Implementing Blockchain for Secure Electronic Medical Certifications: An Analytical Study

Khalil Youssef[1,*], Tawhib Amer[2], Yasmine Ibrahim[3,*], Doaa Abdo Othman Qasem[4], Ozgu Can[5], and Fursan Thabit[5]

[1] Department of Information Technology, Faculty of Engineering, Taiz University
[2] Department of Computer Science, Faculty of Engineering, Taiz University
[3] Department of information system Management, School of trade and Science management, the Civilization University, Sana'a Yemen.
[4] Department of Information System Management, Sanaa University, Sana'a Yemen
[5] Department of Computer Engineering, Faculty of Engineering Ege University, Turkey

* Corresponding author. Email: yasmin.ib2014@gmail.com (K.Y.)

Manuscript received March 1, 2024; accepted March 27, 2024, published April 24, 2024
DOI: 10.18178/IJBTA. 2024.2.1.25–37

Abstract: The assessment of Electronic Medical Certification (EMC) plays a pivotal role in modern healthcare infrastructures, serving as a comprehensive repository for patients' medical histories. Given the inherent challenges related to security and privacy within electronic medical certification systems, there exists a critical need to address the issues of system incompatibility that hinders data sharing among healthcare providers. This not only raises concerns over potential data breaches but also underscores the diminished control patients have over their own medical information. Blockchain technology, known for its significance in securing confidential corporate data, offers a promising solution to redefine the management of medical records. By leveraging a decentralized, peer-to-peer network, blockchain has the potential to transform the security dynamics and enhance the integrity of healthcare record exchanges. This research introduces a novel, lightweight blockchain framework, utilizing the Flask technology, aimed at securely storing and presenting patient statuses and detailed logs of disease diagnosis transactions. Within this envisioned blockchain architecture, patients are represented as unique assets, with their historical health data forming the individual blocks of the chain. The findings of this study suggest that by adopting blockchain technology, healthcare entities can surmount existing barriers, paving the way for a more effective and patient-focused electronic medical certification system. Such advancements promise to fortify the Electronic Health Record (EHR) systems, ensuring a secure, transparent, and efficient healthcare delivery model.

Keywords: blockchain, transaction, Electronic Medical Certification (EMC), cryptography, decentralized

1. Introduction

The healthcare landscape is on the cusp of a digital revolution, driven by the advent of electronic health technologies and the shifting needs of an aging population. This digital transformation is expected to minimize the reliance on physical interventions, reserving them for only the most critical cases. The conceptualization of public health systems as networks reveals a complex web of interactions among various stakeholders, including both altruistic non-profit organizations and profit-driven private sector entities. Central to this transformation are Electronic Health Records (EHRs), which embody real-time, patient-centric databases that provide secure, encrypted access to patient information for authorized personnel [1].

The origins of blockchain technology can be traced back to the late 1980s and early 1990s, but it was not until the emergence of bitcoin in 2008 that the concept of a secure, decentralized ledger system entered the mainstream consciousness. Blockchain serves as a foundational technology that ensures the integrity and transparency of transactions across a distributed network. In the context of healthcare, blockchain technology promises to address some of the most pressing security concerns, including the risk of cyberattacks that have increasingly targeted vulnerable healthcare data [2].

The decentralized nature of blockchain facilitates a system where data integrity is safeguarded against unauthorized access and manipulation. This technological innovation holds the potential to revolutionize patient data management, offering a level of security and control previously unattainable with traditional database systems. The key to blockchain's applicability in healthcare lies in its ability to provide a secure, immutable record of medical information, thereby empowering patients and healthcare providers alike [3].

With the healthcare system's digitalization, the management of electronic medical certification emerges as a critical area of focus (Fig. 1). Traditional methods of storing and accessing patient information are fraught with vulnerabilities, including the risk of data breaches and unauthorized access. Blockchain technology, with its unique attributes of data immutability, decentralized control, and enhanced security, presents a viable solution to these challenges. It not only secures medical records against tampering but also decentralizes control, thereby eliminating the single point of failure associated with central authority systems [4].

The expanded introduction underscores the transformative potential of blockchain technology in the healthcare sector, setting the stage for a detailed exploration of its applications and benefits. By addressing the vulnerabilities inherent in traditional patient information management systems, blockchain technology offers a path toward a more secure, efficient, and patient-centric healthcare ecosystem [5].

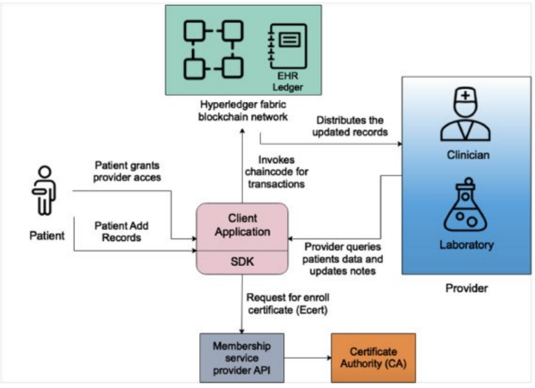
EHR
Ledger
Hyperledger fabric blockchain network
Distributes the updated records
Clinician
Invokes chaincode for transactions
Patient grants provider acces
Patient
Patient Add Records
Client Application
SDK
Provider queries patients data and updates notes
Laboratory
Provider
Request for enroll certificate (Ecert)
Membership service provider API
Certificate Authority (CA)

Fig. 1. Electronic Medical Certification (EMC).

The healthcare industry has notably revolutionized the healthcare economy, highlighting the importance of trusted sharing of patient health-related data for success in digital healthcare [6]. Ensuring system integrity is paramount, as any security flaws could erode patient trust in the e-healthcare market. Networks within this context allow for individual or multiple participants to own and manage nodes, which are differentiated by their functionalities as outlined in the sections below.

1.1. Distributed Ledger

A Distributed Ledger (DL) is utilized to record the data of each node, capturing the Blockchain's (BC) current state while storing transaction data duplicates. This mechanism is crucial in the blockchain architecture, with every record associated with a hash value, organized within the DL as a Merkle tree [7].

1.2. Symmetric Cryptography

Symmetric cryptography is defined by the use of identical keys for encryption and decryption, contrasting with asymmetric cryptography, where keys are unique and distinct. Our framework employs asymmetric cryptography to bolster security beyond what symmetric methods can offer [8].

1.3. Consensus Mechanism

A consensus mechanism is a process where a majority (at least 51%) of the network's peers must concur to validate a transaction, often referred to as the 51% rule in blockchain contexts.

1.4. P2P Network

Peer-to-Peer (P2P) Networks describe a system of computers or devices connected without a central server, relying on a consensus algorithm to validate decisions by a majority of nodes within the network [9]. The rise of cryptocurrencies like Ethereum and Bitcoin has propelled blockchain research into a focal point of interest. Blockchain's capacity for decentralized, immutable, and trustworthy data storage and sharing eliminates the need for intermediaries, facilitating direct transaction verification within the network [10]. Blockchain simplifies the process of sharing Personal Health Records (PHR) by leveraging the combined computational power of the network, enhancing both speed and computational capabilities. It supports various applications and processes, including consensus protocols, hashing, P2P topology, immutable ledgers, and mining, governed by smart contracts.

1.5. Hyperledger Fabric

Hyperledger Fabric, a tool based on Linux for cross-organizational networks, supports customizable modules like encryption, identity management, consensus protocols, and membership services. Known as a consortium blockchain network, it incorporates diverse nodes, smart contracts (or chaincode), and a ledger that records transactions and state databases. This paper's contributions are multifaceted, introducing a novel cross-domain blockchain framework for healthcare record access that includes:

1. The utilization of a certificate authority for public and private key management across domains, emphasizing the necessity for organizations to have intermediate CAs.
2. The implementation of attribute-based access control within the cross-domain blockchain for flexible adaptation.
3. The application of Hyperledger Fabric to support consortium blockchain networks in healthcare, accommodating both private and public systems.
4. The introduction of a ring signature for signature endorsement, offering a lightweight yet secure solution.

The paper is structured as follows: Section 2 reviews related literature. Section 3 discusses problem formulation and introduces the proposed framework. Section 4 details the methodology and algorithms. Section 5 describes the experimental setup, dataset, results, and discussions. Section 6 concludes the paper and outlines future research directions.

2. Related Work

The exchange of medical information, inherently critical and highly sensitive, poses substantial challenges within the healthcare system due to the risks of data exposure or tampering during operational processes. The necessity for medical institutions to access a patient's history for improved treatment outcomes exposes the insufficiency of current systems in providing secure, private, and effective management and sharing of medical records. This situation underscores an urgent need for innovation in healthcare systems to enable the secure sharing of patients' sensitive medical information among various stakeholders without the risks of unauthorized disclosure or manipulation. It is imperative to establish an efficient data access mechanism that bolsters security and guarantees patient medical information access solely to authorized participants, ensuring patients retain full control over who can access their data.

In recent years, the application of blockchain technology within the healthcare sector has garnered significant attention. Blockchain is poised to address the limitations of current electronic medical records systems, enhancing the treatment process and enabling secure remote access to patient medical information, thus safeguarding healthcare data privacy. Our research has delved deeply into blockchain technology and its potential utility in healthcare, specifically for managing electronic medical records. Although much of the existing literature adopts a theoretical stance, a few studies have explored the actual implementation of blockchain-based medical record systems.

Murugan *et al.* [11] introduced a conceptual framework for accessing and sharing electronic health records, leveraging blockchain and smart contracts to propose a decentralized healthcare platform. This platform aims to improve the preservation of patients' medical records and provide an efficient access mechanism. Li *et al.* [12] developed a blockchain-based system focused on the preservation of electronic medical records, prioritizing patient privacy and offering a dependable solution for record storage while ensuring data verifiability and integrity. Their prototype, built on the Ethereum platform—a permissionless blockchain—highlights the practical application of these concepts. Xue *et al.* [13] discussed a medical data sharing model grounded in blockchain technology, outlining the system's principles and components, despite facing implementation challenges. MedRec, as proposed by Azaria *et al.* [14], represents another implementation of a blockchain-based medical record management system utilizing the Ethereum blockchain. This system employs a Proof of Work (PoW) consensus algorithm, which, due to its resource-intensive nature, is considered a costly solution for mining operations. In the realm of blockchain applications within healthcare and data management, recent research has paved the way for innovative frameworks and systems aimed at enhancing security, privacy, and efficiency. Chen brought a novel perspective to evaluating performance parameters specifically within the Hyperledger Fabric framework, showcasing the potential for improved operational efficiency in blockchain applications. Chakraborty *et al.* [15] ventured into the cloud, proposing a blockchain-based framework designed for enhanced scalability and security in data management. A pivotal development in ensuring the security of clinical records is highlighted by Yazdinejad *et al.* [16], where the design of a prototype for a cross-domain access control system introduces a more efficient means of safeguarding healthcare information. This system, identified as coarse-grained access control, though criticized for its lack of precision, marks a significant step towards robust security measures in clinical data management. The exploration of healthcare information exchange is furthered in [17], where authors delve into mechanisms for storing and sharing vast amounts of healthcare-related data. In an effort to optimize transaction response times within the healthcare sector, Jiang *et al.* [18] introduces a fairness-dependent data packing strategy for Industrial IoT environments, leveraging Permissioned Blockchains to ensure equitable data processing. Privacy and efficiency in blockchain applications receive attention from [19], discussing the challenges and solutions related to conducting multi-keyword searches over encrypted data. This research underscores the importance of balancing search functionality with privacy preservation in encrypted blockchain environments. Shen et al. revisit the concept of coarse-grained access control, echoing the sentiments of in advocating for a system that, despite its lack of granularity, aims to bolster the security framework for clinical records. Lazaroiu and Roscia [20] contribute to this discourse by designing a clinical data exchange system founded entirely on blockchain technology, incorporating a series of verification mechanisms to elevate the security and privacy of healthcare systems. Privacy management within healthcare data sees innovative approaches from [21], proposing a model that leverages blockchain technology to enhance data privacy and management. Sengupta *et al.* [22] further this initiative by developing a blockchain-based health information system, focusing on securing privacy across the healthcare ecosystem. These contributions collectively signal a forward-moving trajectory in blockchain research, emphasizing security, privacy, and efficient data management as cornerstone elements in the evolution of healthcare systems. As seen the study by [23–33] many cryptography algorithms were applied in for data security in medical health

3. Methods and Material

This research explores the application of blockchain technology across three proposed reference models, highlighting its role as a foundational digital ledger technology. Blockchain's unique attribute lies in its ability to digitally store data blocks in a manner that renders them nearly immutable. The term "blockchain" originates from the cryptographic signatures that link (or "chain") one block to another. Utilizing distributed networks, consensus algorithms are employed to determine which transactions should be recorded, enabling the data within the ledger to be disseminated and accessed by any authorized party. This technology is revolutionary in its elimination of the need for a trusted third party, thereby ensuring the integrity and privacy of each recorded transaction.

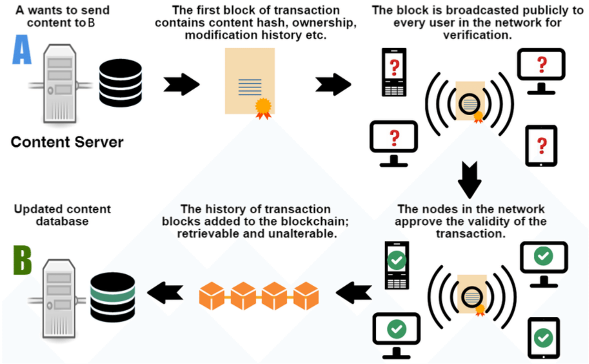
A wants to send content to B
The first block of transaction contains content hash, ownership, modification history etc.
The block is broadcasted publicly to every user in the network for verification.
A
Content Server
?
Updated content database
The history of transaction blocks added to the blockchain; retrievable and unalterable.
The nodes in the network approve the validity of the transaction.
B

Fig. 2. Fundamental principle of blockchain.

The core operation of blockchain technology is illustrated in Fig. 2 which outlines the fundamental principles underpinning this innovative digital ledger system.

- **Node**: In the blockchain ecosystem, a node refers to any computer that participates in the blockchain network, capable of sending and receiving transactions. A "full node" is a device that contains a complete copy of a blockchain's data, allowing it to fully verify transactions independently.
- **Transaction:** The basic unit of data storage in a blockchain is known as a transaction. Transactions are grouped into blocks, which are then validated through consensus mechanisms and disseminated across all network nodes.
- **Chain:** The blockchain itself is a sequence of blocks linked in a specific order through digital signatures. These signatures, created using public key encryption, are attached to digitally transmitted documents to verify the authenticity of their contents.
- **Record:** Within a blockchain network, a record pertains to the information provided by an individual or device to a smart contract. This information can be used to verify a particular event or outcome.
- **Smart Contract:** Distinguished from traditional contracts, a smart contract is a software program whose terms are encoded in machine-readable language rather than written text. These contracts execute coded procedures automatically upon the fulfillment of predefined conditions.

Blockchain's capacity to securely and transparently manage data without the need for central oversight presents a transformative approach to digital information management. Through the implementation of smart contracts, blockchain technology facilitates automated, secure, and direct interactions between parties, setting a new standard for digital transactions and record-keeping in various sectors.

4. Proposed Work

Blockchain technology offers a transformative approach to managing public health data during infectious disease outbreaks. Medical departments and government bodies face significant challenges in tracking health data, where blockchain can play a pivotal role in ensuring data is decentralized and securely managed.

Additionally, e-patient data management presents an opportunity for blockchain to revolutionize interoperability, data standards, security, privacy, scalability, and e-governance.

4.1. Blockchain Terminologies

In blockchain architecture, a block comprises several key components: a hash of the previous block, a timestamp, a nonce, and data from one or more transactions. These elements undergo cryptographic processing to generate a unique hash for each block, serving as digital fingerprints for blockchain transactions. The interconnected nature of blocks through these hashes ensures the chain's immutability and secures the data within each block through cryptography.

Transactions on the blockchain are secured with unique private keys known only to the transaction participants. Encryption is applied using the private key during transaction creation, ensuring the transaction's confidentiality. Public keys allow for the decryption and verification of transaction contents by recipients, maintaining the integrity of the data and indicating any tampering attempts through invalid digital signatures.

The decentralized nature of blockchain, devoid of any central controlling authority, enhances the impartiality, efficiency, and security of the system.

4.2. Electronic Medical Certification Using Blockchain

Blockchain technology could vastly improve the Electronic Medical Certification (EMC) process. By facilitating secure data sharing between healthcare providers using patient-specific private keys, blockchain ensures the protection of sensitive healthcare information. Each healthcare institution connected to the blockchain maintains an independent, up-to-date copy of the healthcare ledger, enhancing security and mitigating risks associated with data breaches. This decentralized technology offers new perspectives on data security and operational efficiency, potentially reducing healthcare costs by providing a secure and cost-effective means of storing and accessing patient records.

The electronic nature of EMCs enables smoother exchange across healthcare organizations, addressing issues such as patient data loss during facility transfers and streamlining data collection for research through improved information sharing and collaborative initiatives.

We propose a novel architecture leveraging blockchain technology to facilitate the sharing and management of EMC data, particularly for cardiac patient care. The prototype aims to create an information exchange network for cardiac patients and their physicians, encompassing medical history, treatments, test results, and medications as seen in the Fig. 3.

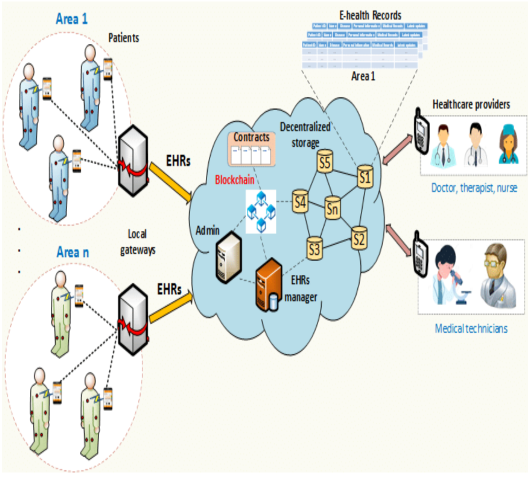

Fig. 3. Blockchain in electronic medical certification.

4.3. Transaction Developing Nodes

Our proposed system includes a network of therapeutic certification and patient-visit-certified treatment centers in major cities, with the blockchain member therapeutic association serving as the administrative body. This setup allows patients to be treated as assets within the blockchain, enhancing the daily management of patient conditions through smart contracts and peer verification, including by specialists from the therapeutic association.

4.4. Design Goals

Our blockchain utilizes cryptographic hashing methods like SHA-512 and RSA, alongside Proof-of-Work, AES, and Triple DES to ensure data authenticity and create an immutable record of EMCs. This approach detects unauthorized data alterations and secures data integrity through cryptographic hashing algorithms.

4.5. Establishing a Safe and Reliable EMC System

Our blockchain framework aims to ensure consistent and invariable records, enhancing accountability and transparency in electronic health records management. Encryption and access management protocols provide patients with control over their health information, while consensus mechanisms like Proof of Work validate and approve transactions, safeguarding against unauthorized data changes. The system promotes secure and standardized information sharing among healthcare professionals, preserving patient confidentiality through advanced encryption and smart contract technologies.

The integration of blockchain into electronic medical certification processes promises a future of secure, efficient, and patient-centered healthcare data management.

Certainly, let's include a comprehensive overview of the proposed work including the detailed explanation of the algorithms:

5. Proposed Work

Blockchain technology is poised to significantly enhance public health data management during outbreaks of infectious diseases. Medical departments and government authorities encounter substantial challenges in tracking public health data, a process that can be revolutionized through the decentralized and secure capabilities of blockchain. Additionally, the management of e-patient data presents an excellent opportunity for blockchain to innovate in terms of interoperability, data standards, security, privacy, scalability, and e-governance.

5.1. Blockchain Terminologies

Blockchain technology's foundation is built on several key terminologies:

- **Node**: Any computer in the blockchain network capable of sending and receiving transactions. A full node downloads the entire blockchain data and verifies transactions.
- **Transaction:** The basic data storage unit on a blockchain, stored in blocks.
- **Chain:** A series of blocks linked in order through digital signatures, ensuring document validation.
- **Record:** Information provided to a smart contract by a person or machine, used for authentication.
- **Smart Contract:** Software that executes coded procedures automatically under specified conditions.

5.2. Electronic Medical Certification Using Blockchain

Blockchain can significantly improve Electronic Medical Certification (EMC) systems by facilitating secure data sharing between healthcare providers with a patient's private key and maintaining a secure, independently updated healthcare ledger at each institution. This decentralized approach enhances security and efficiency, potentially reducing healthcare costs and improving patient data management.

5.3. Transaction Developing Nodes

The proposed system involves a network of specialists and treatment centers, with blockchain technology enabling secure and efficient data management and sharing across the healthcare ecosystem.

5.4. Design Goals

The goal is to utilize cryptographic methods like SHA-512, RSA, Proof-of-work, AES, and Triple DES to ensure data authenticity and integrity within the blockchain, creating an immutable and secure record of EMCs.

5.5. Establishing a Safe and Reliable EMC System

The blockchain framework aims to provide consistent and secure electronic health records, with enhanced encryption and access management for patient data, and consensus mechanisms like Proof of Work to validate transactions and prevent unauthorized data tampering.

5.6. Algorithms in the Proposed Work

This algorithm ensures the secure and authenticated transaction of patient records within the blockchain.

Algorithm 1: Patient Record Transactions Using Blockchain

Input:

- Doctor Address
- Doctor Private Key
- Patient Address
- Patient ID

Process:

- Sign the transaction with the doctor's private key (RSA) to authenticate.
- Confirm transaction details to finalize.
- Use the recipient's public key to allow decryption and verification of the transaction by the intended recipient.

Output:

- Successful transaction completion.
- Verification of transaction integrity.
- Accessibility of transaction details via a URL node for audit and verification purposes.

This algorithm focuses on securing and verifying health record transactions in the blockchain environment.

Algorithm 2: Hospital Health Record Configuration

Process:

- Ensure that transactions are signed with the sender's private key and verified by the recipient's public key.
- Transactions are added to the blockchain after verification.
- Utilize SHA-512 for creating a secure hash of each block.
- Implement Proof of Work to validate new blocks and ensure the chain's integrity.

Validation:

- Verify the authenticity and integrity of each transaction and block.
- Check the blockchain's validity continuously to prevent tampering.

These algorithms collectively ensure the secure, private, and efficient management of electronic medical certifications, leveraging blockchain technology to enhance data integrity, accessibility, and interoperability in healthcare systems.

6. Performance Validation

This section delves into the effectiveness of blockchain technology in safeguarding sensitive Electronic Medical Certification (EMC) data. By detailing our experimental setup and presenting the data obtained from our tests, we aim to demonstrate the technology's robustness and security.

6.1. Experimental Setup

In our experimental setup, the configuration parameters are modified as per assessment, such as block size, block time, endorsement policy, channel, resource allocation, and ledger database, etc. The specification required for our simulations and configuration setup meets the following hardware and software criteria given as follows. Core i7, Intel 2.7 GHz, RAM 16 GB, Hyperledger Caliper, Python, Chaincode, Origionlab pro.

Testbed Configuration: Our experimental model was developed using Python 3.7, a widely supported programming language ideal for processing and securing patient health records within a blockchain framework. The simulation was carried out in the PyCharm Integrated Development Environment (IDE), which is known for its comprehensive support for Python. Within this environment, we deployed a Flask-based blockchain client application. By interacting with this application, users can initiate blockchain transactions and simulate the handling of EMC data. The experimental dataset, comprising EMC patient illness records, was sourced from publicly available repositories on GitHub, providing a realistic basis for our tests.

6.2. Data Sharing Mechanism

In addressing the critical challenges of data theft and manipulation—risks that could compromise patient identities and treatment details during blockchain transactions—we designed our system with heightened security measures. This experiment focuses on verifying data integrity using asymmetric cryptography, a method that employs a pair of keys for encryption and decryption processes: a public key and a private key. The private key remains confidential, ensuring the security of the communication, while the public key facilitates the verification process, enhancing the system's overall efficiency and effectiveness.

The implementation of the Rivest-Shamir-Adleman (RSA) algorithm, a well-established method in public-key cryptography, plays a pivotal role in our data protection strategy. Additionally, we employ the Secure Hashing Algorithm (SHA-512) for its robust cryptographic hash capabilities. This function is essential for verifying digital transactions and is instrumental in the generation and validation of new addresses within digital asset protocols such as Bitcoin. Through these methods, our system not only secures data sharing across the blockchain network but also ensures the authenticity and integrity of the data exchanged.

By meticulously configuring our experimental setup and employing advanced cryptographic techniques, we aim to showcase the formidable capacity of blockchain technology in protecting EMC data against unauthorized access and tampering. The results of our experiments affirm the potential of blockchain as a secure and efficient platform for managing sensitive health information.

7. Result

In this initiative, we focus on securely gathering patient data and administering tests, assigning each patient a unique private key based on their actions post-test results. All information is securely transmitted and stored on the blockchain, ensuring the confidentiality and integrity of patient data.

7.1. Patient Record Generator

The system utilizes public keys for the encryption of sensitive information, while private keys are employed for both encryption and decryption processes. This ensures that only the sender and recipient have access to each other's private keys, maintaining the confidentiality of the communication. Public keys, on the other hand, can be distributed to multiple users without compromising security.

7.2. Patient Health Record Transaction

To facilitate a patient healthcare record transaction, the system requires four essential pieces of information from the sender. This data is organized in a Python dictionary format, excluding the sender's private key for security reasons. The sign_record method processes this record information, utilizing the sender's private key to authenticate the record securely. An Application Programming Interface (API) is designed to accept inputs such as the doctor's address, the doctor's private key, the patient's address, and the record to be sent. It returns the record (sans private key) alongside a digital signature. This functionality is encapsulated within a Python class, defined with four attributes: doctor's address, doctor's private key, patient's address, and the record to be transmitted.

Key Operations in Blockchain Management:

- **Mining**: Involves reviewing past transaction blocks and the personal information of blockchain users to verify and add new transactions to the blockchain.
- **Configure**: Essential for establishing communication protocols between nodes within the blockchain network.

Core Components of the Blockchain System:

- **Records**: This attribute holds the data pending to be included in the upcoming block, ensuring organized and sequential data management.
- **Chain**: Represents the series or sequence of blocks that constitute the blockchain, maintaining a chronological record of all transactions.
- **Nodes**: This is an array of URLs for various nodes within the blockchain network. These nodes are critical for retrieving information from other nodes and ensuring the blockchain remains updated and synchronized. The process culminates in the verification of transaction information, followed by the entry of a blockchain node URL and the final confirmation of the transaction.

Through the implementation of these methodologies and systems, the initiative aims to bolster the security framework of blockchain applications in healthcare, enhancing the protection of patient information while facilitating efficient and verified transactions across the network.

Electronic Medical Certification Transaction via Blockchain:

This initiative is focused on the secure and distributed storage of individual segments of both historical and current medical records through blockchain technology. The seamless transfer of a patient's comprehensive treatment history, when they are transferred or referred to another healthcare facility, is crucial. It ensures the continuity of care by providing the new medical team with immediate access to the patient's previous medical interventions and outcomes. This capability significantly reduces the time required for healthcare professionals to adapt and apply the most up-to-date diagnostic and treatment approaches for the patient's condition.

8. Comparative Analysis with Existing Systems

Evaluating the effectiveness, advantages, and limitations of various Electronic Medical Certification (EMC) systems incorporating blockchain technology is crucial for a comprehensive analysis. Blockchain's features such as encryption, decentralized storage, and immutability significantly enhance data security, offering robust protection for sensitive patient information by reducing the risk of security breaches and unauthorized access. We have conducted a comparative study focusing on these aspects to assist healthcare stakeholders in making informed decisions regarding the adoption and implementation of blockchain-based EMC systems. The findings of this study are summarized in the revised Table 1 below.

Table 1. Comparative study on patient confidentiality in EMC systems

System/Features	Reference [20]	Reference [23]	Our Proposed System
Architecture	Smart Contract	Permissioned Blockchain	Private Blockchain
Platform	Hyperledger	Hyperledger Fabric	Decentralized Platform
Functionality	Encrypted IPFS for Health Data	Smart Contracts for Consent Management	EMC Data Storage and Retrieval
Security	End-to-End Secure Data Sharing	Signature Verification	Public/Private Key Encryption
Privacy	Compliance with Patient Privacy Laws	Data Verification via Signature Keys	Pseudonymized Data, End-to-End Encryption
Framework	SmartMed Chain	Spring Framework	Flask Web Framework
Performance	Average Throughput, Mitigates Single Points of Failure	Reduces Impact of Single Points of Failure	Protection Against Cyber Attacks
Algorithm	AES Symmetric Algorithm	Proxy Re-Encryption	SHA-512, RSA, Proof-of-Work, AES, Triple DES

9. Impact of Proposed Work

The proposed system aims to significantly enhance the security of patient records, preventing data leaks and potential economic losses. By exploring blockchain technology within the EMC domain, this research contributes to advancing knowledge, fostering acceptance, and facilitating the adoption of blockchain-based healthcare solutions. Through the detailed evaluation and comparison presented, the potential benefits and advancements offered by our proposed blockchain-based EMC system are underscored, highlighting its capability to address current challenges in securing patient information while ensuring compliance with privacy regulations and improving overall healthcare delivery.

10. Conclusion

Our research advocates for the adoption of Blockchain technology in the management of Electronic Medical Certification (EMC) for patient disease diagnosis. This innovative system empowers patients to select their preferred healthcare facilities and practitioners, directly linking these choices to their medical histories. This integration significantly accelerates the diagnostic process, enabling quicker initiation of treatment. Patient records are securely stored in time-stamped, immutable blockchain blocks, accessible only to authorized network participants. This ensures that each patient's medical information, including their private key, patient ID, treatment details, and test reports, becomes part of a secure, unalterable E-Patient Medical Record collection. Such a collection not only safeguards patient data but also facilitates deeper insights into patient care.

The proposed blockchain-based system offers substantial support to local authorities in efficiently managing healthcare resources, including the distribution and allocation of medical personnel across recognized hospitals. It also enhances the monitoring of healthcare scenarios and medical staff activities. Healthcare organizations and professionals can access EMCs stored on the blockchain with heightened confidence, knowing the data is secure and reliable. Looking forward, there is potential to expand this work by integrating advanced resource management strategies and decision-making processes for emergency care scenarios, further optimizing healthcare delivery.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Khalil Youssef, Yasmine Ibrahim write the manuscript; Tawhib Amer, Doaa Abdo Othman Qasem, Ozgu Can, and Fursan Thabit review the manuscript, all authors had approved the final version.

References

[1] J. A. H. Rensaa, "VerifyMed-Application of blockchain technology to improve trust in virtualized healthcare services," 2020.

[2] Y. Zhuang, L. R. Sheets, and Y. W. Chen, *et al.*, "A patient-centric health information exchange framework using blockchain technology," *IEEE J. Biomed. Heal. Informatics*, vol. 24, no. 8, pp. 2169–2176, 2020.

[3] S. Chakraborty, S. Aich, and H. Kim, "A secure healthcare system design framework using blockchain technology," in *Proc. 2019 21st Int. Conf. Adv. Commun. Technol.*, 2019.

[4] M. Usman and U. Qamar, "Secure electronic medical records storage and sharing using blockchain technology," P*rocedia Comput. Sci.*, vol. 174, pp. 321–327, 2020.

[5] G. G. Daghe, J. Mohler, and M. Milojkovic, *et al.*, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustain. Cities Soc.*, vol. 39, 2018.

[6] A. Ali, H. A. Rahim, and M. F. Pasha, *et al.*, "Security, privacy, and reliability in digital healthcare systems using blockchain," *Electron.*, vol. 10, no. 16, 2021.

[7] T. Fatokun, A. Nag, and S. Sharma, "Towards a blockchain assisted patient system for electronic health records," *Electron.*, vol. 10, no. 5, 2021.

[8] R. Sangeetha, B. Harshini, and A. Shanmugapriya, *et al.*, "Electronic Health Record System using Blockchain," *Int. Res. J. Multidiscip. Technovation*, 2019.

[9] S. Zhai, Y. Yang, and J. Li, *et al.*, "Research on the Application of Cryptography on the Blockchain," *J. Phys. Conf. Ser.*, vol. 1168, no. 3, 2019.

[10] Y. Sharma and B. Balamurugan, "Preserving the Privacy of Electronic Health Records using Blockchain," *Procedia Comput. Sci.*, vol. 173, 2020.

[11] A. Murugan, T. Chechare, and B. Muruganantham, *et al.*, "Healthcare information exchange using blockchain technology," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 1, 2020.

[12] A. Shahnaz, U. Qamar, and A. Khalid, "Using blockchain for electronic health records," *IEEE Access*, vol. 7, 2019.

[13] X. Chen, J. Ji, C. Luo, W. Liao, and P. Li, "When machine learning meets blockchain: A decentralized, privacy-preserving and secure design," in *Proc. the 2018 IEEE International Conference on Big Data (Big Data)*, Seattle, WA, USA, December 2018, pp. 1178–1187.

[14] A. Roehrs, C. A. da Costa, and R. da Rosa Righi, *et al.*, "Analyzing the performance of a blockchain-based personal health record implementation," *J. Biomed. Inform.*, vol. 92, 103140, 2019.

[15] S. Chakraborty, S. Aich, and H.-C. Kim, "A secure healthcare system design framework using blockchain technology," in *Proc. the 2019 21st International Conference on Advanced Communication Technology (ICACT)*, PyeongChang, Korea, February 2019, pp. 260–264.

[16] A. Yazdinejad, R. M. Parizi, and A. Dehghantanha, "Choo, K.-K. P4-to-blockchain: A secure blockchain-enabled packet parser for software defined networking," *J. Comput. Secur.,* vol. 88, pp. 101–629, 2020.

[17] S. Jiang, J. Cao, H. Wu, Y. Yang, M. Ma, and J. He, "Blochie: A blockchain-based platform for healthcare information exchange," in *Proc. the 2018 IEEE International Conference on Smart Computing (Smartcomp)*, Taormina, Italy, June 2018, pp. 49–56.

[18] S. Jiang, J. Cao, H. Wu, and Y. Yang, "Fairness-based packing of industrial IoT data in permissioned blockchains," I*EEE Trans. Ind. Inform.,* vol. 17, pp. 7639–7649, 2020.

[19] A. Dorri, S. Kanhere, R. S. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Proc. the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom workshops)*, Kona, HI, USA, March 2017, pp. 618–623.

[20] C. Lazaroiu and M. Roscia, "Smart district through IoT and blockchain," in *Proc. the 2017 IEEE 6th International Conference on Renewable Energy Research and Applications*, San Diego, CA, USA, November 2017, pp. 454–461.

[21] Lacity, "Addressing Key Challenges to Making Enterprise Blockchain Applications a Reality," *J. Mis Q. Exec.,* vol. 17, no. 3, 2018.

[22] J. Sengupta, S. Ruj, and S. D. Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *J. Netw. Comput. Appl.*, vol. 149, 102481, 2020.

[23] H. Honar Pajooh, M. Rashid, F. Alam, and S. Demidenko, "Multi-layer blockchain-based security architecture for internet of things," *Sensors*, vol. 21, 772, 2021.

[24] F. Thabit, S. Alhomdy, and S. Jagtap, "Security analysis and performance evaluation of a new lightweight cryptographic algorithm for cloud computing," *Glob. Transitions Proc.*, 2021. doi: 10.1016/j.gltp.2021.01.014

[25] K. Al-Sani and F. Thabit, "An evaluation study of the degree of need for classification criteria for Jordanian universities from the point of view of administrative academics in Jordanian universities," *Int. J. Adv. Eng. Manag. Sci.*, 2021. doi: 10.22161/ijaems.75.2

[26] S. Alhomdy, F. Thabit, F. H. Abdulrazzak, A. Haldorai, and S. Jagtap, "The role of cloud computing technology: A savior to fight the lockdown in COVID 19 crisis, the benefits, characteristics and applications," *Int. J. Intell. Networks*, vol. 2, pp. 166–174, 2021. doi: 10.1016/j.ijin.2021.08.001

[27] F. Thabit, S. Alhomdy, and S. Jagtap, "A new data security algorithm for the cloud computing based on genetics techniques and logical-mathematical functions," *Int. J. Intell. Networks*, vol. 2, 2021. doi: 10.1016/j.ijin.2021.03.001

[28] F. Thabit, A. P. S. Alhomdy, A. H. A. Al-Ahdal, and P. D. S. Jagtap, "A new lightweight cryptographic algorithm for enhancing data security in cloud computing," *Glob. Transitions Proc.*, 2021. doi: 10.1016/j.gltp.2021.01.013

[29] F. Thabit, O. Can, S. Alhomdy, G. H. Al-Gaphari, and S. Jagtap, "A novel effective lightweight homomorphic cryptographic algorithm for data security in cloud computing," *Int. J. Intell. Networks*, vol. 3, pp. 16–30, 2022. doi: https://doi.org/10.1016/j.ijin.2022.04.001

[30] F. Thabit, O. Can, A. O. Aljahdali, G. H. Al-Gaphari, and H. A. Alkhzaimi, "Cryptography algorithms for enhancing IoT security," *Internet of Things (Netherlands)*, 2023. doi: 10.1016/j.iot.2023.100759

[31] E. Abduljalil, P. R. Patil, F. Thabit, and S. B. Thorat, "A new secure 2PL real-time concurrency control algorithm (ES2PL)," *Int. J. Intell. Networks*, vol. 3, pp. 48–57, Jan. 2022. doi: 10.1016/J.IJIN.2022.05.001

[32] F. Thabit, S. A.-H. Alhomdy, and S. B. Jagtap, "Toward a model for cloud computing banking in Yemen," *SSRN Electron. J.*, 2019. doi: 10.2139/ssrn.3484881

[33] F. Thabit, O. Can, R. U. Z. Wani, M. A. Qasem, S. B. Thorat, and H. A. Alkhzaimi, "Data security techniques in cloud computing based on machine learning algorithms and cryptographic algorithms: Lightweight algorithms and genetics algorithms," *Concurr. Comput. Pract. Exp.*, 2023. doi: 10.1002/cpe.7691