Blockchain Technology for Integrating Electronic Records of Digital Healthcare System

Md. Halimuzzaman[1], Dr. Jaideep Sharma[2], Tapan Bhattacharjee[3], Bilash Mallik[4], Rashadur Rahman[5], Mohammad Rezaul Karim[6], Mostafa Masrur Ikram[7], Md Fokhrul Islam[8]

Abstract

Background: In most healthcare facilities, the shift from paper-based medical records to electronic health records (EHRs) has taken place. However, there are issues with credibility, management, and secure data storage with the existing EHR systems. In the healthcare industry, interoperability and user control over personal data are also major challenges. Block chain technology has become a potent tool that can provide immutability, security, and user control over records that are saved; yet, its potential usage in EHR systems is still not well understood. Objectives: This research attempts to close this knowledge gap by developing an EHR framework that is built on blockchain technology and is compatible with many national and international EHR standards, including HL7 and HIPAA. Methods: In order to investigate the state of the art in the field of EHRs, including blockchain-based EHR implementations, a systematic literature review is the study approach used. Results: The report analyzes numerous national and international EHR standards, identifies the interoperability needs based on these standards, and outlines the interoperability challenges in the current blockchain-based EHR frameworks. Without the requirement for centralized systems, the suggested framework can give the healthcare industry safer ways to exchange health information while also offering the features of immutability, security, and user control over stored records. Conclusion: This work contributes to the understanding of Blockchain technology's potential application in EHR frameworks and offers an interoperable Blockchain-based EHR framework that can meet the requirements outlined in multiple national and international EHR standards.

Keywords: Blockchain; Healthcare; Security; Electronic Health Records (EHRs); Health information management (HIM)

Introduction

It is anticipated that smart contracts and blockchain will create new avenues for protecting patient data that is accessible and exchanged through electronic health records (EHRs). Blockchain healthcare infrastructure integration will greatly enhance people's life (Adesh Mukati, 2023). Electronic Health Record (EHR) systems are growing in popularity as a practical way to transfer medical information across different healthcare institutions. However, because current EHR databases are either geographically limited or specifically linked to a particular healthcare provider, accessing

Significance | This study determined the multifaceted benefits of blockchain in enhancing the overall efficiency, effectiveness, and integrity of digital healthcare systems.

*Correspondence. Md. Halimuzzaman, School of Business, Galgotias University, Greater Noida, Uttar Pradesh, India.
E-mail: halim.helal@gmail.com

Editor Md Shamsuddin Sultan Khan, And accepted by the Editorial Board Jul 04, 2024 (received for review Mar 05, 2024)

Author Affiliation.
[1] School of Business, Galgotias University, Greater Noida, Uttar Pradesh, India.
[2]School of Business, Galgotias University, Greater Noida, Uttar Pradesh, India.
[3]Department of Sociology, Victoria Govt. College, Cumilla, Bangladesh.
[4]Department of Sociology, Govt. Brojomohun College, Bangladesh.
[5]Shanto-Mariam University of Creative Technology, Bangladesh.
[6]Shanto-Mariam University of Creative Technology, Bangladesh.
[7] Jahangirnagar University, Bangladesh.
[8] International Studies, University of Wyoming, USA.

Please cite this article.
Md. Halimuzzaman, Dr. Jaideep Sharma et al. (2024). Blockchain Technology for Integrating Electronic Records of Digital Healthcare System, Journal of Angiotherapy, 8(7), 1-11, 9740

necessary patient records from several EHRs can be challenging (Walid et al., 2023).

Blockchain-based data access and storage can benefit patients by enabling remote monitoring, cutting expenses, and enhancing care received outside of medical facilities. The increasing usage of IoT devices creates a number of privacy and security issues, particularly in the healthcare industry where patient information confidentiality must be maintained (Swapnil Singh, 2022). Blockchain will transform the interchange and processing of electronic health records by protecting them via a distributed peer-to-peer network and offering a secure means of medical data sharing for improved healthcare efficiency. It is suggested that the blockchain approach be used to maintain the current process for understanding distributed ledger technology. The primary purpose of blockchain technology was to store digital records of cash-related transactions that are not reliant on centralized authorities or commercial partnerships (Erdoğdu & Ünüsan, 2022). The blockchain substructure that covers a product's whole life cycle will include data interchange, improved access to medical information, and framework monitoring (Quasim et al., 2023). It will greatly enhance the patient care services system (Taherdoost, 2023). This research has the potential to significantly alter the healthcare system by combining two EHR platforms. The intention is to show how the HL7 and HIPAA frameworks may cooperate to exchange data for the high-level improvement of health systems. People's comfort and lifestyles are being improved by the increasing use of IoT devices (Capuzzo et al., 2022). It is suggested that blockchain technology be used to safeguard IoT devices in order to stop tampering and unauthorized access. MedRec uses the permission-less blockchain to achieve two key goals: giving patients more control over their health data and facilitating the more effective transfer of data between different providers via compatible query strings (Singh et al., 2023).

The Fast Health Interoperability Resource (FHIR) and Health Level 7 (HL7) standards for the sharing of health-related data are encapsulated in the blockchain-based FHIR Chain framework (Rudzidatul Akmam Dziyauddin, 2023). Data interoperability is intended to be made possible by the consensus algorithm. This solution uses network-wide keys and smart contracts to provide further security features to the blockchain (Xue et al., 2022). Thus, the obvious answer to the serious concerns and problems with exchanging healthcare data is blockchain-based data exchange. Spreadsheets, available EHR archetypes, and template authors are used in the configuration of input forms in EHR systems. A framework for promoting the reuse of free EHR prototypes and template semantics has been proposed by Sundvall (Adel et al., 2020). Ancile is a blockchain-based system designed to protect patients' vital information while organizing access to health records for patients, providers, and third parties in a safe manner. Ancile leverages smart contracts and upholds accessibility and interoperability to deliver significant data integrity and privacy preservation. This framework creates storage and a blockchain system that is affordable by utilizing particular Ethereum features. The importance of access control and security is determined by how well authorization and encryption are used (Mahendra Pratap Singh, 2023). The blockchain framework satisfies several requirements of a workable healthcare system and eliminates third parties' access to secure health data. It has been demonstrated that the blockchain framework generalizes across the different healthcare system areas (Fatima et al., 2022). It is imperative that we are aware of these downsides and weigh the benefits of the current options before implementing blockchain technology on a big scale (Pandey & Litoriya, 2020).

Blockchain technology offers an architectural model for the arrangement of dispersed personal health data. It suggests a theoretical prototype that relies on blockchain technology in a peer-to-peer network to manage the private medical data collected from several healthcare providers (Bigini et al., 2023). In the European Union (EU) and the European Economic Area (EEA), there is a data protection and privacy regulation known as the General Data Protection Regulation GDPR (Amit Doegar, 2021). The HIPAA Regulations allow employees to benefit from workplace coverage and health benefits (Daniel J. Solove, 2020). HIPAA's enhance the overall efficiency of the healthcare systems and prevent the improper use of medical data for for one's own benefit (Adane et al., 2019). Health information management (HIM) professionals, such as advanced practice nurses (APNs), are essential to enhancing patient outcomes (Angelika Haendel, 2022). The need of practitioners being aware of HITECH and HIPAA regulations pertaining to electronic health record systems and patient medical information was emphasized by Kaneko and Yuda (Maryam Farhadi, 2022). HIPAA relates to transferring pension funds from an employee to another upon employment transition, which sets it apart from the Consolidated Omnibus Budget and Reconciliation Act (COBRA). In addition, COBRA permits the maintenance of healthcare coverage, provided that full market prices are not paid (Aaron M. Gamino, 2021).

The following benefits are highlighted by the HIPAA for the beneficiary: (1) new employers are required to offer coverage to their hires and their dependents; (2) a person can continue to access healthcare after losing coverage; (3) employers are not allowed to place restrictions on how often their employees can use their insurance; and (4) people can choose to renew their health insurance through their new employers.

Double-spending is the practice of making the same transaction more than once. In a manner similar to this, in blockchain-based healthcare apps, an attacker can alter the transaction state and perform the same transaction twice (Kumar et al., 2023). IPFS is a

distributed file system that utilizes blockchain technology to establish secure communication channels and store data. Blockchain employs a P2P network that makes it impossible for hackers to intercept or sniff messages (Kulüke et al., 2023). Interoperability of health data has been a challenge for the healthcare industry for the last ten years, according to numerous prior study reports. In light of this, Suljanović et al. (2019) covered a number of useful methods for resolving interoperability issues that support better communication and increase the use of information technology in data exchange procedures. In light of this, applying digital health trends to enhance artificial intelligence is thought to be an efficient way to address interoperability issues. According Priya & Palanisamy (2022), the use of technology facilitates the sharing of patient data and helps management provide better patient care. Furthermore, the technique to improve patient data access was covered in the study by (Khan et al., 2021), since this will provide easy access to all data in real time for the healthcare management. Ganta et al. (2023) claim that strategies for connected data accessibility make it possible for caregivers, patients, and healthcare professionals to effectively share health information. Transferring patient data to aid in the information sharing process is greatly aided by the act of transmitting or receiving patient health information through health information exchange (HIE). Healthcare professionals can effectively monitor the effects of a patient's care with the use of this technique (Gandhi & Walker, 2022). FHIR standards are also being used in the integration of personalized machines and wearable data. Within two months, a project called SMART for FHIR (2010) was shown. Its goal was to allow health applications to be used across different medical information systems without requiring changes(Govindaraj & Murugan, 2023). A new medical data standard called FHIR is being developed to interchange medical electronic data and integrate and model unstructured data from an EHR for use in a variety of scientific research applications. In order to advance FHIR. Zandvakili & Pulaski (2023) used the EHR's phenotyping framework for the documentation of obese patients and how obesity contributes to the advancement of other diseases. This information was gathered from half-structured discharge summaries that supported a "FHIR-based clinical data normalization pipeline (NLP2FHIR)". The study's findings showed that using half-structured discharge summaries, the FHIR-based HER-phenotyping technique could successfully identify the obese state and its related diseases and impacts (Fabacher et al., 2023). A framework for facilitating EHR interoperability for reasoning services and suggested transformations for clinical knowledge and data was created by (Adel et al., 2020). Refillable mappings constitute the main constituent of workflows, which form the basis of the study's structure. (Nobari et al., 2022). In order to conform EHR data to EHR-semantic web standards, medical data alteration workflows can be configured and executed using the CLIN-IK-LINKS platform. As a result, CLIN-IKLINKS plays a significant role in improving the semantic interoperability of the EHR systems in question (Adel et al., 2019).

Methods and Materials

The previously described HL7 and HIPAA frameworks can now be compatible thanks to the proposed blockchain-based interoperable framework (BCIF-EHR). Data sharing and data retrieval from frameworks is enabled for the HL7 framework. In a significant number of institutions and healthcare systems, it is frequently used. It has been widely employed for the past three decades due to its adaptability and capacity to connect effectively with patient incoming and outgoing data. However, HIPAA is an EHR architecture with excellent web services and privacy capabilities.

One of the most dependable and safe EHR frameworks is HIPAA, which offers the finest privacy and security for sensitive health data. The HIPAA framework facilitates the processing and sharing of data between the frameworks by having a distinct user privacy layer that limits the amount of patient data. Because HIPAA includes a specific web services layer, it is the finest framework for offering online services. Our suggested framework is also very advantageous because it makes several modifications to the way that web platforms in healthcare are handled. Ensuring secure transportation of data supplied to the HL7 framework is the most advantageous aspect of the HIPAA framework. This is when the HIPAA framework's transport security layer becomes relevant. Because it offers us the highest level of data security and dependability while exchanging data with other frameworks, it makes it technically feasible for the two suggested frameworks to be interoperable. A framework known as the BCIF-EHR blockchain interoperable framework is created to address the issues with electronic health record systems. The framework seeks to enhance collaboration across various blockchain-based healthcare organizations, including insurance providers, clinics, and hospitals. Data sharing and integration are made easy by the BCIF-EHR framework, which supports. The framework does, however, prioritize safeguarding patient data, especially the confidentiality and integrity of electronic health information.

In the field of interoperability, a lot of research is being done. When exchanging EHRs between two blockchain platforms, it is quite important. These EHR transfers present a number of difficulties.

1. Every blockchain has a different transaction format;
2. Every system may have different EHR standards;
3. Data transmission methods between blockchain platforms vary.

We have assumed in the architecture that the EHR system is located in two distinct hospitals on two separate platforms. Each healthcare stakeholder should use a smart contract or chain code to register in

one of the systems. In addition to uploading the EHR, the concerned physician should speak with the individual patient. The hash value of the EHR will be hashed and stored in the blocks. The patient will be assigned this EHR, signifying ownership. We have suggested dividing the EHR into online and offline sections. The patient's identifying attributes will be saved during the online data upload process and mapped to offline data. You can upload offline data to any database that is document-oriented. The patient's consent will be sent whenever any stakeholder in the same system requests access to the EHR. The patient may choose who has access to and how much of the EHR data is provided (George Karway, 2022).

For this study we applied a hash-lock based approach. This technique is utilized if the EHR is to be accessed from a different platform. Assume for the sake of clarity that we have techniques; A and B. A hash lock is created for the associated EHR in the event that any stakeholder from B requests access to A's patient EHR. B's stakeholder shares that hash lock. After then, the B stakeholder will be able to access the EHR. The infrastructure for exchanging electronic health records based on blockchain is depicted in Figure 1.

The government agency responsible for issuing and managing the electronic health records, the healthcare providers, and the patients. The patient is at the heart of the process when receiving medical treatment, and they can employ user agents and digital wallets to manage their electronic health records. They are in total control of their data, which includes virtual health records that are stored electronically. To verify the information, traditional healthcare practitioners need to receive access to the complete electronic health record. Both on-chain and off-chain storage are used for health data. Data saved in document-oriented databases are referred to as off-chain data. Cloud agents and wallets are used by the proposed BCIF-EHR blockchain-based interoperable architecture to store electronic health records, increase their accessibility, and secure communication with other healthcare organizations. Additionally, the framework stores publicly signed keys, electronically verifiable data, and the virtual certificates schemas for electronic health records for authenticity using blockchain technology. Revocation data are likewise stored on the blockchain to allow for open validation of the information's privacy-preserving characteristics. Government organizations interact with patients and healthcare providers both during and after the healthcare process by using institutional agents created especially for issuing and managing electronic health records. They also utilize these agents to confirm the legitimacy of electronic health records.

Qualifications are the cornerstone of the BCIF-EHR concept; they are a set of statements provided by the issuer about a patient. According to this criterion, digital badges, test results, prescriptions, and medical histories are all regarded credentials. Instead of employing humans to authenticate credentials as is typically done, the BCIFEHR method relies on standards, cryptography, distributed ledgers, and front-facing apps that allow machines to do it.

Four essential functions are carried out by the BCIF-EHR system. First, the patient completes a crucial task in the verifiable information exchange. Second, the organizations that create validated credentials—such as clinics, hospitals, and insurance companies—are the issuers in the BCIF-EHR context. The medical service provider serves as the relying or validating entity and is typically tasked with confirming the authenticity of the credentials they have been given. In conclusion, the information registry/recorder comprises of frameworks that keep track of the data needed to verify a certain credential.

After receiving data from the subject, a legitimate information issuer disseminates information on a particular patient. The patient provides identification for validation. The healthcare provider uses a conventional verification process to confirm the information by combining the credentials with legitimate data records, including the one containing the cryptographic keys of the issuers. This makes it possible for the regulator to carry out his duties without needing the healthcare provider to get in touch with the issuer for confirmation.

To use the electronic health record (EHR) system, patients and healthcare providers must register if they do not have a digital wallet, health record, or any virtual certificates. UML sequence diagrams are utilized in this instance to show the procedure. A government agency must complete a one-time bootstrapping step in order for registration to be permitted under the BCIF-EHR architecture. During this procedure, a public digital identity and its corresponding DID document are kept on a distributed ledger. Patients' and medical professionals' electronic health records can now be accessed and shared securely and swiftly thanks to this. A sequence diagram for the registration step is shown in Figure 2.

Patients can visit a nearby branch or use laptops or smartphones to access websites run by public agencies in order to exchange electronic medical records. In order to stop future partisan information sharing, patients establish a secret link in an online certificate that connects various credentials. In order to finish the exchange of electronic health records, patients can utilize the public digital identity that has been created to create an encrypted connection with the government agency. The subjects connect to the electronic health record cloud agent and scan their wallet applications to finish the process. The government agency receives a linking request from the electronic health records endpoint whenever a new public digital identity is generated. A linkage answer is delivered to the federal agency's wallet. Right

now, the patient can now securely share information with the government agency as they have established a secure link. The patients give the government agency the details about themselves that are required to validate their identities as they lack virtual certificates. Governmental organizations can confirm patients' physical identity details when they open accounts. Once the data has been verified and the patient has been identified, the government can provide the information to the patient. The terms and conditions for revocation of the credentials, an overview of the information to be accepted, and the expiration date are all included in the information given.

This permits individuals and healthcare professionals to efficiently receive personal health information while maintaining data confidentiality and integrity. A third party is not needed because the blockchain offers unchangeable data recordings. PHI information is collected from multiple healthcare institutions linked together via blockchain technology. With the help of our approach, the parties will be able to manage and gather PHI data with a single, highly effective view and be reasonably assured of the integrity of the datasets. The public key of the healthcare provider, the pairwise DID of the government organization, and the service endpoint that the patient or owner can use to get in touch with the organization are all contained in this connection request. After confirming the connection, the patient's or owner's digital wallet creates a pairwise DID and keys for the government agency. After receiving the connection response, the government agency's cloud agent/wallet forwards it to the interface. Thanks to their encrypted end-to-end relationship, the patient/owner can now safely exchange messages, public keys, VCs, and VPs with the government agency. Since the patient or identity owner has not yet gotten any VCs, they need to be verified. The patient or owner provides the required physical identity information on paper to the government agency by scanning it and emailing it or sending it through a newly established link. If the patient or owner creates an account, these physical identity details and medical records can be easily confirmed at a government agency branch. The government agency may provide a credential to the patient/owner edge user agent after data and patient/owner identification verification. Along with the credentials' expiration dates and revocation information, this credential offer also offers a preview of the data that has to be attested. After that, it is transferred in blinded form, together with the connection secret, to the government agency. The selective disclosure is permitted under this certificate. This implies that the owner/patient can merge claims from several VCs and only include the properties verified by the VC that the verifier needs.

In order to submit a request to the BCIF-EHR government agency, patients and healthcare providers who wish to share their electronic health records during the pre-contract phase must create a pairwise public digital identity. At this stage, information, VCs, public keys, and VPs can be shared between the patient and the government agency through a safe and impenetrable connection. Through their online wallet, patients provide the government agency the mandatory public digital identification of their electronic health records for authentication. The government agency's BCIF-EHR online entity publishes the EHR sharing request in the data records when the patient's identity has been confirmed. Healthcare practitioners can visit a physical location to directly identify the necessary EHR, or they can use smart devices to identify patients' EHRs in the government agency's online portal. The healthcare practitioner accesses the patient's electronic health data and then submits validation requests to the BCIF-EHR online government agency. The agency verifies the legitimacy of the credentials associated with the virtual certificates and provides the patients with the necessary proof of non-cancellation. When the BCIF-EHR online agent determines that the EHR validation procedure is finished, healthcare providers can release a credential that was provided to the patient in accordance with the formed linkage.

The healthcare practitioner will examine the patient's electronic health records and then send a verification request to the BCIF-EHR cloud agent. The agent will assess the veracity of the VPs connected to the VC and furnish the required evidence of non-revocation to the patients. Using the established connection, the healthcare provider can send a credential offer to the patient/owner end user agent once the BCIF-EHR cloud agent certifies that the EHR verification status is satisfactory.

An overview of the data that will be verified is provided by this credential offer, which includes details on the credential issuer, the VC's expiration date, and information about credential revocation. After confirming, the patient/owner gives the BCIF-EHR cloud agent the credential offer. The name of the credential issuer, the VC's expiration date, and details on its revocation will also be sent in this pre-agreement share request to the ledger.

The government agency BCIF-EHR online entity updates the database with the pre-contract demand to exchange electronic records, and it also notifies the patient/healthcare provider online agent about the EHR sharing procedure. Following notification from the government agency, the healthcare provider submits a legitimate request to grant access to the EHR to the government agency. The steps involved in creating certificates and transferring funds between banks are shown in Figure 3.

The online entity of the government agency sends a money transfer request that includes the public digital identity of the EHR. The online agent of the healthcare provider submits the virtual certificate of funds transfer and settlement information as soon as the funds are effectively settled. Furthermore, the government agency sends the virtual certificates with details about its online

portal and alerts the patient and the healthcare provider's online agents about efficient EHR exchange.

In this case, a patient with blockchain BNA is registered in hospital HA. Another hospital, HB, has a blockchain network powered by BNB. A hash key that has been agreed upon by BNA will be used by BNB in order to grant access to the patient's health record from HA for any healthcare stakeholder from HB. BNB can access the patient's medical record until and unless it has been locked. The same procedure will be followed if HA requests access to HB's medical record.

To ensure that the two frameworks could communicate with each other, blockchain technology was applied along with all of its requirements and rules. The two interoperable frameworks, HL7 and HIPAA, where the data is synchronized and accessible by either framework, now have heterogeneity because to blockchain technology. Users have diverse access to the framework, allowing them to edit and add new patients. The suggested method was created to help analysts and software architects follow health informatics guidelines when working on healthcare initiatives. The technique is included into a TIBCO plugin that is compatible with the HIPAA and HL7 standards. The method automates and formalizes data exchange between the two disparate frameworks. It contains examples of how to apply such profiles to the suggested framework as well as tool modifications for identifying and creating those profiles.

The suggested method may aid in the creation of HL7 implementation frameworks for diverse technologies, in addition to the obvious advantage of automatically generating implementation components from UML analysis classes. EJB, CORBA, or NET components that follow the HL7 semantics (class types, entities, and data types) can be included in any HL7 class (concept). Additionally, the same model-driven methodology can be easily used to create behavioral components (like the control classes in the example) that manage any HL7 message using the current HL7 XML schema definition (XSD) documents. An analogous approach might still be used to resolve the issue of harmonizing other health informatics standards that are not part of the HL7 specifications and incorporating them into the development process. Further research will be necessary to formalize the mappings and transformations of models. It comprises confirming that the model transformation complies with standards in terms of syntactic and semantic accuracy. The BCIF-EHR implementation details are shown in Table 1.

Results and Discussion

We have examined widely used interoperable EHR standards, such as SNOMED-CT, HL7, HIPAA, open EHR, and DICOM. HIPAA and HL7 standards are two examples of these standards. We have examined the significance of blockchain technology in the healthcare industry based on the literature review. The poll also contributed to the analysis of HL7 and HIPAA's significance. Together with other current frameworks, we have proposed the BCIF-EHR framework. We have outlined the advantages of our framework over others. Interoperability between HL7 and HIPAA, the two EHR standards, is the main focus of the proposed architecture. Through the use of blockchain technology, this interoperability aids in the creation of a novel combination system that combines the two suggested frameworks for the sharing of services and data. We also suggested cross-chain EHR exchange in our system. Ethereum to Hyperledger Fabric and vice versa EHR exchange is possible. Interoperability has been achieved between the two frameworks, allowing processed data to be accessible from either platform. To ensure dependability, a backup copy of the information is stored and can be accessed when necessary. This combined system complies with the most recent blockchain conventions and adheres to all fundamental blockchain technology guidelines. The proposed architecture incorporated a range of strategies for maintaining privacy while facilitating data sharing. Finding a specific patient with just their data is really difficult. We reduce the likelihood of unauthorized access to the patient private data by using encryption techniques on the data that is stored on the blockchain inside the proposed framework. The main purpose of this system was to maintain EHRs, which keep data private yet provide external access, and to safeguard data privacy. We will investigate whether implementing the differential privacy model is feasible in the future and see if noise and blockchain size are related. We suggest an effective and safe blockchain-based architecture for EHR exchange and upkeep. Blockchain-based EHR interoperability was an additional choice. Patients alone will have authority over their health data under this patient-centric approach. By contrasting popular blockchain interoperable products on the market according to their interoperability standards, this article discusses the importance of BCIF-EHR. It is clear from the comparisons that none of the BCIF-HER values are fully complied with by any of the existing BCIF-EHR solutions. The stages and requirements for BCIF-EHR utilization in the electronic health record system are also identified in this study. The report offers a thorough analysis of the implementation of fully functional interoperable BCIF-EHR electronic health record systems by healthcare institutions. The BCIF-EHR model and architectural elements have been presented in this article, together with a summary of the BCIF-EHR components required to develop BCIF-EHR solutions and how BCIF-EHR interoperability requirements can be met. In order to address issues with traditional electronic health record structures, this paper concludes by discussing the implementation of BCIF-EHR in the electronic health record model. The primary limitation of this research, however, is that the proposed model has not been implemented well and, as a result,

Table 1. Implementation details of BCIF-EHR systems.

Sl. No.	Steps	Summary
1	Review of health policies and EHR development.	Study of the guidelines related to the health policies in EHR frameworks.
2	Meta-analysis guidelines and systematic review	To identify the use and application of blockchain-based technology in electronic healthcare systems.
3	Review of blockchain technology	To identify the pros and cons of blockchain technology in EHR frameworks.
4	I am using a public blockchain	To study how blockchain technology allows controlled access to public health-related data
5	Review of EHR adoption	Study the flow and growth of EHR-based systems in health care
6	Review and implementation of security techniques in EHR frameworks	Study the advanced security techniques used in the EHR frameworks and choose the best
7	Previous work in EHR interoperability	To review the previous efforts to achieve interoperability between EHR frameworks
8	Scope of EHR interoperability	To study the whole scenario to forecast the future scope of interoperability in EHR frameworks
9	Effective interoperability framework	EHR networks established and maintained at regional and national levels worldwide provide effective and standard access to and operational use of large amounts of health data
10	Blockchain-based framework	Smart techniques are utilized in an interoperable blockchain-based EHR architecture for mystification and knowledge control, with the sophisticated methodology used for additional security

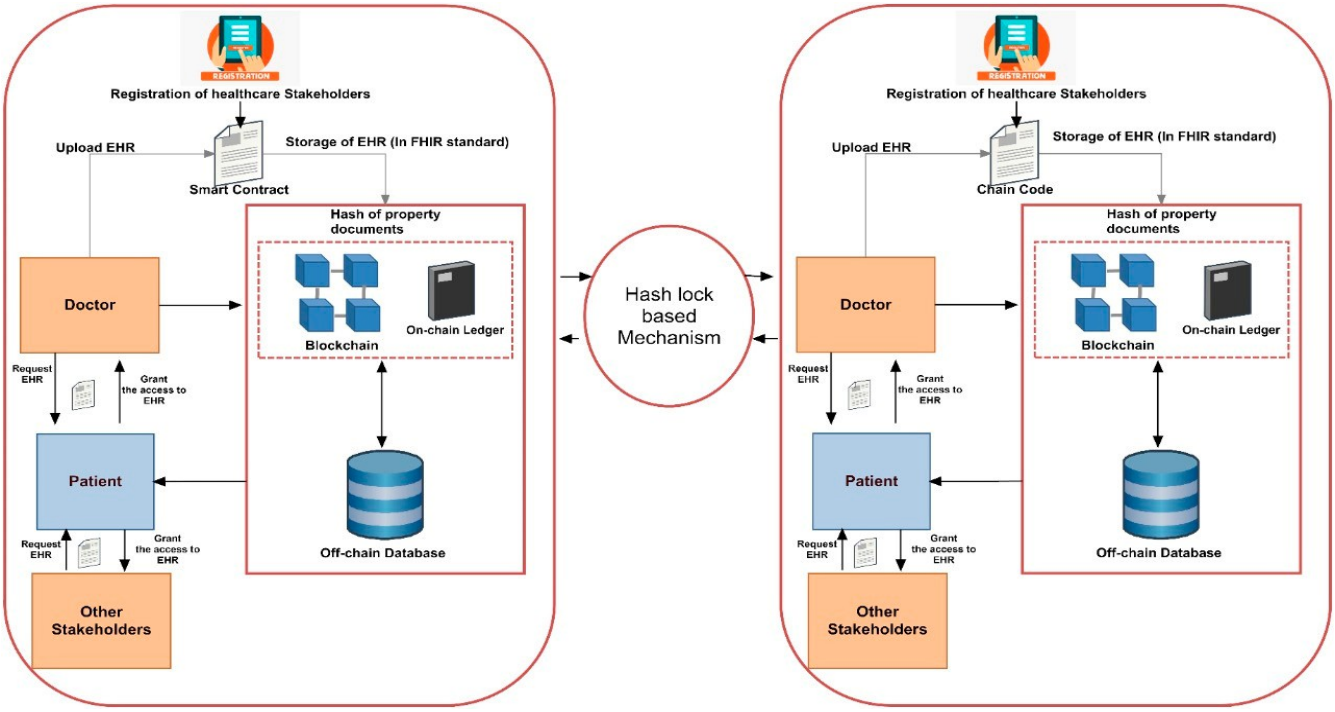

Figure 1. BCIF-EHR-Based Electronic Health Record Sharing Framework.

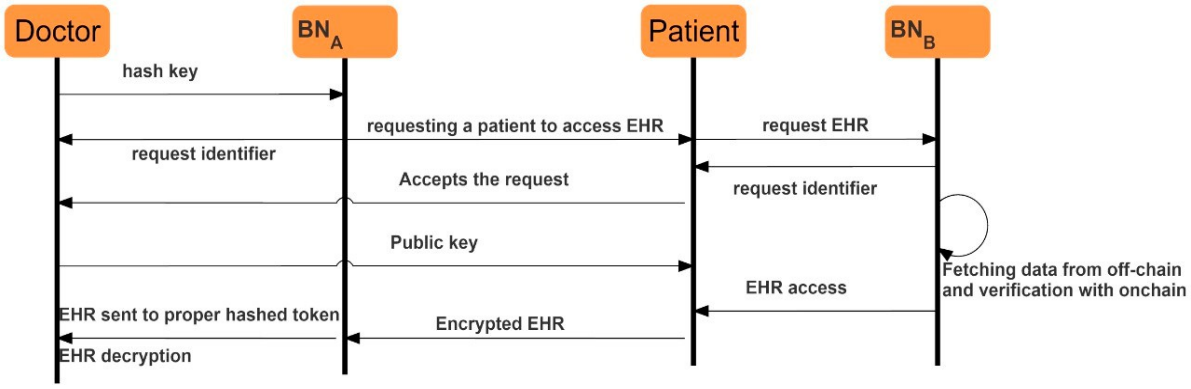

Figure 2. Sequence diagram for registration phase.

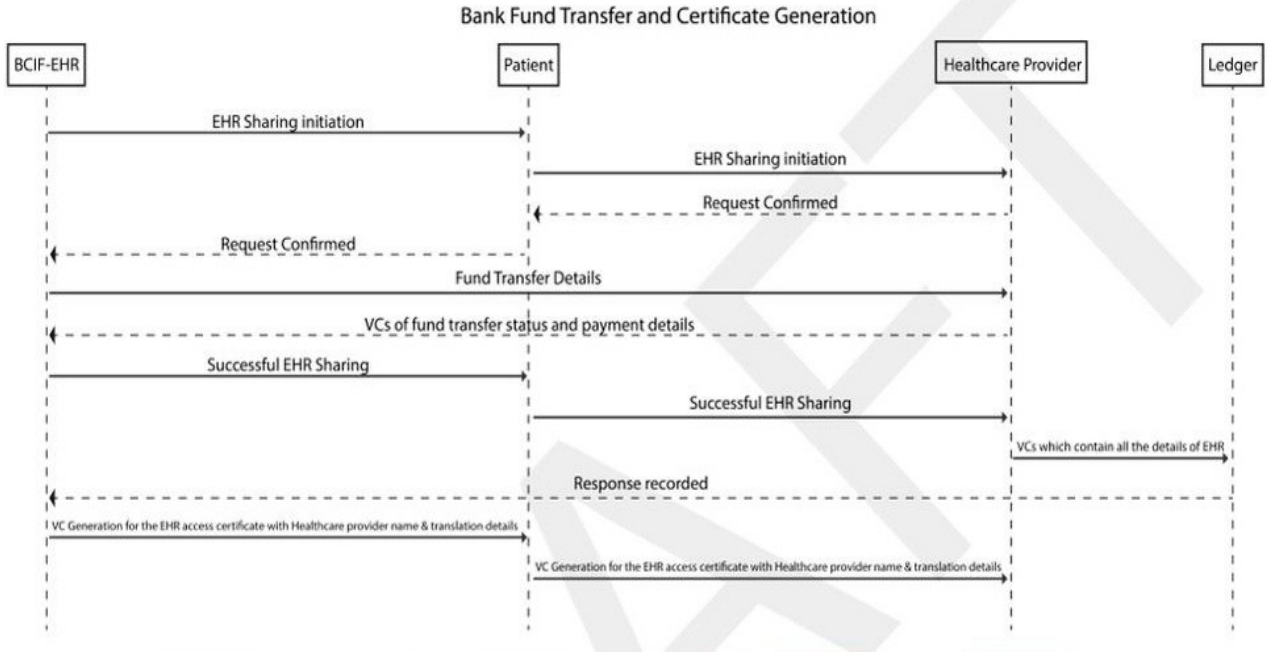

Figure 3. Bank fund transfer and certificate generation.

cannot be applied to actual users of electronic health record systems. As a result, this article suggests additional actions, like government and stakeholder involvement in evaluating the suitability of BCIF-EHR and technology models and legislative, regulatory, and other stakeholders in the electronic health record system acknowledging the innovative idea of BCIF-EHR.

The goal of the suggested framework is to encourage scalability across different systems. To save storage capacity, only the hashes and little EHRs on the blockchain need to be kept. Moreover, when performing private patient transactions, a small number of nodes require validated transactions with data hashes. As a result, mining and storage expenses on the blockchain will be further decreased. On the other hand, the CLC search time would surely increase as more users sign up for the system. Because of this, unique and innovative methods are required to effectively search CLC using large local databases.

The results of this study demonstrated the compatibility of the two EHR frameworks, HL7 and HIPAA. This interoperability contributes to the creation of a special hybrid system that combines the two suggested frameworks with data sharing and blockchain technology. Interoperability between the two frameworks allows processed data to be accessed from either platform. To ensure dependability, a backup copy of the information is stored and can be accessed when necessary. This combined system complies with the most recent blockchain conventions and adheres to all fundamental blockchain technology guidelines.

The proposed architecture incorporated a range of strategies for both data exchange and privacy preservation. Utilizing just their data to follow a particular patient requires a lot of work. We used encryption methods to reduce the possibility of unauthorized access to the patient private data kept on the blockchain within the recommended scope.

An electronic version of a patient's medical history is called an electronic health record, or EHR. Numerous issues related to data processing and security have been rectified. EHR interoperability is still hampered by the absence of standards and regulations surrounding file sharing, and using the blockchain approach presents challenges that healthcare administrators need to take seriously. Integrating EHR reduces the possibility of errors and hackers and is essential for any healthcare provider using it. Adoption of EHR standards is necessary for compliance with certain legal requirements. The study's concerns and challenges center on blockchain technology and EHR interoperability. Furthermore, a workable interoperability solution is provided. This study contributes to the discussion of related challenges and solutions in the areas of EHR rollout, data management, and patient information. It was found that the advantages of a creative, blockchain-based interoperability architecture worked. Currently, there isn't a single compatible system in use in the real world. Therefore, this research cannot be meaningfully compared to any current systems. It is unique, founded on a novel concept, and has the capacity to be preserved and developed further for the advancement of the healthcare sector.

Conclusion

Putting the BCIF-EHR architecture into practice in actual electronic health record systems to assess how well it works and how efficient it is in terms of interoperability and data sharing. Examining the privacy and security consequences of integrating BCIF-EHR into electronic health record systems. This can entail researching the framework's possible weaknesses and creating countermeasures. Creating techniques for linking BCIF-EHR with other electronic health record systems that are currently in use, even if they are not blockchain-based. Examining BCIF-EHR's scalability, especially as more healthcare institutions adopt the framework and share a greater amount of data. Investigating the automation of specific procedures, like permissions and data sharing agreements, through the use of smart contracts in BCIF-EHR. Analyzing the legal and regulatory ramifications of integrating BCIF-EHR in electronic health record systems and creating compliance standards.

Author contributions

M.H. is the principal author, setting objectives, developing the hypothesis, performing data analysis, and final revision. J.S. wrote the abstract, methods, and materials. B.M. wrote the introduction. T.B. conducted the literature review. R.R.I. wrote the results and discussion. M.M.I. collected data. M.R.K. did the final revision. M.F.I. wrote the significance, keywords, and conclusion.

Acknowledgment

We sincerely thank all participants for their valuable time and involvement in this study. We also extend our gratitude to the anonymous reviewers and editors for their insightful feedback and prompt responses.

Competing financial interests

The authors have no conflict of interest.

References

Aaron M. Gamino, A. M. G. (2021, September 30). The impact of the consolidated omnibus reconciliation act of 1985 on young adult health insurance coverage: Applied Economics: Vol 54 , No 17—Get Access. https://www.tandfonline.com/doi/full/10.1080/00036846.2021.1983142

Adane, K., Gizachew, M., & Kendie, S. (2019). The role of medical data in efficient patient care delivery: A review. Risk Management and Healthcare Policy, Volume 12, 67–73. https://doi.org/10.2147/RMHP.S179259

Adel, E., El-Sappagh, S., Barakat, S., & Elmogy, M. (2019). Chapter 14—A unified fuzzy ontology for distributed electronic health record semantic interoperability. In N. Dey, A. S. Ashour, S. J. Fong, & S. Borra (Eds.), U-Healthcare Monitoring Systems (pp. 353–395). Academic Press. https://doi.org/10.1016/B978-0-12-815370-3.00014-1

Adel, E., Sappagh, S. E., Barakat, S., & Elmogy, M. (2020). A semantic interoperability framework for distributed electronic health record based on fuzzy ontology. International Journal of Medical Engineering and Informatics, 12(3), 207. https://doi.org/10.1504/IJMEI.2020.107081

Adesh Mukati, A. M. (2023, May 30). D40900412423. Indian Journal of Cryptography and Network Security (IJCNS). https://www.ijcns.latticescipub.com/portfolio-item/d40900412423/

Amit Doegar, S. R. M. S. (2021, May 21). Data Collection and Processing in Health Care | SpringerLink. https://link.springer.com/chapter/10.1007/978-981-16-0415-7_4

Angelika Haendel, M. A. (2022, July 26). The View of Health Information Managers (HIM): Strategic Insights Through Data Analytics | SpringerLink. https://link.springer.com/chapter/10.1007/978-3-030-91237-6_10

Bigini, G., Zichichi, M., Lattanzi, E., Ferretti, S., & D'Angelo, G. (2023). On the Decentralization of Health Systems for Data Availability: A DLT-based Architecture. 2023 IEEE 20th Consumer Communications & Networking Conference (CCNC), 372–377. https://doi.org/10.1109/CCNC51644.2023.10059701

Capuzzo, M., Zanella, A., Zuccotto, M., Cunico, F., Cristani, M., Castellini, A., Farinelli, A., & Gamberini, L. (2022). IoT Systems for Healthy and Safe Life Environments. 2022 IEEE 7th Forum on Research and Technologies for Society and Industry Innovation (RTSI), 31–37. https://doi.org/10.1109/RTSI55261.2022.9905193

Daniel J. Solove, D. J. S. (2020). HIPAA Mighty and Flawed: Regulation has Wide-Reaching Impact on the Healthcare Industry. Journal of AHIMA, 84(4), 30–31.

Erdoğdu, M., & Ünüsan, Ç. (2022). The Importance and Use of Blockchain Technology in International Payment Methods. International Journal on Engineering, Science and Technology, 4(3), Article 3. https://doi.org/10.46328/ijonest.146

Fabacher, T., Sauleau, E.-A., & Leclerc Du Sablon, N. (2023). Evaluating the Portability of Rheumatoid Arthritis Phenotyping Algorithms: A Case Study on French EHRs. In Caring is Sharing – Exploiting the Value in Data for Health and Innovation (pp. 768–772). IOS Press. https://doi.org/10.3233/SHTI230263

Fatima, S., Aun, M., Hussain, S., Din, B. ul, Sajjad, W., Shahzadi, N., & Jameel, R. (2022). A Secure BlockChain Framework for IoT Healthcare. 2022 International Conference on Emerging Trends in Electrical, Control, and Telecommunication Engineering (ETECTE), 1–6. https://doi.org/10.1109/ETECTE55893.2022.10007122

Gandhi, J., & Walker, I. A. (2022). Patient monitoring techniques. Surgery - Oxford International Edition, 40(6), 370–377. https://doi.org/10.1016/j.mpsur.2022.03.018

Ganta, T., Appel, J. M., & Genes, N. (2023). Patient portal access for caregivers of adult and geriatric patients: Reframing the ethics of digital patient communication. Journal of Medical Ethics, 49(3), 156–159. https://doi.org/10.1136/medethics-2021-107759

George Karway, M. A. G. (2022, December 1). My Data Choices: Pilot evaluation of patient-controlled medical record sharing technology—George Karway, Julia Ivanova, Tina Kaing, Michael Todd, Darwyn Chern, Anita Murcko, Kazi Syed, Mirtha Garcia, Michael Franczak, Mary J Whitfield, Maria Adela Grando, 2022. https://journals.sagepub.com/doi/10.1177/14604582221143893

Govindaraj, V., & Murugan, S. D. A. (2023). An Early Warning Smart Healthcare Kit to Avoid Road Accidents. 2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS), 1–5. https://doi.org/10.1109/ICICCS56967.2023.10142341

Hoang, H. D., Duy, P. T., Tien, N. T., Thu Hien, D. T., & Pham, V.-H. (2022). A Blockchain-based approach and Attribute-based Encryption for Healthcare Record Data Exchange. 2022 RIVF International Conference on Computing and Communication Technologies (RIVF), 65–70. https://doi.org/10.1109/RIVF55975.2022.10013886

Khan, F., Khan, S., Tahir, S., Ahmad, J., Tahir, H., & Shah, S. A. (2021). Granular Data Access Control with a Patient-Centric Policy Update for Healthcare. Sensors, 21(10), Article 10. https://doi.org/10.3390/s21103556

Kulüke, M., Kindermann, S., & Kölling, T. (2023). IPFS Pinning Service for Open Climate Research Data (EGU23-6311). EGU23. Copernicus Meetings. https://doi.org/10.5194/egusphere-egu23-6311

Kumar, A., Kumar Sah, B., Mehrotra, T., & Rajput, G. K. (2023). A Review on Double Spending Problem in Blockchain. 2023 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES), 881–889. https://doi.org/10.1109/CISES58720.2023.10183579

Mahendra Pratap Singh, M. P. S. (2023, April 17). Role of Access Control in Information Security: A Security Analysis Approach | IntechOpen. https://www.intechopen.com/chapters/86916

Maryam Farhadi, H. S. (2022). Assessing HIPAA Compliance of Open Source Electronic Health Record Applications | IGI Global. https://www.igi-global.com/gateway/chapter/309039

Micelle J. Haydel, P. F. E. (Director). (2021, February 4). Health Insurance Portability and Accountability Act. StatPearls Publishing. https://typeset.io/papers/health-insurance-portability-and-accountability-act-zlzig9kezk

Nobari, A. H., Srivastava, A., Gutfreund, D., & Ahmed, F. (2022). LINKS: A dataset of a hundred million planar linkage mechanisms for data-driven kinematic design (arXiv:2208.14567). arXiv. https://doi.org/10.48550/arXiv.2208.14567

Pandey, P., & Litoriya, R. (2020). Implementing healthcare services on a large scale: Challenges and remedies based on blockchain technology. Health Policy and Technology, 9(1), 69–78. https://doi.org/10.1016/j.hlpt.2020.01.004

Patel, P., & Barton, J. (2023). Administrative Inefficiency and The United States Healthcare System. Journal of Student Research, 11(3). https://doi.org/10.47611/jsr.v11i3.1674

Priya, J., & Palanisamy, C. (2022). Novel Block Chain Technique for Data Privacy and Access Anonymity in Smart Healthcare. Intelligent Automation & Soft Computing, 35(1), 243–259. https://doi.org/10.32604/iasc.2023.025719

Quasim, M. T., Mobarak, M. M., Nisa, K. U., Meraj, M., & Khan, M. Z. (2023). Blockchain-based Secure Health Records in the Healthcare Industry. 2023 7th

International Conference on Trends in Electronics and Informatics (ICOEI), 545–549. https://doi.org/10.1109/ICOEI56765.2023.10125802

Rudzidatul Akmam Dziyauddin, F. A. R. (2023, April 7). Sustainability | Free Full-Text | Blockchain-Based Framework for Interoperable Electronic Health Records for an Improved Healthcare System. https://www.mdpi.com/2071-1050/15/8/6337

S. Farjana Farvin, R. Nithyashree, R. Sivanandhini, & D. R. Subasri. (2023). U-MEDCHAINA Blockchain Based System for Medical Records Access and Permissions Management. International Journal of Advanced Research in Science, Communication and Technology, 297–303. https://doi.org/10.48175/IJARSCT-9133

Singh, S., Gupta, S., & Indu. (2023). MedEHR-Electronic health Record using Blockchain. 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN), 58–62. https://doi.org/10.1109/CICTN57981.2023.10141053

Sosu, R. N. A., Quist-Aphetsi, K., & Nana, L. (2019). A Decentralized Cryptographic Blockchain Approach for Health Information System. 2019 International Conference on Computing, Computational Modelling and Applications (ICCMA), 120–1204. https://doi.org/10.1109/ICCMA.2019.00027

Suljanović, N., Souvent, A., Taylor, G., Radi, M., Cantenot, J., Lambert, E., & Morais, H. (2019). Design of Interoperable Communication Architecture for TSO-DSO Data Exchange. 2019 IEEE Milan PowerTech, 1–6. https://doi.org/10.1109/PTC.2019.8810941

Sundvall, E., Terner, A., Broberg, H., & Gillespie, C. (2019). Configuration of Input Forms in EHR Systems Using Spreadsheets, openEHR Archetypes and Templates. In MEDINFO 2019: Health and Wellbeing e-Networks for All (pp. 1781–1782). IOS Press. https://doi.org/10.3233/SHTI190645

Swapnil Singh, D. K. (2022). Medical IoT: Opportunities, Issues in Security and Privacy—A Compreh. https://www.taylorfrancis.com/chapters/edit/10.1201/9781003239895-6/medical-iot-opportunities-issues-security-privacy-comprehensive-review-deepa-krishnan-swapnil-singh

Taherdoost, H. (2023). The Role of Blockchain in Medical Data Sharing. Cryptography, 7(3), Article 3. https://doi.org/10.3390/cryptography7030036

Vishal Patel, V. P. (2019). A framework for secure and decentralized sharing of medical imaging data via blockchain consensus—Vishal Patel, 2019. https://journals.sagepub.com/doi/10.1177/1460458218769699

Walid, R., Joshi, K. P., & Geol Choi, S. (2023). Semantically Rich Differential Access to Secure Cloud EHR. 2023 IEEE 9th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), 1–9. https://doi.org/10.1109/BigDataSecurity-HPSC-IDS58521.2023.00012

Xue, L., Liu, D., Huang, C., Shen, X., Zhuang, W., Sun, R., & Ying, B. (2022). Blockchain-Based Data Sharing With Key Update for Future Networks. IEEE Journal on Selected Areas in Communications, 40(12), 3437–3451. https://doi.org/10.1109/JSAC.2022.3213312

Zandvakili, I., & Pulaski, M. (2023). A phenotypic approach to obesity treatment. Nutrition in Clinical Practice, 38(5), 959–975. https://doi.org/10.1002/ncp.11013