Available online at www.HighTechJournal.org

HighTech and Innovation Journal

ISSN: 2723-9535

Vol. 4, No. 3, September, 2023

Advancing Healthcare Security: A Cutting-Edge Zero-Trust Blockchain Solution for Protecting Electronic Health Records

Rihab Benaich [1*], Saida El Mendili [1], Youssef Gahi [1]

[1] *National School of Applied Sciences of Kenitra, Ibn Tofail University, Kenitra, Morocco.*

Received 08 June 2023; Revised 19 August 2023; Accepted 26 August 2023; Published 01 September 2023

Abstract

The effective management of electronic health records (EHRs) is vital in healthcare. However, traditional systems often need help handling data inconsistently, providing limited access, and coordinating poorly across facilities. This study aims to tackle these issues using blockchain technology to improve EHR systems' data security, privacy, and interoperability. By thoroughly analyzing blockchain's applications in healthcare, we propose an innovative solution that leverages blockchain's decentralized and immutable nature, combined with advanced encryption techniques such as the Advanced Encryption Standard and Zero Knowledge Proof Protocol, to fortify EHR systems. Our research demonstrates that blockchain can effectively overcome significant EHR challenges, including fragmented data and interoperability problems, by facilitating secure and transparent data exchange, leading to enhanced coordination, care quality, and cost-efficiency across healthcare facilities. This study offers practical guidelines for implementing blockchain technology in healthcare, emphasizing a balanced approach to interoperability, privacy, and security. It represents a significant advancement over traditional EHR systems, boosting security and affording patients greater control over their health records.

Keywords: Blockchain; Data Security; Data Management; Smart Contracts; EHR.

1. Introduction

The healthcare industry has undergone a significant transformation with the widespread adoption of electronic health records (EHRs), marking a paradigm shift in the management and utilization of medical information. The transition to digital platforms has brought several benefits, including but not limited to improved accessibility of patient data for healthcare professionals, streamlined data management processes, and efficient healthcare delivery (Figure 1). Integrating advanced technologies in EHRs has facilitated the aggregation and analysis of large datasets that can be pivotal in advancing medical research and enhancing patient outcomes. Nonetheless, this transformation has been challenging. The digitization of sensitive health information has raised significant concerns regarding data security and the protection of patient privacy. The healthcare industry has witnessed a disturbing increase in incidents such as data breaches, unauthorized access to patient records, and the misuse of personal health information. These occurrences compromise patient confidentiality and erode public trust in the healthcare system. The loss of trust poses a significant threat to the integrity and effectiveness of healthcare services. These occurrences compromise patient confidentiality and undermine public trust in the healthcare system. This erosion of trust poses a significant threat to the integrity and effectiveness of healthcare services.

In light of these challenges, researchers have turned to blockchain technology, which is renowned for its robust security features and decentralized nature. A considerable body of literature, including studies such as [1, 2], has explored the

* Corresponding author: rihab.benaich@uit.ac.ma

http://dx.doi.org/10.28991/HIJ-2023-04-03-012

theoretical application of blockchain in healthcare. These studies have unanimously acknowledged the potential of blockchain for enhancing data integrity, ensuring transparency, and safeguarding against unauthorized access. However, there is a notable gap in translating these theoretical models into practical, scalable solutions for healthcare environments. A critical examination of existing literature reveals a significant disconnect between theoretical proposals and their practical applications. While experts widely agree on the potential of blockchain, researchers need to create more comprehensive models that seamlessly integrate blockchain technology with existing electronic health record systems. For instance, Hajian et al. [3] provided valuable insights into the theoretical framework of blockchain for healthcare data management but must address the complexities of real-world implementation. Similarly, Srivastava et al. [4] focused on the security aspects of blockchain but does not propose a functional model for EHR systems.

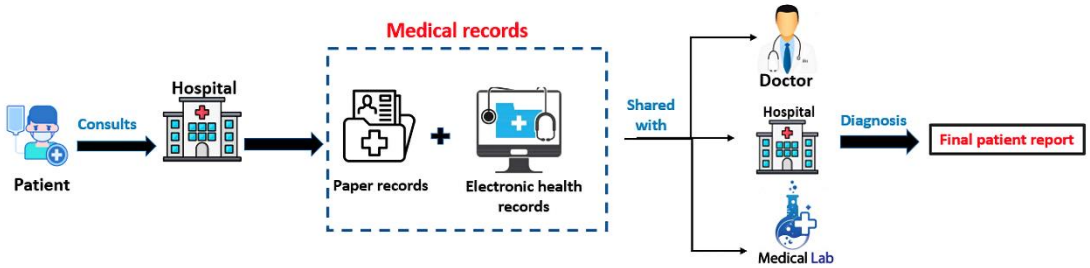

Figure 1. The classical method of electronic health records processing

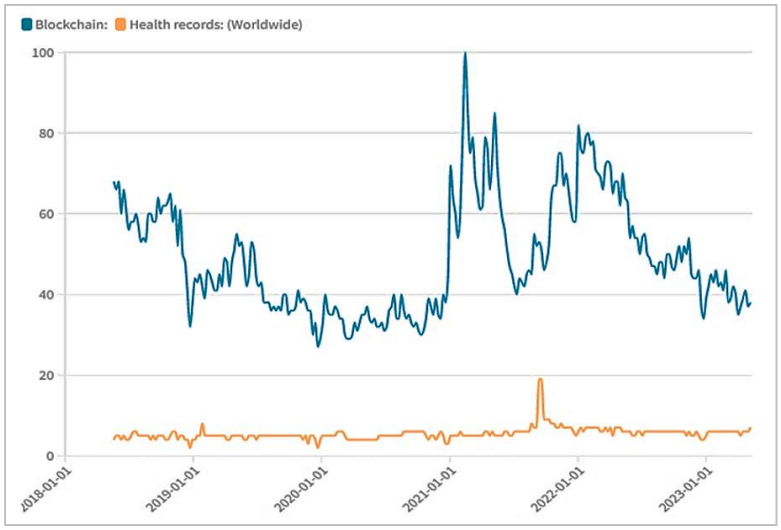

Figure 2. Google Trends data visualization on the topic of Blockchain/Health records (from 2018 to 2023)

The present study aims to address a critical gap in the security of Electronic Health Record (EHR) systems by proposing a novel zero-trust blockchain solution. Unlike previous attempts, this study combines the inherent security features of blockchain technology with advanced zero-trust principles, thereby ensuring a higher level of data protection and privacy. The proposed architecture introduces a system design that fortifies the security of EHRs and enhances scalability and efficiency, thereby making it a viable solution for contemporary healthcare institutions. The study's findings have significant implications for the healthcare industry, as they offer a promising approach to mitigate the security challenges associated with EHR systems.

Despite the expanding interest in blockchain technology for healthcare applications, the current literature needs comprehensive information on the challenges and issues that arise when implementing blockchain technology in the healthcare industry (see Figure 2). Significant obstacles include interoperability, data privacy, and security issues. Our approach involves developing a decentralized, blockchain-based framework that we can integrate with existing EHR systems. This model promises to provide more data protection, mitigate risks associated with centralized data storage, and enhance overall trust in healthcare data management.

The remainder of this paper is structured as follows: Section 2 presents the research approach undertaken for the literature review. Section 3 provides an in-depth review of the most relevant studies that address the issue of electronic health record security. In section 4, we emphasize the significance of blockchain technology in the context of electronic health records. This is followed by Section 5, which offers a comprehensive overview of the underlying mechanisms of blockchain technology, including relevant details. Section 6 outlines the implementation of the proposed assessment framework and compares the observed results with existing frameworks. Finally, the paper summarizes key findings and discusses potential avenues for future research.

3. Research Methodology

We conducted an in-depth literature review to identify and summarize studies on using blockchain technology to secure electronic health records (EHRs). To ensure a rigorous and comprehensive review, we adhered to [5] a three-step methodology, as mentioned in Figure 3. The methodology entailed identifying pertinent studies through a systematic search, filtering the studies based on predefined inclusion and exclusion criteria, and extracting and synthesizing data from the selected studies.

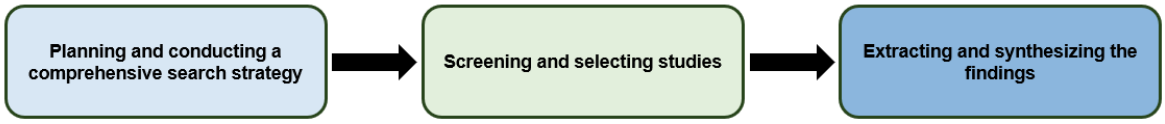

Figure 3. Research strategy

2.1. Planning and Conducting a Comprehensive Search Strategy

This review aims to identify and summarize studies investigating the use of blockchain technology for EHR security. This initial stage entails planning and executing a comprehensive search strategy to identify relevant studies concerning integrating blockchain technology into electronic health records (EHRs) to improve security. This initial phase attempts to develop a thorough search strategy that ensures the incorporation of every pertinent study and provides a clear understanding of the research question and objectives. This review also aims to include studies that propose frameworks or systems employing blockchain technology to address EHR security challenges. Additionally, we will consider studies evaluating the effectiveness of such systems.

2.2. Screening and Selecting Relevant Studies

In this step, the review process was conducted by searching for and selecting studies on blockchain security in electronic health records or medical records within the defined scope. Initially, we performed a primary search using generic expressions such as 'blockchain technology,' 'electronic health records,' 'medical records,' and 'security.' Then, specific expressions such as "blockchain-based EHR security" and "blockchain integration in medical records" were used to capture relevant studies.

We initially screened papers with titles matching the selected keywords and excluded irrelevant papers by reviewing their abstracts. Table 1 presents the papers' distribution based on the keywords defined in the following digital libraries: IEEE Xplore, ScienceDirect, Scopus, Wiley, PubMed, and MDPI.

Table 1. Distribution of related papers depending on keywords

Keywords / Digital libraries	IEEE XPLORE	ScienceDirect	Scopus	Wiley library	PubMed	MDPI
Blockchain technology AND healthcare	28	21	36	24	15	30
Blockchain AND EHRs	15	11	20	5	5	14
EHRs AND Decentralised technology	10	15	11	4	7	0
Blockchain integration AND medical records	4	8	4	12	9	13
Total	57	55	71	45	36	57

2.3. Digital Libraries

We limited our exploration to scholarly publications in recognized academic journals and conference proceedings to ensure a comprehensive and rigorous search. We conducted our research utilizing reputable digital libraries, adhering to a strict methodology to guarantee the selection of relevant and high-quality sources.

Table 2. The digital libraries used in our related works review

Digital library	Link
IEEE Xplore	https://ieeexplore.ieee.org
ScienceDirect	https://www.sciencedirect.com
Scopus	https://www.scopus.com
Wiley library	https://onlinelibrary.wiley.com
PubMed	https://pubmed.ncbi.nlm.nih.gov
MDPI	https://www.mdpi.com

2.3. Inclusion and Exclusion Criteria

After conducting a literature review, the next phase limits the papers based on relevance, availability, and content. We showed a diagonal reading of the collected studies after excluding unrelated ones based on the inclusion criteria listed in Table 3.

Table 3. Inclusion and Exclusion Approach

Inclusion criteria	Exclusion Criteria
Papers published in the English language	Papers published in different languages
Published from 2020 to 2023	Papers published before 2020
Papers focusing on blockchain integration in the healthcare sector	Papers focusing on blockchain integration in broader sectors
Papers focusing on the security of EHRs/ healthcare	Papers focusing on using blockchain in management focus

A total of 51 papers were chosen after a thorough analysis. In addition, a detailed search was conducted on the references of the selected studies. This resulted in the selection of three additional papers deemed relevant to the scope of our research. Then, after thoroughly examining the selected articles, 20 studies were considered pertinent to our research area. The descriptive details of the articles were then reviewed and inserted into a Zotero database. The methodology adopted for the literature search is depicted in Figure 4.

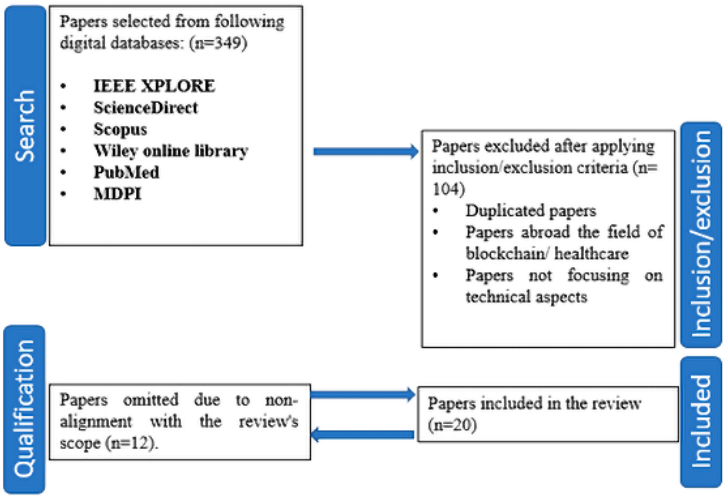

Figure 4. The methodology adopted for the literature

2.4. Reporting the Review

In the concluding phase of the research process, the key findings from the literature review are reported, and conclusions are formed. A significant gap was identified in the literature regarding the use of advanced methods for securing electronic health records. This discovery inspired us to comprehensively analyze the current state of the art to fill the gap and significantly contribute to the field. The following section of the report examines the 20 papers selected for this study and outlines the main findings from the literature review.

3. Background Literature

The increasing prevalence of electronic health records has given rise to worries over the safety of patient information. Because it provides a tamper-proof and decentralized system for storing and managing sensitive data, blockchain technology has emerged as an intriguing option for securing EHRs. EHRs can be securely shared between healthcare providers, patients, and other authorized parties using blockchain, eliminating the risk of data breaches or unauthorized access.

Several studies have explored the potential benefits of blockchain technology for securing EHRs and addressing the healthcare industry's challenges. In this context, the authors in [6] proposed a comprehensive blockchain-based framework for securing electronic health records (EHRs), which included a blockchain-based storage system, smart contracts, encryption and access control mechanisms, and interoperability with existing EHR systems. The blockchain-based storage system ensured the secure and efficient storage of EHRs on a blockchain network, while smart contracts enforced access control, data sharing, and privacy policies. Encryption and access control mechanisms protect the confidentiality of EHRs. Interoperability with existing EHR systems was achieved using open standards and APIs. Another study by d'Aliberti and Clark [7] proposes a new approach to preserving patient privacy when performing computations on shared electronic health record (EHR) data. The proposed method combines differential privacy and data-splitting techniques to protect patient information and prevent unauthorized access. Differential privacy adds random noise to the EHR data to protect against re-identification attacks.

In contrast, data splitting separates the data into multiple disjoint sets to prevent any single entity from accessing the complete dataset. The authors demonstrate the effectiveness of their approach using real-world healthcare datasets and show that their method can preserve privacy while still achieving high accuracy in computations. Furthermore, the authors in [8] proposed a comprehensive security and privacy framework for healthcare blockchains that address various concerns, including confidentiality, integrity, availability, and accountability. Their proposed hybrid consensus mechanism and privacy-preserving smart contract enable secure and efficient healthcare data sharing and management in a decentralized environment. The author's contribution is developing a practical and efficient framework incorporating advanced security techniques such as cryptographic algorithms, access control mechanisms, and data anonymization to protect sensitive healthcare information while enabling efficient sharing and analysis. The effectiveness of their framework is demonstrated through a case study and evaluation of its performance, scalability, and security. Likewise, in [9], the authors investigated a new medical data access management approach using blockchain technology. The authors use Ethereum smart contracts, Truffle Suite, and Web3 to create a decentralized system that provides granular control over medical data access. These tools and methods enable the system to offer secure and decentralized medical data management, significantly contributing to this research. The paper explains the architecture and implementation of the system, including its security features and evaluation results. Table 4 presents a global review of the relevant studies done in the context of blockchain utilization in the case of health records security.

Table 4. Relevant studies were done in the context of blockchain integration in the healthcare industry

Ref	Year	Main Contribution	Methods and tools	Blockchain type	Metrics
[9]	2023	The authors proposed a novel blockchain-based system model for patient-centric secure data sharing of PHRs in cloud computing under a multiple-receiver setting.	-Smart contracts -Attribute-based encryption	Consortium blockchain	- Correctness - Completeness - Efficient user revocation
[10]	2023	The authors developed a health record management system that leverages blockchain to store and manage patient medical records across multiple hospitals.	-Smart contracts -User interface -Encryption tools	Not specified	- Data integrity - Security
[11]	2023	The paper proposed a privacy-preserving and efficient data-sharing scheme with trust authentication based on blockchain technology to address user privacy leakage issues, mobile users' low computing efficiency, and centralized and untrusted authentication of access rights in mHealth.	-Privacy-preserving access control mechanism -The blockchain-based trust authentication mechanism -Semi-trusted cloud servers	Not specified	- Key generation - Encryption - Decryption - Authentication
[12]	2023	The authors proposed an architectural model for personal health records (PHR) using distributed network technologies like blockchain and hash tables (DHT) to store and share health records securely.	-Distributed hash tables -Data steward Shared data vault	Not specified	- Security and privacy - Storage occupation - Interoperability -Performance
[13]	2023	The authors focused on developing an efficient Blockchain-based architectural framework for storing electronic health record data in Big Data storage systems.	-Smart contracts -Big data systems -Clusters	Not specified	- Cost efficiency - Data storage - Security
[14]	2023	The paper introduced a Privacy by Design (PbD) framework titled "PbDinEHR" for securely and at scale managing electronic health records (EHR). The proposed framework is built on a distributed data storage and sharing architecture that uses blockchain technology to guarantee data integrity, confidentiality, and availability.	-Ethereum -Private Inter-Planetary File System (IPFS)	Permissioned blockchain	- User performance - Security - Effectiveness
[15]	2023	The article provides a framework called "MyEasyHealthcare," a blockchain-based healthcare system that improves security while lowering costs on multiple levels.	-Smart contracts -InterPlanetary File System (IPFS) -Remix	Not specified	- Gas consumption - Transaction cost - Execution cost - Bandwidth utilization
[16]	2022	The authors designed a medical blockchain double-chain system (MBDS) that combines private and consortium blockchains to store and share medical data securely among offline medical institutions and Internet medicine platforms.	-Delegated Proof of Stake - DPoS algorithm -Practical Byzantine Fault Tolerance (pBFT) algorithm -Cloud	Consortium Private	- Data security - Scalability
[17]	2022	The authors proposed a scheme based on attribute-based encryption protection to improve patient control over their electronic health records (EHRs) in edge cloud environments	-Attribute-Based Encryption (ABE) -CEC-ABE Algorithm	Not specified	- Performance in key generation - Outsourced decryption
[18]	2022	The authors proposed a decentralized, blockchain-based smart healthcare assistance system to support medical record privacy and security without affecting system accessibility.	-Edge Computing -InterPlanetary File System (ipfs)	Private Public	- Latency - Privacy - Anonymity - Integrity - Version Control
[19]	2022	The authors proposed a blockchain-based mobile app integrated with a wallet to perform transactions for storing and retrieving data on a blockchain network.	-Off-chain system -Role-based access control -IPFS	Permissioned blockchain	- Atomicity - Consistency - Integrity

[20]	2022	The authors proposed a patient-controlled sharing scheme for Electronic Health Records (EHRs), which combines cloud computing and blockchain technology.	-Node-state-checkable Practical Byzantine Fault Tolerance consensus algorithm (sc-PBFT) -Attribute-based encryption -Multi-keyword encryption	Not specified	- Consensus latency
[21]	2022	The authors proposed a blockchain-based solution for enhancing the security and privacy of EHRs in healthcare systems	-Proof of work -Java Eclipse -MongoDB	Public	- Data security
[22]	2022	The authors proposed a blockchain-based environment for electronic health records	-Smart contracts -Non-fungible tokens -Hybrid-access control -Public key cryptography	Not specified	- Data security - Data storage
[23]	2022	The authors proposed an architectural framework that can be employed for implementing blockchain technology in electronic health records (EHR) systems within the healthcare sector. This framework provides numerous benefits to the EHR system, including scalability, security, and increased efficiency in sharing medical data.	-Smart contracts	Not specified	- Scalability - Security
[24]	2021	The authors introduced a novel eHealth system called SPChain, which is based on blockchain technology and aims to facilitate medical data sharing while ensuring individuals' privacy.	-Proxy re-encryption -Byzantine-resilient consensus protocol (BFT SMaRt)	Public	- Throughput - Storage overhead - Time complexity
[25]	2021	The authors proposed platform is designed to facilitate the efficient and secure sharing of medical data while maintaining the privacy of individuals in the context of COVID-19.	-Fabric alliance chain -Hyperledger Fabric CA (certificate authority) -Smart contract	Private	- Read and write performance - Security
[26]	2021	The authors introduced a blockchain-based framework for electronic health records (EHR) called MyBlockEHR. This framework is designed with a focus on privacy preservation and access control.	-Ethereum -Smart contract -On-chain/ Off-chain storage	Not specified	- Read and write throughput - Gas cost
[27]	2021	The authors proposed a secure architecture for electronic health records (EHR) that protects patient privacy, facilitating the development of EHR systems in Colombia.	-Hyperledger Fabric -Smart contracts -Proof of concept (PoC)	Private	- Latency - Availability
[28]	2020	The authors proposed a keyless signature infrastructure to guarantee the confidentiality of digital signatures and data integrity.	-Keyless signature infrastructure (KSI)	Private	- Average time - Size - Cost of data storage
[29]	2020	The authors designed an Ethereum blockchain-based smart contract to provide patients with immutable, transparent, and traceable data control.	-Ethereum -Proof of work (PoW) -Smart contracts -Proxy re-encryption -Interplanetary file systems (IPFS)	Public	- Cost - Correctness
[30]	2020	The authors proposed a solution to enhance data accessibility between healthcare providers by integrating the access control policy algorithm.	-Hyperledger Fabric -Byzantine Fault Tolerance (BFT) Crash Fault Tolerance (CFT)	Private	- Latency - Throughput Round Trip Time (RTT)
[31]	2020	The authors proposed a hybrid architecture based on Hyperledger blockchain and edge nodes to enhance EHR management.	-Hyperledger Fabric -Attribute-based multi-signature (ABMS) -Multi-authority attribute-based encryption (ABE)	Private	- Signing time - Verification time
[32]	2020	The authors proposed an architecture for electronic medical records that integrates various clinical providers, focusing on maintaining data integrity during connectivity disruptions while incorporating usability, security, and privacy features.	-Ethereum -Proof of authority (PoA)	Private	- Efficiency - Security
[33]	2020	The authors proposed an approach to developing a distributed system for electronic medical records using consortium blockchain and Hyperledger Fabric. The system employs a ledger distributed across peer nodes that records the address of each patient's medical record in an existing EHR system.	-Hyperledger Fabric -Practical Byzantine fault-tolerant (PBFT) -Proxy re-encryption	Private	- Privacy - Scalability - Availability

The efforts to secure electronic health records have encountered substantial challenges, including insufficient confidentiality safeguards and limited privacy protection methods. These limitations have raised concerns about the vulnerability of sensitive patient data to unauthorized access. While encouraging outcomes have been obtained, it is critical to recognize that these problems remain. For this reason, there is an urgent need to solve these pressing challenges to secure a complete and resilient solution for properly safeguarding EHRs. The following section provides the significance of blockchain in addressing the challenges of electronic health records.

4. Blockchain's Role in Addressing Healthcare Challenges

Electronic health records (EHRs) have become an integral element of contemporary healthcare, allowing for the digital storage and dissemination of patient health information. Data privacy, security, and interoperability concerns have arisen due to the pervasive implementation of EHRs. Blockchain technology has emerged as a potential solution to these problems. Blockchain is a decentralized and distributed ledger technology that, through its pertinent characteristics as defined in Figure 5, can provide secure and transparent transactions.

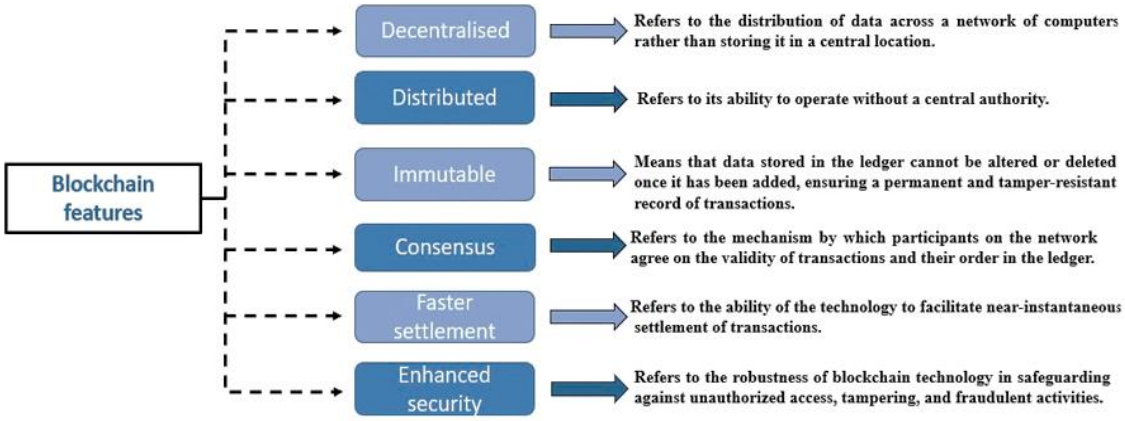

Figure 5. The main features of blockchain

Blockchain can provide a secure and tamper-resistant system for storing and sharing EHRs in healthcare. Blockchain, which utilizes a decentralized and distributed ledger system, enables multiple parties to access and verify Electronic Health Records (EHR) data without a central authority. This facilitates a secure and transparent system in which each participant has a copy of the distributed ledger and can validate transactions, ensuring all parties have access to the same data. Moreover, using smart contracts can automate the sharing and amending of EHRs, further improving the efficacy of healthcare services. Additionally, blockchain technology's distributed and decentralized nature makes it more secure and tamper-resistant than conventional EHR systems. Multiple parties validate each transaction on the blockchain, and once it is added to the distributed ledger, it cannot be altered or removed. This assures the confidentiality and security of patient's health information, making it nearly impossible for anyone to compromise the data. In addition to the benefits listed previously, blockchain technology offers several additional advantages for safeguarding electronic health records (EHRs). First, the decentralized nature of the blockchain system guarantees no singular point of failure or vulnerability, making it more resistant to cyberattacks. This feature significantly strengthens the security of EHRs, making them less susceptible to data breaches and malicious intrusions.

Using cryptographic algorithms and digital signatures adds a supplementary layer of security to the blockchain system, ensuring that every transaction is encrypted and authenticated. This feature provides the data's integrity and privacy, making it more reliable and trustworthy. As they can grant or revoke access to their EHRs, blockchain technology enables patients to exercise greater control over their health information. This permits greater transparency and accountability in the sharing and using patient data, thereby enhancing patient privacy and autonomy. Incorporating blockchain technology into EHRs can reduce data management and interoperability costs by eliminating the need for intermediaries and manual verification procedures. Therefore, combining blockchain technology with EHRs can result in a more secure, transparent, and efficient healthcare system, which is advantageous for all parties involved.

5. Blockchain Technology Components

Blockchain technology is a revolutionary concept that has disrupted traditional business structures in various industries. In 2008, an enigmatic figure known by the pseudonym Satoshi Nakamoto [34] introduced it. Since then, the technology has become synonymous with Bitcoin, based on a blockchain infrastructure. Blockchain technology is fundamentally a decentralized, distributed ledger that enables the secure documentation of transactions. Once recorded, transactions cannot be modified without the consensus of the entire blockchain network. This renders blockchain technology exceptionally secure and resistant to tampering, fraud, and hacking attempts.

5.1. Blockchain Architecture

A network of nodes holds a copy of the blockchain ledger and collaborates to validate and corroborate transactions. A complex cryptographic process creates a unique digital signature for each blockchain block. This signature connects the current block to the previous block, resulting in an unbreakable chain of blocks that can be traced back to the first block in the chain, also known as the genesis block (Figure 6). Using hashes and cryptographic signatures ensures the blockchain's integrity, as the network promptly detects any attempt to interfere with a block.

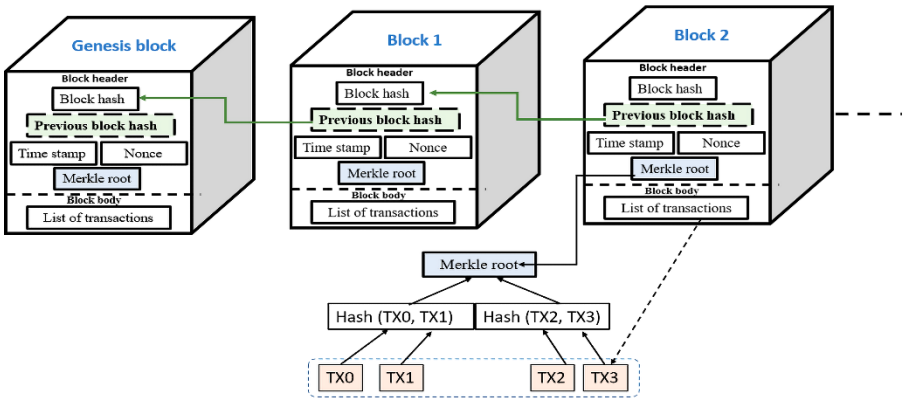

Figure 6. Representation of Blockchain

One of the key benefits of the blockchain architecture is its transparency. Since all nodes in the network have a copy of the blockchain ledger, any changes made to the ledger can be immediately detected and traced back to their source. This provides high accountability and transparency, making it an attractive option for various industries, including finance, supply chain management, and healthcare.

5.2. Blockchain Layers

Blockchain technology comprises five components (Figure 7), each critical to ensuring a blockchain network's security, scalability, and efficiency. The five layers are the infrastructure, network, data, consensus, and application layers.

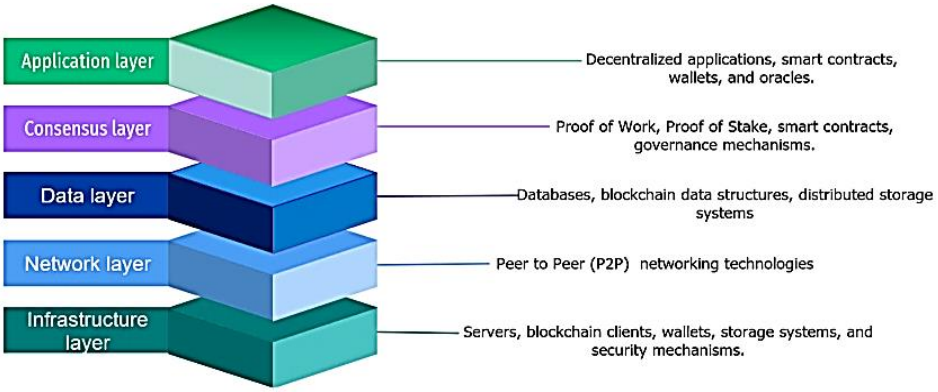

Figure 7. Blockchain Layers

***Infrastructure Layer*:** This layer consists of servers, blockchain client applications, wallets, storage systems, and security mechanisms. Infrastructure is required to guarantee the efficient and secure operation of the blockchain network. For instance, hardware devices must be dependable and effective, while software tools must be secure and scalable.

***Network layer*:** This layer manages communication between nodes in a blockchain network, including protocols, P2P networking technologies, routing algorithms, and transport mechanisms. This layer enables secure and efficient communication between nodes. For instance, network protocols and P2P networking technologies must be developed to prevent spam attacks and surveillance.

On a blockchain network, the data layer manages the storage and retrieval of data, including databases, blockchain data structures, distributed storage systems, and data privacy mechanisms. This layer guarantees that the blockchain network can securely and efficiently store and manage large amounts of data. For instance, the data structures of blockchains must be designed to prevent data tampering, while distributed storage systems must be prepared to avoid data loss.

***The Consensus Layer*:** One of the core components of blockchain layers, it manages the consensus between nodes in a blockchain network regarding the ledger's state. This stratum comprises consensus algorithms, intelligent contracts, and governance mechanisms; it is the blockchain's foundation. The consensus layer ensures the blockchain network can reach a secure and decentralized consensus on the ledger's state. For example, consensus algorithms and smart contracts must be developed to prevent double-spending attacks and malicious actors from exploiting code vulnerabilities.

The Application Layer consists of the user-facing elements of blockchain-based applications, such as decentralized applications, smart contracts, wallets, and oracles. This layer is responsible for making blockchain-based application user interaction straightforward and intuitive. Smart contracts must be transparent and predictable, whereas user interfaces must be intuitive.

5.3. Categories of Blockchain Technology

Blockchain technology can be divided into three categories based on access and governance models: public, private, and consortium (Figure 8).

Public Blockchains: are decentralized networks where individuals can participate and process transactions without permission or authorization. They validate transactions through a network of nodes using a consensus mechanism, and participants are rewarded with cryptographic tokens. Public blockchains are ideal for use cases requiring transparency, censorship resistance, and community-driven governance, such as cryptocurrencies, decentralized finance, and identity management.

***Private Blockchain*:** Private blockchains are well suited for use cases that require privacy, data confidentiality, and controlled access. They are frequently used for internal organizational operations where data privacy and control are essential. A single entity or group with strict access control policies manages private blockchains. Participants in private blockchains must be granted permission to join and transact on the network.

Consortium Blockchain: combines public and private blockchains where a group of organizations manages the network collectively and agrees on the rules and management model. They balance public blockchains' transparency with decentralization and private blockchains' privacy and control. Consortium blockchains are ideal for use cases that require multiple parties to collaborate and coordinate.

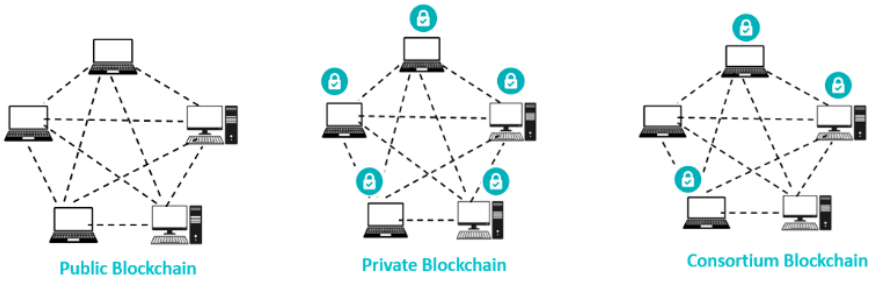

Figure 8. Blockchain Types

6. Preliminaries

Ethereum:

Ethereum is a blockchain platform for developing smart contracts and decentralized applications (DApps). It was created by Vitalik Buterin [35] in 2014 and has become one of the most prevalent and extensively used blockchain technologies. As its primary objective, Ethereum enables programmers to create decentralized and middleman-free applications. It accomplishes this by employing smart contracts, which are contracts that execute themselves and in which the parameters of the buyer-seller agreement are encoded directly into lines of code. Ether (ETH) facilitates transactions on the Ethereum platform and recompenses miners for validating and verifying transactions. Ethereum's flexibility and programmability allow developers to construct various DApps with varying degrees of complexity. Ethereum is regarded as a highly secure and transparent technology with the potential to revolutionize numerous industries due to its decentralized and trustless nature.

Smart Contracts:

Smart contracts are self-executing computer programs that enable parties to exchange value under predefined conditions. They are encoded and stored on a distributed ledger, enabling decentralized and transparent execution. Automating contractual terms, reducing costs, and increasing productivity eliminate the need for intermediaries such as solicitors and banks. Smart contracts are extensively used in industries requiring secure and transparent transactions, such as healthcare, finance, and supply chain management. They enable payments, asset transfers, and the automation of business processes. Once deployed on a blockchain, the immutability of smart contracts ensures that they cannot be altered, providing a high level of security and trust that can help reduce corruption and fraud. Solidity is a widely used and popular programming language for developing smart contracts. It is a contract-oriented, statically typed, high-level programming language with inheritance, libraries, and elaborate user-defined types explicitly designed for Ethereum smart contract development. The security features of Solidity include exception handling, contract-level permissions, and access control modifiers, which prevent vulnerabilities such as re-entry attacks and integer overflows. Due to its prevalence and robustness, Solidity has become the preferred language for developing smart contracts on the Ethereum platform.

InterPlanetary File System (IPFS):

The InterPlanetary File System is a peer-to-peer file-sharing and storage protocol. IPFS divides files into smaller chunks, each with a different hash. These chunks are then distributed among nodes to form a decentralized linked-data web. When users request a file, their computer retrieves chunks from multiple nodes, validates their integrity with the

unique hash, and reconstructs the file. IPFS allows users to save files to their local machine, ensuring they are accessible even if the original uploader goes offline. IPFS is censorship-resistant and has high data redundancy, making it an efficient and secure way of storing and sharing files on the blockchain. Using IPFS, Ethereum can store more data without congesting the blockchain, adding additional security and censorship resistance. Users can benefit from the advantages of both technologies by combining IPFS and Ethereum, resulting in a more solid and efficient decentralized platform.

Ethereum Virtual Machine:

The Ethereum Virtual Machine (Figure 9) is the runtime environment for smart contracts on the Ethereum blockchain. It is a safe and predictable environment in which smart contracts can be implemented, ensuring that all nodes on the network arrive at the same state after the contract is executed. The EVM is in charge of executing bytecode generated by compiling high-level programming languages like Solidity. The Ethereum virtual machine also manages gas, a unit of account for the cost of running a network transaction or contract.

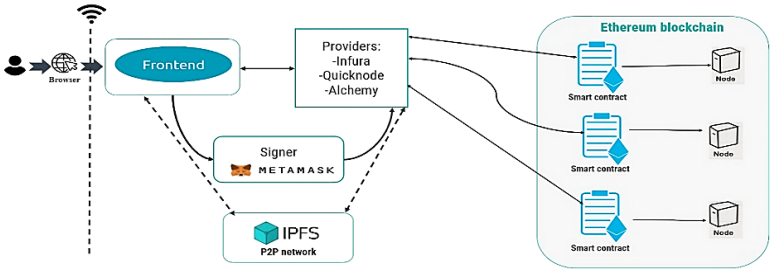

Figure 9. Pipeline of The Main Modules in Decentralized Applications Based on Ethereum Blockchain

Ethereum Transaction:

The Ethereum transaction is based on four primary elements: the nonce, gas price, gas limit, and recipients' addresses.

- ***Nonce*** refers to a unique identifier assigned to each transaction that prevents processing duplication.
- ***Gas price*** refers to the amount the sender is willing to pay per unit of gas consumed during the transaction. It is measured in ether units (ETH).
- ***The gas limit*** determines how much gas can be used during the transaction.
- ***The recipient's address*** identifies the account or smart contract receiving the transaction. Furthermore, the transaction may contain data that activates a smart contract or provides additional information to the recipient.

Several formulas are used to connect these components:

- ***The total cost of a transaction*****:** Total cost = gas limit **x** gas price.
- ***Gas used*****:** gas used = gas price **x** gas consumed.
- ***Ether spent*****:** ether spent = gas used **x** gas price.
- ***Maximum gas*****:** maximum gas = block gas limit.
- ***Gas refund*****:** gas refund = gas price **x** gas refunded.
- ***Effective gas price*****:** effective gas price = (gas price offered by sender) **x** (1 + maximum priority fee per gas) /10^9).

The following section presents a comprehensive and in-depth analysis of our proposed system to emphasize its numerous structural layers.

7. System Design

The system design process is an essential element of any framework, serving as the foundation for the system's development from its conceptualization. The development stage includes creating modules, architecture, and various components seamlessly integrated to form the framework of the overall system. Considering the sensitivity and privacy of health records, it is critical to establish a strong and dependable framework capable of adequately protecting patient data privacy and security while providing healthcare providers with seamless access to relevant data. The proposed framework aims to employ blockchain technology to create a decentralized system that is tolerant to tampering, highly secure, and capable of protecting the confidentiality of electronic health records. The proposed framework involves a variety of users with distinct degrees of authority, including patients, doctors, administration, and medical laboratories.

Granular access is given to ensure that the system is used efficiently and securely. This approach also allows for scalability, permitting the incorporation of new users in the future without risking system performance or security. Figure 10 represents the entire architecture of our proposed system.

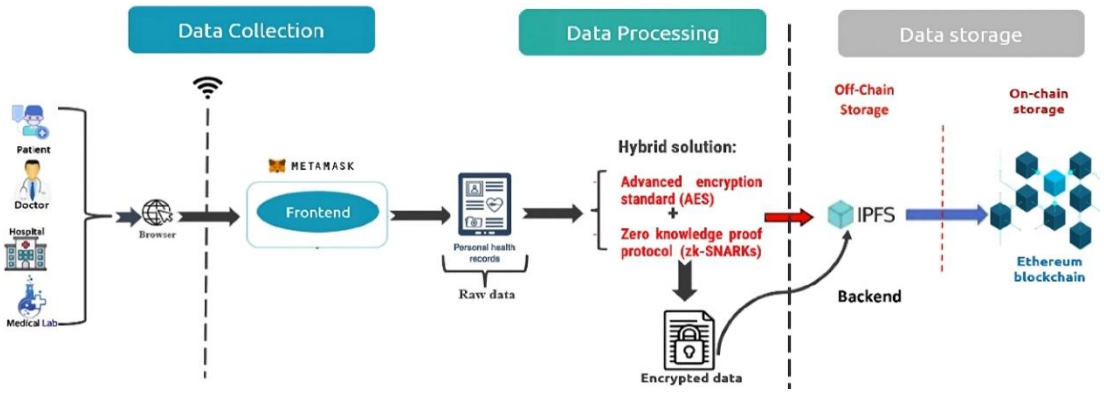

Figure 10. Design of Our Proposed System

7.1. First Layer: Data Collection

The data collection layer is the initial layer of our proposed framework, and it plays a vital role in gathering raw data from the system's leading actors, which include doctors, patients, hospitals, and medical labs. This layer involves interacting with our system's front end to collect electronic health records (EHRs) containing critical medical information. Medical histories, test results, diagnoses, and medications may all be included in EHRs. Our framework aims to provide an extensive view of a patient's health and medical history by collecting this information from several decisions and providing better care. The data collection layer operates as the framework's base, and its effectiveness is critical in ensuring the accuracy and completeness of the data employed in the following layers.

7.2. Second Layer: Data Processing

The second layer of the proposed framework is the backbone of our solution, which involves applying a hybrid approach to data security. Our solution uses Advanced Encryption Standard 256 (AES-256) and Zero-Knowledge Proof protocols, specifically zk-SNARKs, to ensure the confidentiality and integrity of sensitive data. AES-256 is a widely adopted encryption standard renowned for its exceptional security measures, particularly within industries of a sensitive nature, including the healthcare sector. The AES algorithm is leveraged to safeguard patient medical records through encryption to fortify the confidentiality and integrity of such sensitive data.

7.2.1. The Fundamentals of Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES), commonly referred to as Rijndael [36], is a symmetric block cipher used for encryption and decryption of data. It operates on blocks of 128 bits and supports three different key lengths: 128 bits, 192 bits, and 256 bits. The National Institute of Standards and Technology (NIST) officially standardized and published AES in 2001. Figure 11 represents the advanced encryption standard.

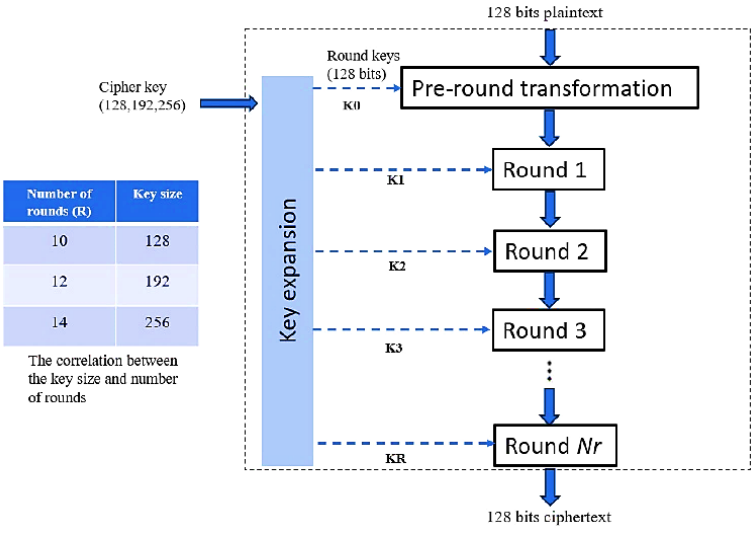

Figure 11. Advanced Encryption Standard

AES operates on a state, a 4 × 4 array of bytes organized in a column-wise order. Each byte within the state represents a single element of data. For example, if there are 16 bytes in total, they are arranged in a two-dimensional array format.

The AES algorithm consists of three phases (Figure 12): the initial, primary, and final rounds. Each phase employs a combination of sub-operations, which are applied differently based on their specific roles within the algorithm. The breakdown of the phases and their corresponding sub-operations is as follows:

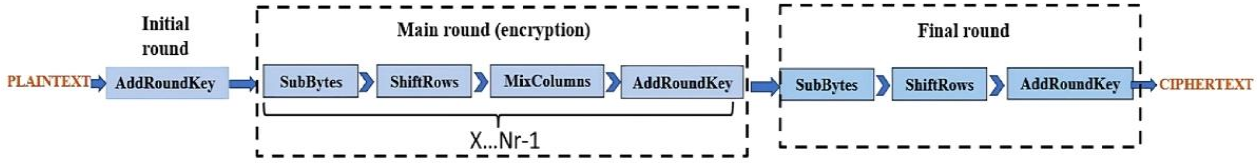

Figure 12. Rounds of AES

- ***AddRoundKey*** is an operation in cryptography where a 128-bit State matrix is combined with a 128-bit round key through a bitwise XOR operation. The XOR operation is applied to each corresponding pair of bits in the matrices, resulting in a new matrix.
- In the Advanced Encryption Standard (AES) algorithm, ***SubBytes*** is a nonlinear replacement step. Each byte of the current state matrix is replaced with a matching byte from the AES S-Box. The AES S-Box is a preconfigured lookup table that maps input and output byte values one-to-one. This procedure helps introduce confusion and non-linearity into the encryption algorithm.
- ***ShiftRows*****:** A transposition step in which the state's four rows are shifted to the left continually by offsets of 0, 1, 2, and 3.
- ***MixColumns*** is a linear mixing technique that multiplies a fixed matrix by the current State Matrix.

7.2.2. Fundamentals of zk-SNARKs

In cryptography, zk-SNARK is defined as a proof protocol that enables a party to demonstrate ownership of certain information without disclosing the information or requiring interaction between the parties engaged in proving and verifying the information. Zk-SNARKs possess the following features that make them distinct:

- ***Succinctness*****:** The proofs generated by zk-SNARKs are small, allowing for quick verification within a few milliseconds.
- ***Noninteractivity*****:** The proof transcript involved in zk-SNARKs consists of a single message sent from the prover to the verifier, eliminating the need for back-and-forth communication.
- ***Argument of Knowledge*****:** zk-SNARKs provide computationally sound proofs, meaning they maintain soundness even when the prover attempts to exploit polynomial-time algorithms.

A (zk-)SNARK protocol, like any other non-interactive proof system, consists of three distinct algorithms with the following functionalities:

- ***Gen*** (Setup Algorithm): This algorithm generates a necessary string *crs*, utilized in the proving process, along with a verification key *vrs*. Sometimes, the verification key is assumed to be secret and accessible only to the verifier. A trusted party typically executes the Gen algorithm.
- ***Prove*** (Prover function): The Prove algorithm inputs the CRS, the statement u, and a corresponding witness *w* as input. It then produces the proof π, representing the statement's validity and witness.
- ***Verify*** (Verification Algorithm): The Verify algorithm accepts the verification key *vrs*, the statement u, and the proof π as input. It performs the necessary computations and returns a result of 1, indicating acceptance of the proof, or 0, indicating rejection.

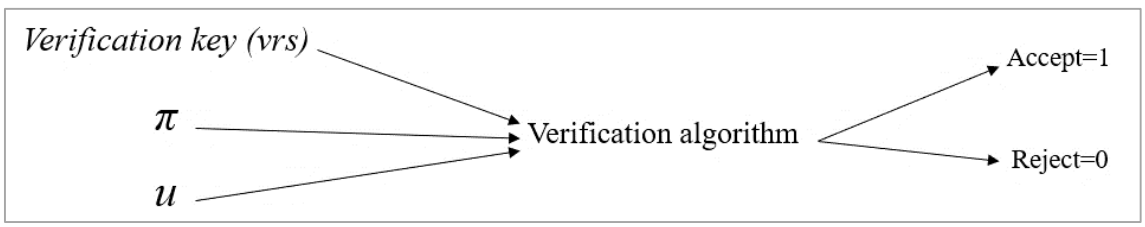

Figure 13.Verification process of zk-SNARK protocol

Implementing AES-256 encryption provides robust protection against data breaches and unauthorized access, thereby contributing to the broader effort to ensure the privacy and security of personal medical information. Meanwhile, ZKP protocols, such as zk-SNARKs, allow for data verification without revealing sensitive information, ensuring privacy and confidentiality.

7.2.3. The Relevance of The Advanced Encryption Standard (AES) in Ensuring Data Security within our Framework

Our system utilizes the advanced encryption algorithm AES-256 to ensure the confidentiality and integrity of patient medical records. AES-256 is widely recognized as the gold standard for protecting sensitive data due to its robustness and efficacy in safeguarding against cyberattacks. This symmetric key algorithm generates a securely stored key accessible to authorized personnel. When a doctor seeks access to a patient's medical record, the AES-256 key is deployed to decrypt the data without retaining it on the device or browser, thus minimizing the risk of unauthorized access or data theft. Moreover, utilizing a unique key for each round significantly increases the encryption process's complexity. This makes it more difficult for attackers to decipher the encrypted data. Also, the byte substitution step operates nonlinearly, obscuring identifiable patterns between the original plaintext and the resulting ciphertext. This adds an extra layer of security by preventing unauthorized parties from deducing the original information. Furthermore, shifting rows and mixing columns further enhance the encryption by dispersing and rearranging the data, making it even more challenging to decipher. These features collectively make the algorithm highly secure, ensuring the confidentiality and integrity of the encrypted data.

7.2.4. The Significance of Using the Zero-Knowledge Proof Protocol in our Proposed System

The proposed system architecture employs advanced Zero Knowledge Proof (ZKP) technology, specifically Zero-Knowledge Succinct Non-Interactive Argument of Knowledge, which is highly accurate and widely used in blockchain applications for secure computation. The significant benefits of using zk-SNARKs in our proposed system are:

- ***Privacy*:** zk-SNARKs effectively provides anonymity and confidentiality for patients by hiding their identities and transaction details.
- ***Scalability*:** zk-SNARKs can reduce the size of data required to execute transactions, allowing for more efficient processing and potentially increasing the scalability of the proposed system. This is accomplished by utilizing succinct proofs, which can verify the correctness of a computation without the need to execute it.
- ***Transparency*:** zk-SNARKs can create publicly verifiable proofs of transactions or computations. This can increase trust in the proposed framework by allowing anyone to verify that it operates correctly.
- ***Security*:** zk-SNARKs can provide cryptographic proofs that ensure the validity of transactions or computations without revealing sensitive information. This can help prevent fraud and protect against attacks such as double-spending.

When a patient intends to share a medical record with a doctor, the application generates a zk-SNARK proof that the doctor has access rights to the record. The proof does not contain any details about the record or other doctors' access privileges, but it enables verification that the doctor has the necessary permissions to access the data.

The system ensures secure proof transmission to the intended recipient, who utilizes it to verify the doctor's access rights and decrypt the record. As the proof mathematically proves that the proof has the required permissions to access the data, the recipient does not necessarily have trust in the sender or the underlying encryption algorithm.

7.2.5. The Relevance of the Combination of Advanced Encryption Standards and zk-SNARKs

Compared to existing techniques, combining AES and zk-SNARK algorithms into a blockchain-based system provides an outstanding improvement in safeguarding electronic health records (EHRs). While previous solutions frequently had limits and obstacles, such as insufficient confidentiality safeguards or a lack of privacy-preserving procedures, the suggested combination overcomes these shortcomings. Through robust encryption, AES guarantees the security of EHR data, protecting critical information from unwanted access. Privacy-preserving searches and proof techniques are achieved by integrating zk-SNARK, allowing users to validate EHR characteristics without disclosing underlying data. Furthermore, the immutability and distributed consensus provided by blockchain technology gives an additional integrity layer.

7.3. Third Layer: Data Storage

Scalability is one of the significant issues regarding storing medical records in a decentralized system. Therefore, we have adopted an off-chain/on-chain approach in our system architecture. The encrypted medical documents are stored on the InterPlanetary File System (IPFS), while the associated metadata is stored on the Ethereum blockchain. IPFS is

a decentralized peer-to-peer network that allows for storing and sharing enormous files, making it ideal for keeping the immense amounts of data contained in medical records. In contrast, the Ethereum blockchain provides a secure and transparent method for storing medical record metadata. This method enhances system scalability by preventing data saturation and ensures the metadata's integrity by leveraging blockchain technology's immutability.

8. System Implementation

This section comprehensively analyzes the proposed framework for protecting patients' medical records. Our approach enhances the security and privacy of data stored on the decentralized Ethereum blockchain by combining advanced techniques such as AES 256 encryption and a zero-knowledge proof protocol. This hybrid method ensures high transparency and accessibility for authorized users while protecting sensitive medical information.

8.1. Material and Tools

This section comprehensively explores the essential tools used in our proposed framework. Our analysis sheds light on the techniques and software required in our framework. We demonstrate our dedication to implementing a sophisticated solution prioritizing data privacy and security by examining these tools in detail.

- ***Ganache***

Ganache is a personal blockchain for Ethereum development that enables developers to test and deploy smart contracts on a local network. Ganache is a local test network in our proposed framework to experiment and fine-tune smart contracts before deployment on the leading Ethereum network. This allows for faster and more efficient development, reducing the risk of errors or security breaches when deploying to the live network. Ganache's user-friendly interface and versatile functionality make it a valuable tool for optimizing smart contract development and testing within our framework.

- ***MetaMask***

MetaMask is a browser extension that acts as an Ethereum blockchain digital wallet, allowing users to store and manage their Ethereum-based assets securely from their web browser. MetaMask is a convenient and secure way to access the decentralized application (dApp) that manages medical data on the Ethereum blockchain in our proposed framework. By incorporating MetaMask, patients and doctors can interact with the dApp easily and securely without having to manage their private keys or wallets, enhancing the accessibility and user-friendliness of our framework.

- ***Remix IDE***

Remix is a web-based integrated development environment (IDE) that facilitates the development and testing of smart contracts for the Ethereum blockchain. By providing a range of tools and features, Remix streamlines the smart contract development process, reducing the risk of errors or vulnerabilities when deploying to the Ethereum network.

- ***Django***

Django is a Python web framework that simplifies the development of web applications. In our framework, Django is the backbone of the dApp that manages sensitive medical data on the Ethereum blockchain. Its robust security and performance make it reliable for building complex, decentralized applications. Django's modular architecture and scalability simplify integration with other framework components, streamlining the building process.

- ***Solidity***

Solidity is a programming language designed mainly for creating smart contracts on blockchain platforms like Ethereum. It ensures blockchain-based applications should conduct transactions and operations, ensuring the execution of secure and decentralized processes.

- ***SNARKJS Library***

SNARKJS library creates secure and privacy-preserving proof of a user's authorized access to a medical record without revealing any record information. This proof is then shared with the intended recipient, who can verify the user's access rights and decrypt the record. Our framework leverages this advanced cryptographic technology to ensure the secure and reliable management of sensitive medical data, providing robust privacy and protection to patients and healthcare providers.

- ***MythX***

MythX functions as a security analysis service designed specifically for Ethereum smart contracts. It empowers individual developers and development teams by enabling them to seamlessly incorporate security measures into the

entire lifecycle of smart contract development. Notably, MythX is seamlessly integrated into popular tools like Truffle and Remix, making it readily accessible and convenient for widespread adoption.

8.2. Smart Contract

In our proposed solution, the smart contract is considered a significant component. We deployed three main ones, as follows:

- ***Contract*:** This smart contract is responsible for the global functioning of the proposed solution.
- ***Roles*:** This smart contract assigns roles to different users (administrators, doctors, and patients).
- ***Verifier*:** The verifier smart contract is responsible for the crucial security task by including zero-knowledge succinct, non-interactive arguments of knowledge (zk-SNARKs).

The following code snippet represents the smart contract for cryptographic proof verification within our decentralized electronic health records solution. The contract's "verify" function validates a provided proof by performing different checks and calculations, leveraging a verifying key, input values, and proof components to assure the integrity of the verification process. The contract improves the security and dependability of the EHR system by performing extensive cryptographic validation, including product pairing assessments. The public "verify proof" method acts as an interface for outside callers, returning a boolean result that certifies the proof's validity. This excerpt demonstrates the careful implementation of cryptographic validation logic, which provides a solid basis for protecting the integrity and privacy of sensitive health information in decentralized EHR systems.

A SNIPPET OF THE SMART CONTRACT RESPONSIBLE FOR PROOF VERIFICATION

```
function verify(uint[] memory input, Proof memory proof) internal view returns (uint) {
    VerifyingKey memory vk = verifyingKey();
    require(input.length + 1 == vk.IC.length, "verifier-bad-input");
    Point vk_x = Point(0, 0);

       for (uint i = 0; i < input.length; i++) {
        require(input[i] < snark_scalar_field, "verifier-gte-snark-scalar-field");
        vk_x = Point.addition(vk_x, Point.scalar_mul(vk.IC[i + 1], input[i]));
       }
    vk_x = Point.addition(vk_x, vk.IC[0]);
    if (!Pairing.pairingProd4(
        Point.negate(proof.A),
        proof.B,
        vk.alfa1,
        vk.beta2,
        vk_x,
        vk.gamma2,
        proof.C,
        vk.delta2
    )) {
        return 1;
    } else {
        return 0;
    }
}
function verifyProof(
    uint[2] memory a,
    uint[2][2] memory b,
    uint[2] memory c,
    uint[1] memory input
) public view returns (bool r) {
    Proof memory proof;
    proof.A = Point(a[0], a[1]);
    proof.B = Point([b[0][0], b[0][1]], [b[1][0], b[1][1]]);
    proof.C = Point(c[0], c[1]);
    uint[] memory inputValues = new uint[](input.length);
    for (uint i = 0; i < input.length; i++) {
        inputValues[i] = input[i];
    }
    if (verify(inputValues, proof) == 0) {
        return true;
    } else {
        return false;
    }
}
```

8.3. Experimental Setup

We conducted experiments with the following configurations to test the performance of the proposed framework:

- 11th Gen Intel(R) Core (TM) i7-1165G7 @ 2.80GHz processor
- And 16.00 GB of memory with Windows 64-bit OS (version 10).

9. Results

In this section, we depict and analyze the results of our proposed system based on various performance metrics such as total cost used by functions, function cost analysis, processing time, and more.

- ***Gas Analysis***

Gas analysis is a crucial component of any blockchain system, as it provides insights into the efficiency and scalability of the system. Our study analyzed the gas usage of several vital functions within a medical record management smart contract. The functions analyzed include addDoctor, addPatient, getPatientDetails, ShareMedicalRecords, saveMedicalRecord, getPatientRecords, and verifyProof. We comprehensively analyzed gas consumption for 103 function calls on our decentralized application, as depicted in Figure 14.

We meticulously recorded gas usage for each transaction to ensure the results presented were relevant and representative. We strategically excluded multiple repetitions of the getPatientRecord function call with zero gas usage to avoid skewing the data with non-representative values. The selection process for the data presented focused on the significance of the proposed functionality and representativeness. As a result, we chose a set of 30 transactions that best represent the observed range of gas usage, encompassing scenarios of both high and low gas consumption. Table 5 details the hash transactions and the corresponding gas consumption obtained from the performance of these 30 transactions. Our analysis revealed varying levels of gas consumption across the different functions. For instance, the addDoctor function exhibited higher gas usage than addPatient, possibly due to the increased complexity and data requirements associated with registering a new healthcare provider. This disparity in gas consumption highlights areas within our smart contract that may benefit from optimization for more efficient resource utilization.

We meticulously crafted the methodology for recording gas usage to ensure accuracy and relevance. The exclusion of repetitive zero gas usage calls like getPatientRecord was a deliberate decision to maintain the integrity of the data, ensuring that only meaningful transactions were analyzed. Comparing our findings with other blockchain systems in healthcare, our model demonstrates a competitive edge in terms of efficiency for specific functions. However, as highlighted in the analysis, there are areas where our gas consumption is on par or slightly higher than industry averages, indicating potential avenues for future optimization. The practical implications of these findings are significant for the operational costs of deploying our blockchain system in a healthcare setting. We could target areas identified as high gas consumers for future optimizations to reduce overall costs. Figure 14 and Table 5 have been designed for clarity and ease of understanding. They include explanatory notes and legends, making it straightforward for readers to interpret the data. Table 5 details hash transactions and the corresponding gas consumption obtained from the performance of 30 transactions.

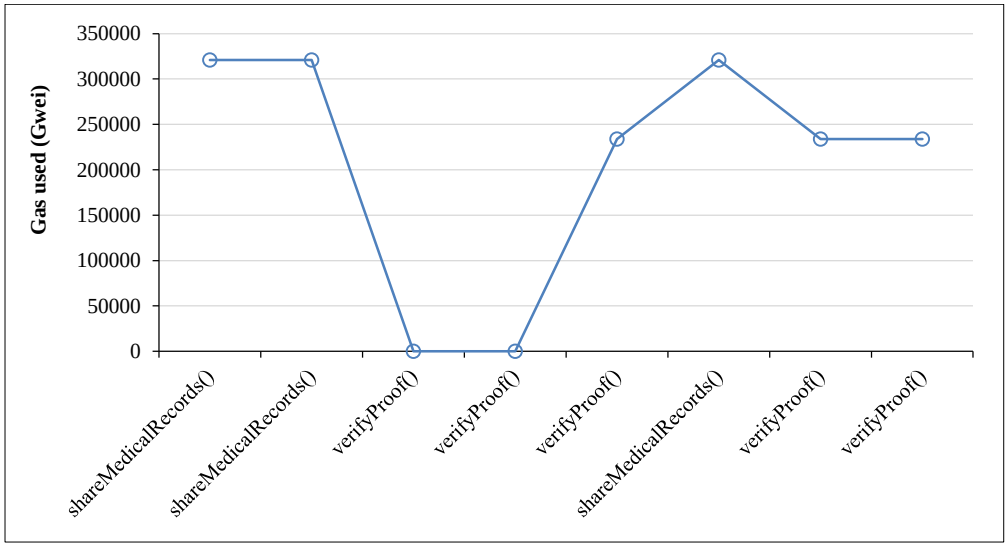

Figure 14. Total gas used by functions (103 transactions)

After thoroughly analyzing gas usage in our medical record management smart contract, we observed that certain functions consumed significantly more gas than others. In particular, we found that the *ShareMedicalRecords()* function for both patients and doctors (functions 320875 and 320873, respectively) incurred the highest gas costs among the 30 transactions analyzed, as depicted in Figure 15. To provide a more comprehensive view of these results, we measured the gas usage for these functions in gwei, which can be converted to ETH and USD using the prevailing exchange rate. Our findings revealed that the highest gas value of 320875 gwei can be converted to 0.000320875 ETH, equivalent to approximately 0.59 USD (at an exchange rate of 1 ETH = 1835,14 USD). In contrast, we also observed that certain functions did not consume any gas, as indicated by a gas value 0.

Table 5. Gas Used Data

Id	Function name	Hash transaction	Gas used (Gwei)
1	addDoctor()	0xdfdb4D7fC885E41263f81D11d6D9eDC0C2CBae32 : (Admin)	46621
2	addPatient()	0x75070012Ae3F94c86EB4480593256A2844a222D2 : (Patient)	157017
3	addPatient()	0x75070012Ae3F94c86EB4480593256A2844a222D2 : (Patient)	157048
4	getpatientDetails()	0x75070012Ae3F94c86EB4480593256A2844a222D2 : (Patient)	0
5	addPatient()	0x75070012Ae3F94c86EB4480593256A2844a222D2 : (Patient)	157040
6	addDoctor ()	0xdfdb4D7fC885E41263f81D11d6D9eDC0C2CBae32 : (Admin)	46599
7	addPatient()	0x75070012Ae3F94c86EB4480593256A2844a222D2 : (Patient)	157040
8	addDoctor()	0xdfdb4D7fC885E41263f81D11d6D9eDC0C2CBae32 : (Admin)	46599
9	ShareMedicalRecords()	0x75070012Ae3F94c86EB4480593256A2844a222D2 : (Patient)	320873
10	getpatientDetails()	0x75070012Ae3F94c86EB4480593256A2844a222D2 : (Doctor)	0
11	addDoctor()	0xdfdb4D7fC885E41263f81D11d6D9eDC0C2CBae32 : (Admin)	46599
12	addPatient()	0x75070012Ae3F94c86EB4480593256A2844a222D2 : (Patient)	157040
13	getpatientDetails()	0x75070012Ae3F94c86EB4480593256A2844a222D2 : (Patient)	0
14	ShareMedicalRecords()	0x75070012Ae3F94c86EB4480593256A2844a222D2 : (Patient)	320875
15	saveMedicalRecord()	0x9bB6208f81B5fD0Fb556735d244d383a0981A0e4 : (Doctor)	181626
16	verifyProof()	0x9bB6208f81B5fD0Fb556735d244d383a0981A0e4 : (Doctor)	0
17	verifyProof()	0x9bB6208f81B5fD0Fb556735d244d383a0981A0e4 : (Doctor)	0
18	getPatientRecords()	0x75070012Ae3F94c86EB4480593256A2844a222D2 : (Doctor)	0
19	verifyProof()	0x9bB6208f81B5fD0Fb556735d244d383a0981A0e4 : (Doctor)	233858
20	getPatientRecords()	0x75070012Ae3F94c86EB4480593256A2844a222D2 : (Doctor)	0
21	addDoctor()	0xdfdb4D7fC885E41263f81D11d6D9eDC0C2CBae32 : (Admin)	46599
22	addPatient()	0x75070012Ae3F94c86EB4480593256A2844a222D2 : (Patient)	157040
23	shareMedicalRecords()	0x75070012Ae3F94c86EB4480593256A2844a222D2 : (Patient)	320851
24	verifyProof()	0x9bB6208f81B5fD0Fb556735d244d383a0981A0e4 : (Doctor)	233856
25	getpatientDetails()	0x75070012Ae3F94c86EB4480593256A2844a222D2 : (Doctor)	0
26	saveMedicalRecord()	0x9bB6208f81B5fD0Fb556735d244d383a0981A0e4 : (Doctor)	181626
27	verifyProof()	0x9bB6208f81B5fD0Fb556735d244d383a0981A0e4 : (Doctor)	233856
28	saveMedicalRecord()	0x9bB6208f81B5fD0Fb556735d244d383a0981A0e4 : (Doctor)	181626
29	saveMedicalRecord()	0x9bB6208f81B5fD0Fb556735d244d383a0981A0e4 : (Doctor)	181626
30	getPatientRecords()	0x75070012Ae3F94c86EB4480593256A2844a222D2 getPatientRecords: (Doctor)	0

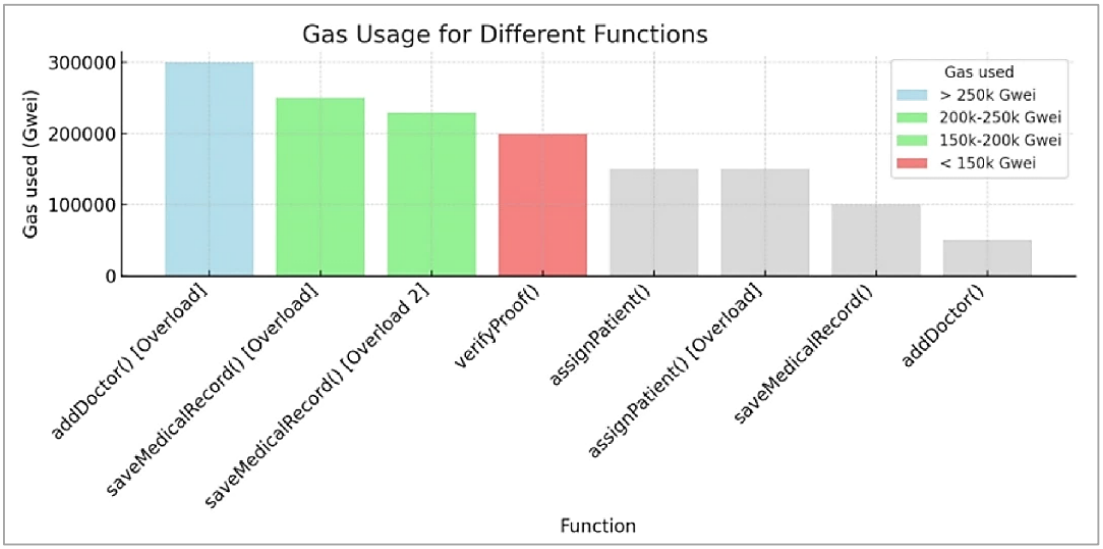

Figure 15. Total gas used by functions (30 selected transactions)

- **Time Analysis**

In our detailed time analysis, illustrated in Figure 16, we meticulously assessed the execution times of various functions within our blockchain-based Electronic Health Records (EHR) system. This analysis revealed significant differences in execution efficiency, which are crucial for understanding and improving the system's performance. The getPatientDetails function recorded the longest execution time, which we could attribute to several factors. These factors include the complexity and volume of patient data retrieved, the computational intensity required for processing this data, or potential inefficiencies in the data retrieval algorithms. This finding points to a critical area for optimization. Enhancing the efficiency of getPatientDetails could involve algorithmic improvements, restructuring of data storage, or streamlining the data processing steps. Such optimizations are vital as they directly impact the system's responsiveness and user experience, especially in time-sensitive medical scenarios where rapid access to patient details is crucial.

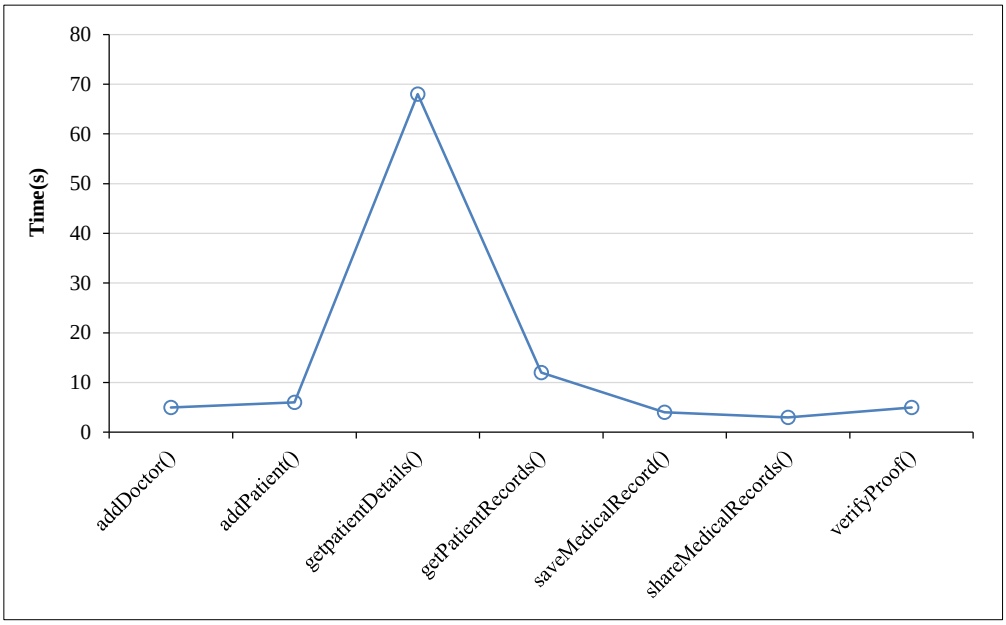

Figure 16. Function time analysis

On the other end of the spectrum, the shareMedicalRecords function demonstrated remarkable efficiency, boasting the shortest execution time among the assessed functions. This efficiency indicates effective optimization within the system, particularly in data sharing and management mechanisms. The quick execution of this function is essential for ensuring seamless and real-time sharing of medical records, a vital requirement for collaborative healthcare environments.

- ***Security Analysis of the Smart Contract***

Our detailed security evaluation of the verifier.sol smart contract, crucial to our blockchain-based healthcare system, is thoroughly presented in Figure 17. This in-depth analysis identified only a low-level vulnerability, indicating the contract's inherent security strength. Deep static analysis techniques, including advanced tools like MythX, were instrumental in meticulously examining the contract for potential vulnerabilities such as reentrancy issues or unsafe function calls. While minor, discovering the low-level vulnerability was critical as it provided a focal point for enhancing the contract's security. It highlighted the need for specific improvements in the contract's coding to mitigate any possible security risks. We took swift and targeted actions to rectify this vulnerability, strengthening the contract's defense against potential threats and attacks. This proactive stance in addressing security concerns not only fixes the immediate issue but also sets a precedent for ongoing vigilance and adaptability in the face of emerging cyber threats. Overall, the findings from our security analysis affirm the reliability and integrity of our smart contract, reinforcing the trustworthiness of our comprehensive blockchain solution in managing and protecting sensitive healthcare data.

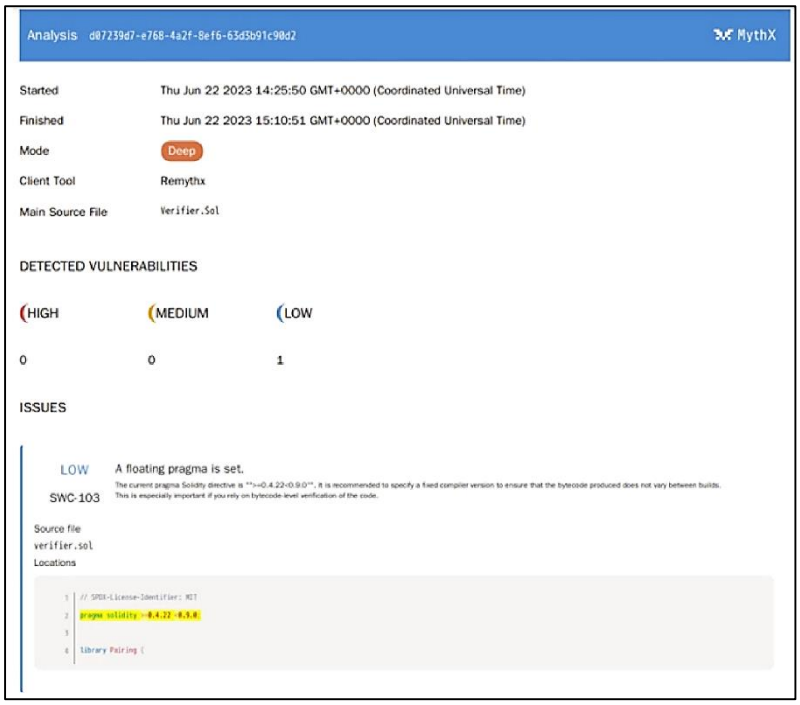

Figure 17. Security analysis of the contract (Verifier.sol)

10. Comparative Study

This section compares crucial aspects of securing electronic health records, namely access control mechanisms, privacy preservation, integrity, and scalability, focusing on blockchain-based EHR systems. In comparison to existing solutions, our proposed system covers all these features. Table 6 represents our proposed solution in comparison to the following existing studies based on access control, integrity, scalability, and privacy-preserving:

Table 6.Comparative study of our proposed system and related works

	Sahoo et al. [37]	Zhang et al. [38]	Rehman et al. [39]	Ren et al. [40]	Our proposed solution
Access control	×	✓	×	✓	✓
Blockchain	✓	✓	✓	✓	✓
Integrity	✓	✓	✓	✓	✓
Scalability	✓	×	✓	✓	✓
Privacy-preserving	✓	✓	✓	×	✓

- ***Access Control***

Access control is vital to safeguarding electronic health records in our system. Hence, we use Role-Based Access Control (RBAC) in conjunction with blockchain technology to ensure the confidentiality and integrity of patient information. In our solution, RBAC enables us to give individuals (patients, doctors, and administrators) unique roles based on their tasks, allowing them suitable access rights. Conversely, blockchain integration creates a decentralized and tamper-proof record, increasing the transparency and traceability of all EHR interactions. By merging RBAC and blockchain, we create a robust access control system that protects EHRs from unauthorized access while maintaining data integrity.

- ***Blockchain***

Blockchain technology is critical to our system, significantly improving the security of electronic health records (EHRs). We protect the integrity and immutability of patient data by employing blockchain, delivering an auditable and tamper-proof record of all EHR transactions. This decentralized and transparent ledger prevents unauthorized changes or data breaches, establishing trust in the system and protecting sensitive medical information.

- ***Integrity***

Integrity refers to the dependability and consistency of data and systems. It is critical in ensuring information correctness, dependability, and completeness. Maintaining the integrity of data is essential to our suggested solution. We have established solid processes and protocols to prevent unwanted changes, data corruption, or manipulation. Our

technology ensures the security of all information saved and processed within the system by utilizing modern encryption algorithms and rigorous validation processes.

- ***Scalability***

Scalability refers to a system's capacity to manage rising workloads and demands while retaining optimal performance and responsiveness. In our system, scalability is considered a significant design aspect. Hence, we merge on-chain and off-chain storage techniques, including IPFS. On-chain storage guarantees that crucial and unchangeable data, such as transaction records and system information, is safely kept within the blockchain. This facilitates information access and verification while utilizing blockchain technology's distributed nature and inherent security characteristics. To accommodate more extensive data sets and media assets, we use the off-chain storage mechanism IPFS in addition to on-chain storage. By adopting this combination, we reduce the pressure on the blockchain network and improve the overall scalability of our system by employing IPFS. This hybrid storage architecture enables our system to handle increasing data and user interactions while maintaining velocity.

- ***Privacy-preserving***

Privacy preservation is an elementary requirement for electronic health records. The solution includes advanced cryptographic techniques to ensure the confidentiality and anonymity of sensitive data. For this reason, we have integrated two powerful tools: Advanced Encryption Standard and zk-SNARKs. The proposed system provides a high degree of confidentiality and privacy by combining the strength of AES encryption with the privacy-preserving capabilities of zk-SNARKs. Patients are more encouraged to interact and share their medical records, knowing that their sensitive data is safe from illegal access and that their privacy is safeguarded throughout the process.

11. Discussion

The primary achievement of our research is the successful incorporation of the Advanced Encryption Standard (AES) within an electronic health record system, ensuring robust security for patient data. This is particularly evident in the 'getPatientDetails' function, where, despite increased execution times, the security integrity remained uncompromised. In contrast, the "ShareMedicalRecords" function demonstrated efficiency, primarily involving data encryption tasks.

Compared to conventional EHR systems, which are often vulnerable due to centralized data storage, our blockchain-based solution offers a significant advancement in security and decentralization. This approach effectively mitigates risks associated with single points of failure and common security breaches. Our system's performance, in terms of execution time and gas cost, also holds its own compared to other blockchain-based healthcare solutions, marking a notable improvement over traditional models.

The findings highlight a crucial trade-off between security and performance in healthcare data systems. While providing high security, the AES algorithm introduces complexity and execution delays. Our research suggests that future studies should explore alternatives to optimize this balance through advanced cryptographic techniques like zero-knowledge proofs, including zk-SNARKs.

A significant strength of our work lies in the innovative application of blockchain technology in EHR systems, providing a decentralized, secure, and scalable solution. This represents a significant leap forward in protecting patient data integrity and privacy in the healthcare sector. However, the study has limitations. The increased computational demands and execution times associated with AES encryption highlight areas for improvement. Addressing these limitations could involve exploring alternative cryptographic methods that maintain security while enhancing system efficiency.

Our study's essential contribution is demonstrating a feasible blockchain-based EHR system that balances high-end security and operational efficiency. This contribution is pivotal in the current landscape of digital health records, where protecting sensitive patient information is paramount. By advancing a solution that tackles security concerns and performance challenges, our research sets a new benchmark for future innovations in healthcare data management.

12. Conclusion

This study has successfully developed a comprehensive security framework for electronic health records by integrating zero-trust principles with blockchain technology, addressing significant concerns related to data breaches and privacy in healthcare. Combining zero succinct proof advanced encryption standards with blockchain's immutability, our approach establishes a secure environment for patients and healthcare providers. Incorporating smart contracts further strengthens this system, creating a highly secure and efficient platform for managing sensitive health information. We employed innovative on-chain and off-chain data storage strategies to address the scalability issues associated with traditional EHR systems, enhancing the system's efficiency and reliability. This potent blend of technologies aims to establish an impenetrable shield for patient data protection, thereby significantly advancing the

field of healthcare data management. Our comparative analysis with existing solutions highlights the originality and superiority of our approach, particularly in terms of cost-efficiency and security. Looking forward, our future work will focus on implementing this system on the existing Ethereum blockchain network, aiming to optimize resource efficiency and further secure patient data. Additionally, we plan to explore new strategies to improve security measures and reduce resource consumption, ultimately enhancing the effectiveness and viability of EHR systems in the healthcare industry. This forward-thinking approach will enable healthcare providers to deliver exceptional care while upholding the highest patient privacy and data security standards.

13. Declarations

13.1. Author Contributions

Conceptualization, R.B.; methodology, R.B.; software, R.B.; validation, Y.G. and S.M.; formal analysis, R.B.; investigation, Y.G. and S.M.; resources, R.B., Y.G., and S.M.; data curation, R.B.; writing—original draft preparation, R.B.; writing—review and editing, S.M. and Y.G.; visualization, R.B.; supervision, S.M. and Y.G.; project administration, Y.G. and S.M. All authors have read and agreed to the published version of the manuscript.

13.2. Data Availability Statement

Data sharing is not applicable to this article.

13.3. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

13.4. Institutional Review Board Statement

Not applicable.

13.5. Informed Consent Statement

Not applicable.

13.6. Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

14. References

[1] Ghosh, P. K., Chakraborty, A., Hasan, M., Rashid, K., & Siddique, A. H. (2023). Blockchain Application in Healthcare Systems: A Review. Systems, 11(1), 38. doi:10.3390/systems11010038.

[2] Sadeghib R, J. K., Prybutok, V. R., & Sauser, B. (2022). Theoretical and practical applications of blockchain in healthcare information management. Information and Management, 59(6), 103649. doi:10.1016/j.im.2022.103649.

[3] Hajian, A., Prybutok, V. R., & Chang, H. C. (2023). An empirical study for blockchain-based information sharing systems in electronic health records: A mediation perspective. Computers in Human Behavior, 138, 107471. doi:10.1016/j.chb.2022.107471.

[4] Srivastava, S., Pant, M., Jauhar, S. K., & Nagar, A. K. (2022). Analyzing the Prospects of Blockchain in Healthcare Industry. Computational and Mathematical Methods in Medicine, 2022, 3727389. doi:10.1155/2022/3727389.

[5] Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review. British Journal of Management, 14(3), 207–222. doi:10.1111/1467-8551.00375.

[6] Han, Y., Zhang, Y., & Vermund, S. H. (2022). Blockchain Technology for Electronic Health Records. International Journal of Environmental Research and Public Health, 19(23), 1577. doi:10.3390/ijerph192315577.

[7] d'Aliberti, O. G., & Clark, M. A. (2022). Preserving Patient Privacy during Computation over Shared Electronic Health Record Data. Journal of Medical Systems, 46(12), 85. doi:10.1007/s10916-022-01865-5.

[8] Zhang, R., Xue, R., & Liu, L. (2022). Security and Privacy for Healthcare Blockchains. IEEE Transactions on Services Computing, 15(6), 3668–3686. doi:10.1109/TSC.2021.3085913.

[9] Lan, C., & Li, H. (2023). BC-PC-Share: Blockchain-Based Patient-Centric Data Sharing Scheme for PHRs in Cloud Computing. CMES - Computer Modeling in Engineering and Sciences, 136(3), 2985–3010. doi:10.32604/cmes.2023.026321.

[10] Vernekar, A., Sakhare, A., Bhapkar, P., Jadhav, S., & Adhao, R. B. (2023). Blockchain Based Record Management System in Hospitals. 2023 International Conference on Innovative Trends in Information Technology, ICITIIT 2023, 1–4. doi:10.1109/ICITIIT57246.2023.10068685.

[11] Xu, S., Zhong, J., Wang, L., He, D., Zhang, S., & Shao, W. (2023). A privacy-preserving and efficient data sharing scheme with trust authentication based on blockchain for mHealth. Connection Science, 35(1), 2186316. doi:10.1080/09540091.2023.2186316.

[12] Vanin, F. N. da S., Policarpo, L. M., Righi, R. da R., Heck, S. M., da Silva, V. F., Goldim, J., & da Costa, C. A. (2023). A Blockchain-Based End-to-End Data Protection Model for Personal Health Records Sharing: A Fully Homomorphic Encryption Approach. Sensors, 23(1), 14. doi:10.3390/s23010014.

[13] Mahammad, A. B., & Kumar, R. (2023). Scalable and Security Framework to Secure and Maintain Healthcare Data using Blockchain Technology. Proceedings of International Conference on Computational Intelligence and Sustainable Engineering Solution, CISES 2023, 417–423. doi:10.1109/CISES58720.2023.10183494.

[14] Semantha, F. H., Azam, S., Shanmugam, B., & Yeo, K. C. (2023). PbDinEHR: A Novel Privacy by Design Developed Framework Using Distributed Data Storage and Sharing for Secure and Scalable Electronic Health Records Management. Journal of Sensor and Actuator Networks, 12(2), 36. doi:10.3390/jsan12020036.

[15] Agrawal, K., Aggarwal, M., & Tanwar, S. (2023). MyEasyHealthcare: An efficient and secure three-tier blockchain-based healthcare system. Security and Privacy, 6(6), 314. doi:10.1002/spy2.314.

[16] Li, C., Liu, J., Qian, G., Wang, Z., & Han, J. (2022). Double chain system for online and offline medical data sharing via private and consortium blockchain: A system design study. Frontiers in Public Health, 10, 1012202. doi:10.3389/fpubh.2022.1012202.

[17] Jiang, Y., Xu, X., & Xiao, F. (2022). Attribute-Based Encryption with Blockchain Protection Scheme for Electronic Health Records. IEEE Transactions on Network and Service Management, 19(4), 3884–3895. doi:10.1109/TNSM.2022.3193707.

[18] Egala, B. S., Pradhan, A. K., Gupta, S., Sahoo, K. S., Bilal, M., & Kwak, K. S. (2022). CoviBlock: A Secure Blockchain-Based Smart Healthcare Assisting System. Sustainability (Switzerland), 14(24), 16844. doi:10.3390/su142416844.

[19] Gupta, A., Rodrigues, R., Tripathi, A., Coutinho, R., & Gomes, J. (2022). Blockchain for EHR: an off-chain based approach. 2022 IEEE Region 10 Symposium, TENSYMP 2022, 1–6. doi:10.1109/TENSYMP54529.2022.9864405.

[20] Pang, Z., Yao, Y., Li, Q., Zhang, X., & Zhang, J. (2022). Electronic Health Records Sharing Model based on Blockchain with Checkable State PBFT Consensus Algorithm. IEEE Access, 10, 87803–87815. doi:10.1109/ACCESS.2022.3186682.

[21] Nasreen, M., & Singh, S. K. (2022). Implementation of Blockchain based Electronic Health Record System using Java Eclipse and MongoDB. 2022 IEEE International Conference on Blockchain and Distributed Systems Security, ICBDS 2022, 1–6. doi:10.1109/ICBDS53701.2022.9935933.

[22] Jayasinghe, J. G. L. A., Shiranthaka, K. G. S., Kavith, T., Jayasinghe, M. H. D. V., Abeywardena, K. Y., & Yapa, K. (2022). Blockchain-based Secure Environment for Electronic Health Records. 2022 13th International Conference on Computing Communication and Networking Technologies, ICCCNT 2022, 1–6. doi:10.1109/ICCCNT54827.2022.9984371.

[23] Sexena, P., Singh, P., John, A., & Rajesh, E. (2022). Blockchain Powered EHR in Pharmaceutical Industry. In Digitization of Healthcare Data Using Blockchain. John Wiley & Sons, Ltd., 137-157. doi:10.1002/9781119792734.ch7.

[24] Zou, R., Lv, X., & Zhao, J. (2021). SPChain: Blockchain-based medical data sharing and privacy-preserving eHealth system. Information Processing and Management, 58(4), 102604. doi:10.1016/j.ipm.2021.102604.

[25] Yu, K., Tan, L., Shang, X., Huang, J., Srivastava, G., & Chatterjee, P. (2021). Efficient and Privacy-Preserving Medical Research Support Platform against COVID-19: A Blockchain-Based Approach. IEEE Consumer Electronics Magazine, 10(2), 111–120. doi:10.1109/MCE.2020.3035520.

[26] Sonkamble, R. G., Phansalkar, S. P., Potdar, V. M., & Bongale, A. M. (2021). Survey of Interoperability in Electronic Health Records Management and Proposed Blockchain Based Framework: MyBlockEHR. IEEE Access, 9, 158367–158401. doi:10.1109/ACCESS.2021.3129284.

[27] Rincón, E. A. P., & Moreno-Sandoval, L. G. (2021). Design of an architecture contributing to the protection and privacy of the data associated with the electronic health record. Information (Switzerland), 12(8), 313. doi:10.3390/info12080313.

[28] Nagasubramanian, G., Sakthivel, R. K., Patan, R., Gandomi, A. H., Sankayya, M., & Balusamy, B. (2020). Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. Neural Computing and Applications, 32(3), 639–647. doi:10.1007/s00521-018-3915-1.

[29] Madine, M. M., Battah, A. A., Yaqoob, I., Salah, K., Jayaraman, R., Al-Hammadi, Y., Pesic, S., & Ellahham, S. (2020). Blockchain for Giving Patients Control over Their Medical Records. IEEE Access, 8, 193102–193115. doi:10.1109/ACCESS.2020.3032553.

[30] Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. Journal of Information Security and Applications, 50, 102407. doi:10.1016/j.jisa.2019.102407.

[31] Guo, H., Li, W., Meamari, E., Shen, C. C., & Nejad, M. (2020). Attribute-based Multi-Signature and Encryption for EHR Management: A Blockchain-based Solution. In IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2020. doi:10.1109/ICBC48266.2020.9169395.

[32] Gutiérrez, O., Romero, G., Pérez, L., Salazar, A., Wightman, P., & Charris, M. (2020). Healthyblock: Blockchain-based it architecture for electronic medical records resilient to connectivity failures. International Journal of Environmental Research and Public Health, 17(19), 1–38. doi:10.3390/ijerph17197132.

[33] Tith, D., Lee, J. S., Suzuki, H., Wijesundara, W. M. A. B., Taira, N., Obi, T., & Ohyama, N. (2020). Application of blockchain to maintaining patient records in electronic health record for enhanced privacy, scalability, and availability. Healthcare Informatics Research, 26(1), 3–12. doi:10.4258/hir.2020.26.1.3.

[34] Nakamoto, S. (2008). A Peer-to-Peer Electronic Cash System. Bitcoin. Available online: https://bitcoin.org/bitcoin.pdf (accessed on May 2023).

[35] Ethereum (2023). Ethereum Whitepaper. Available online: https://ethereum.org (accessed on May 2023).

[36] Daemen, J., Rijmen, V. (2023). AES Proposal: Rijndael; Technical Report; National Institute of Standards and Technology: Gaithersburg, Maryland, United States.

[37] Sahoo, M. S., & Baruah, P. K. (2018). HBasechainDB – A scalable blockchain framework on Hadoop ecosystem. In R. Yokota & W. Wu (Eds.), Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Springer, Vol. 10776 LNCS, 18–29. doi:10.1007/978-3-319-69953-0_2.

[38] Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2018). FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data. Computational and Structural Biotechnology Journal, 16, 267–278. doi:10.1016/j.csbj.2018.07.004.

[39] Rehman, A., Abbas, S., Khan, M. A., Ghazal, T. M., Adnan, K. M., & Mosavi, A. (2022). A secure healthcare 5.0 system based on blockchain technology entangled with federated learning technique. Computers in Biology and Medicine, 150, 106019. doi:10.1016/j.compbiomed.2022.106019.

[40] Ren, J., Li, J., Liu, H., & Qin, T. (2022). Task offloading strategy with emergency handling and blockchain security in SDN-empowered and fog-assisted healthcare IoT. Tsinghua Science and Technology, 27(4), 760–776. doi:10.26599/TST.2021.9010046.