

Received 20 May 2024, accepted 3 June 2024, date of publication 11 June 2024, date of current version 19 June 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3412793

RESEARCH ARTICLE

Securing EHRs With a Novel Token-Based and PPoS Blockchain Methodology

RIHAB BENAICH^{ID}, SAIDA EL MENDILI^{ID}, AND YOUSSEF GAHI^{ID}, (Senior Member, IEEE)

Engineering Sciences Laboratory, National School of Applied Sciences, Ibn Tofail University, Kenitra 14000, Morocco

Corresponding author: Rihab Benaich (rihab.benaich@uit.ac.ma)

ABSTRACT Blockchain technology is vital in strengthening the security of private information, particularly in the healthcare sector. Its features, such as confidentiality, decentralization, security and privacy, address challenges traditional healthcare systems face, such as phishing, denial of service and identity theft attacks. In this regard, our research paper presents a security solution specifically tailored for healthcare applications. This solution integrates decentralized identity management (DIDs) for identity verification, employs the advanced ChaCha20-Poly1305 encryption algorithm to ensure data confidentiality, and utilizes a token-based mechanism for immutable record keeping. Furthermore, it incorporates a pure proof of stake (PPoS) consensus mechanism to enhance system security while optimizing efficiency. This comprehensive and scalable system showcases improvements in cost effectiveness, time efficiency of an average of 6,5 seconds and overall data protection compared to traditional approaches used in healthcare data security.

INDEX TERMS Blockchain, data security, decentralized identifiers, EHRs, healthcare, PPoS.

I. INTRODUCTION

The healthcare field is critical, particularly regarding the security and privacy of patient data. In this context, medical records are more than documents; they contain health information that plays a crucial role in patient care. It is vital to protect this data to maintain confidentiality and ensure the effectiveness of medical treatments and healthcare services. However, ensuring a balance between safeguarding this information and providing authorized personnel access can be difficult, especially considering the rising occurrence of data breaches and cyber threats. Traditional medical records systems, which play a vital role in healthcare management, encounter significant challenges, especially in cost and security. Similarly, storing records incurs expenses related to space requirements, maintenance and ensuring their physical protection. This leads to inefficiencies in retrieving and managing data as an increased risk of damage or loss. Likewise, handling medical records manually increases the chance of human error mistakes, such as incorrect data entry, misinterpreting handwriting, or mishandling information, which have severe consequences for patient treatment

The associate editor coordinating the review of this manuscript and approving it for publication was Sedat Akleylek^{ID}.

and diagnosis. These errors place safety at risk and expose healthcare providers to potential legal and reputational issues.

Moving from the classic medical records management, the digitization of healthcare systems marked a significant milestone in the evolution of modern medicine and has fundamentally transformed the management and accessibility of electronic health records (EHRs). This shift from traditional paper-based documents to digital platforms has been instrumental in enhancing the efficiency of healthcare delivery [1], facilitating rapid access to patient information, and enabling the broader utilization of data for research and public health initiatives. However, this digital transformation is accompanied by substantial challenges, particularly in data security, privacy, and efficient management. While digitization offers numerous benefits, it exposes healthcare data to cyber threats [2], [3]. The security of EHRs is a complex issue that encompasses protecting sensitive patient information from unauthorized access and breaches and maintaining data integrity. As cyber threats evolve in sophistication, from ransomware and phishing to more advanced tactics [4], healthcare systems face increasing risks. This situation is further complicated by the need to uphold rigorous privacy standards in healthcare, where the confidentiality of patient

records is not just a technological requirement but also a regulatory and ethical imperative.

Furthermore, the introduction of digitized records adds another layer of complexity. Healthcare providers often rely on security methods and algorithms that effectively safeguard patient information but need help with the demands for speed and efficiency. While these traditional security measures ensure data integrity, they are often slow and unmanageable, causing quick access and information sharing bottlenecks, such as emergencies or real-time decision-making for patient care.

Additionally, the efficiency of managing these digitized records remains a significant concern. Despite their advancements, many existing electronic health records systems require more scalability and flexibility. Scalability is essential to accommodate the growing volume of data and the expanding network of users. At the same time, flexibility is crucial for adapting to dynamic healthcare practices, technological changes, and regulatory demands. The current rigidity of many EHR systems leads to inefficiencies such as data silos, redundant processes, and slow information retrieval, adversely affecting patient care and operational productivity. Moreover, electronic health records systems often need to be able to retrieve and process data due to their reliance on storage. These delays occur, especially when there are requests for access at the time. Moreover, integrating data sources, like laboratories, pharmacies, and other healthcare providers, can worsen these latency issues. As a result, it affects the efficiency of accessing data and interferes with the timely update and retrieval of patient records, thus impacting healthcare services' overall responsiveness and effectiveness. Furthermore, healthcare providers frequently utilize systems to manage records, which can cause a lack of standardized protocols for exchanging data [5]. These interoperability issues require improvement in sharing information across various healthcare platforms, potentially resulting in treatment delays and obstacles in delivering coordinated care.

The existing literature underscores these gaps, revealing a critical need for EHR frameworks that are robust, scalable, and adaptable to the complexities of the digital healthcare environment [6]. The traditional models must comprehensively address the intertwined challenges of securing sensitive health information, ensuring privacy, and maintaining operational efficiency. Conversely, integrating blockchain technology presents an appealing solution to these challenges in managing medical records [7], [8], [9]. Its decentralized structure reduces the risk of data breaches since there is no central point of failure. The inherent immutability of blockchain ensures that once a record is added, it cannot be modified, thus guaranteeing data integrity. This aspect is particularly significant in healthcare, where record accuracy is essential. Additionally, blockchain enables interoperability by establishing an unalterable and transparent system for recording information that all authorized stakeholders in the healthcare network can access. This results in enhanced patient care coordination [8] and efficient data handling.

To tackle these issues, this study seeks to investigate the following research questions:

- How can blockchain technology be used efficiently to safeguard the privacy and accuracy of EHRs from unauthorized access?
- What effects do integrating decentralized identity management (DIDs) and advanced encryption algorithms such as ChaCha20-Poly1305 and a token-based access control system have on the security and integrity of EHRs?
- How does implementing a PPoS consensus mechanism improve the effectiveness and security of EHR systems?

Keeping this in mind, this paper presents a novel, multi-layered security framework for EHRs to address the critical data protection, privacy, and efficiency gaps within healthcare information systems. Keeping this in mind, we propose a framework that integrates several advanced technologies, each contributing uniquely to a comprehensive and user-centric EHR system.

The main contributions of this paper are:

- 1) **Improving Identity Management:** Our solution introduces a Decentralized Identity Management (DID) system that empowers users to control their identities without depending on central authorities. Blockchain enables participants to create, manage, and share their identities securely. By storing identity information on the blockchain, our DID system significantly boosts resilience against cyber-attacks and improves data integrity.
- 2) **Enhancing Data Security with ChaCha20-Poly1305:** We employ the advanced ChaCha20-Poly1305 algorithm, optimizing the balance between strong encryption and high performance, ensuring the integrity and confidentiality of health records.
- 3) **Integration of Algorand Blockchain and PPoS consensus:** Our approach utilizes Algorand's blockchain technology and PPoS consensus mechanism, enhancing the traceability and security of health records while reducing costs and latency. This marks a significant advancement in data management.
- 4) **Simplifying Access with Token-Based Control:** Our system introduces a token-based access control mechanism, reducing administrative overhead and enhancing security by restricting access to sensitive health data to authorized personnel only. This is achieved through generated tokens that undergo validation and are associated with specific user roles and permissions, ensuring a secure and efficient access management process.

The rest of the paper is organized as follows: Section II delves into the problem statement. Then, we highlight some relevant studies in Section III. Section IV provides information on the background of the proposition, including blockchain, DIDs, token-based access and ChaCha20-Poly1305. Afterwards, section V highlights the key steps followed to achieve the solution. Moving forward to Section VI, we present our proposed solution in detail. In Section VII, we discuss the

results and aspects of implementation. Section VIII concludes with a summary and some future works.

II. CHALLENGES IN TRADITIONAL METHODS MANAGEMENT

The following section provides an overview of three key areas: the challenges associated with conventional medical records systems, the issues inherent in electronic health records, and the significance of integrating blockchain technology into electronic health records.

Traditional paper-based medical records face enormous challenges in healthcare management due to their reliance on non-digital methods. The physical constraints of paper records, such as the requirement for storage space, susceptibility to damage and limited access for one user at a time, contribute to increased expenses, inefficiencies and the potential for data inaccuracies.

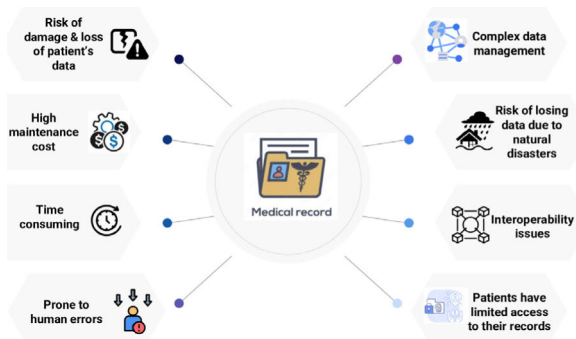


FIGURE 1. Challenges of traditional medical records.

These challenges (FIGURE 1) often lead to poor patient care as vital information is slowly updated and exchanged between healthcare providers, emphasizing the need for a cohesive system.

Adopting electronic health records has revolutionized healthcare operations by simplifying data management. However, transitioning to electronic records comes with risks, particularly regarding data security. The surge in data breaches during the COVID-19 pandemic highlights vulnerabilities in EHR systems exacerbated by challenges in interoperability that delay smooth information sharing among healthcare networks while adding administrative complexities for healthcare professionals.

While incorporating cloud computing into record systems improves accessibility, it raises substantial security concerns (FIGURE 2). Storing information on cloud platforms makes it susceptible to cyber threats, complicates compliance with data protection regulations, and raises concerns about data ownership and system reliability.

To address these security challenges, blockchain technology emerges as a solution for fortifying EHR systems. The decentralized aspect addresses the vulnerability problem, significantly decreasing the chance of cyberattacks. Blockchain guarantees that records remain unchanged and traceable, which is essential for ensuring the precision and

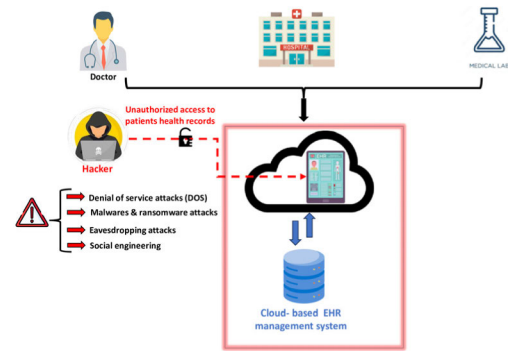


FIGURE 2. Cybersecurity threats to cloud-based EHR systems.

dependability of data. Through smart contracts, blockchain allows for the secure handling of access permissions, ensuring that data access follows regulations and is managed. It also improves the trustworthiness and confidentiality of healthcare information within various systems.

III. RELATED WORKS

In the same context, numerous studies have recently explored integrating blockchain and relevant technologies into EHR security, reflecting a growing recognition of its potential benefits. These research efforts highlight how blockchain and advanced approaches can address the inherent vulnerabilities in traditional EHR systems. This section highlights the main contributions made regarding EHRs and healthcare security.

A. SECURITY SOLUTIONS DESIGNED FOR ELECTRONIC HEALTH RECORDS AND HEALTHCARE

Many studies have explored advanced technologies to enhance healthcare security across various domains. This section summarizes fundamental studies and findings contributing to this regard. In [10], the authors proposed a novel certificateless Provable Data Possession scheme for securely managing electronic health records on cloud servers. This scheme addresses the challenge of ensuring correct storage and integrity of EHRs by distributing multiple copies across various cloud servers, enhancing data recoverability. It introduces a new data structure, the Map-Version Marker Table, for dynamic operations and traceability at the block level, enabling authorized doctors to access historical EHRs. The paper asserts the scheme's security based on the computational Diffie-Hellman problem's intractability and demonstrates its practicality for cloud-based EHR applications.

In [11], the authors address security challenges in healthcare IoT, particularly for cloud-based EHRs. They propose a system providing fine-grained access control and dynamic user groups, enhancing scalability and functionality. The system includes an efficient revocation mechanism, ensuring forward and backward secrecy and revocable storage to prevent unauthorized data access. This solution is secure against real-world threats, addressing the critical need for robust

TABLE 1. Relative works made regarding EHRs and healthcare security.

Paper	Year	Blockchain in the context of EHR/healthcare Security?	Contribution
[15]	2023	YES	The authors introduced LightMED, a method that improves security and privacy in healthcare systems by combining devices with cloud technology. This strategy ensures the protection of data transmission and collection from gadgets using encryption and digital signatures, addressing the security gaps often overlooked in current systems. LightMED combines fog computing, CP-ABE and blockchain to enable the scalable sharing of electronic medical records (EMRs). It includes encryption, a privacy-focused access policy, and a policy update mechanism that allows EMR owners to securely and efficiently control access.
[16]	2023	YES	The authors proposed a new method for searching medical blockchain data, featuring an encryption-based approach with an integrated access control mechanism. This innovation addresses issues such as limited search methodologies and risks of privacy breaches.
[17]	2023	YES	The authors proposed a secure blockchain-based application for generating, maintaining, and validating healthcare certificates. This proposition bridges the backend blockchain network and application entities like hospitals, patients, physicians, and IoT devices. It focuses on providing and validating medical certificates while providing essential security characteristics like confidentiality, authentication, and access control using smart contracts.
[18]	2023	YES	The authors proposed a novel scheme integrating ciphertext-policy attribute-based encryption and blockchain for secure PHR management in intelligent health systems. This method mitigates unauthorized access and privacy breaches, ensuring data integrity while enabling malicious user traceability and revocation.
[19]	2023	YES	The authors developed a blockchain solution for EHR storage in a decentralized cloud-assisted environment. The system ensures data integrity and security by leveraging the blockchain's immutable and transparent nature. This approach addresses critical healthcare data management issues, such as tampering and unauthorized access. The blockchain-based system significantly advances secure, efficient healthcare data management in cloud environments.
[20]	2023	YES	The authors proposed a novel technique for preserving electronic health records (EHRs) privacy. It utilizes a convolutional neural network (CNN) to classify normal and abnormal users in healthcare data and integrates blockchain with a cryptography-based federated learning module. This approach effectively processes and removes abnormal users from the database, ensuring secure access to health records.
[21]	2023	YES	The authors proposed a solution to address the challenges of traditional EHR systems, such as inconsistent data handling, limited access, and poor coordination across facilities. The proposed solution leverages the Ethereum blockchain and advanced encryption techniques, like the Advanced Encryption Standard and Zero-Knowledge Proof Protocol.
[22]	2023	YES	The authors proposed a new searchable encryption scheme designed explicitly for cloud-assisted EHRs. This scheme addresses privacy concerns when searching for sensitive data in the cloud. The system uses blockchain and hash-proof chains, enabling public verification of search results without a trusted authority. It supports dynamic datasets with enhanced security through a novel hidden data structure.
[23]	2022	YES	The authors introduced an architecture for protecting privacy in healthcare utilizing Blockchain and Federated Learning technologies. This innovative architecture combines cloud platforms based on Blockchain to strengthen security and privacy measures in healthcare systems, especially within the context of a smart city. The integration of Federated Learning technology enables machine learning applications at scale, authorizing users to leverage trained models without compromising their data by sending it to the cloud.
[24]	2022	YES	The authors proposed a cryptographic scheme for EHRs in edge cloud environments, integrating attribute-based encryption (ABE) with blockchain. It enhances EHR security by enabling confidential transmission of treatment information and uses blockchain to ensure data integrity and traceability. This approach allows for fine-grained attribute revocation in ciphertext management, improving key generation and decryption performance and reducing computational overhead compared to other algorithms.
[25]	2022	YES	The authors presented a novel, delectable consortium blockchain-based EHR storage model for cloud-assisted healthcare. It integrates EHR operations into a consortium blockchain, ensuring the confidentiality, integrity, and correctness of outsourced EHRs. The model employs collaborative multi-cloud storage for durability and availability, arranging transactions by EHR type for efficient block deletion.
[26]	2022	YES	Using blockchain technology, the authors proposed a secure e-health system for managing patient EHRs. This system protects EHRs from tampering or unauthorized access by leveraging pairing-based cryptography to create tamper-proof records. These records are integrated into blockchain transactions, ensuring verifiability and protection against illegal modifications. Additionally, the system includes secure payment protocols using blockchain-based smart contracts for diagnostic and storage services.

TABLE 1. (Continued.) Relative works made regarding EHRs and healthcare security.

[27]	2022	YES	The authors proposed a secure data-sharing framework for the industrial healthcare system that combines permissioned blockchain, smart contracts, and deep learning. The solution registers and verifies entities through a blockchain-based system with zero-knowledge proof and an intelligent contract consensus mechanism. It also features a novel deep learning scheme combining stacked sparse variational autoencoder and self-attention-based bidirectional long short-term memory for transforming healthcare data and enhancing attack detection.
[28]	2021	YES	The authors designed a novel blockchain-based system named SPChain that enhances the sharing and privacy of electronic medical records. It innovatively speeds up data retrieval and motivates healthcare institutions to participate through a unique reputation system. Additionally, the system employs proxy re-encryption for secure data sharing.
[29]	2021	YES	The authors proposed a solution based on blockchain technology to improve the security and privacy of health monitoring sensors within a network, especially in the healthcare sector. The method involves utilizing edge devices to create blocks on a blockchain for transmitting healthcare data, which helps minimize the risk of data tampering and protects confidentiality. The system's effectiveness was through block preparation time, header generation time, tensor reduction ratio and approximation error. These improvements ensure a more dependable method of managing healthcare data.
[30]	2019	YES	The authors proposed a prototype based on blockchain that enhances the reliability and trustworthiness of data in trials. This innovative system ensures that clinical trial data remains unchangeable, traceable and highly dependable. Accurate data from a completed trial was employed to validate its effectiveness, demonstrating its ability to resist any attempts at tampering with the data and providing an audit trail for regulators.

privacy protection in healthcare data management. Also, [12], the authors proposed a secure system for managing electronic health records (EHRs) in the cloud. It employs a hybrid cryptographic approach combining the Improved Key Generation Scheme of RSA and Blowfish algorithms for data encryption. Additionally, it integrates steganography-based access control for secure key sharing. The system enhances EHR security and ensures efficient retrieval.

Moreover, to ensure data security, the authors [13] designed a Privacy-Preserving Federated Learning Scheme with Homomorphic Encryption to tackle the privacy and security concerns surrounding healthcare data. The approach combines encryption on the client side to ensure the confidentiality of shared training models and Access Control technology to verify user identities and their trustworthiness. An acknowledgement mechanism was employed on the server side to handle users efficiently, reducing communication overhead and addressing user dropout during training. This dual strategy effectively strengthens privacy protection and optimizes the federated learning process in healthcare applications. Furthermore, [14], the authors developed a mechanism named BtRaI, which combines technology and trusted reputation assessment to improve security in healthcare services. The main goal of BtRaI is to enhance healthcare services, such as accurate time monitoring and remote disease diagnosis. It accomplishes this by providing a comprehensive reputation assessment system that encourages participation in the consensus process, thus discouraging malicious behavior. Some key features of BtRaI include incorporating factors for a multidimensional reputation assessment, a PBFT algorithm for improved efficiency in blockchain consensus and a token-based reward and punishment system.

B. BLOCKCHAIN-BASED SOLUTIONS

In this section, we present the relevant studies done in the context of EHRs and Healthcare incorporating the adoption of blockchain-based solutions. Table 1 summarizes studies investigating the uses, advantages, obstacles and innovative approaches to integrating blockchain into healthcare information systems. Each study outlined in the table presents a viewpoint or strategy for leveraging a blockchain-based approach to enhance the security, effectiveness and patient-centeredness of EHRs platforms. The topics covered include frameworks, architectural suggestions, and practical trials and implementations. These studies commonly explore how blockchain can establish an unchangeable record for health data, maintain data accuracy, facilitate the sharing of patient information among authorized parties and empower patients to have more control over their health data.

This section explored research and studies on improving the security of electronic health records and healthcare systems. These efforts have contributed to overcoming obstacles and establishing a solid foundation for more secure and efficient healthcare data management. Despite these advancements, challenges still need to be addressed in EHR security. Concerns like scalability, transaction speed, and cost remain at the forefront of discussions. Additionally, with the evolving era of cyber threats, it becomes imperative to implement layers of security to protect sensitive healthcare information effectively.

Advances in ledger technology have brought about new options, such as LedgerDB and VeDB, representing cutting-edge developments stemming from blockchain systems. These innovative technologies address the performance

constraints often encountered in classical blockchain systems that manage healthcare data.

In this regard, LedgerDB offers an optimized solution for settings that require transaction processing and dynamic data access [31]. In healthcare, this means access to records and efficient updating and querying of health information, which is especially crucial in urgent medical scenarios. Moreover, LedgerDB maintains blockchains' security and privacy features while emphasizing scalability and speed, making it well-suited for health systems dealing with data volumes and transaction needs.

Further, VeDB signifies an advancement in ledger databases by providing performance and audit capabilities [32]. By leveraging frameworks like Merkle trees and incorporating software and hardware elements, VeDB enables more efficient data processing and validation. This is important in healthcare settings where prompt and reliable data management is vital. Adopting VeDB could enhance health record systems' effectiveness and regulatory compliance, aligning with progressions in healthcare information technology.

The integration of LedgerDB and VeDB can significantly enhance efficiency within health record systems by offering blockchain features with enhanced performance standards.

Implementing these technologies enables the handling and organization of data while prioritizing the safety and reliability of information in the healthcare sector. Nevertheless, integrating these advancements into healthcare systems demands a meticulous strategy. Evaluating their implementation should consider aspects such as adhering to regulations, sustainability and compatibility with existing healthcare IT infrastructures. Despite the improvements anticipated from these ledger databases, their novelty requires testing in healthcare environments to grasp their benefits and limitations.

Recognizing these challenges, the next section of this paper will focus on our proposed solution. This solution addresses these issues and aims to enhance the effectiveness and security of EHR systems within the rapidly changing digital healthcare environment.

IV. BACKGROUND

The following section presents the proposition's pillar constituents. These include blockchain technology, decentralized identifiers, encryption, and token-based access control.

A. BLOCKCHAIN TECHNOLOGY

A blockchain, described as a decentralized ledger that runs across several computers, constantly grows by adding data blocks that are securely linked via encryption. Each block contains the preceding block's cryptographic hash, a timestamp, and transaction data. Its distributed, public nature ensures that recorded transactions cannot be modified retrospectively without affecting the following blocks and achieving network consensus. Bitcoin was the first blockchain application, which has subsequently grown in

popularity. Researchers in healthcare use blockchain, particularly Ethereum, to address health-related issues [33] [34], demonstrating the technology's versatility beyond its initial financial context.






The Algorand blockchain is a decentralized system operating across a computer network. Its primary purpose is to record transactions in a tamper-proof way. Like other well-known blockchains, Algorand grows by adding blocks of securely linked data using cryptographic principles. Each block on the Algorand blockchain contains a hash of the block, a timestamp, and transaction data.

What sets Algorand apart is its consensus mechanism, which aims to be more efficient and scalable compared to blockchain systems like Bitcoin and Ethereum. It utilizes a Pure Proof of Stake (PPoS) protocol where block validators are selected randomly and discreetly from users who hold its native cryptocurrency called Algo. This approach aims to reduce energy consumption and computational requirements often associated with Proof of Work (PoW) systems used by blockchains like Bitcoin. In Algorand's Pure Proof of Stake consensus, a user's influence in determining a new block is proportional to their token holdings, commonly known as their stake. The possibility of a user being selected to propose or vote on blocks and the impact of such suggestions and votes is directly proportional to the quantity of their stake. Table 2 provides an analysis and comparison of consensus methods that form the backbone of blockchain networks. It assesses each method using metrics that impact how blockchain systems function: decentralization, scalability, security and energy efficiency. These metrics highlight the equilibrium that blockchain networks aim to maintain between being broadcasted and democratic (decentralization), able to handle increasing transaction volumes and users (scalability), resilient against attacks and unauthorized changes (security), and environmentally sustainable in their energy usage (energy efficiency).

The pure proof of stake mechanism is a multi-step process that includes a random selection of proposing nodes and committees for voting, many rounds of voting to ensure robustness, and integrating a new block into the blockchain. This approach ensures that the network achieves agreement without the extensive computational work required by traditional Proof of Work systems, and it is intended to be more scalable and cost-effective. FIGURE 3 describes the process of PPOS in Algorand. It consists of four key steps:

1. **Block Proposal:** In the first step, a cryptographic random selection mechanism selects node candidates to propose the new block. This operation is done via a Verifiable Random Function (VRF), ensuring the process is random and fair.
2. **Soft Vote:** Nodes selected in the first step propose a block. Among these, the account with the lowest hash value is chosen to suggest the next block. A committee of verifiers, also selected randomly via VRF, then performs what is known as a "Soft Vote" to agree on this new block.

TABLE 2. Comparative table of consensus mechanisms.

Consensus mechanism	Main attributes	Decentralization	Scalability	Security	Energy efficiency	Example
Proof of work (PoW)	Miners solve complex mathematical problems to validate transactions and create new blocks.	High	Low	High	Low	 ethereum
Proof of stake (PoS)	Validators are selected based on the number of coins they own and are willing to stake	Medium	Medium	High	High	 CARDANO
Delegated proof of stake (DPoS)	Coin holders vote for a few delegates who validate transactions and create blocks.	Medium	High	High	High	 TRON
Pure proof of stake (PPoS)	All validators can participate, with the probability of being selected proportional to their stake.	High	High	High	High	 Algorand
Proof of Authority (PoA)	Validators, known as approved accounts, validate transactions and blocks.	Low	High	Medium to High	High	 vechain

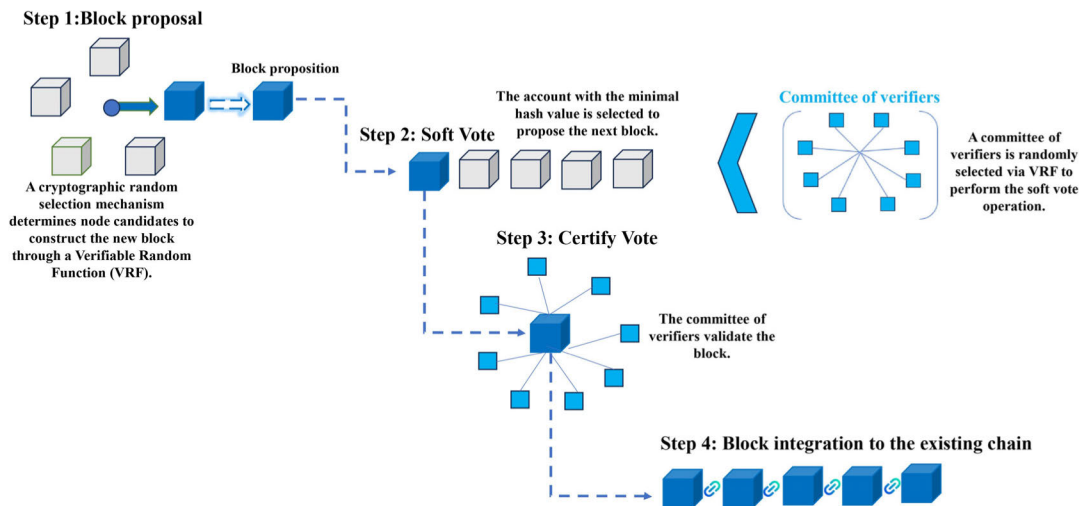


FIGURE 3. Algorand pure proof of stake consensus mechanism.

- Certify Vote:** Following the Soft Vote, the committee of verifiers performs another round of voting to certify the block. This step is crucial as it adds another layer of confirmation that the proposed block is valid.
- Block Integration to the existing Chain:** In this final step, once the block has been certified, it is added to the existing blockchain. This step is represented by the new block linking with the chain of previous blocks, indicating that the block has been accepted and its transactions are confirmed.

B. DECENTRALIZED IDENTIFIERS (DIDs)

The concept of centralized identifiers, which includes emails, usernames, and passwords, has been the standard approach for accessing websites, apps, and services for many years. However, this model is increasingly problematic due to

several inherent issues. Table 3 highlights the difficulties associated with centralized identifiers. These include security risks stemming from having storage points that are susceptible to attacks, concerns about privacy when personal data is shared with service providers, the risk of system-wide disruption due to a single point of failure control issues arising from policies dependent on authority figures inefficiencies in user experience resulting from managing numerous passwords, limitations in interoperability, across different platforms and challenges related to scalability that require significant resources to accommodate increasing numbers of users and data.

Given the outlined limitations and risks permanent in centralized identification systems, the emerging paradigm of decentralized identifiers offers a promising alternative. It addresses these challenges by empowering users with

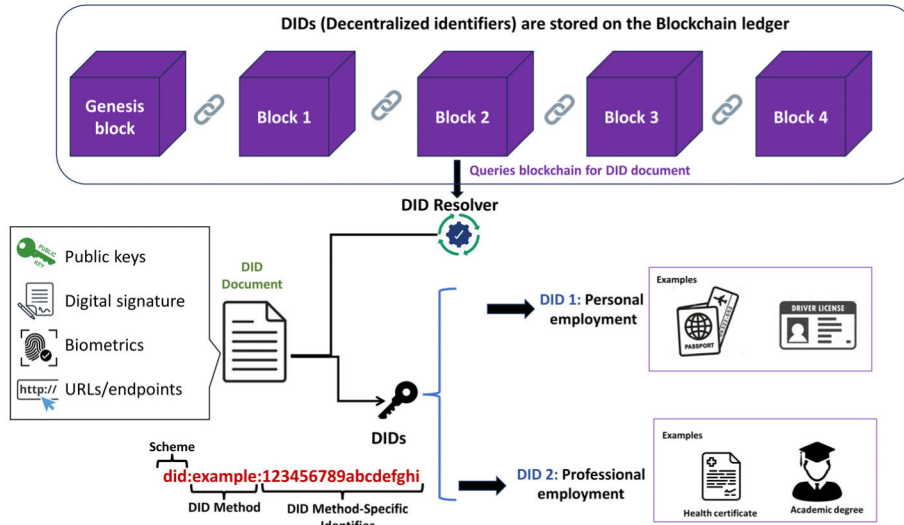


FIGURE 4. Decentralized identifier management on blockchain technology.

TABLE 3. Challenges associated with centralized identifiers.

Issue category	Detail
Security risks	Centralized identifiers are known for storing user data in one location, which increases the potential for cyberattacks, and the usage of weak or reused passwords increases this issue.
Privacy concerns	Centralized identifiers require users to share personal information with service providers to use it in advertising and profiling.
Single point of failure	Centralized systems have a single point of failure, including risks such as distributed denial-of-service attacks.
Control autonomy issues	Using centralized identifiers, users become subject to the central authority’s policies and practices, creating a power imbalance and reducing user control over their digital identities.
Inefficiency user experience issues	Managing multiple passwords is inconvenient and often leads to unsafe practices like using simple or repeated passwords across websites.
Lack of interoperability	Centralized identifiers are always adequate only with specific platforms, which minimizes seamless service integration and complicates the user experience.
Scalability problems	As the number of users and systems increases, robust resources are required to manage user credentials and ensure system security.

greater control, security, and flexibility in managing their digital identities. Delving into their foundational principles and functionalities is essential to understanding the significance of decentralized identifiers.

Decentralized Identifiers, commonly known as DIDs, are unique identifiers within a decentralized database system. These identifiers are designed to function on blockchain technology, facilitating the identification and verifying of individuals or entities. Unlike traditional identifiers, DIDs utilize cryptographic techniques, including digital signatures,

to ensure the validation of the subjects they represent. The role of DIDs extends beyond mere verification of authenticity; they play a crucial part in upholding the integrity of the identity owners or subjects on the blockchain network.

FIGURE 4 illustrates the step-by-step flow of how DIDs work on the blockchain. It begins with storing DIDs on the ledger, starting from the genesis block and progressing to the final block. These DIDs are then linked to DID documents containing keys, digital signatures, biometric data and URLs/endpoints for identity verification. A DID Resolver interacts with the blockchain to fetch a document. The DIDs adhere to a structure depicted in the middle, which assigns an identifier to each DID. This process is exemplified by showcasing two types of DIDs being utilized to access relevant documents: one for personal employment and another for professional credentials.

- **Key generation:** The critical generation process involves using prime number generation and modular arithmetic. To illustrate, RSA keys are created by carefully selecting two sizable prime numbers, p and q , and calculating their product $n = p \times q$, used as the modulus for public and private keys.
- **Data signature:** The concept of a digital signature involves utilizing hash functions and exponentiation. In this process, a hash of the information is taken, and then using the private key d , the signature s is generated by raising the hash to the power of d modulo n (for RSA): $s = hash^d \text{ mod } n$.
- **Verification:** Verifiers perform the inverse operation by using the signer’s public key to raise the signature to the power of the public exponent e modulo n to verify.

C. ENCRYPTION MECHANISM

The relevance of encryption expands when it comes to sensitive information, such as patient medical data, for which

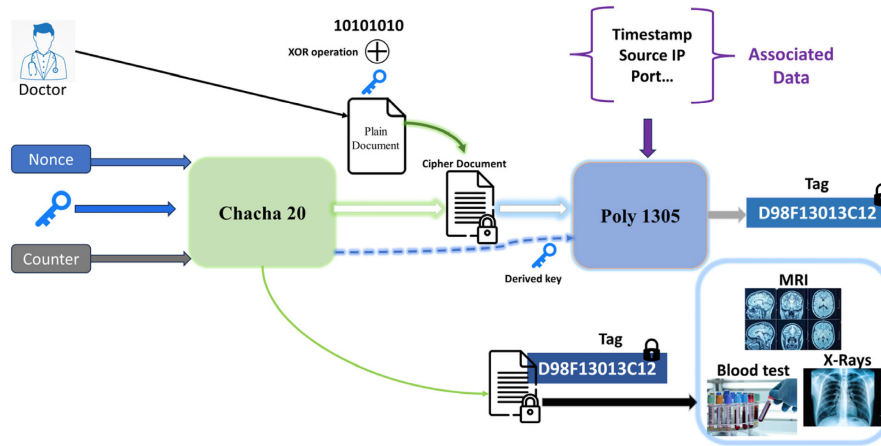


FIGURE 5. ChaCha20-Poly1305 algorithm workflow in medical use case.

strong security is critical. In this case, various encryption mechanisms are implemented to provide protection and privacy, with the ChaCha20-Poly1305, designed by Daniel J. Bernstein [14], [15], being one of them. ChaCha20-Poly1305 is considered an excellent encryption algorithm for safeguarding health records, especially compared to other encryption methods. Its key advantage lies in its ability to provide security while maintaining speed, which is crucial in healthcare environments where quick access to data is as important as keeping it confidential. Unlike algorithms such as AES (Advanced Encryption Standard) or DES (Data Encryption Standard), which can be resource-intensive and slower with large datasets, ChaCha20-Poly1305 operates with impressive efficiency. This makes it well-suited for encrypting the extensive and continuously growing health records. Furthermore, its resilience against attacks ensures the integrity and privacy of sensitive patient information.

Table 4 compares encryption algorithms, such as DES, RSA, AES and ChaCha20-Poly1305. Each algorithm's unique characteristics make it suitable for specific uses and settings. For instance, though necessary, DES is now deemed insecure due to its key length. RSA, a public key cryptography system, is commonly used for data transmission but is not typically employed for large-scale data encryption due to its computational complexity. On the other hand, AES is a widely accepted symmetric encryption standard known for its efficiency and security features. It performs well in hardware setups supporting AES New Instructions (AES NI), greatly enhancing encryption and decryption speeds. ChaCha20-Poly1305 combines the ChaCha20 stream cipher with the Poly1305 message authentication code to provide security and excellent performance in environments lacking specialized cryptographic hardware.

When deciding which encryption algorithm to use for a healthcare system for Electronic Health Records, various factors need to be considered, such as security, performance

and compatibility with existing systems. AES is well known for its security measures and fast processing speed in systems with AES-NI capabilities. These capabilities allow the system to execute AES instructions directly on the CPU, enhancing performance and efficiency. This aspect makes AES an option for environments with hardware support like this, offering a quick and secure encryption solution. However, some may not support AES-NI in the case of EHR systems, which involve a range of devices and systems.

On the other hand, ChaCha20-Poly1305 emerges as a versatile choice. It provides security measures to AES and does not rely on specialized hardware for high performance. This is particularly useful in healthcare settings where data needs to be accessed or shared across devices and platforms, from servers to mobile devices, without AES-NI support. Moreover, ChaCha20-Poly1305 is known for its resistance to analysis, making it a reliable option for safeguarding sensitive health data. Under specific circumstances, its design is less vulnerable to attacks impacting block ciphers such as AES. Hence, we adopted ChaCha20-Poly1305 for our approach because of its flexibility, security features and excellent performance on various platforms. This combination makes it ideal for the changing landscape of EHR systems, guaranteeing that confidential health information remains safe and available whenever necessary, regardless of the hardware used.

FIGURE 5 illustrates the general process of the ChaCha20-Poly1305 algorithm as applied in a medical use case scenario. This figure shows how data encryption is used in healthcare, with a doctor securing data using the ChaCha20 cipher. A unique key is created for each encryption by combining a nonce and a counter. The data, which is information, is then mixed with a key through an XOR operation. Following this, the ChaCha20 algorithm encrypts the data, and the Poly1305 algorithm includes a tag for verification. The result is a document with a tag that ensures the integrity and authenticity of the data. This encrypted information pertains

TABLE 4. Comparative table of encryption algorithms.

Characteristic	DES	RSA	AES	ChaCha20-Poly1305
Security	Moderate	High	High	Very High
Speed	Slow	Moderate	Fast	Very Fast
Efficiency	Low	Moderate	High	Very High
Resistance to attacks	Weak	Strong	Strong	Very Strong
Suitability for voluminous data	Poor	Moderate	Good	Excellent
Resource usage	Low	High	Moderate	Low
Implementation difficulty	Easy	Complex	Easy	Moderate

to healthcare-related items such as MRI images, blood tests and X-rays.

The ChaCha20-Poly1305 algorithm combines the ChaCha20 encryption technique with the Poly1305 message authentication code (MAC) to ensure secrecy and data integrity. The following steps describe the algorithm’s workflow.

Step 1: Key and Nonce generation:

- A 256-bit unique key K is produced for the encryption procedure. This key must be kept secret.
- A 96-bit nonce N (a number that is only used once) is also created. The nonce assures that the same plaintext is not encrypted to the same ciphertext twice, which increases the encryption’s security.

Step 2: ChaCha20 encryption

- Chacha20 is a stream cipher. It produces a keystream using the key and nonce.
- The plaintext denoted P is merged with the keystream KS generated by ChaCha20 via the XOR function. This implies that each bit of the plaintext is XORed with the matching bit of the keystream to generate the encrypted text.
- The ciphertext C is computed as $C = P \oplus KS$, which \oplus denotes the XOR operation.

Step 3: Poly1305 authentication

- Poly1305 creates an authentication tag that functions as a MAC.
- Poly1305 employs a 256-bit one-time key OTK created from the ChaCha20 key K and nonce N . This ensures that the MAC is unique for each communication.
- It computes an authentication tag denoted T as MAC over the ciphertext C and any associated authenticated data denoted AAD , such that $T = POLY1305(C||AAD, OTK)$.

Step 4: Output Combination

- The encryption operation produces ciphertext C concatenated with the Poly1305 tag T , represented as $C||T$. This tag ensures the discovery of any ciphertext or associated data alterations.
- When decrypting, the recipient generates the keystream with the same key and nonce before decrypting the ciphertext using the XOR technique.

- After decrypting the message using the same associated authenticated data, the recipient uses Poly1305 to validate the tag. If verification fails, it indicates tampering has occurred with the data.

D. TOKENS-BASED ACCESS CONTROL

Token-based access control is a security method that regulates user access to resources in a system. Unlike traditional access control methods that depend on fixed credentials, token-based access employs created encoded tokens containing information about the user’s identity, permissions, and session status. In healthcare, incorporating blockchain technology through the use of tokens brings forth prospects for managing and accessing healthcare services. One notable application is the utilization of tokens to securely access records, empowering patients with control over who can view their health information. Additionally, these tokens can facilitate transactions for services, ensuring enhanced traceability and transparency. In instances, tokens may serve as a means to incentivize behaviors or enable participation in medical research, thereby transforming the consumption and administration of healthcare services.

The process starts with user authentication, where users provide their credentials (username and password). After authentication, the system generates an access token. This token undergoes digital encryption to maintain its integrity and confidentiality. It then includes details about the user’s identity, roles, permissions and other attributes essential for resource access. In terms the token generation process can be represented as follows:

Step 1: User authentication:

Confirming users’ identities is crucial in a healthcare environment for safeguarding patient data. Whether it is healthcare professionals such as doctors, nurses, administrative staff, or patients, verifying their identity is essential to accessing health records. The user authentication phase involves users providing their credentials, which are then validated to verify their identity.

• **User credentials:**

Healthcare professionals typically use a username and password provided by their institution for authentication. Patients may need to give details like an email address and a private password for identification.

Formally represented as: $U = \{username, password\}$

• **Authentication function:**

The system validates these credentials against its database. The user is considered legitimate if a match exists and can proceed further. This process resembles a digital check-in at a hospital or clinic to ensure authorized individuals can view information.

Mathematically expressed as: $Auth(U) \rightarrow \{True, False\}$

Algorithm 1 represents the process used to verify the identity of a user attempting to enter the system, ensuring the security and integrity of healthcare information. The algorithm verifies the user’s credentials; if they are

Algorithm 1 AuthenticateUser**Input:** username,password.**Output:** Authenticated token or authenticated failure message.

1. If isValidCredentials(username, password)
Then
2. $user \leftarrow getUserDetails(username)$
 $token \leftarrow generateToken(user)$
Return token
3. Else
Return “Failed Authentication”
4. End if

Algorithm 2 GenerateToken**Input:** User.**Output:** Encrypted and signed token.

```

tokenAttributes ← {
    'UserID': user.ID,
    'Roles': user.roles,
    'Expiry': currentTime + tokenValidityDuration
}
token ← encryptAndSign(tokenAttributes, secretKey)
Return token

```

valid, it returns a token; otherwise, it indicates a failed authentication.

Step 2: Token Creation (if Authentication is True):

Once the user’s identity is confirmed, the system generates a token acting as a temporary pass for accessing patient records. This step consists of the following:

- **Token attributes:**

The token contains information such as the User ID (which could be an employee ID for a healthcare provider or a patient ID), their Roles (such as doctor, nurse, or patient), Expiry (the time when this token expires), and Metadata (which may include the department, specialization, or patient blood group).

Token attributes formally represented as: $T_{attrs} = \{UserID, Roles, Expiry, Metadata\}$

- **Function for Generating Tokens:**

The system encrypts this data into a token using a secret key. It is similar to securing a patient’s record in an envelope that can only be opened by those with the right key. This process is summarized as: $TokenGen(T_{attrs}, K) \rightarrow Token$; where K is the secret key used for encryption.

Algorithm 2’s primary function is to generate a token for a user, which is essential for controlling access within the system.

Step 3: Token Validation:

Whenever a user needs to access EHRs, the system must validate the token to ensure it is still valid and provide the authorization, which is obtained by the token validation function.

Algorithm 3 ValidateToken**Input:** Token**Output:** Token attributes or validation failure message

```

tokenAttributes ← decryptAndVerify(token, secretKey)
If tokenAttributes AND isNotExpired(tokenAttributes['Expiry']) Then
    Return tokenAttributes
Else
    Return “Invalid or Expired Token”
End if

```

Algorithm 4 AccessResource**Input:** Token, resource**Output:** Access Permission status

```

tokenAttributes ← ValidateToken(token)
If tokenAttributes AND userHasAccess(tokenAttributes['UserID'], resource) Then
    Return “Access granted”
Else
    Return “Access Denied”
End if

```

- **Token Validation Function:**

With each access attempt, the system reviews the token by decrypting it using the key and verifying its content and expiration date. This process resembles an authentication method confirming whether the user can view the requested patient data. In healthcare, this verification process is defined as $Validate(Token, K) \rightarrow \{True, False, T_{attrs}\}$.

Algorithm 3 highlights the process for verifying a user token’s validity each time they try to access resources or perform actions, granting permissions accordingly.

Once the token validation is complete, the user (whether a healthcare professional or patient) is granted access as outlined in Algorithm 4, which details the process. It determines whether users should be given access to requested resources based on their token’s validity and permissions. If the token is authenticated and the user is authorized, the algorithm responds with “Access granted,” allowing the user to proceed. Otherwise, it issues an “Access Denied” response to protect sensitive data and operations.

Token-based access control is relevant in the healthcare sector, protecting sensitive information. Its primary function is to prevent individuals from accessing data such as medical records, diagnoses, and treatment plans. By following healthcare privacy guidelines, token-based systems guarantee the confidentiality of information; moreover, in an industry where data breaches can result in outcomes, tokens offer a layer of security. They serve as a defense mechanism that is more secure than static passwords, which are susceptible to being easily compromised. Tokens have limitations in

terms of time and access, reducing risks even if traditional credentials are stolen or exposed. This method ensures that access rights and transactions are securely and transparently managed, which is especially important in the healthcare sector, where maintaining data confidentiality and integrity is essential. After analyzing our study's aspects and fundamental issues, the upcoming section represents a transition from the preliminaries to the theoretical approach. The next section highlights the details of our suggested solution, explaining its design, functionality and main actors. The proposed solution is designed in response to the limitations and gaps we identified in existing methods.

V. RESEARCH METHODOLOGY

This section describes the approach used in this study, explaining the steps taken from presenting the solution idea to assessing the outcomes. The methodology comprises five phases (FIGURE 6): Literature Review, Framework Design, Implementation, Simulation and Evaluation and Results and Discussion. These stages are interconnected to ensure a thorough research process.

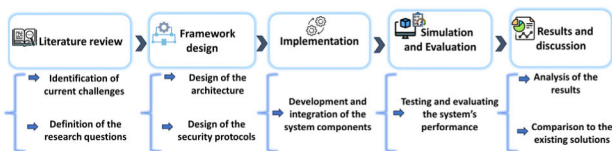


FIGURE 6. Overview of the adopted research methodology.

1. Review of existing literature:

The first step involves examining the literature to pinpoint the challenges and gaps in electronic health record systems, specifically focusing on security, privacy, and efficiency.

- **Sourcing Materials:** Collect papers, articles, and case studies from databases like IEEE Xplore, ScienceDirect, Taylor & Francis, PubMed, and Google Scholar.
- **Critical Assessment:** Assessing the strengths and weaknesses of existing solutions while highlighting areas that require enhancements.
- **Formulation of Research Questions:** Developing research questions based on insights from the literature review.

2. Development of Framework:

The next phase revolves around designing a framework for EHRs. This stage encompasses:

- **Structuring System Architecture:** Designing the structure of the proposed solution incorporating elements such as technology, decentralized identifiers (DIDs) and advanced encryption algorithms.
- **Component Specification:** Clarifying the responsibilities of each user within the system (like hospitals, doctors, patients) and how they interact with each other.
- **Security Measures:** Definition of security protocols and methods, such as access control based on tokens and incorporating the ChaCha20-Poly1305 encryption algorithm.

3. Implementation

The third step involves putting the planned framework into action. This includes:

- **Development Environment:** Establishing the development environment using JavaScript for both the front and back end, supplemented with TypeScript, HTML, and CSS. This setup also includes integration with the Algorand blockchain and Pera wallet.
- **Coding and Integration:** To ensure seamless communication, write and integrate code for system components.
- **Data Security:** Implementing ChaCha20-Poly1305 encryption for data security and generating unique identifiers for secure identity management.

4. Testing and Evaluation

The fourth step entails testing the proposed framework through simulations and evaluating its performance. This phase covers:

- **Simulation Setup:** Configuring simulation environment using Helia IPFS for data storage and Algorand test network for transactions.
- **Performance Evaluation Criteria:** Identify critical performance metrics, such as transaction expenses, token usage patterns, and processing speed, evaluating them as indicators of security strength.
- **Examination:** Conduct various assessments to measure the system's functionality, including analyzing delays and costs and ensuring security.

5. Results and Discussion

The last step involves examining and discussing the results acquired from the simulation and assessment. This includes:

- **Understanding Data:** Analyzing the information gathered during the simulation to assess the effectiveness of the proposed solution.
- **Contrasting with Solutions:** Evaluating how well the suggested framework performs compared to existing EHR systems to showcase any enhancements.
- **Conclusions:** Drawing deductions based on the findings and discussing their implications for research advancements and real-world implementation.

VI. PROPOSED WORK

This paper presents a framework that employs blockchain technology, the InterPlanetary File System (IPFS), and decentralized identifiers to efficiently maintain and verify health information. Our proposed system handles various operations, such as encrypting data, allowing token access, and preserving records. Users may engage with the site using their digital wallets, giving them a safe method to manage their health information. We use powerful encryption algorithms such as ChaCha20-Poly1305 to improve security further. Furthermore, our design includes a pure proof of stake consensus mechanism to provide an efficient, fast and scalable platform for gathering, encrypting, and storing healthcare data.

Moreover, choosing Algorand as our foundational blockchain technology to enhance the security of our EHRs framework is a strategic move, underlined by its

renowned transactional speed and efficiency. We are highly aware of the paramount importance of security within EHR systems. Recognizing that Algorand has faced its share of challenges, we emphasize the importance of thorough security evaluations. Our commitment to Algorand is predicated on its continual improvements and the robust security protocols established in response to previous vulnerabilities.

Therefore, to fortify the security and ensure the confidentiality and integrity of EHR data, our framework is designed with multiple layers of defense, including:

- **Advanced Encryption Techniques:** Besides Algorand's inherent security features, we employ advanced encryption methods such as ChaCha20-Poly1305 to provide an additional safeguard for data, ensuring comprehensive protection during storage and transmission phases.
- **Proactive Security Assessments:** Given the evolving nature of cyber threats, our framework is equipped with mechanisms for regular security evaluations and updates, enabling swift identification and rectification of any potential vulnerabilities within the Algorand infrastructure.
- **Implementation of Decentralized Identifiers:** To enhance our security and privacy measures, we leverage DIDs to facilitate reliable identity management, eliminating reliance on centralized authorities and enhancing user privacy.
- **Token-Based Access Control:** To complement Algorand's security features, our framework integrates a token-based access system, adding an extra verification layer to ensure that only authorized personnel can access sensitive EHR information.

By integrating these sophisticated security measures with the Algorand blockchain, we aim to tackle its transactional capability while prioritizing safeguarding EHR data. Our adaptable system is designed to swiftly respond to emerging threats, upholding the highest security standards in managing healthcare information.

The proposed system has three main actors: Hospitals, Doctors and Patients. Each of these actors has roles and responsibilities within the system. The Hospital takes on the administrator role, overseeing tasks like distributing tokens and assigning patients to doctors. This central role ensures that the system operates smoothly and efficiently. On the other hand, doctors are responsible for accessing patient records, adding entries and using them in their medical duties. This allows them to provide informed and timely healthcare services. Lastly, patients are responsible for sharing their records and accessing their health information. This empowers them to manage their health actively and promotes communication with their healthcare providers. With this three-part structure in place, we can ensure an efficient and secure healthcare management system.

FIGURES 6 and 7 show the proposed blockchain healthcare data management system. Initially, hospitals will register

and give access tokens. To interact with the system, doctors and patients must register via digital wallets and authenticate their identities, with tokens enabling safe access. Medical data is encrypted and associated with unique identifiers to protect privacy. This encrypted data is saved on a decentralized file system, with blockchain references ensuring safe and immutable record-keeping.

FIGURE 8 enhances FIGURE 7 by offering a step-by-step guide for system users, such as administrators/hospitals and patients/doctors. While FIGURE 7 concentrates on incorporating wallets, access based on roles and secure data storage/encryption, FIGURE 8 delves into the procedures and responsibilities related to data management, ensuring verification and encryption processes. Together, these illustrations present an extensive overview of our proposed system.

- **Step 1: Initial Connection and Registration:**

The process begins with the hospital and users (doctors and patients) connecting their wallets to the platform. The hospital then registers, creates specific roles within the system, issues digital tokens corresponding to these roles, and defines access permissions.

- **Step 2: Token Creation and Opt-In Process:**

After the hospital issues tokens, it manages opt-in requests from doctors and patients. These requests are essential for users to perform their roles within the system, such as accessing medical records or managing patient data. Algorithm 5 depicts the process of token creation.

- **Step 3: Verification and Assignment:**

Doctors and patients connect with their wallets and undergo a verification process. Based on the opt-in information, verified doctors are assigned patients, allowing them to consult with their assigned patients using their tokens.

- **Step 4: Data Handling and Encryption:**

Unassigned doctors and patients enter their details into the system. This information is encrypted using the ChaCha20-Poly1305 algorithm for data security. Each user also creates a Decentralized Identifier (DID), establishing a unique and secure identity within the system. Algorithm 6 highlights the encryption steps for user data, and Algorithm 7 shows the process used for DID creation.

- **Step 5: Uploading to IPFS:**

The encrypted data, now linked to a user's DID, is uploaded to the InterPlanetary File System. This decentralized storage solution ensures the data's availability and redundancy across multiple nodes.

- **Step 6: Blockchain Integration for Immutable Record-Keeping:**

In the final step, the system records references to the encrypted data and associated DIDs on the Algorand blockchain. This step creates an immutable ledger that verifies the integrity of the medical records and supports traceability for all interactions on the platform.

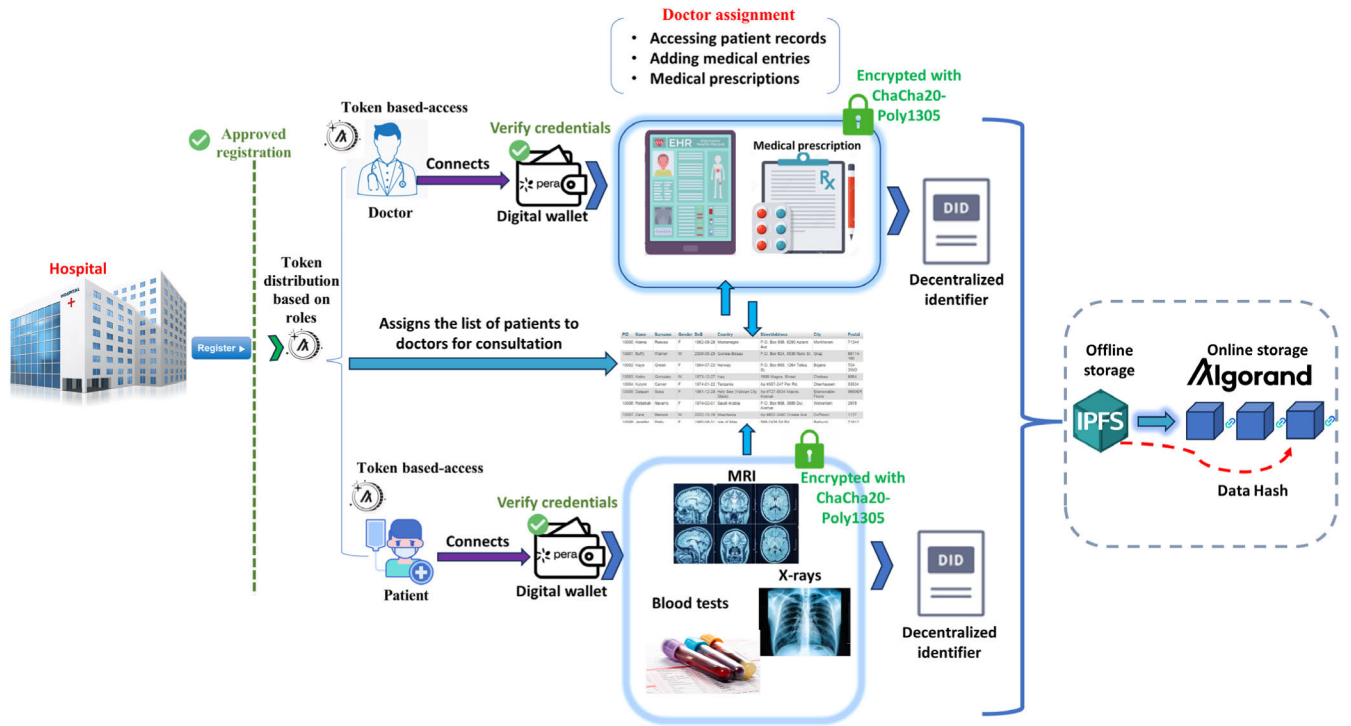


FIGURE 7. Proposed solution.

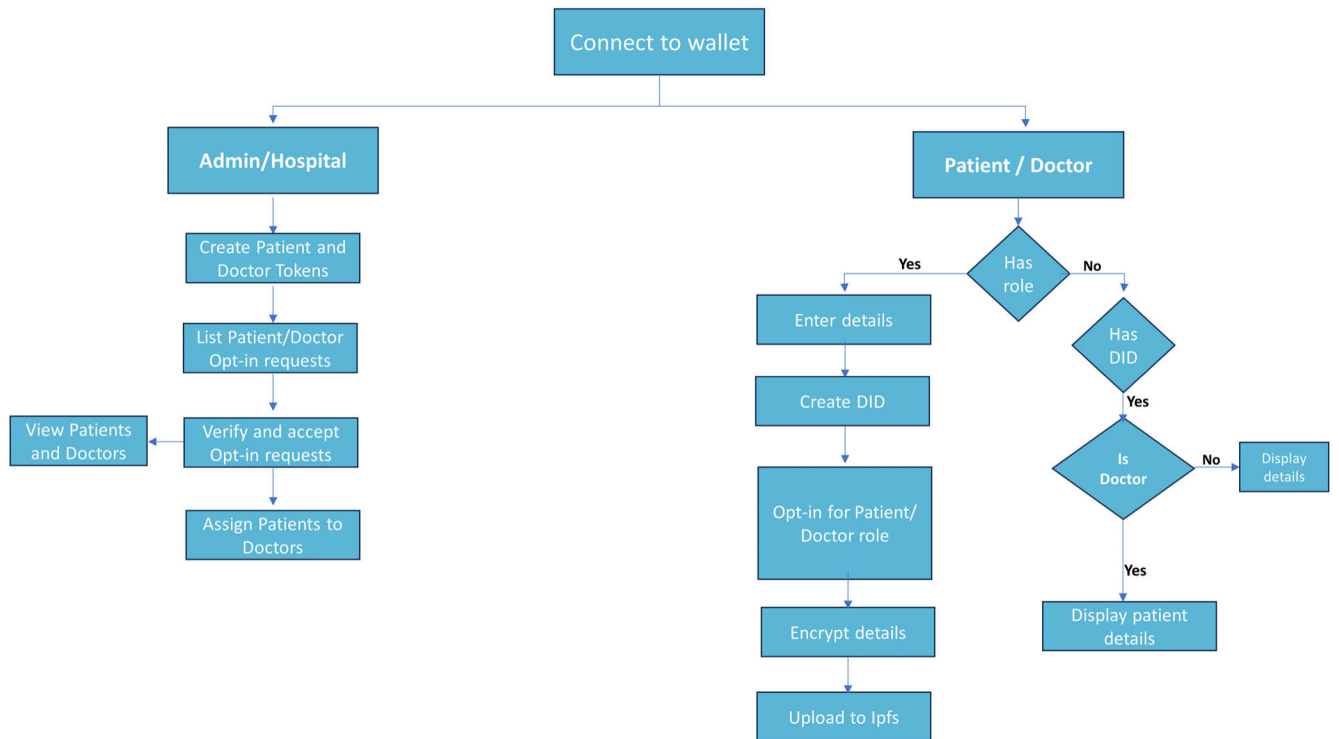


FIGURE 8. Workflow of the proposed solution.

VII. IMPLEMENTATION AND RESULTS

This section of the document explores the effectiveness of the proposed approach. Initially, it describes the setup, which

includes components like the front end, back end, server, tools, host, programming language integrated development environment (IDE) and the test network. Afterwards, we

Algorithm 5 *CreateTokens***Input:** Active Address of the Admin/Hospital.**Output:** Patient and Doctor tokens are created.

1. *Admin/Hospital (ActiveAddress) → Blockchain*
2. *Blockchain (ProcessRequest)*
 - a. *CreateToken (type: 'patient', name: 'EHR_PATIENT', total: 1000) → Blockchain*
 - b. *CreateToken (type: 'doctor', name: 'EHR_DOCTOR', total: 1000) → Blockchain*
3. *Blockchain (SendTransaction)*
 - a. *Group (Transaction(patientToken), Transaction(doctorToken)) → Blockchain*
4. *Sign (GroupedTransactions) → Admin/Hospital*
5. *Blockchain (RecordTransaction) → Update Ledger*
6. *Share (TokenIDs) → Admin/Hospital*

Algorithm 6 *EncryptUserData***Input:** User data in JSON format, Active Address of the User.**Output:** Encrypted user data string.

1. *Import ChaCha20 Encryption Library*
2. *Define secret key and nonce for encryption*
3. *Prepare buffer padding function to ensure correct block size*
4. *Define encryption function:*
 - a. *Convert text data to buffer format*
 - b. *Pad secret key and nonce to required lengths*
 - c. *Create a new ChaCha20 encryption instance with a padded key and nonce*
 - d. *Encrypt the text buffer with ChaCha20 instance*
 - e. *Convert encrypted data to string format*
5. *Apply encryption function to user data, including address, role assignment status, and DID*
6. *Return the encrypted data string*

Algorithm 7 *CreateDID()***Input:** Request for new DID generation.**Output:** A newly created Decentralized Identifier (DID).

1. *Import the DidKeyMethod module from the 'web5/dids' library.*
2. *Initialize the DID creation process by invoking the create() function from the DidKeyMethod.*
3. *Capture the returned DID in a variable for subsequent use within the system.*

evaluate how well the suggested method performs using metrics such as deployment and operational costs, latency, processing time and security robustness. Lastly, we also analyze our proposed solution and existing methodologies.

A. EXPERIMENTAL SETUP

The proposed solution utilizes Next JS to create an efficient front and back-end platform. TypeScript and JavaScript are employed for scripting, while HTML and CSS are used to structure and style the web interface. The system operates on the Algorand network, known for its decentralized framework due to its Pure Proof of Stake (PPoS) consensus mechanism. Also, the Pera wallet is incorporated into the system to ensure asset management and transaction handling, offering a user interface. Thorough testing and deployment are facilitated through a test network within the Algorand ecosystem. Furthermore, Helia IPFS is integrated into the system to enhance data storage and distribution capabilities

to achieve scalability. Additionally, we employed web5 to create decentralized identities, further enhancing platform functionality and security in managing identities Table 5 and FIGURE 9 present the details of the experiment setup it outlines the technology stack for our proposed system, which includes front-end and back-end components. It is designed to manage data using identity management and storage methods. The front-end utilizes technologies like React, Next.js and TypeScript with user interactions powered by JavaScript. On the back-end, decentralized identity creation is supported by Web3 technologies and data encryption is managed through the ChaCha20-Poly1305 algorithms. Storage solutions consist of off-chain storage using IPFS for distributed file storage and on-chain storage with Algorand, which involves storing transaction records or hashes on the Algorand blockchain. A digital wallet regulates permissions access and authorizes record management through token-based authentication.

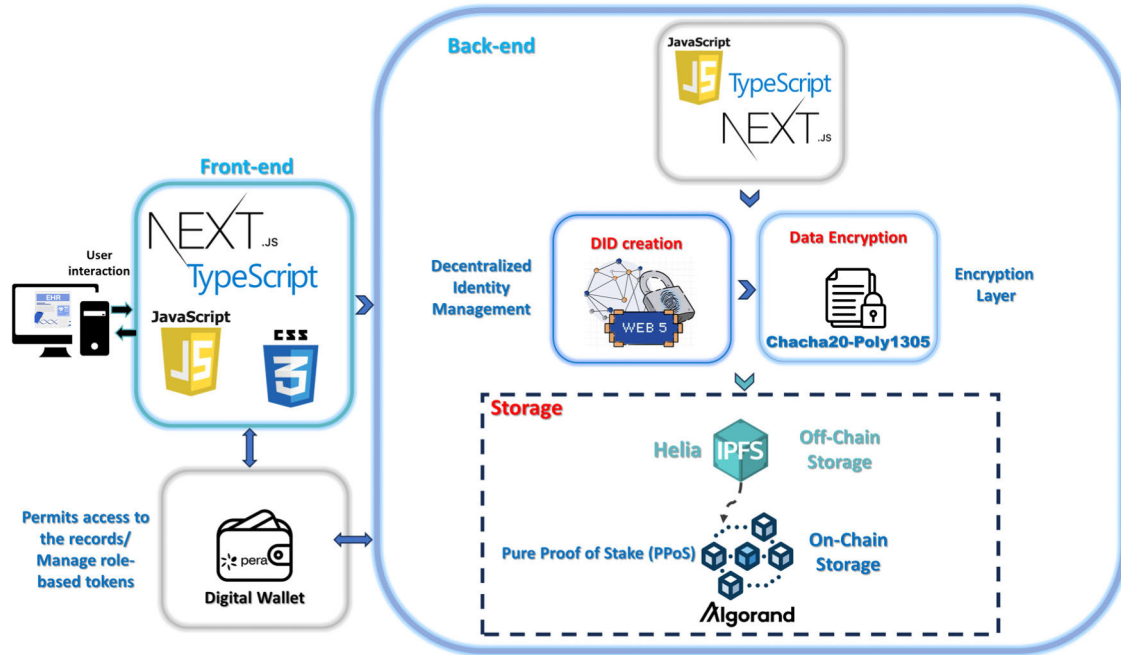


FIGURE 9. Functional and Application architecture of the proposed system.

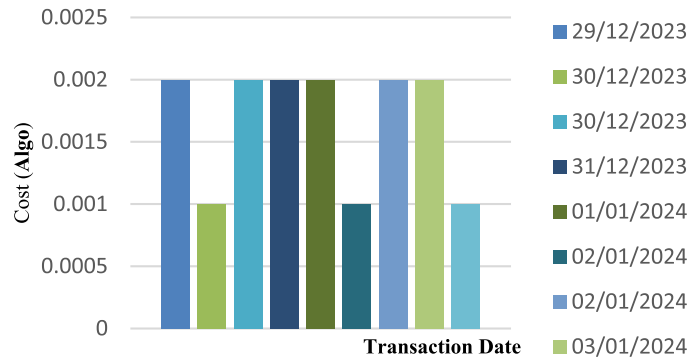


FIGURE 10. Corresponding cost of the various transactions on different dates.

B. PERFORMANCE ANALYSIS

In this subsection, we assess the performance of our solution by considering measures: the costs associated with transactions, the number of tokens used, the time required for processing and the level of security. Each measure is crucial for comprehending how effective and dependable our solution is in real-world scenarios.

1) COST ANALYSIS

Our proposed solution used Algorand’s blockchain to integrate with the Pera wallet. Our activities included creating tokens using the *CreateTokens()* function, encrypting user data with *EncryptUserData()* and generating decentralized identities through DID. The graph (FIGURE 10) depicts that

transaction costs showed variations between December 29th, 2023 and January 3rd, 2024. These fluctuations remained between 0,001 and 0,002 Algos, indicating Algorand’s fee structure. The slight differences in costs on dates relate to the tasks performed within the application, such as registering patients/doctors and handling encrypted medical data.

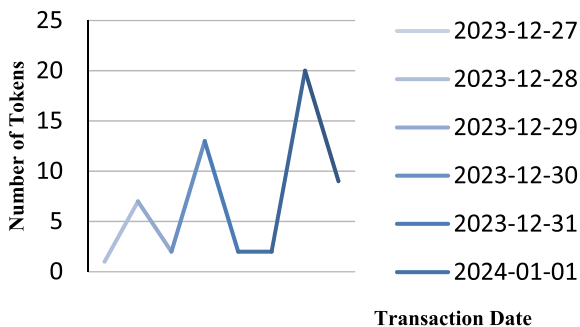
2) TOKEN ANALYSIS

FIGURE 11 shows a fluctuation in the number of tokens used for different functions. The token consumption ranges from as low as one token to a maximum of 20 tokens. When one token is used, it typically represents processes like assigning initial roles. On the other hand, dates with operations require 20 tokens, indicating high activity. These transactions include

TABLE 5. Different components used in the proposed solution.

Component	Detail
System	Dell Intel Core i7
Processor	11th Gen Intel® Core™ i7-1165G7 @ 2.80GHz
Operating system	Windows 10
RAM	16 GB
Blockchain	Algorand
Digital wallet	Pera wallet
Ipfs	Helia
Back-end	Next, JS, Typescript, Javascript
Front-end	Next, JS, Typescript, Javascript, HTML, CSS
DID creation	Web5

distributing several tokens, processing batch transactions, creating DID instances and encrypting significant volumes of user data. This variation in usage highlights the functionalities and workload the proposed solution manages on different transaction dates.

**FIGURE 11.** Number of tokens used in the function of transactions.

3) LATENCY ANALYSIS

To assess the transaction processing time in our system, we executed 41 transactions. Table 6 shows a selection of these transactions, specifically highlighting cases where the time difference between the “Confirmed round” and the “First valid” round varied from 6 to 9 seconds. The “Confirmed round” represents the round when a transaction is officially recorded, while the “First valid” refers to the round in which the transaction was eligible for confirmation. This “time difference” indicates latency; in our transaction confirmation process, it is calculated as follows ($\text{Time difference} = \text{Confirmed round} - \text{First valid}$).

The graph in Figure 12 depicts the durations of 41 transactions, showing time intervals between 6 and 9 seconds. These fluctuations in transaction delays are linked to the execution of functions within our system: *CreateTokens()*, *CreateDID()* and *EncryptUserData()*. Each function execution adds to the time required for a transaction to be

confirmed, starting from its valid entry until it is confirmed within the blockchain network.

4) SECURITY ANALYSIS

It is crucial to analyze the security elements to effectively evaluate the robustness of our proposed solution against cyber threats. Therefore, in this subsection, we explore evaluating integrity, confidentiality, authentication, authorization, availability and non-repudiation within our suggested framework. We focused on the following security features: **integrity, confidentiality, availability, authentication and non-repudiation.**

Integrity: Integrity refers to the data is accurate and remains unchanged. Our system ensures integrity by using algorithms within Algorand’s framework. This means that once data is recorded on the blockchain, it cannot be tampered with and can be trusted. This is especially important in healthcare, where data accuracy is a primary concern.

Confidentiality: Confidentiality is defined as only authorized individuals can access information. Our system based on Algorand achieves this by using the ChachaPoly1305 encryption algorithm. Combining this method with controlled access to decryption keys ensures that sensitive user information remains safe and private. Our method of ensuring confidentiality goes beyond traditional techniques by combining the ChaCha20-Poly1305 encryption with a dynamic token-based access control system designed specifically for the complex demands of electronic health records in healthcare. This fusion enhances security measures and introduces a fresh perspective on data confidentiality. At the core of our confidentiality strategy lies the ChaCha20-Poly1305 encryption, selected for its blend of security and efficient performance. This algorithm is known for its ability to withstand attacks and safeguard healthcare information from unauthorized entry.

In addition to the encryption, our token-based access control model adds a layer of security. It adjusts based on user roles and data sensitivity to ensure suitable data access. This flexibility is crucial in healthcare settings, where access requirements vary and depend on various contexts.

Moreover, combining encryption with access control is not just a supplementary measure but transformative. Encryption guarantees data confidentiality, while token-based access control effectively manages data accessibility, significantly reducing the risk of breaches. This dual approach maintains data availability, ensuring the healthcare system’s operational efficiency remains unaffected.

We also decentralize trust by utilizing blockchain technology to manage access control policies, enhancing system resilience and transparency. This distributed method helps reduce the dangers linked to control, improving our systems’ security against threats and targeted attacks.

Availability: This refers to the assurance that authorized users can reliably access information and related assets whenever needed. Our system utilizes Algorand’s proof of stake

TABLE 6. Selected transactions processing latency.

Transaction ID	Time difference
ZIACD6544LMEHTGPLD3K7LXUEC2JFXATGRGJH5FIQPKE56B5BVLA	4 Seconds
KRO2FUOFWGBYLR3RXVPNZZTEO5RXEIOKKMGB76MP43RKS6P3WKQA	5 Seconds
CIVWPMRT7DUKIGAUGRS3EHUNMC75VGRTLQIJPH3DC2BULWYCGRA	6 Seconds
HQL4CKAVBIBOCH5NMNFJVL6YISAVZAZ47D3TG5CYAPQMOK4TXT7Q	7 Seconds
GIU62BBCAA3E5XDXZX3XONM7QE7X6GYSTONIIIEE2KXDA2Q56YA	8 Seconds
HG6LR6INTDECMRCU5ZOMNVVW3MR7VKQVCLQVYNV2MESXXCU5A5Q	9 Seconds

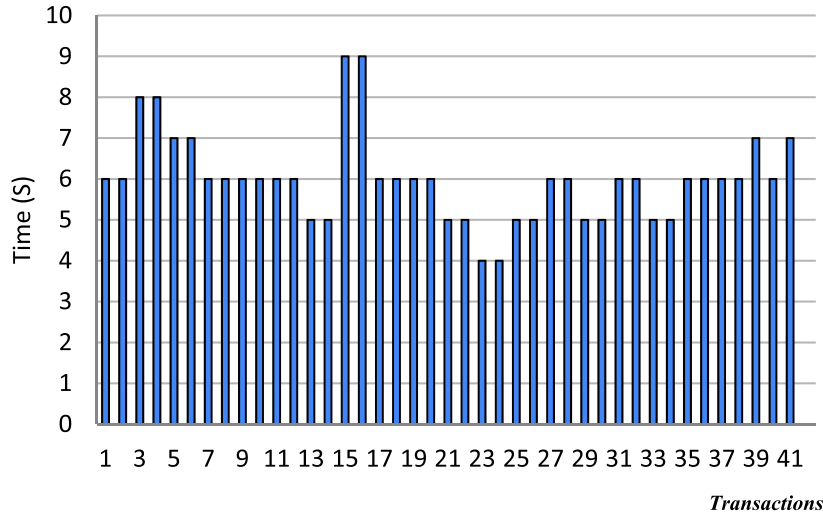


FIGURE 12. Assessment of transaction processing latency.

protocol and Helia IPFS to store data and manage system load to address user requests. This method reduces downtime, upholds availability, and guarantees reliable access to crucial healthcare information and assets. Ensuring availability is decisive in security analysis as it ensures the system remains operational and accessible during peak demand.

The *handleRequest* function monitors the load on the Algorand network. If the load is below capacity, requests are processed immediately to manage traffic efficiently. When the network reaches capacity, it queues requests for processing to prevent system overload and avoid request loss. Additionally, the process function integrates Helia IPFS for data storage, securely storing data off-chain while keeping transaction references on the Algorand blockchain for data integrity and security while sustaining availability. The *manageQueue* function processes queued requests promptly once network resources become available. This regular check helps maintain operations and prevents request backlogs to ensure user access. By initializing both the Algorand network and Helia IPFS, the system is well-prepared to handle requests. Ensuring that the queue management function is scheduled regularly helps to keep the system responsive and operating efficiently.

Algorithm 8 EnsureAvailability

Input: Request from user

Output: Reliable access to assets

handleRequest(request):

if AlgorandNetwork.load < max_capacity:

 process(request)

Else

 queue(request)

process(request)

 ipfsHash = IPFS.store(request.data)

 transaction = createTransaction(ipfsHash)

 AlgorandNetwork.submitTransaction(transaction)

manageQueue()

 while AlgorandNetwork.isAvailable() and not requestQueue.isEmpty()

process(requestQueue.pop())

initialize AlgorandNetwork, IPFS

schedule *manageQueue*(interval = 5 seconds)

Authentication: Authentication is the process of verifying the identity of a user or entity. In our system, we achieve authentication through token-based access control. During

login, each user’s credentials are validated to ensure legitimate access to the application. This method plays a role in maintaining the integrity of user roles and permissions within the healthcare framework. FIGURE 13 indicates that the proposed system has restrictions and can only be viewed by individuals with Admin or Hospital credentials. It serves as a way to control access within the application, where specific permissions are needed to access electronic health records. This figure demonstrates the implementation of measures for authentication and authorization.

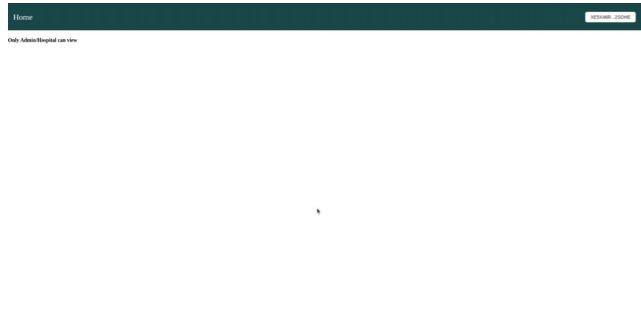


FIGURE 13. Example of authentication measure in our system.

Non-Repudiation: Non-repudiation prevents individuals or entities from denying their actions. In our system, we have integrated identifiers (DIDs). Secure logging mechanisms are implemented on the Algorand blockchain to establish transparent audit trails, ensuring accountability for all activities within the application. This feature is important in healthcare environments as it addresses compliance requirements by enabling the traceability of every transaction and interaction.

C. SUMMARY OF KEY FINDINGS

This section summarizes key findings of the proposed system’s performance, assessed based on transaction costs, token usage, processing speed, and security. Table 7 summarizes performance measures for the proposed blockchain system for managing healthcare data. Each measure is evaluated to indicate how well the system meets the healthcare industry’s requirements.

TABLE 7. Summary table of the key findings.

Metrics	Detail
Transaction cost	Costs vary from 0.0001 to 0.0002 Algos, demonstrating affordability and alignment with Algorand's fee structure.
Token usage	The token requirements range from 1 to 20, which shows how versatile and practical the system is for handling diverse tasks.
Processing speed	Transactions are verified in 6 to 9 seconds, vital for healthcare responses and improving the quality of care.
Security evaluation	Data integrity and confidentiality are ensured by using ChaCha20-Poly1305 encryption, access based on tokens, and DIDs, which boost security measures and limit access to verified users.

The assessment highlights the promising system’s performance, confirming its suitability for managing healthcare

data requirements. This system proves to be cost-effective, which is particularly beneficial in healthcare environments with constrained resources. Its flexibility and adaptability in using tokens enhances its ability to scale and adapt operationally, which is crucial for healthcare purposes.

Moreover, fast transaction processing times ensure access to medical information, essential for enhancing responsiveness in patient care. Strong security measures, including ChaCha20-Poly1305 encryption and token-based access control, establish a defense against internal and external threats. This is crucial for ensuring confidentiality and promoting trust within healthcare systems.

Furthermore, viewed in the context of healthcare applications, these findings suggest that the system could replace traditional EHR systems that often face enormous security and scalability issues. The results support existing research advocating blockchain technology’s potential to enhance data integrity and simplify access control in healthcare settings. By incorporating these combined functionalities, the system highlights its operational efficiency and security and serves as a model that can be replicated for future adaptations. Its ability to balance cost-effectiveness with data processing positions it as a feasible solution for modernizing healthcare data management.

D. COMPARATIVE ANALYSIS

In this subsection, we compare the performance of the Algorand blockchain in healthcare applications to blockchain platforms, explicitly looking at transaction costs. Furthermore, we compare the time processing of our proposed approach with existing systems to showcase our system’s enhancements.

1) TRANSACTION COSTS

Transaction costs play a role in healthcare applications, especially considering the number and importance of transactions. Maintaining these costs at a level that ensures the system’s sustainability while maintaining the security measures required to safeguard sensitive health records is essential. Reasonable transaction fees enable secure updates and access to data, making advanced healthcare solutions more accessible without compromising the security and privacy of patient information. In this regard, the nature of Algorand’s system ensures that transaction costs are kept as low as possible. This is especially important in healthcare applications, where the security and frequency of transactions are critical. Algorand achieves this by using a proof of stake consensus mechanism and an efficient network structure, which allows it to handle several transactions at a much lower cost than traditional proof of work blockchains. This cost efficiency is crucial for preserving the security of health records because it enables encryption and frequent data updates without incurring fees.

Ultimately, this supports the development of a sustainable healthcare infrastructure. Table 8 depicts the cost difference between different blockchains with Algorand with

0,001 USD, which reflects the advantage of incorporating it in healthcare problems.

TABLE 8. The cost difference between blockchains.

Blockchain	Cost per transaction
Bitcoin	20\$-30\$
Binance Smart Chain	<1\$
Solana	0.1\$
Algorand	0.001\$

2) STORAGE SCALABILITY

Our solution integrates Algorand Pure Proof of Stake (PPoS) to improve storage scalability in EHR systems. Algorand’s PPoS is well known for its fast block creation time, which reduces latency compared to Ethereum’s 15 seconds delay. This quick block generation enables data processing and integration that are crucial for the healthcare sector. Our approach maintains a balance with a block creation time of 6.5 seconds, addressing the mix of speed and stability. This adjustment ensures data storage per block while keeping performance levels high. This is vital for handling critical data in EHR systems and ensuring seamless storage of extensive patient records without hindering network performance. Moreover, the Algorand protocol excels in storage efficiency, storing data compactly to minimize required space while maximizing accessibility and security. This feature reduces storage costs and enhances scalability, which benefits healthcare organizations with IT budgets. Table 9 provides a detailed comparison of key parameters related to storage scalability among various blockchain solutions. This includes our proposed solution based on Algorand’s PPoS alongside Ethereum, Cardano, and Tezos-based solutions.

TABLE 9. Comparison of storage scalability among various blockchain solutions.

Parameters	Our Algorand-based Solution	Ethereum-based Solutions	Cardano-based solutions	Tezos-based solutions
Block creation time	6,5 seconds	15 seconds	20 seconds	60 seconds
Data storage efficiency	High	Medium	High	Medium
Transaction throughput	<1000 TPS	30 TPS	250 TPS	40 TPS

Compared to blockchains like Cardano and Tezos, our solution shines due to its combination of block creation time, high data storage efficiency and impressive transaction throughput. Cardano takes 20 seconds to create a block, which is slower but offers security features. However, this latency may not be ideal for the demands of EHR systems. On the other hand, Tezos has a 60 seconds block creation time, focusing more on governance and adaptability than speed. By customizing Algorand’s PPoS to suit our needs, our solution achieves a high transaction throughput of over 1,000

transactions per second. This capability ensures that our system can efficiently process several transactions for healthcare systems, managing multiple patient records simultaneously. Our solution effectively addresses block creation time, block size, and data storage requirements, making it a superior choice for health record management to other blockchain platforms.

3) TIME PROCESSING

Comparing the time taken to process transactions is part of evaluating how efficient and suitable blockchain platforms are for applications such as electronic health records. In healthcare, where timely access to information is essential, being able to execute and confirm transactions is of utmost significance. Based on Algorand, our EHR system proves its value in this context. By ensuring that transactions are processed rapidly, we improve the responsiveness of the healthcare system, enabling access to patient data. This efficiency does not only enhance the user experience. It also has significant implications for patient care, where every second counts. The following graph (FIGURE 14) compares the time processing of our proposed solution with existing methods, such as kernel methods with a processing time of (16 seconds), IoT-based monitoring with (12 seconds), exploratory data analysis with (10 seconds), and wearable sensor systems with (8 seconds) and our proposed approach with an average of time of (6,5 seconds).

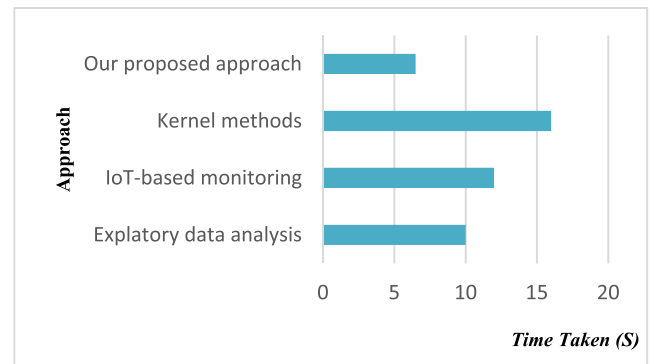


FIGURE 14. Comparison of processing time between different approaches.

VIII. CONCLUSION

In this digitalized era, where cyber security threats are increasingly common, protecting health records has become more critical than ever. To tackle this issue, we proposed a solution that combines the Algorand blockchain with the advanced ChaCha20-Poly1305 encryption algorithm. This strategic integration is carefully designed to enhance the security framework of health records. It takes advantage of the efficiency and strength of the Algorand blockchain, its Pure Proof of Stake consensus mechanism, and the robust ChaCha20-Poly1305 algorithm. We further strengthen this approach by incorporating token-based access and

decentralized identifiers to defend against cyber threats. This comprehensive approach improves security and maximizes performance and cost efficiency. The integration of these strategies has generated promising results, demonstrating a level of protection while maintaining low costs and fast processing times with an average of just 6.5 seconds. This represents an advancement in protecting health records, aligning with the paced and high-risk nature of the digital generation. Hence, our solution demonstrates its suitability for application in the healthcare sector. Although the outcomes are promising, some drawbacks remain with our solution.

While the Algorand blockchain is efficient, it could encounter challenges with scalability when dealing with high transaction volumes. This necessitates exploration into scalability solutions. The ChaCha20-Poly1305 encryption method and token-based access control require periodic updates to tackle emerging cyber threats, emphasizing the importance of adaptive security measures. Testing in simulated environments might capture only some of the complexities of real-world scenarios. Therefore, it is crucial to incorporate real-world testing in studies. For future work, we focus on improving system performance during emergencies to ensure trustworthy access to health records.

REFERENCES

- [1] O. Ayaad, A. Alloubani, E. A. ALhajaa, M. Farhan, S. Abuseif, A. Al Hroub, and L. Akhu-Zaheya, "The role of electronic medical records in improving the quality of health care services: Comparative study," *Int. J. Med. Informat.*, vol. 127, pp. 63–67, Jul. 2019, doi: [10.1016/j.ijmedinf.2019.04.014](https://doi.org/10.1016/j.ijmedinf.2019.04.014).
- [2] J. Pool, S. Akhlaghpour, F. Fatehi, and A. Burton-Jones, "A systematic analysis of failures in protecting personal health data: A scoping review," *Int. J. Inf. Manage.*, vol. 74, Feb. 2024, Art. no. 102719, doi: [10.1016/j.ijinfomgt.2023.102719](https://doi.org/10.1016/j.ijinfomgt.2023.102719).
- [3] I. Keshta and A. Odeh, "Security and privacy of electronic health records: Concerns and challenges," *Egyptian Informat. J.*, vol. 22, no. 2, pp. 177–183, Jul. 2021, doi: [10.1016/j.eij.2020.07.003](https://doi.org/10.1016/j.eij.2020.07.003).
- [4] L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," *Maturitas*, vol. 113, pp. 48–52, Jul. 2018, doi: [10.1016/j.maturitas.2018.04.008](https://doi.org/10.1016/j.maturitas.2018.04.008).
- [5] *Interoperability in Healthcare*. HIPAA Journal. Accessed: Jan. 23, 2024. [Online]. Available: <https://www.hipaajournal.com/interoperability-in-healthcare/>
- [6] E. Negro-Calduch, N. Azzopardi-Muscat, R. S. Krishnamurthy, and D. Novillo-Ortiz, "Technological progress in electronic health record system optimization: Systematic review of systematic literature reviews," *Int. J. Med. Informat.*, vol. 152, Aug. 2021, Art. no. 104507, doi: [10.1016/j.ijmedinf.2021.104507](https://doi.org/10.1016/j.ijmedinf.2021.104507).
- [7] M. U. Chelladurai, D. S. Pandian, and D. K. Ramasamy, "A blockchain based patient centric electronic health record storage and integrity management for e-health systems," *Health Policy Technol.*, vol. 10, no. 4, Dec. 2021, Art. no. 100513, doi: [10.1016/j.hlpt.2021.100513](https://doi.org/10.1016/j.hlpt.2021.100513).
- [8] A. Hasselgren, K. Kravlevska, D. Gligoroski, S. A. Pedersen, and A. Faxvaag, "Blockchain in healthcare and health sciences—A scoping review," *Int. J. Med. Informat.*, vol. 134, Feb. 2020, Art. no. 104040, doi: [10.1016/j.ijmedinf.2019.104040](https://doi.org/10.1016/j.ijmedinf.2019.104040).
- [9] R. Benaich, S. el Mendili, and G. Youssef, "Moving towards blockchain-based methods for revitalizing healthcare domain," in *Proc. 4th Joint Int. Conf. Deep Learn., Big Data Blockchain*, 2023, pp. 16–29, doi: [10.1007/978-3-031-42317-8](https://doi.org/10.1007/978-3-031-42317-8).
- [10] R. Shen, P. Zeng, K. R. Choo, and C. Li, "A certificateless provable data possession scheme for cloud-based EHRs," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 1156–1168, 2023, doi: [10.1109/TIFS.2023.3236451](https://doi.org/10.1109/TIFS.2023.3236451).
- [11] S. Xu, J. Ning, X. Huang, Y. Li, and G. Xu, "Untouchable once revoking: A practical and secure dynamic EHR sharing system via cloud," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 6, pp. 3759–3773, Nov. 2022, doi: [10.1109/TDSC.2021.3106393](https://doi.org/10.1109/TDSC.2021.3106393).
- [12] P. Chinnasamy and P. Deepalakshmi, "HCAC-EHR: Hybrid cryptographic access control for secure EHR retrieval in healthcare cloud," *J. Ambient Intell. Humanized Comput.*, vol. 13, no. 2, pp. 1001–1019, Feb. 2022, doi: [10.1007/s12652-021-02942-2](https://doi.org/10.1007/s12652-021-02942-2).
- [13] B. Wang, H. Li, Y. Guo, and J. Wang, "PPFLHE: A privacy-preserving federated learning scheme with homomorphic encryption for healthcare data," *Appl. Soft Comput.*, vol. 146, Oct. 2023, Art. no. 110677, doi: [10.1016/j.asoc.2023.110677](https://doi.org/10.1016/j.asoc.2023.110677).
- [14] Y. Liu, Z. Liu, Q. Zhang, J. Su, Z. Cai, and X. Li, "Blockchain and trusted reputation assessment-based incentive mechanism for healthcare services," *Future Gener. Comput. Syst.*, vol. 154, pp. 59–71, May 2024, doi: [10.1016/j.future.2023.12.023](https://doi.org/10.1016/j.future.2023.12.023).
- [15] S. Fugkeaw, L. Wirz, and L. Hak, "Secure and lightweight blockchain-enabled access control for fog-assisted IoT cloud based electronic medical records sharing," *IEEE Access*, vol. 11, pp. 62998–63012, 2023, doi: [10.1109/ACCESS.2023.3288332](https://doi.org/10.1109/ACCESS.2023.3288332).
- [16] C. Gan, H. Yang, Q. Zhu, Y. Zhang, and A. Saini, "An encrypted medical blockchain data search method with access control mechanism," *Inf. Process. Manage.*, vol. 60, no. 6, Nov. 2023, Art. no. 103499, doi: [10.1016/j.ipm.2023.103499](https://doi.org/10.1016/j.ipm.2023.103499).
- [17] P. Sharma, S. Namasudra, R. Gonzalez Crespo, J. Parra-Fuente, and M. Chandra Trivedi, "EHDHE: Enhancing security of healthcare documents in IoT-enabled digital healthcare ecosystems using blockchain," *Inf. Sci.*, vol. 629, pp. 703–718, Jun. 2023, doi: [10.1016/j.ins.2023.01.148](https://doi.org/10.1016/j.ins.2023.01.148).
- [18] Q. Wu, G. Meng, L. Zhang, and F. Rezaeibagha, "Collusion resistant multi-authority access control scheme with privacy protection for personal health records," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 35, no. 8, Sep. 2023, Art. no. 101677, doi: [10.1016/j.jksuci.2023.101677](https://doi.org/10.1016/j.jksuci.2023.101677).
- [19] D. Ramesh, R. Mishra, P. K. Atrey, D. R. Edla, S. Misra, and L. Qi, "Blockchain based efficient tamper-proof EHR storage for decentralized cloud-assisted storage," *Alexandria Eng. J.*, vol. 68, pp. 205–226, Apr. 2023, doi: [10.1016/j.aej.2023.01.012](https://doi.org/10.1016/j.aej.2023.01.012).
- [20] J. A. Alzubi, O. A. Alzubi, A. Singh, and M. Ramachandran, "Cloud-IoT-Based electronic health record privacy-preserving by CNN and blockchain-enabled federated learning," *IEEE Trans. Ind. Informat.*, vol. 19, no. 1, pp. 1080–1087, Jan. 2023, doi: [10.1109/TII.2022.3189170](https://doi.org/10.1109/TII.2022.3189170).
- [21] R. Benaich, S. El Mendili, and Y. Gahi, "Advancing healthcare security: A cutting-edge zero-trust blockchain solution for protecting electronic health records," *HighTech Innov. J.*, vol. 4, no. 3, pp. 630–652, Sep. 2023, doi: [10.28991/hij.2023-04-03-012](https://doi.org/10.28991/hij.2023-04-03-012).
- [22] B. Chen, T. Xiang, D. He, H. Li, and K. R. Choo, "BPVSE: Publicly verifiable searchable encryption for cloud-assisted electronic health records," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 3171–3184, 2023, doi: [10.1109/TIFS.2023.3275750](https://doi.org/10.1109/TIFS.2023.3275750).
- [23] S. Singh, S. Rathore, O. Alfarraj, A. Tolba, and B. Yoon, "A framework for privacy-preservation of IoT healthcare data using federated learning and blockchain technology," *Future Gener. Comput. Syst.*, vol. 129, pp. 380–388, Apr. 2022, doi: [10.1016/j.future.2021.11.028](https://doi.org/10.1016/j.future.2021.11.028).
- [24] Y. Jiang, X. Xu, and F. Xiao, "Attribute-based encryption with blockchain protection scheme for electronic health records," *IEEE Trans. Netw. Service Manage.*, vol. 19, no. 4, pp. 3884–3895, Dec. 2022, doi: [10.1109/TNSM.2022.3193707](https://doi.org/10.1109/TNSM.2022.3193707).
- [25] R. Mishra, D. Ramesh, D. R. Edla, and L. Qi, "DS-chain: A secure and auditable multi-cloud assisted EHR storage model on efficient deletable blockchain," *J. Ind. Inf. Integr.*, vol. 26, Mar. 2022, Art. no. 100315, doi: [10.1016/j.jii.2021.100315](https://doi.org/10.1016/j.jii.2021.100315).
- [26] G. Zhang, Z. Yang, and W. Liu, "Blockchain-based privacy preserving e-health system for healthcare data in cloud," *Comput. Netw.*, vol. 203, Feb. 2022, Art. no. 108586, doi: [10.1016/j.comnet.2021.108586](https://doi.org/10.1016/j.comnet.2021.108586).
- [27] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, A. K. M. N. Islam, and M. Shoruffzaman, "Permissioned blockchain and deep learning for secure and efficient data sharing in industrial healthcare systems," *IEEE Trans. Ind. Informat.*, vol. 18, no. 11, pp. 8065–8073, Nov. 2022, doi: [10.1109/TII.2022.3161631](https://doi.org/10.1109/TII.2022.3161631).
- [28] R. Zou, X. Lv, and J. Zhao, "SPChain: blockchain-based medical data sharing and privacy-preserving eHealth system," *Inf. Process. Manage.*, vol. 58, no. 4, Jul. 2021, Art. no. 102604, doi: [10.1016/j.ipm.2021.102604](https://doi.org/10.1016/j.ipm.2021.102604).

- [29] G. S. Aujla and A. Jindal, "A decoupled blockchain approach for edge-envisioned IoT-based healthcare monitoring," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 2, pp. 491–499, Feb. 2021, doi: [10.1109/jsac.2020.3020655](https://doi.org/10.1109/jsac.2020.3020655).
- [30] D. R. Wong, S. Bhattacharya, and A. J. Butte, "Prototype of running clinical trials in an untrustworthy environment using blockchain," *Nature Commun.*, vol. 10, no. 1, Feb. 2019, Art. no. 1, doi: [10.1038/s41467-019-08874-y](https://doi.org/10.1038/s41467-019-08874-y).
- [31] X. Yang, Y. Zhang, S. Wang, B. Yu, F. Li, Y. Li, and W. Yan, "LedgerDB: A centralized ledger database for universal audit and verification," *Proc. VLDB Endowment*, vol. 13, no. 12, pp. 3138–3151, Aug. 2020, doi: [10.14778/3415478.3415540](https://doi.org/10.14778/3415478.3415540).
- [32] X. Yang, R. Zhang, C. Yue, Y. Liu, B. C. Ooi, Q. Gao, Y. Zhang, and H. Yang, "VeDB: A software and hardware enabled trusted relational database," *Proc. ACM Manage. Data*, vol. 1, no. 2, pp. 1–27, Jun. 2023, doi: [10.1145/3589774](https://doi.org/10.1145/3589774).
- [33] H. Saeed, H. Malik, U. Bashir, A. Ahmad, S. Riaz, M. Ilyas, W. A. Bukhari, and M. I. A. Khan, "Blockchain technology in healthcare: A systematic review," *PLoS ONE*, vol. 17, no. 4, Apr. 2022, Art. no. e0266462, doi: [10.1371/journal.pone.0266462](https://doi.org/10.1371/journal.pone.0266462).
- [34] A. Tandon, A. Dhir, A. K. M. N. Islam, and M. Mäntymäki, "Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda," *Comput. Ind.*, vol. 122, Nov. 2020, Art. no. 103290, doi: [10.1016/j.compind.2020.103290](https://doi.org/10.1016/j.compind.2020.103290).
- [35] D. J. Bernstein, "ChaCha, a variant of Salsa20," Tech. Rep., 2008.
- [36] D. J. Bernstein, "The Poly1305-AES message-authentication code," in *Fast Software Encryption* (Lecture Notes in Computer Science), H. Gilbert and H. Handschuh, Eds. Berlin, Germany: Springer, 2005, pp. 32–49, doi: [10.1007/11502760_3](https://doi.org/10.1007/11502760_3).



RIHAB BENAICH received the master's degree in information systems security from the Moroccan Engineering School ENSA, Kenitra. She is currently pursuing the Ph.D. degree with the School of Applied Sciences, Morocco. Her doctoral work explores using blockchain technology in healthcare security.



SAIDA EL MENDILI received the state engineering Diploma degree in computer engineering from Cadi Ayyad University, Morocco, and the Ph.D. degree in computer science from Ibn Tofail University, Morocco. She is an Assistant Professor with the Institute of Sport Professions, Ibn Tofail University. Her research interests include artificial intelligence, big data analytics, machine learning, and smart cities.



YOUSSEF GAHI (Senior Member, IEEE) received the M.Sc. and Ph.D. degrees in computer science from Mohammed Vth University, in 2008 and 2013, respectively. He is an Associate Professor with the National School of Applied Sciences, Ibn Tofail University, Morocco. Before starting his academic career in 2017, he worked for many international firms from 2008 to 2017 as a Software Engineer, a Solution Architect, and an IT Consultant. His research topics focus on big data management, big data quality, security, and recommendation systems.

...