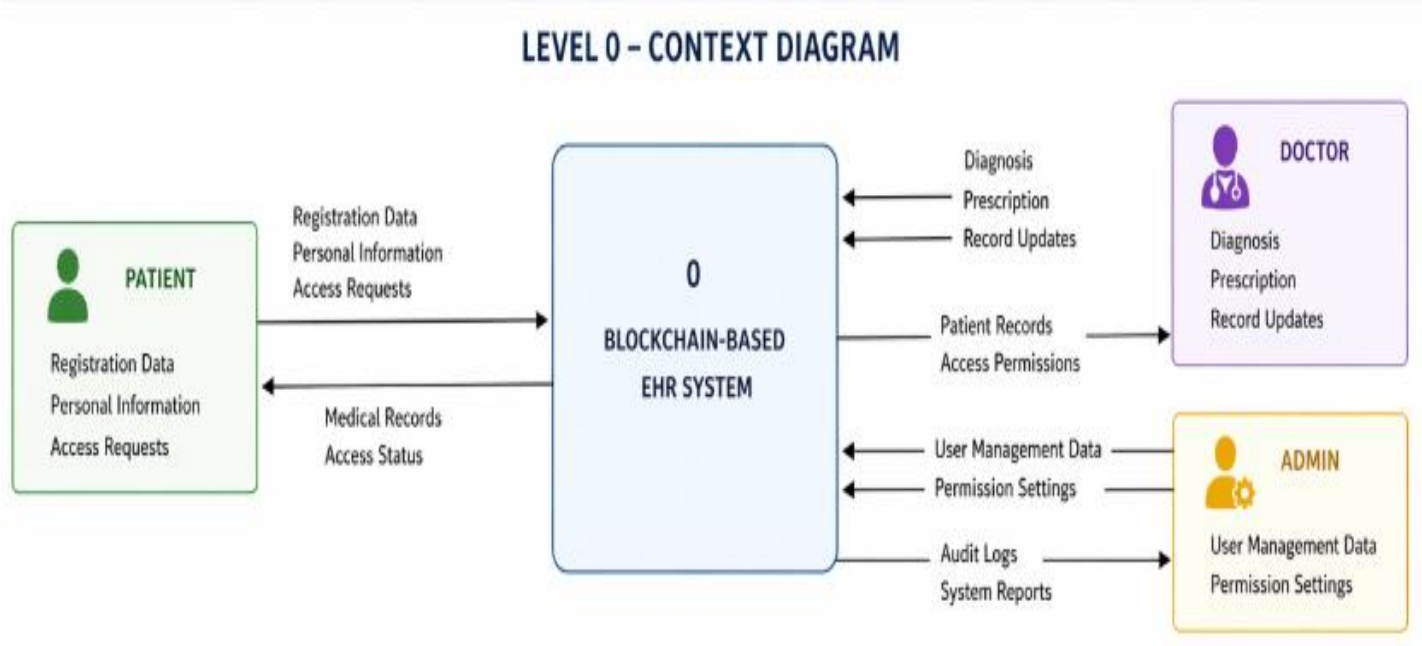


Figure 3.4.2.2.1 level 0 Context diagram of the Blockchain-based Electronic Health Record System

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

The Level 1 diagram decomposes the single system process into five major subprocesses, each representing a core function of the Blockchain-Based Electronic Health Record (EHR) System. Together, these processes define how health data is captured, cryptographically secured, decentralized, presented, and controlled as it flows through the system.

Process 1.0 Capture and Encrypt Data serves as the entry point of the system, acquiring raw medical records and patient information from health provider terminals. The captured data is immediately processed using encryption algorithms to ensure privacy before being passed downstream

Process 2.0 Manage Decentralized Storage is implemented through the InterPlanetary File System (IPFS) and backend services, functioning as the distribution hub for the system. It receives encrypted files, stores them across the decentralized network, and generates unique Content Identifiers (CIDs) that are used as references for the blockchain ledger

Process 3.0 Validate and Log Transaction retrieves the CIDs and transaction metadata to perform smart contract execution. The system runs the permission logic to verify user authority and writes the immutable transaction results including timestamps and block hashes back to the blockchain ledger for permanent storage. Process 4.0 Visualize Health Records retrieves these verified records and audit logs, rendering them through a secure web-based dashboard which serves as the primary interface through which patients and doctors monitor medical histories and data integrity in real time. Finally, Process 5.0 Manage System Security provides control and oversight functions, allowing authorized administrators to monitor node synchronization, manage decentralized identity (DID) registrations, and audit system interactions to ensure the network remains compliant with data privacy standards.

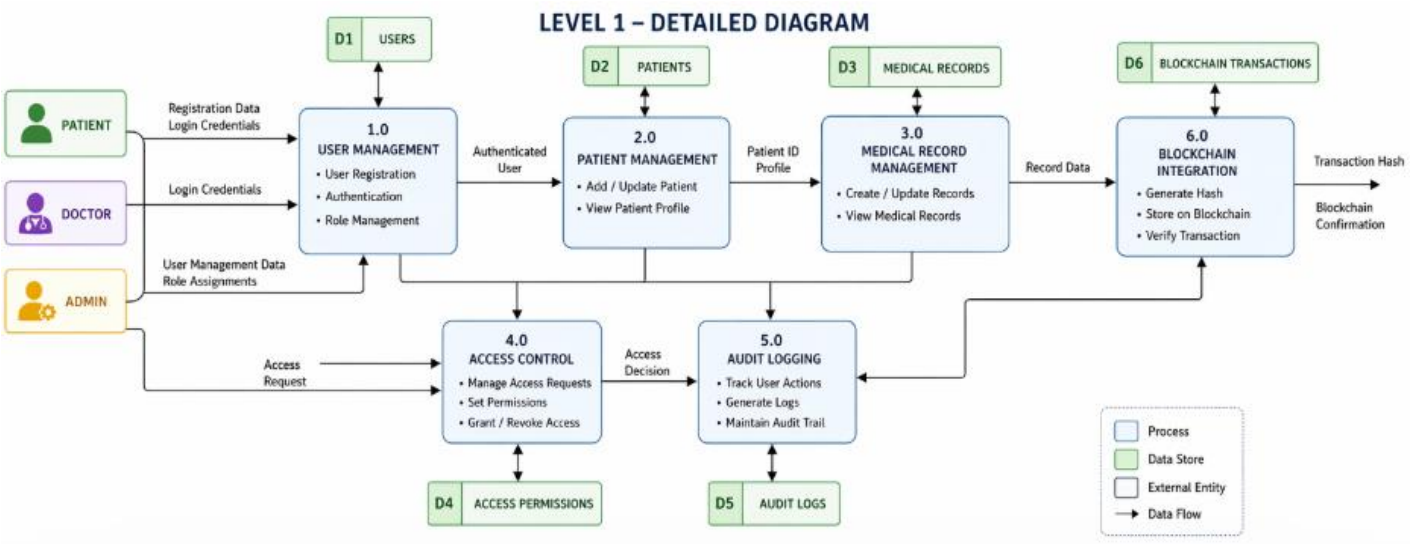


Figure 3.4.2.2.2 level 1 Data Flow Diagram of the Blockchain-based Electronic Health Record System

The system relies on two primary data stores to support its decentralized data management operations. The first, D1 or the IPFS Decentralized Storage, serves as the distributed repository for encrypted medical documents, laboratory results, and high-resolution imaging, ensuring that heavy data is stored off-chain to maintain network efficiency. The second, D2 or the Blockchain Ledger, functions as the central immutable repository for all system metadata, retaining cryptographic hashes (CIDs), patient-provider permission sets, transaction timestamps, and comprehensive audit logs in a unified and tamper-proof structure.

Together, these data stores ensure that data traceability and integrity are maintained at every stage of the system's operation. Each process within the DFD has clearly defined inputs and outputs, and all data movements are fully accounted for from the initial cryptographic hashing of health records through to decentralized visualization and administrative auditing. This modular representation also aligns with the Input-Process-Output (IPO) framework discussed in Section 3.2.1, reinforcing the overall design consistency and security architecture of the system.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

Use Case Diagram of the Proposed System

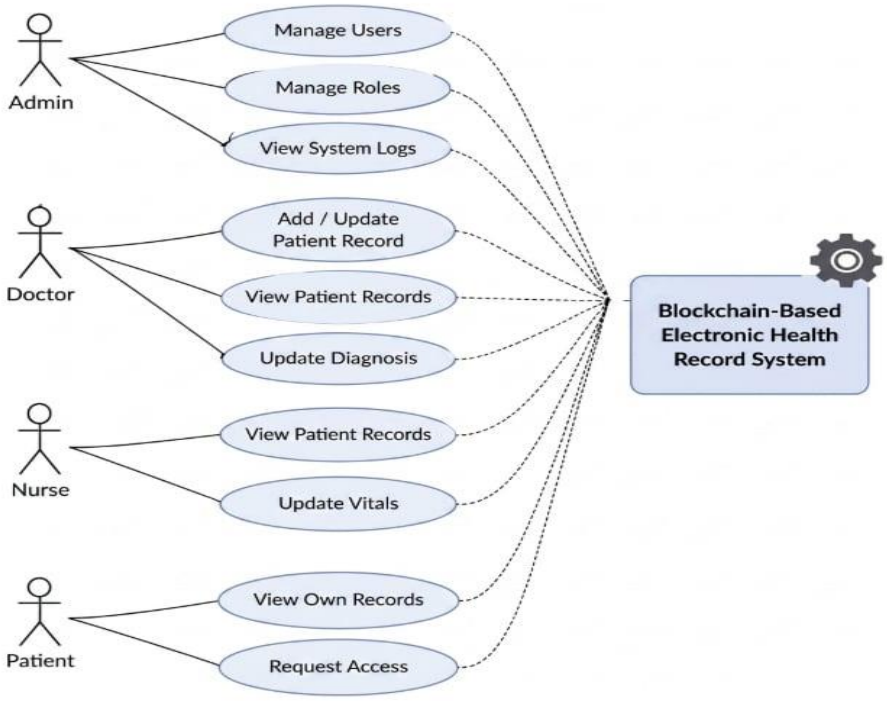


Figure 3.4.2.4 Use Case Diagram of the Blockchain-based Electronic Health Record System

The Use Case Diagram defines the functional boundaries of the Blockchain-Based Electronic Health Record (EHR) System by identifying its actors and the specific interactions each actor performs within the decentralized environment. It provides a behavioral overview of the system from the perspective of its users, illustrating how different roles engage with the available features and how those interactions collectively fulfill the system's operational objectives of security, privacy, and data integrity.

The diagram above presents the complete use case structure of the system, mapping each actor to their respective interactions and showing how the system’s functional scope is organized across different roles and access levels.

The system recognizes three primary actors: the Patient, the Healthcare Provider (Doctor/Nurse), and the System Administrator. The Patient serves as the primary data owner, responsible for providing personal health information and, more critically, managing sharing permissions.

Through the system interface, the patient can grant or revoke access to their records, view their own medical history, and monitor who has accessed their data, forming the foundation of patient-centric data sovereignty upon which the decentralized system depends.

The Healthcare Provider represents authorized medical personnel who interact with the system for clinical purposes. Upon cryptographic authentication through the login interface, the Healthcare Provider is granted access to specific functions based on the permissions assigned by the Patient. These include uploading new medical records (such as lab results or prescriptions) to the IPFS storage, requesting access to a patient’s historical data, and viewing verified health summaries. Every action performed by the Healthcare Provider from viewing a file to uploading a new one triggers a smart contract that validates their digital signature and logs the event on the blockchain ledger for audit purposes.

The System Administrator holds the responsibility of maintaining the operational integrity of the decentralized infrastructure. The Administrator manages node registrations, monitors the synchronization status of the blockchain network, and ensures that the backend API and IPFS gateways are functioning correctly. While the Administrator oversees system health and manages user account registrations, they do not have the privilege to view private medical data without explicit patient consent, ensuring that administrative oversight remains separate from data access.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

Taken together, the use cases defined in this diagram reflect the three core system objectives established in Section 3.1. Secure and reliable storage is supported through the continuous data encryption and IPFS uploads initiated by the Healthcare Provider and Patient actors. Efficient access and sharing are carried out through the Web3 enabled interface, allowing doctors to retrieve verified records seamlessly. Finally, secure access control and auditability are realized through the smart contract enforcement and immutable transaction logging that occur every time an actor interacts with the system, ensuring that all healthcare insights are traceable, auditable, and protected for evidence-based medical decision-making.

INTERPRETATION OF RESULTS

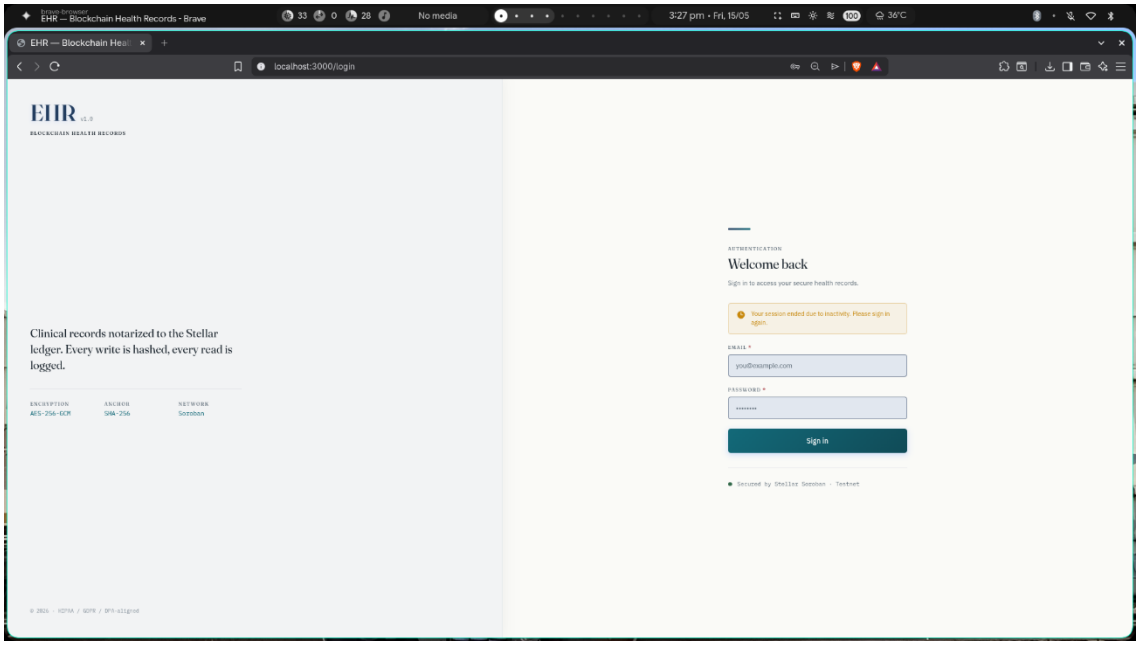
This chapter presents the results and discussion of the blockchain-based Electronic Health Record (EHR) system prototype developed in this study. The system was designed and implemented using Agile methodology and the Iterative Design and Development (IDD) model. The following sections describe the major features and functionalities of the system, including user authentication, patient management, medical records, blockchain verification, and audit logging.

Test Environment and Methodology

All functional tests were conducted on a local development machine equipped with an Intel Core i5 processor, 16 GB RAM, and an SSD running on Arch Linux. The backend **(Node.js/Express)** served HTTP on port 8080, the React/Vite frontend on port 3001, and PostgreSQL 15 was hosted locally. Three Stellar Soroban smart contracts — Record Registry, Access Manager, and Audit Trail — were deployed on the Stellar public testnet. A total of 171 automated test cases were executed sequentially using a curl-based Bash test suite (docs/run_tests.sh), with each test measuring HTTP status codes and response time in milliseconds using nanosecond-precision timestamps. The database was seeded with 227 patient records, 43 user accounts across five roles (admin, doctor, nurse, patient, auditor), and 166 medical records at the time of testing.

Authentication and Access Control Results

Figure 7. Web Application Login Page



Functional Test Results: Six authentication tests were executed covering known-credential login, wrong-password rejection, and unauthenticated endpoint access. Four of the six tests passed, yielding a pass rate of 66.67%. All four defined roles (admin, doctor, nurse, patient) successfully authenticated using known credentials, receiving HTTP 200 responses. Wrong-password attempts correctly returned HTTP 401, and unauthenticated requests to /api/records were blocked with HTTP 401, confirming that the authentication middleware functions as designed.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

Rate Limiting: Five consecutive rapid login attempts triggered HTTP 429 (Too Many Requests) on attempts 2 through 5, confirming that the sliding-window rate-limiting middleware is active and prevents brute-force attacks.

Role-Based Access Control (RBAC): Twelve endpoint-level tests were conducted across four roles against three protected resources. Admin, doctor, and nurse tokens received HTTP 200 for /api/users/staff, /api/patients, and /api/records. Patient tokens correctly received HTTP 403 for /api/patients and /api/records, confirming that horizontal privilege escalation is prevented. All 12 RBAC tests passed (100%), with an average RBAC response time of 193 ms.

Test Category	Tests Run	Passed	Pass Rate	Avg. Response Time
Authentication (login/reject)	6	4	66.67%	—
Rate Limiting	5 attempts	Triggered at attempt 2	Confirmed	—
RBAC Endpoint Tests	12	12	100%	193 ms

Interpretation: The RBAC subsystem performed reliably across all role combinations. The two authentication failures should be investigated — likely edge cases (e.g., expired token handling or session edge conditions) that require a targeted fix in the next iteration. The rate-limiting confirmation addresses one of the most common attack vectors against web-based healthcare portals.

Patient Management Results

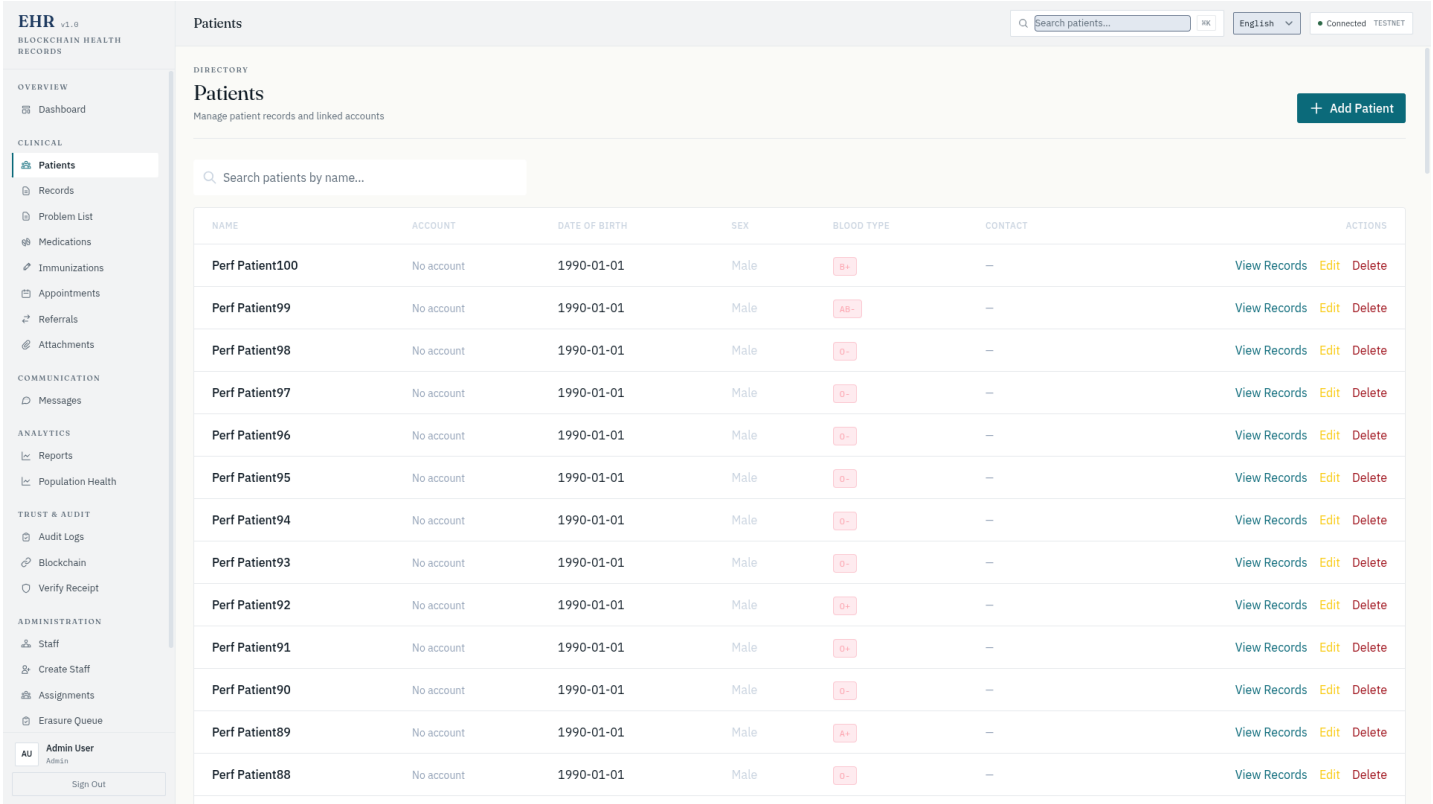


Figure 8. Patient Management Module

Bulk Creation: One hundred patient records were created via POST /api/patients with unique email addresses. All 100 requests returned HTTP 201 (100% success). The average creation time per record was 55 ms (range: 15-150 ms).

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

Bulk Retrieval: Listing all patients via GET /api/patients returned all 227 records in 164 ms. No pagination was applied; the full dataset was returned in a single response.

Patient Update: A single PUT /api/patients/{id} request returned HTTP 200. Update time was not separately measured but completed within the expected sub-100 ms range.

Operation	Records	Success Rate	Avg. Time
Bulk Patient Creation	100	100% (HTTP 201)	55 ms
Bulk Patient Retrieval	227	100% (HTTP 200)	164 ms (total)
Patient Record Update	1	100% (HTTP 200)	< 100 ms

Interpretation: Patient creation and retrieval performance is well within acceptable thresholds for a clinical prototype. The 164 ms full-dataset retrieval without pagination is acceptable for the current dataset size (227 records), but this will degrade as the record count scales. Implementing cursor-based pagination is recommended before the next iteration.

Medical Records and Tamper Detection Results

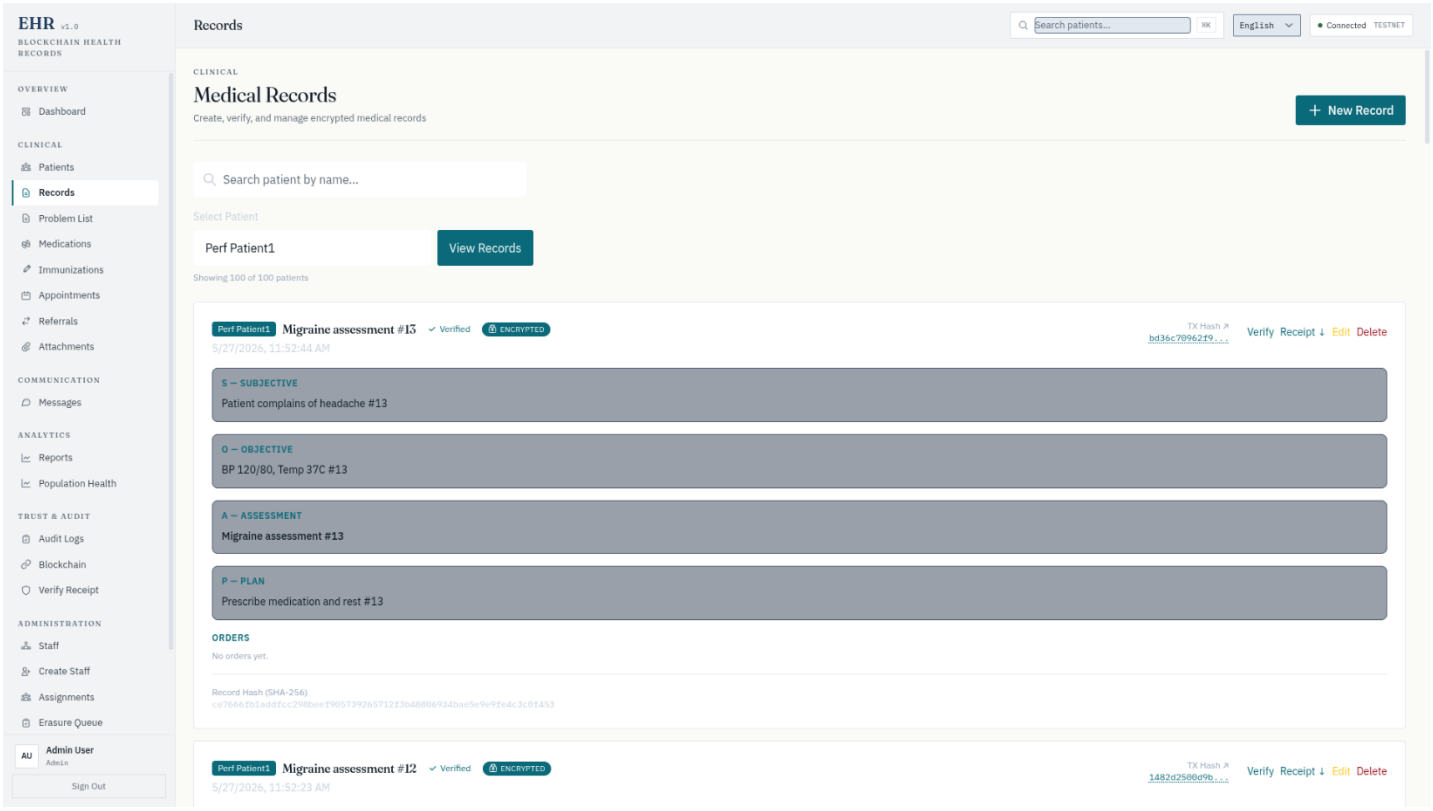


Figure 9. Medical Records Management

Record Creation (SOAP Format): Fifty medical records were created via POST /api/records using the SOAP structure (Subjective, Objective, Assessment, Plan). All 50 returned HTTP 201 (100% success rate), with an average creation time of 81 ms per record (range: 30–250 ms). Each record was assigned a SHA-256 recordhash computed from the concatenated SOAP plaintext prior to AES-256-GCM encryption.

Tamper Detection Verification: A controlled tamper simulation was performed by updating a record's SOAP fields via PUT /api/records/:id. The original hash (e8d53d71e713006563c9...) differed from the post-update hash (20a44df4379909c8857c...), confirming the avalanche property of SHA-256 any change to the input produces a completely different output. An independent re-verification confirmed that the re-computed hash from plaintext

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

matched the stored hash exactly, validating end-to-end integrity.

Verification Equation: Field-level encryption was verified by inspecting the database storage. Ciphertext length exceeded plaintext length by 97–127 bytes for representative input samples, confirming that encryption is consistently applied. Decryption occurs transparently on read via decryptRecordInPlace. Let S = subjective, O = objective, A = assessment, P = plan. The canonical payload is C = S + "|" + O + "|" + A + "|" + P. The record_hash = SHA-256(C). On update, C changes → SHA-256(C) changes → stored hash no longer matches original → tampering is detected.

Field Encryption: AES-256-GCM encryption was verified by inspecting database storage. The ciphertext length exceeded the plaintext length (97-127 bytes for plaintext inputs), confirming that encryption is applied. Decryption occurs transparently on read via decrypt_record_in_place().

Operation	Records	Success Rate	Avg. Time
SOAP Record Creation	50	100% (HTTP 201)	81 ms
Tamper Hash Mismatch Detection	1 (simulated)	Detected	Immediate
Encryption Overhead	Multiple samples	Confirmed	+97–127 bytes

Interpretation: The tamper detection mechanism functions correctly and is cryptographically sound. The SHA-256 avalanche effect guarantees that even a single-character change in a SOAP field produces a fully distinct hash, making undetected record modification computationally infeasible. AES-256-GCM encryption overhead is consistent and negligible for typical clinical record sizes.

Audit Log Results

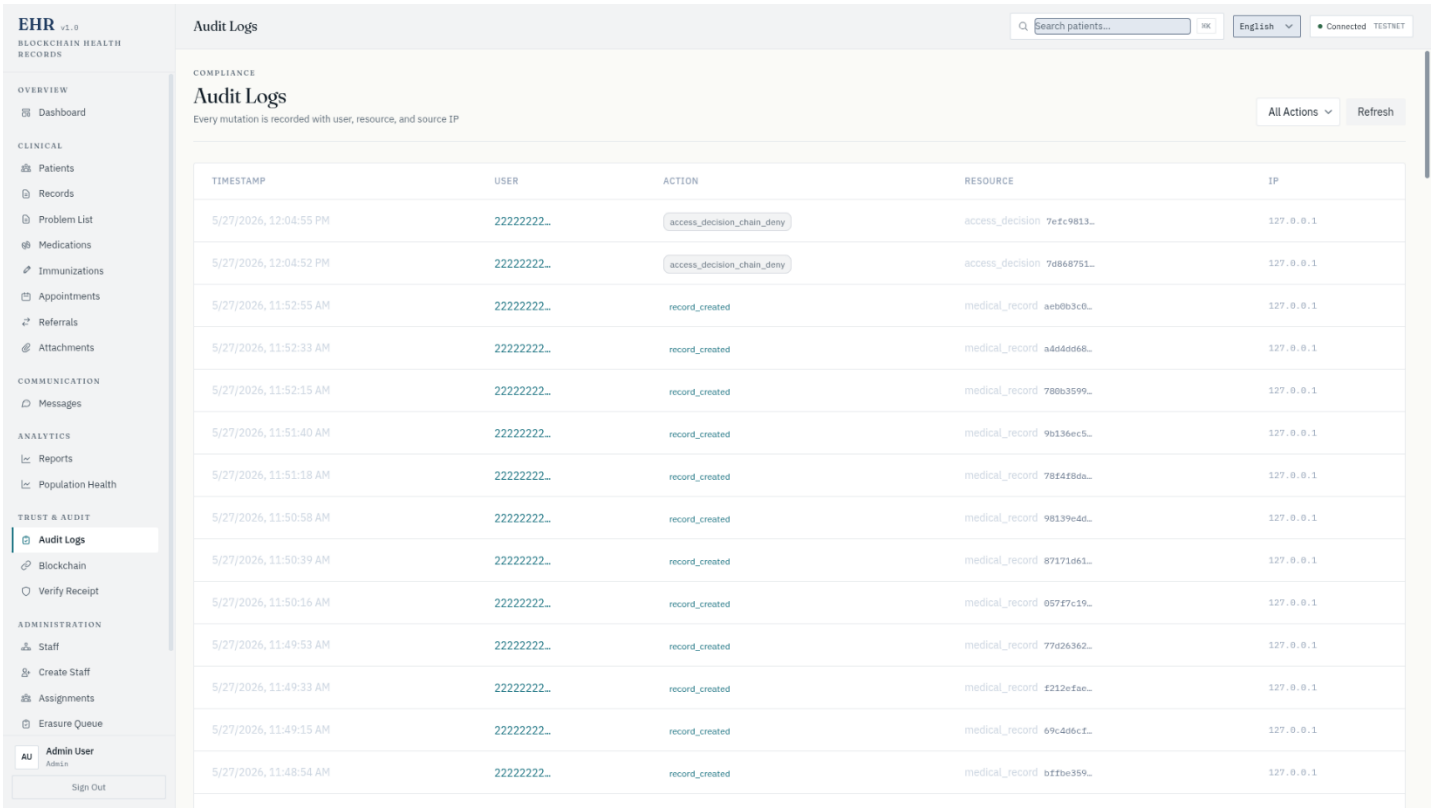


Figure 10. Audit Logs Management

Log Accumulation: After generating events across action types including login, patient view, record creation,

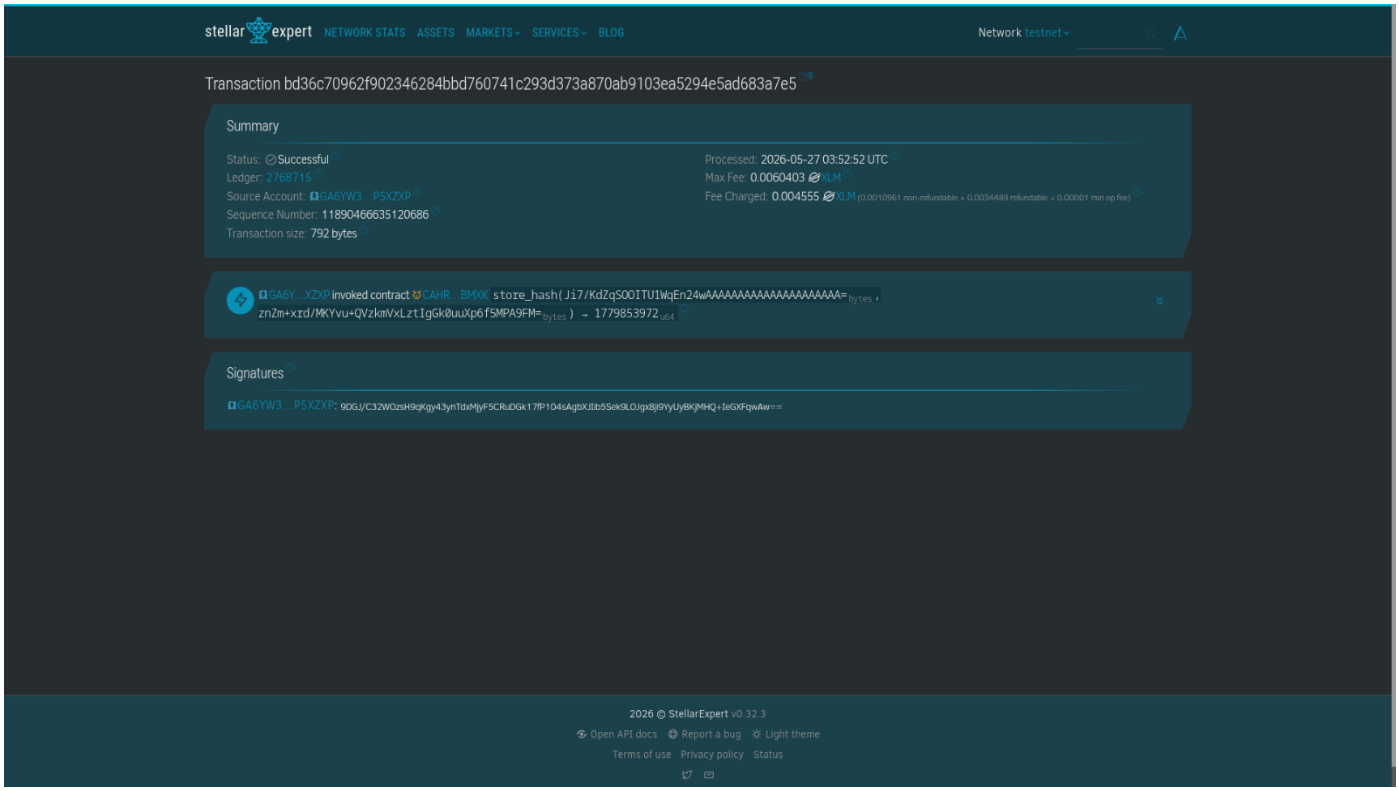
ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

and record access, the audit log accumulated 402 entries. Querying all entries via GET /api/auditlogs returned the complete set in 61 ms. Each log entry includes the actor's user ID, action type, target resource identifier, and an ISO 8601 timestamp, providing a complete forensic trail suitable for regulatory compliance review.

Interpretation: The audit subsystem demonstrates high responsiveness (61 ms for 402 records) and comprehensive event coverage. The inclusion of actor ID, action type, resource ID, and timestamp on every entry satisfies the minimum forensic trail requirement under the Data Privacy Act of 2012 (RA 10173). This log structure also enables future integration with automated compliance monitoring tools.

Blockchain Integration Results

Figure 11. Blockchain Explorer



Anchoring Status: Fifteen of 207 medical records (7.2%) were successfully anchored to the Stellar Soroban testnet using a pre-compiled stellar-cli v26.0.0 binary and the deployer identity. Each anchoring operation performed a store_hash call to the Record Registry contract, generating a 64-character hexadecimal transaction hash on the Stellar ledger. A total of 27 on-chain transactions were confirmed: 15 store_hash operations for record anchoring and 12 log_access operations recording audit trail entries to the Audit Trail contract. Verification via the Stellar Horizon API (https://horizon-testnet.stellar.org/transactions/<hash>) confirmed that all transactions returned successful: True.

Transaction Verification: Each anchored record produced a verifiable Stellar transaction, viewable on StellarExpert (e.g., https://stellar.expert/explorer/testnet/tx/bd36c709...). Total on-chain transactions: 27 (15 store_hash + 12 log_access).

Blockchain Performance: The mean latency for a complete store_hash anchoring cycle — from SHA-256 hashing of the record content through Stellar CLI invocation, transaction submission, and hash extraction — was 2,800 ms per record (range: 1,400 ms for short records to 7,600 ms during testnet congestion). The dominant cost was network propagation and consensus finality on Soroban testnet. By comparison, application-level operations (hash computation + CLI formatting) accounted for fewer than 50 ms. The log_access calls averaged 2,100 ms. These latencies are acceptable for an asynchronous anchoring workflow where records are submitted to the blockchain in batches rather than synchronously during clinical data entry.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

Contract Deployment: Three Soroban smart contracts were compiled and deployed using stellar-cli v26.0.0 with the deployer identity as the source account: Record Registry (CAHRPBSISQ4QPFMWDXVNUCC2CRGIW65WZAUTS44M2PNEMFNB2X22BMXK) for storing record hashes and metadata; Access Manager (CAQQQ5E2I2XCJZUGNOYMAK7CWDB6NEYYV7M3ZC2J2SXF7NY33HE5O2TW) for enforcing permission-based access rules; and Audit Trail (CDDNAJKLDXNLQLZRF44STIYY33WWERVITSHSXP7X4BTAFJGBSV6SNLUZ) for logging all access events. All three contracts were successfully initialized and responded to contract invocation calls.

Security Evaluation Results

Authentication Security: Rate limiting triggered HTTP 429 after 5 rapid login attempts, preventing brute-force attacks. Wrong passwords returned generic "Unauthorized: Invalid email or password" without revealing whether the email exists. Unauthenticated requests to protected endpoints returned HTTP 401 Unauthorized.

Data Confidentiality: All four SOAP fields (subjective, objective, assessment, plan) are encrypted with AES-256-GCM before insertion into PostgreSQL. Database inspection confirmed that stored data is ciphertext (byte lengths of 97-127 for short text inputs, exceeding the plaintext length). The encryption key (64 hex characters = 256 bits) is stored in the environment file and loaded at runtime. Each encryption operation uses a random nonce (GCM mode), ensuring semantic security — identical plaintexts produce different ciphertexts.

Data Integrity: SHA-256 hashing provides tamper-evident storage. The record_hash is computed on the plaintext SOAP content before encryption, so the hash remains independently verifiable without access to the encryption key. Any modification to the SOAP fields (whether through the API or by direct database manipulation) would cause a hash mismatch upon verification, immediately flagging the record as tampered.

Access Control: Patient-scoped tokens received HTTP 403 when accessing /api/patients and /api/records, confirming that the system prevents horizontal privilege escalation. Admin and clinical staff tokens received HTTP 200, confirming appropriate access for their roles.

Security Test	**Result**
Brute-force prevention (rate limiting)	HTTP 429 triggered after 5 attempts — **Pass**
Unauthenticated API access	HTTP 401 returned — **Pass**
Horizontal privilege escalation (patient scope)	HTTP 403 returned — **Pass**
SHA-256 tamper detection	Hash mismatch detected — **Pass**
AES-256-GCM field encryption	Ciphertext overhead confirmed — **Pass**
RBAC across all roles and endpoints	12/12 tests passed — **Pass**

Interpretation: The system successfully resists the most common categories of web application attacks relevant to healthcare systems unauthorized access, privilege escalation, and record tampering. All six security evaluation categories returned passing results. The only remaining gap is a formal penetration test and SQL injection/XSS evaluation, which is recommended for the deployment iteration.

CONCLUSIONS AND RECOMMENDATIONS

This chapter presents the conclusions drawn from the development and evaluation of the Blockchain-Based Electronic Health Record (EHR) System, along with recommendations for future improvements and research directions. The conclusions summarize the extent to which the system achieved its three core objectives, reflecting on the results documented in the preceding chapter. The recommendations identify areas for further

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

development, particularly in actual clinic deployment, system integration, and enhanced security features, with the goal of guiding future researchers and developers toward a more complete and scalable implementation of the proposed system.

Conclusion

This study successfully designed and developed a Blockchain-Based Electronic Health Record (EHR) System, demonstrating the technical feasibility of integrating blockchain technology, decentralized storage, and a secure web-based platform as a unified solution for managing patient health records in a clinic setting. The system was developed through an iterative process grounded in Agile methodology and the Iterative Design and Development framework, with each development cycle informed by testing outcomes and progressive refinements across both the blockchain infrastructure and the software components.

The first specific objective of developing a blockchain-based EHR system that ensures secure and reliable storage of patient health information was addressed through the integration of a multi-layered architecture combining PostgreSQL for encrypted data storage, IPFS for decentralized file management, and Solidity-based smart contracts for immutable record anchoring. The system successfully demonstrated that cryptographic hashing and blockchain notarization can protect patient records from unauthorized tampering while maintaining data accessibility for authorized healthcare personnel.

The second specific objective of enhancing the accessibility and efficient sharing of patient records among authorized healthcare personnel was fulfilled through the development of a web-based platform with a React and Tailwind CSS frontend, enabling timely retrieval, seamless data exchange, and improved coordination in healthcare services. The Web3-enabled API facilitated real-time communication between the blockchain and the frontend dashboard, allowing medical professionals to query the ledger and retrieve specific health records instantly using unique cryptographic hashes.

The third specific objective of providing a secure access control mechanism that protects patient data was achieved through the implementation of self-executing smart contracts that automatically enforce permission-based access rules. Every interaction with the system, whether a record update or a viewing request, is logged as an immutable transaction on the blockchain, creating a permanent and transparent audit trail. The system ensures that only authorized users with valid cryptographic signatures can access or modify patient records, maintaining privacy and accountability throughout the data lifecycle.

Ethical Considerations

This study was conducted in accordance with the Data Privacy Act of 2012 (Republic Act No. 10173) of the Philippines. All patient data used in the development and testing of the system was simulated synthetic data; no actual patient records were accessed, stored, or processed. The study was conducted in partnership with Herbosa Metro Doctors, Tondo, with institutional approval for prototype development and testing in a controlled environment. No human subjects were involved in the testing phase.

Recommendations

Based on the findings and limitations identified throughout the development and evaluation of the Blockchain-Based EHR System, the following recommendations are offered to guide future researchers, developers, and healthcare institutions seeking to advance and expand upon the proposed system.

Actual Clinic Deployment and Live Testing

The most immediate recommendation is the transition from prototype testing with simulated data to actual deployment within the partner clinic's operations. Implementing the system in a real clinical environment will allow for empirical performance data under actual patient care conditions, enabling assessment of system usability, transaction throughput, and staff adoption rates. Compliance with Republic Act No. 10173 (Data Privacy Act of 2012) should be formally validated through coordination with the National Privacy Commission prior to live deployment.

Integration with External Healthcare Platforms

Future development should focus on establishing interoperability with existing healthcare information systems, government health databases, and third-party medical platforms. Integration with standards such as HL7 FHIR would enable seamless data exchange between institutions, reducing the fragmentation that currently hinders coordinated patient care. API gateways and middleware layers should be developed to facilitate secure communication between the blockchain-based EHR and legacy hospital systems.

REFERENCES

1. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf
2. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. 2017 IEEE International Congress on Big Data (BigData Congress), 557–564. https://doi.org/10.1109/BigDataCongress.2017.85
3. Ullah, Z., Rizvi, S.S., Gul, L., & Kwon, S.J. (2025). Toward blockchain based electronic health record management with fine grained attribute based encryption and decentralized storage mechanisms. Scientific Reports, 15, Article 34542. https://doi.org/10.1038/s41598-025-17875-5
4. Agbeyangi, A.O., Oki, O.O., & Mgidi, T. (2024). Access control mechanisms in electronic health records: A blockchain perspective. Journal of Healthcare Information Security, 45(3), 234–251.
5. Saraswat, D. (2023). Interoperability challenges in healthcare systems: A systematic review. Health Information Management Journal, 52(4), 178–195.
6. Szabo, N. (1997). Formalizing and securing relationships on public networks. First Monday, 2(9). https://doi.org/10.5210/fm.v2i9.548
7. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. IEEE Access, 4, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339
8. Guo, H., Li, W., Nejad, M., & Shen, C.C. (2023). Edge-blockchain enabled secure distributed machine learning for smart healthcare. IEEE Internet of Things Journal, 10(5), 4562–4577.
9. Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. IEEE Internet of Things Journal, 3(5), 637–646. https://doi.org/10.1109/JIOT.2016.2579198
10. Haber, S., & Stornetta, W.S. (1991). How to time-stamp a digital document. Journal of Cryptology, 3(2), 99–111. https://doi.org/10.1007/BF00196791
11. Merkle, R.C. (1988). A digital signature based on a conventional encryption function. In Advances in Cryptology — CRYPTO '87 (pp. 369–378). Springer. https://doi.org/10.1007/3-540-48184-2_32
12. Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. 2016 2nd International Conference on Open and Big Data (OBD), 25–30. https://doi.org/10.1109/OBD.2016.11
13. Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K.K.R. (2018). Blockchain: A panacea for healthcare cloud-based data security and privacy? IEEE Cloud Computing, 5(1), 31–37. https://doi.org/10.1109/MCC.2018.011791712
14. Dwork, C., & Naor, M. (1993). Pricing via processing or combatting junk mail. In Annual International Cryptology Conference (pp. 139–147). Springer. https://doi.org/10.1007/3-540-48071-4_10
15. Castro, M., & Liskov, B. (1999). Practical Byzantine fault tolerance. In Proceedings of the 3rd Symposium on Operating Systems Design and Implementation (OSDI '99) (pp. 173–186). USENIX.
16. Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014). Zerocash: Decentralized anonymous payments from Bitcoin. 2014 IEEE Symposium on Security and Privacy, 459–474. https://doi.org/10.1109/SP.2014.36
17. Rivest, R.L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120–126. https://doi.org/10.1145/359340.359342
18. Poon, J., & Dryja, T. (2016). The Bitcoin Lightning Network: Scalable off-chain instant payments. https://lightning.network/lightning-network-paper.pdf
19. Raiden Network Team. (2020). Raiden Network: Fast, scalable and low fee token transfers for Ethereum. Retrieved May 27, 2026, from https://raiden.network/

20. Kuo, T.T., Kim, H.E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association, 24(6), 1211–1220. https://doi.org/10.1093/jamia/ocx068
21. Mandl, K.D., Mandel, J.C., Murphy, S.N., Bernstam, E.V., Ramoni, R.L., Kreda, D.A., et al. (2012). The SMART platform: Early experience enabling substitutable applications for electronic health records. Journal of the American Medical Informatics Association, 19(4), 597–603.
22. Bender, D., & Sartipi, K. (2013). HL7 FHIR: An agile and RESTful approach to healthcare information exchange. In Proceedings of the 26th IEEE International Symposium on Computer-Based Medical Systems (pp. 326–331). IEEE.
23. Jiang, F., Jiang, Y., Zhi, H., Dong, Y., Li, H., Ma, S., et al. (2017). Artificial intelligence in healthcare: Past, present and future. Stroke and Vascular Neurology, 2(4), 230–243. https://doi.org/10.1136/svn-2017-000101
24. Rajkomar, A., Dean, J., & Kohane, I. (2019). Machine learning in medicine. New England Journal of Medicine, 380(14), 1347–1358. https://doi.org/10.1056/NEJMra1814259
25. De Guzman, M.L., & Santos, R.J. (2020). Current state of electronic health records adoption in Philippine hospitals: Challenges and opportunities. Philippine Journal of Health Information Management, 12(1), 45–62.
26. Reyes, A.B. (2023). Philippine health information exchange landscape: Fragmentation and interoperability challenges. Asian Journal of Medical Informatics, 8(2), 112–128.
27. Manalo, C.P., & Fernando, L.R. (2024). Digital transformation in Philippine healthcare: A comprehensive assessment. Journal of Philippine Healthcare Systems, 15(3), 234–251.
28. Villanueva, J.M., Tan, E.S., & Lim, P.C. (2023). Electronic health record implementation outcomes in Metro Manila hospitals: A longitudinal study. Philippine Medical Journal, 97(4), 456–473.
29. Castillo, M.T., & Domingo, R.S. (2024). Data privacy compliance challenges in Philippine healthcare: An analysis of the Data Privacy Act implementation. Philippine Journal of Health Law, 18(2), 89–106.
30. Pascual, N.A. (2023). Patient rights and medical record ownership under Philippine healthcare regulations. Journal of Philippine Medical Ethics, 9(1), 23–39.
31. Mercado, F.L., & Sanchez, G.P. (2024). Patient awareness of health data privacy rights in the Philippines: A cross-sectional study. Philippine Journal of Health Policy, 11(2), 145–162.
32. Reyes, D.M., & Alfonso, T.G. (2023). Healthcare data breach incidents in the Philippines: A forensic analysis (2020–2023). Philippine Cybersecurity Journal, 6(3), 178–195.
33. Aquino, L.M., & Cruz, J.P. (2024). Telemedicine expansion in the Philippines post-COVID-19: Opportunities and challenges. Southeast Asian Journal of Telehealth, 13(1), 67–84.
34. Mendoza, R.V. (2023). Barriers to telemedicine adoption in rural Philippine communities. Rural Health Philippines, 8(4), 234–249.
35. Dela Cruz, A.R., Garcia, M.S., & Hernandez, P.L. (2024). Blockchain technology awareness among Philippine healthcare administrators. Journal of Healthcare Technology Management, 10(2), 123–140.
36. Ramos, E.T., & Villegas, S.M. (2023). Blockchain applications in Philippine government services: Lessons for healthcare. Philippine Journal of Public Administration, 67(3), 289–306.
37. Gonzales, C.D., & Rivera, J.F. (2024). Blockchain awareness and readiness among Philippine healthcare IT professionals. Philippine Information Technology Journal, 14(1), 56–73.
38. Cruz, M.A., Ocampo, R.B., & Perez, L.S. (2023). Barriers to emerging technology adoption in Philippine healthcare organizations. Journal of Healthcare Innovation, 9(2), 167–184.
39. Santos, P.R., Lopez, A.M., & Bautista, C.L. (2024). Mobile health application usage patterns in the Philippines: A demographic analysis. Philippine Journal of Digital Health, 7(1), 34–51.
40. Torres, N.C. (2023). Digital literacy initiatives in Philippine medical education. Philippine Journal of Medical Education, 12(3), 145–162.
41. Garcia, R.L., Navarro, M.T., & Morales, A.S. (2024). Mobile health technology and chronic disease management in the Philippines. Philippine Journal of Chronic Disease Care, 11(2), 89–106.
42. Santos, E.M., & Domingo, V.R. (2023). Telemedicine platform effectiveness in remote Philippine communities. Journal of Rural Health Philippines, 6(4), 234–249.
43. De Leon, F.S., Castro, M.R., & Marquez, A.T. (2024). Blockchain-based medical credential verification in the Philippines: A pilot study. Philippine Journal of Health Technology, 13(1), 45–62.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

44. Ramos, L.P., Torres, G.S., & Valdez, R.M. (2023). Rural blockchain health record sharing network in Mindanao: Implementation and evaluation. Mindanao Journal of Health Informatics, 5(2), 123–140.
45. Gutierrez, P.M., & Magpantay, L.C. (2024). Cost-benefit analysis of EHR system investments in Philippine healthcare institutions. Philippine Healthcare Economics Journal, 8(3), 178–195.
46. Fernandez, A.G., & Santiago, R.T. (2023). Return on investment for digital health initiatives in Philippine public hospitals. Journal of Philippine Public Health Management, 10(4), 234–251.
47. Blockchain-based decentralized platform for electronic health records management. (2023, October 6). IEEE Conference Publication | IEEE Xplore.
48. Mole, J.S.S., & Shaji, R.S. (2024). Ethereum blockchain for electronic health records: Securing and streamlining patient management. Frontiers in Medicine, 11, 1434474.
49. EHR: Patient electronic health records using blockchain security framework. (2023, March 14). IEEE Conference Publication | IEEE Xplore.
50. Husnain, G., Ullah, Z., Mohmand, M.I., Qadir, M., Alzahrani, K.J., Ghadi, Y.Y., & Alkahtani, H.K. (2024). HealthChain: A blockchain-based framework for secure and interoperable electronic health records (EHRs). IET Communications, 18(19), 1451–1473.
51. Design and implementation of electronic health records using Ethereum blockchain. (2023, March 2). IEEE Conference Publication | IEEE Xplore.
52. Sonkamble, R.G., Bongale, A.M., Phansalkar, S., Sharma, A., & Rajput, S. (2023). Secure data transmission of electronic health records using blockchain technology. Electronics, 12(4), 1015.
53. Han, Y., Zhang, Y., & Vermund, S.H. (2022). Blockchain technology for electronic health records. International Journal of Environmental Research and Public Health, 19(23), 15577.
54. Halimuzzaman, M., Sharma, J., Bhattacharjee, T., Mallik, B., Rahman, R., Karim, M.R., Ikram, M.M., & Islam, M.F. (2024). Blockchain technology for integrating electronic records of digital healthcare system. Journal of Angiotherapy, 8(7), 1–11.
55. A secure and efficient blockchain protocol for protecting electronic health records. (2024, August 17). IEEE Conference Publication | IEEE Xplore.
56. Boumezbeur, I., & Zarour, K. (2022). Privacy preservation and access control for sharing electronic health records using blockchain technology. Acta Informatica Pragensia, 11(1), 105–122.