Journal of Cloud Computing:
Advances, Systems and Applications

RESEARCH

Open Access

Improving cloud storage and privacy security for digital twin based medical records

Haibo Yi[1*]

Abstract

As digital transformation progresses across industries, digital twins have emerged as an important technology. In healthcare, digital twins are created by digitizing patient parameters, medical records, and treatment plans to enable personalized care, assist diagnosis, and improve planning. Data is core to digital twins, originating from physical and virtual entities as well as services. Once processed and integrated, data drives various components. Medical records are critical healthcare data but present unique challenges for digital twins. However, directly storing or encrypting medical records has issues. Plaintext risks privacy leaks while encryption hinders retrieval. To address this, we present a cloud-based solution combining post-quantum searchable encryption. Our system includes key generation using Physical Unable Functions (PUF). It encrypts medical records in cloud storage, verifies records using blockchain, and retrieves records via cloud. By integrating cloud encryption, blockchain verification and cloud retrieval, we propose a secure and efficient cloud-based medical records system for digital twins. Our implementation demonstrates the system provides users efficient and secure medical record services, compared to related designs. This highlights digital twins' potential to transform healthcare through secure data-driven personalized care, diagnosis and planning.

Keywords Digital twin, Blockchain, Medical system, Cloud computing, Privacy protection

Introduction

Digital twin refers to virtual representations of complex physical systems like industrial products, manufacturing facilities, and entire cities [1, 2]. It involves digitally mapping and simulating the structure, behavior, and performance of these systems in real-time. Digital twin technology aims to optimize and maximize their potential through sensing, connectivity, analysis, and interaction capabilities [3, 4].

In healthcare, digital twin technology has gained significant traction and various applications. For example, a central monitoring station can serve as a digital twin of a patient's vital signs, allowing remote monitoring by healthcare professionals. Hospitals can also leverage digital twins to efficiently allocate resources in real-time based on dynamic patient distribution across wards. Government departments have utilized digital twins during epidemics to strategically deploy nucleic acid testing sites according to population flow patterns. As hospitals increasingly deploy smart building sensors and collect diverse medical equipment data, the healthcare sector continues exploring digital twin technology's immense potential to transform care delivery. Overall, digital twins show promise for driving data-driven optimization across complex physical systems in industries like manufacturing and healthcare.

Electronic medical records (EMRs) serve as a digital version of traditional case histories, encompassing the complete medical and health records of patients. EMRs are stored, managed, transmitted, and reproduced electronically, replacing the conventional method of handwritten paper records [5]. The adoption of EMR

*Correspondence:
Haibo Yi
haiboyi@szpt.edu.cn
[1] School of Artificial Intelligence, Shenzhen Polytechnic University, Shenzhen 518055, China

technology has become a prominent focus in the medical field.

Researchers have explored various aspects of EMR technology. For example, Yang proposed a clinical assistant diagnosis system based on convolutional neural networks, leveraging EMRs for improved diagnostic support [6]. Hechter examined the impact of EMR reminders on hepatitis B vaccine initiation and completion rates among insured adults with diabetes mellitus [7]. Delgado investigated the influence of default opioid prescription quantities in the EMR system on prescribing behavior in emergency departments [8]. Kershaw evaluated the effectiveness of EMR reminders in improving HIV screening [9]. Vandeloo conducted a retrospective EMR study to identify determinants of suicide risk preceding psychiatric admission [10]. These studies demonstrate the wide-ranging applications and benefits of EMRs in healthcare research and practice.

In the case of electronic medical records, digital twins can create and maintain detailed digital models of patients. This allows doctors and other healthcare professionals to more effectively understand and manage a patient's health status. This technology can help people simulate and predict a patient's health status, thereby improving treatment outcomes and efficiency. Digital twin electronic medical records not only include basic information about patients, such as age, gender, and ethnicity, but may also include personalized data such as genetic information, lifestyle, and environmental factors. By collecting and analyzing various health data from patients, digital twins can provide a comprehensive health view that includes past disease history, current health status, and future health risks. Digital twins can be updated in real-time with patients' health data to reflect their latest health status. Additionally, by using machine learning and other advanced data analysis techniques, digital twins can predict changes in patients' health and provide customized health advice for them. Digital twins can facilitate collaborative efforts between patients, doctors, and other healthcare professionals. For example, patients can use digital twins to track and manage their health status, doctors can use digital twins to develop and adjust treatment plans, and other healthcare professionals can use digital twins to provide adjunctive health services. Overall, digital twin electronic medical records are an innovative approach that utilizes digital technology to improve healthcare. However, this approach also poses some challenges, such as data security and privacy protection, and ensuring the quality and integrity of data. Therefore, implementing digital twin electronic medical records requires careful consideration of these issues.

Blockchain technology has emerged as a promising solution to address these issues. Initially developed as the foundation for digital currencies, blockchain is now widely applied in various sectors, including finance, commerce, and industry [11]. By using redundancy and cryptographic techniques, blockchain ensures data traceability, immutability, and enhanced security [12]. A blockchain is composed of interconnected blocks, with each block containing data and the hash value of the previous block [13]. The use of blockchain for storing and managing electronic medical records has become a focus in the medical field [14]. By harnessing the inherent characteristics of blockchain, the electronic medical record system achieves tamper resistance, traceability, and increased security and reliability [15].

Method

Digital Twin is a digital representation of physical objects that can monitor and predict equipment status in real-time, while blockchain can ensure the security and trustworthiness of data [16]. Therefore, combining digital twins and blockchain can achieve more efficient and secure business operations [17]. For example, in healthcare, digital twin technology can be used to digitize medical data of patients and monitor their status in real-time [18]. By integrating blockchain technology into digital twins, the trustworthiness and security of data can be ensured [19]. At the same time, cloud computing technology can enable more flexible and efficient data storage and processing capabilities to better support healthcare business operations [20].

Motivation. While blockchain technology provides a promising solution for digital twin medical record systems, there are also challenges that need to be addressed. Firstly, directly storing medical record data on the blockchain in plaintext could compromise privacy and potentially leak sensitive information. Secondly, once the data is encrypted for privacy protection, it becomes difficult to retrieve and access when needed. Lastly, the efficiency of blockchain networks can be relatively low, impacting the usability and performance of the medical record system.

Therefore, it is paramount to focus on advancing the underlying blockchain infrastructure for digital twin medical records to overcome these hurdles. Enhancements should be implemented to ensure robust data privacy and security protocols are in place, such as secure encryption techniques or privacy-preserving computation methods. Efforts should also optimize the scalability and efficiency of blockchain networks to bolster the usability and practical application of the medical record system. By tackling these issues head-on, the blockchain-powered medical record system can become more resilient and dependable for healthcare professionals and

patients. With the proper privacy, security and performance improvements, digital twins leveraging blockchain technology have the potential to revolutionize how medical data is stored, accessed and analyzed for the betterment of patient care.

Our contributions. Existing blockchain-based medical record systems for digital twins face challenges regarding security, efficiency and privacy protection. To address these issues, we propose a novel solution leveraging post-quantum searchable encryption techniques. Our approach consists of several key components. Firstly, we introduce a physical unable function (PUF)-based method for generating unique encryption keys for each medical record. Records are encrypted with a public key and decrypted with a corresponding private key. Secondly, we present an encrypted medical record storage method in the cloud. After each use, all medical data including personal details, symptoms and prescriptions are encrypted and securely stored. Thirdly, we propose a blockchain-powered method for verifying medical records. Hash values of encrypted records are stored in a Merkle tree on the blockchain to ensure integrity and tamper-proofing. Lastly, we introduce an efficient cloud retrieval method allowing keyword searches of symptoms, prescriptions and related records. By integrating secure key generation, encrypted cloud storage, blockchain verification and fast retrieval, our proposed system provides a private and efficient blockchain medical record solution for digital twins in the cloud. Implementation and comparison to other designs demonstrate it offers enhanced security, privacy and usability for medical record services and applications beyond basic record management.

Digital twin technology requires modeling of the human body, which demands a high level of personalization. The process of human body modeling needs to collect and integrate a large amount of personal data, including but not limited to genetic composition, physiological characteristics and lifestyle, all of which are highly sensitive information. Therefore, strong security and privacy protection measures are needed to ensure that these data are not misused or leaked. Powerful security and privacy protections must be in place to ensure this sensitive personal data is not misused or exposed during the process of collecting and integrating the large amounts of individual data needed to create highly personalized digital models of human physiology for digital twin applications. Our solution aims to address existing challenges in digital twin by leveraging post-quantum encryption techniques in a novel integration of blockchain and cloud computing technologies.

Organization. The rest of the paper is organized as follows. Section "Preliminaries" provides background on existing digital twin, blockchain-based medical techniques and searchable encryption technologies. Section "Blockchain system based on searchable encryption and cloud for digital twin" proposes a novel blockchain system leveraging searchable encryption and cloud computing for digital twin. Section "Blockchain medical record system for digital twin on cloud for privacy protection" introduces our proposed blockchain medical record system hosted in the cloud, with an emphasis on privacy protection. Section "Implementation and comparison" details the implementation and evaluation of the blockchain medical record system for digital twin through comparisons to related approaches. Lastly, Section "Conclusion and future work" concludes the paper and discusses potential future work.

Preliminaries

Digital twin and its medical applications

Digital twin is a digital replica of physical assets, processes and systems which can be used to optimize business performance [21]. The concept of digital twins has gained significant traction in recent years with advances in technologies like IoT, AI, cloud computing and 5 of the early applications of digital twins was in manufacturing where virtual replicas of products and production lines helped identify inefficiencies and test design changes before implementation. This reduced costs and sped up product development cycles [22].

Digital twins are now being applied more broadly across sectors like healthcare, transportation and smart cities [23]. In healthcare, digital twins of patients enable remote monitoring and "what-if" scenario planning. For transportation, digital twins of vehicles and infrastructure aid predictive maintenance and traffic management.

The rise of ubiquitous sensors, high-speed networks and cloud infrastructure has enabled digital twins to scale across entire cities and countries. National digital twin initiatives aim to digitally map infrastructure, buildings and natural systems for urban planning, emergency response simulation and sustainability goals [24].

As computing power grows with technologies like edge and fog computing, digital twins are becoming more dynamic, incorporating real-time data to mirror physical counterparts with increasing accuracy. This will open up more opportunities in applications spanning manufacturing to smart spaces [25].

Overall, digital twin technology is evolving rapidly to drive operational efficiencies, reduce costs and enable new datadriven business models across industries by creating living digital simulations of the physical world.

Digital twin technology can digitize patients' physiological parameters, medical records and treatment plans to build personalized digital models for each patient. These digital models can monitor patients' vital signs in real-time and send early warnings for remote monitoring once abnormalities are detected. Through digital model simulation, doctors can formulate and optimize treatment plans in advance in a virtual environment, and test different assumptions to provide support for clinical decision-making. Doctors can also use digital models to conduct pre-operative simulation and training of surgeries to improve actual surgical success rates. Hospitals can utilize digital twins to dynamically manage and allocate medical resources, thereby optimizing resource utilization efficiency. By analyzing a large amount of medical records with digital twin technology, doctors can mine valuable information to improve diagnostic and prognostic capabilities. In general, digital twin technology is expected to comprehensively improve clinical diagnosis and treatment levels through personalized modeling, remote monitoring, decision support, knowledge dissemination and other means.

The threat of quantum computer attacks to digital twins

Quantum computers may pose certain security threats to digital twin medical record systems.

(1) Quantum computers could crack existing public-key cryptosystems, such as RSA and elliptic curve cryptography. This would jeopardize the security of medical records and key exchanges encrypted using public keys in the system.

(2) Quantum computers using quantum period finding algorithms could break hash functions in polynomial time, undermining the medical record verification mechanism based on hash values on the blockchain using Merkle trees.

(3) Quantum computers may use quantum navigation algorithms to crack searchable encryption and disrupt the private query functionality of medical records in the cloud.

(4) The accelerated cryptanalysis capabilities of quantum computers will also increase the risk of cracking offline medical record devices and keys.

To address these potential threats, digital twin medical record systems need to:

(1) Adopt post-quantum secure cryptographic algorithms such as lattice-based cryptography.

(2) Enhance medical record verification mechanisms such as using multi-layer hashing.

(3) Strengthen security protections for endpoint device and key management.

(4) Regularly evaluate security risks and timely upgrade system defense capabilities.

(5) Promote the development of post-quantum cryptanalysis standards to lay the foundation for the post-quantum era.

Overall, quantum computers pose major challenges, and the system will require long-term efforts to continuously strengthen security defenses to address this threat.

Blockchain medical techniques

Blockchain is a distributed ledger or database that is shared among multiple nodes in a network. It allows for the decentralized recording of transactions and sharing of information. Due to the characteristics of distributed accounting, tamper proof and traceability, blockchain has been applied to many fields, such as medical treatment. Using blockchain to improve health care has become one of the hot spots in this field.

The relevant blockchain medical research is as follows. Mertz presented an interview with Beth Israel Deaconess medical center's John Halamka about blockchain potential [26]. Lijing proposed a blockchain-based medical insurance storage system [27]. Tian proposed medical data management on blockchain with privacy [28]. Lee proposed a blockchain-based medical data preservation scheme for telecare medical information systems [29]. Shen proposed a blockchain-based approach for privacy-preserving image retrieval for medical IoT systems [30]. Cheng proposed a design of a secure medical data sharing scheme based on blockchain [31]. Firdaus proposed a mobile device and blockchain based medical data management for root exploit detection and features optimization [32]. Lo proposed a blockchain-enabled iwellchain framework integration with the national medical referral system [33]. Huang proposed a blockchain-based scheme for privacy-preserving and secure sharing of medical data [34]. Cheol proposed efficiently managing medical information in the pain management field based on blockchain [35].

However, blockchain medical techniques also have the following problems.

(1) The medical record data is stored in plaintext, which leads to the problem of privacy leakage.

(2) Once the data is encrypted, it is not easy to retrieve.

(3) The efficiency of blockchain is low, which affects the use of medical record system.

Thus, it is very urgent to improve blockchain system of medical techniques.

Searchable encryption technology

Searchable encryption is to realize the search function in the case of encryption. At present, there are many files that need to be deleted or modified by the server. But sometimes some file contents don't want the server to know and need to encrypt the file. How to store the encrypted file to the remote server and realize the search

and file modification under the condition of confidentiality is the research content of searchable encryption.

There are two methods to realize searchable encryption: symmetric cryptography and public key cryptography. The security of algorithms based on public key cryptography depends on the difficulty of solving complex mathematical problems, mainly using algebraic tools such as bilinear mapping. The algorithm based on symmetric cryptography uses pseudo-random function, hash algorithm and symmetric encryption algorithm, which is faster than the algorithm based on public key cryptography. They are suitable for different application scenarios.

The relevant searchable encryption research is as follows. Li proposed an engineering searchable encryption of mobile cloud networks [36]. Cui proposed an key-aggregate searchable encryption for group data sharing via cloud storage [37]. Sen proposed a searchable symmetric encryption [38]. Wu proposed an efficient searchable encryption against keyword guessing attacks for sharable electronic medical records in cloud-based system [39]. Ma proposed a certificateless searchable public key encryption scheme for industrial Internet of things [40]. Zhou proposed file-centric multi-key aggregate keyword searchable encryption for industrial Internet of things [41]. Lu proposed a pairing-free certificate-based searchable encryption supporting privacy-preserving keyword search function for IIoTs [42]. Li proposed a lightweight fine-grained searchable encryption scheme in fog-based healthcare IoT networks [43]. Zamani proposed a new searchable encryption scheme with integrity preservation property [44]. Padhya proposed a novel approach for key-aggregate searchable encryption for multi-owner data [45]. Cao proposed a searchable encryption cloud storage with dynamic data update to support efficient policy hiding [46]. Li proposed a blockchain-based searchable symmetric encryption scheme [47]. Ayad proposed an efficient and privacy-preserving approximate search in cloud computing [48]. Miao proposed a lightweight fine-grained search over encrypted data in fog computing [49]. Zarezadeh proposed a multi-keyword ranked searchable encryption scheme with access control for cloud storage [50].

Blockchain system based on searchable encryption and cloud for digital twin

Overview of the blockchain system

To address challenges in blockchain-based medical record systems for digital twin, we propose a post-quantum searchable encryption technique to enable secure and efficient record management.

Section "Key generation and key exchange method" details a PUF-based key generation and exchange method that assigns unique random keys to each record. Encryption uses a public key while decryption relies on a corresponding private key.

Section "Encrypted medical record storage method" presents an encrypted medical record storage approach in the cloud. After each use, all medical data including personal information, symptoms and prescriptions are encrypted and stored securely.

Section "Verification method based on blockchain" introduces a blockchain-powered method for verifying medical records integrity. Encrypted record hashes are stored in a Merkle tree on the blockchain.

Section "Cloud retrieval method" proposes an efficient cloud retrieval method allowing keyword searches of symptoms, prescriptions and related records.

By integrating PUF-based keying, encrypted cloud storage, blockchain verification and fast retrieval, our solution aims to overcome limitations in existing blockchain medical record systems through a novel application of post-quantum searchable encryption techniques.

Key generation and key exchange method

We propose a PUF-based key generation and exchange method. Traditional encryption algorithms are vulnerable as keys can easily be stolen, compromising private information. Therefore, keys must be generated randomly in a way that is unpredictable and unique.

Secure key generation and storage relies on two core requirements:

(1) A true random source to guarantee unpredictability and uniqueness of freshly generated keys.

(2) Protected storage to reliably maintain generated key information and prevent unauthorized access.

However, satisfying both requirements is challenging to implement in practice. PUF provides a solution by leveraging the inherent physical properties of integrated circuits.

When powered on, SRAM cells within a PUF chip initialize randomly. This startup behavior differs across chips, manifesting as random bit flips between zero and one. The resulting fingerprint can then be used as a key.

Our proposed PUF approach utilizes an array of transistors. The PUF device sends a signal to the array, assigning 1 or 0 to each bit based on the responses. Unlike digital keys, the PUF key is actively created during each request, generating different keys by activating unique transistor subsets. This allows for unpredictable, one-time-use keys resistant to theft.

The proposed PUF-based key generator meets the two core requirements for secure key generation and storage. It converts the device's unique random physical fingerprint into a cryptographic key via processing. Firstly, no Pseudorandom Number Generator (PRNG)

is required as the device's inherent randomness provides the needed entropy. Secondly, no protected nonvolatile storage space is necessary. The same key can be regenerated on demand by leveraging the random physical fingerprint. Each user possesses a PUF device to generate their private key. Additionally, each record corresponds to a randomly generated symmetric key.

During key exchange, public-key encryption is used along with private key decryption. For example, if users A and B want to exchange a key.

(1) User A uses PUF to generate a private key $priA_0$ and computes the corresponding public key $pubA_0$.

(2) User A uses $pubA_0$ to encrypt $priA_0$ and receive $priA_1$.

(3) User B uses PUF to generate a private key $priB_0$ and computes the corresponding public key $pubB_0$.

(4) User A uses $pubB_0$ to encrypt $priA_1$ and receive $priAB_1$.

(5) User A sends $priAB_1$ to user B.

(6) User B uses $priB_0$ to decrypt $priAB_1$ and receive $priA_1$.

We summary the notations used in the method, which is described in Table 1 and we depict the key generation and key exchange in Fig. 1.

Encrypted medical record storage method

Traditionally, medical record data is stored in plaintext, posing serious privacy risks. We propose an encrypted medical record storage method leveraging the cloud.

Table 1 Key generation and key exchange method

User A			User B		
Private key	**Public key**	**Encrypted key**	**Private key**	**Public key**	**Encrypted key**
$priA_0$	$pubA_0$	$priA_1$	$priB_0$	$pubB_0$	-

Medical records form the core basis for diagnosis, treatment planning, prevention strategies, clinical teaching, research, and serve as important legal documentation. Upon each use, our method encrypts all record data, including personal information, symptoms, prescriptions, and more.

The encrypted records are then stored securely in the cloud. By encrypting sensitive health data before cloud storage, our approach aims to address the shortcomings of plaintext storage which can enable privacy breaches. With encryption, only authorized parties with the proper decryption keys would be able to access the personal medical information.

Securely storing encrypted records in the cloud also provides benefits such as convenient access from different locations, redundancy protection against data loss, and easy integration into electronic health systems. Overall, the proposed encryption method for cloud-based storage seeks to better safeguard individual privacy within medical records while maintaining the critical functions they serve.

For each medical record, it is assigned a record number rec_i, where the personal information, symptom and prescription are denoted by inf_i, sym_i and pre_i, respectively.

(1) The patient uses his private key $priA_0$ to generate three encryption keys $priA_1$, $priA_2$, $priA_3$, encrypts the encryption keys and personal information inf_i with the doctor's public key $pubB_0$, and sends the ciphertext cip_0 to the doctor.

(2) The doctor uses his own private key $priB_0$ to decrypt the ciphertext cip_0 and obtain three encryption keys $priA_1$, $priA_2$, $priA_3$ and patient personal information inf_i.

(3) The doctor fills in the patient's symptoms sym_i and prescriptions pre_i, and encrypts the patient's personal information inf_i, symptoms sym_i and prescriptions pre_i with three keys $priA_1$, $priA_2$, $priA_3$, respectively.

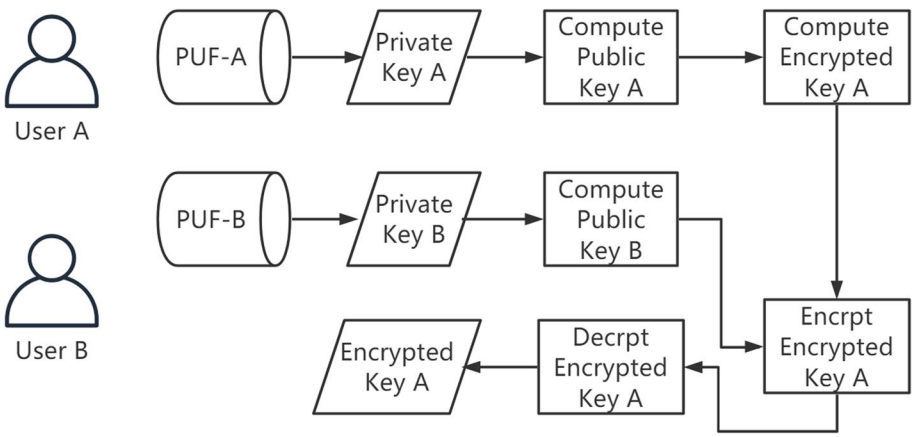

Fig. 1 Key generation and key exchange method

After that, three ciphertexts cip_1, cip_2, cip_3 have been computed.

(4) The doctor uses his own private key $priB_0$ to sign three ciphertexts cip_1, cip_2, cip_3 and the record number rec_i to generate corresponding signature information, i.e., sig_0.

(5) The doctor uploads the record number rec_i, three ciphertexts cip_1, cip_2, cip_3 and signatures sig_0 to the cloud.

(6) Other users can use the doctor's public key $pubB_0$ to verify the signature sig_0 and verify the authenticity of the signature.

We summary the notations used in the method, which is described in Table 2.

Patient and doctor private keys are generated via PUF, leveraging its properties of uniqueness and strong security. Symmetric encryption keys are uniquely generated by each patient's PUF as well.

To securely transmit these keys, patients encrypt their generated keys with the doctor's public key. Doctors then use the received encryption key to cryptographically protect medical record data.

Additionally, doctors sign the encrypted records with their private key. This allows others to verify the data and signature using the doctor's public key, achieving non-repudiation of the medical record information.

In summary, by combining PUF-based key generation, public-key encryption for key exchange, symmetric encryption of data, and digital signatures, our approach ensures the confidentiality, integrity and authenticity of medical records in a cryptographically sound manner during transmission between patients and healthcare providers.

We depict the encrypted medical record storage method in Fig. 2.

In detail, the signature generation process is as follows.

(1) The hash value of the message m is generated via $H(m)$, where H is the SHA-256 algorithm.

(2) The linear transformation is computed via $m' = A \times H(m) + B$, where A denotes a matrix key and B denotes a vector key.

(3) The central map transformation is computed via $F(s') = m'$, where F includes a set of multivariate polynomials and s' is the private key.

(4) The linear transformation is computed via $s = C \times s' + D$, where C denotes a matrix key and D denotes a vector key.

The signature generation process is not complex. The multivariate polynomials are evaluated by $\bar{F}(s) = h'$, where $\bar{F}$ is a set of multivariate polynomials. If $h' = H(m)$, the signature is valid. Otherwise, the signature is forged.

Verification method based on blockchain

We propose a blockchain-powered method for verifying medical record integrity. Blockchain is well-suited for this role due to its ability to solve issues of centralization through decentralization.

Table 2 Encrypted medical record storage method

Patient					Doctor		
Record number	**Medical record**	**Private key**	**Public key**	**Encrypted key**	**Private key**	**Public key**	**Signature information**
rec_i	inf_i, sym_i, pre_i	$priA_0$	$pubA_0$	$priA_1, priA_2, priA_3$	$priB_0$	$pubB_0$	sig_0

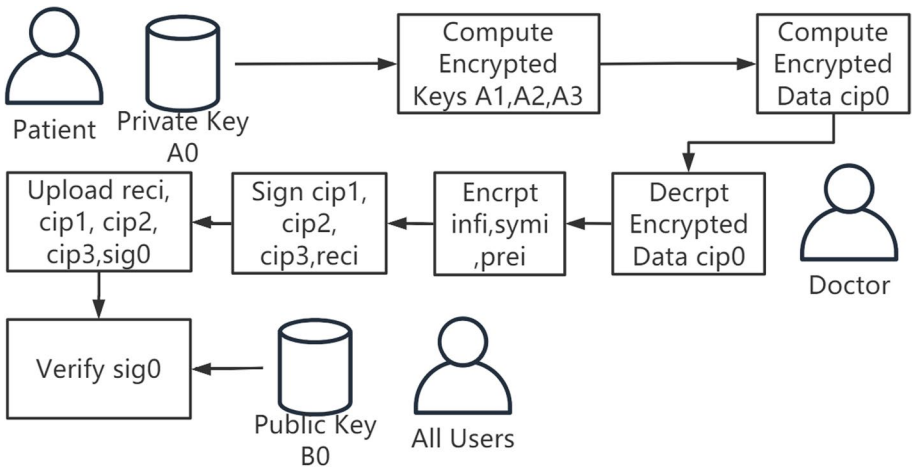

Fig. 2 Encrypted medical record storage method

As the technology underpinning digital currencies, blockchain techniques have seen widespread adoption across finance, commerce, and industry due to key characteristics like data traceability, tamper resistance, and security. A blockchain consists of a chain of blocks, with each block containing data and a hash of the previous block.

Leveraging blockchain for electronic medical record storage and management has become an important area of research in healthcare. Our proposed method involves storing the hashes of encrypted medical records on the blockchain using Merkle trees.

The blockchain network will contain various nodes, including user nodes to access records and a manager node to oversee the system. Through redundancy and cryptography, any changes to the records would be evident on the blockchain, allowing our solution to validate record authenticity and integrity in a decentralized manner.

By integrating blockchain verification of encrypted health data, our approach aims to take advantage of this transformative technology's security and transparency benefits for next-generation medical record systems.

The manager's node stores the full blockchain, which is depicted in Fig. 3.

Each block stores the number of the medical record and the hash value of the medical record, the root of the hash tree in the current block and the hash value of the previous block.

In order to improve efficiency, the user node of blockchain does not store the hash value of medical record, but only stores the root of the hash tree of the current block. The user's node stores the efficient blockchain, which is depicted in Fig. 4.

Each block stores the number of the medical record and the root of the hash tree in the current block and the hash value of the previous block.

In detail, the root of the hash tree is computed in Fig. 5.

Medical record verification is a streamlined process. It only requires obtaining the ciphertext of a record from cloud storage and performing a hash operation to compare the resulting value against the hash stored on the blockchain.

If the two hashes match, the medical record is confirmed to be authentic and untampered. However, a mismatch would indicate the record has been altered and is invalid.

By incorporating blockchain's inherent traits, such as resistance to tampering, transparency and traceability of changes, our electronic medical record system becomes more secure and reliable. Leveraging blockchain verification eliminates the need for a centralized authority while still ensuring the integrity of sensitive health data.

Any unauthorized modifications would be evident on the immutable blockchain. This adds an important layer of validation to confidently establish the authentic provenance and accuracy of individuals' medical histories when needed for clinical purposes.

Cloud retrieval method

We propose a cloud retrieval method based on searchable encryption to enable secure searches on encrypted data. Searchable encryption allows searches to be performed on encrypted data without decrypting it first. Many files stored on remote servers need to be deleted or modified by the server. However, some file contents should remain confidential from the server. Searchable encryption allows files to be encrypted before storing on a remote server while still enabling keyword searches and modifications on the encrypted data.

Our proposed cloud retrieval method utilizes searchable encryption to enable querying symptoms, prescriptions, and corresponding symptom-prescription mappings for individuals through keyword searches. The searchable encryption allows these sensitive medical data to be stored securely on the cloud while still retaining searchability. This allows personalized symptom-prescription mappings to be retrieved securely through keyword searches on the encrypted data.

We created two index tables, as shown in the Table 3.

Each user is assigned a unique user ID. Index 1 allows querying the total number of medical records for a user via their ID. To retrieve a specific encrypted medical record, the user simply provides the record's ID to fetch it from the cloud. If the user wants to exchange plaintext records with another user, they need to exchange decryption keys.

To query prescriptions for a disease, the user searches Index 2 by disease keywords to get the corresponding symptom and prescription locations in the cloud. The user then downloads the encrypted symptoms and prescriptions from the cloud and requests access rights from the owners.

This cloud retrieval method maintains privacy by not exposing personal data, diseases, prescriptions or other sensitive information in plaintext. It also enables secure data sharing through encrypted record retrieval and exchange of decryption keys. The indexing system allows keyword searches on the encrypted data.

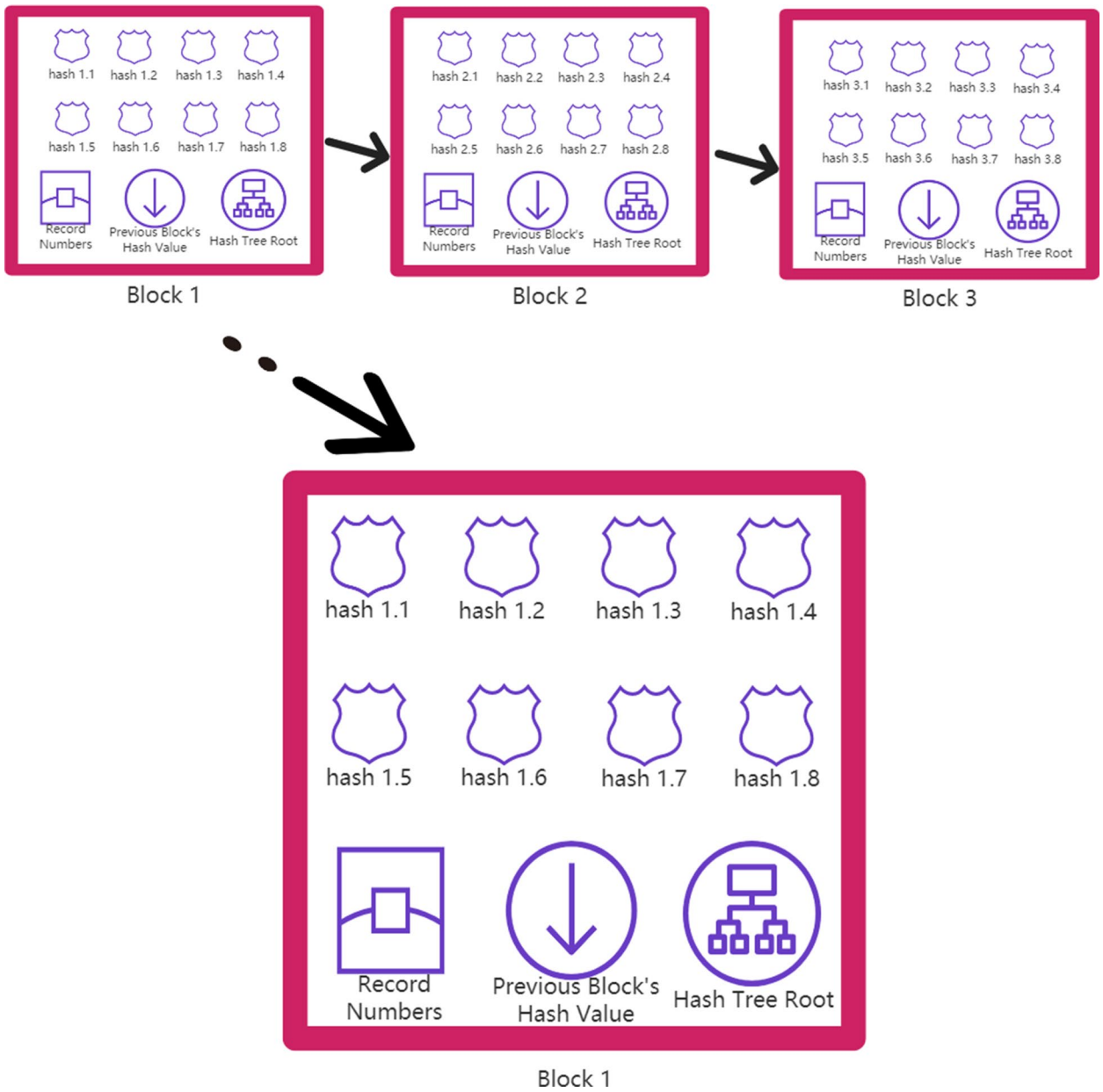

Fig. 3 Full blockchain for verification

Blockchain medical record system for digital twin on cloud for privacy protection

System architecture

By integrating key techniques, cloud based encryption, blockchain verification and cloud retrieval method, we propose a blockchain medical record system for digital twin on cloud for privacy protection.

The process of submitting medical records is depicted in Fig. 6 and is illustrated as follows.

(1) The patient generates three encryption keys using their private key, then encrypts the keys and their personal information with the doctor's public key. The resulting ciphertext is sent to the doctor.

(2) The doctor decrypts the ciphertext using their private key to obtain the three encryption keys and patient's personal information.

(3) The doctor records the patient's symptoms and prescriptions, then encrypts the personal information, symptoms and prescriptions separately with each of the three keys.

(4) The doctor signs the three ciphertexts and record number with their private key to generate signature information.

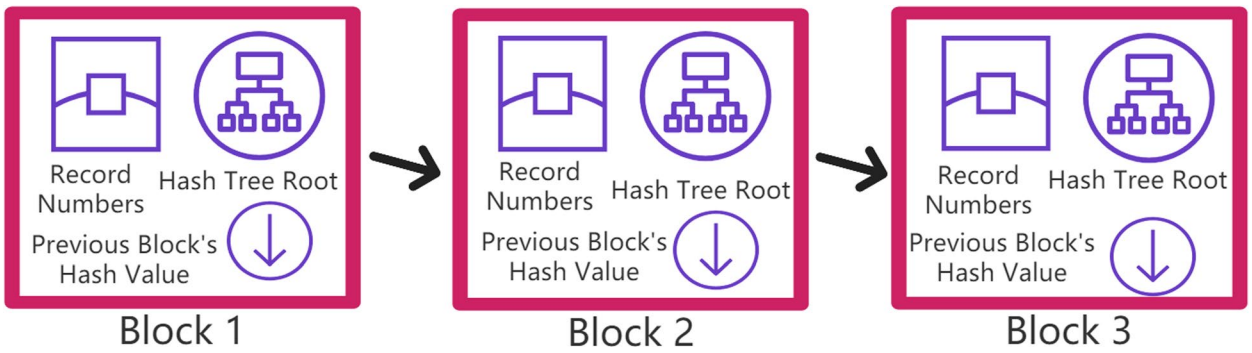

Fig. 4 Efficient blockchain for verification

Table 3 Cloud retrieval method

Index 1		Index 2	
User number	**Record number**	**Symptom**	**Symptoms and prescriptions**
$user_1$	rec_1	tosse	$sym_5, pre_5, sym_7, pre_7, sym_8, pre_8$
$user_2$	rec_2	fever	$sym_{11}, pre_{11}, sym_{12}, pre_{12}, sym_{21}, pre_{21}$
$user_3$	rec_3	headache	$sym_{25}, pre_{25}, sym_{54}, pre_{54}, sym_{72}, pre_{72}$
...	...	...	...
$user_n$	rec_n	...	...

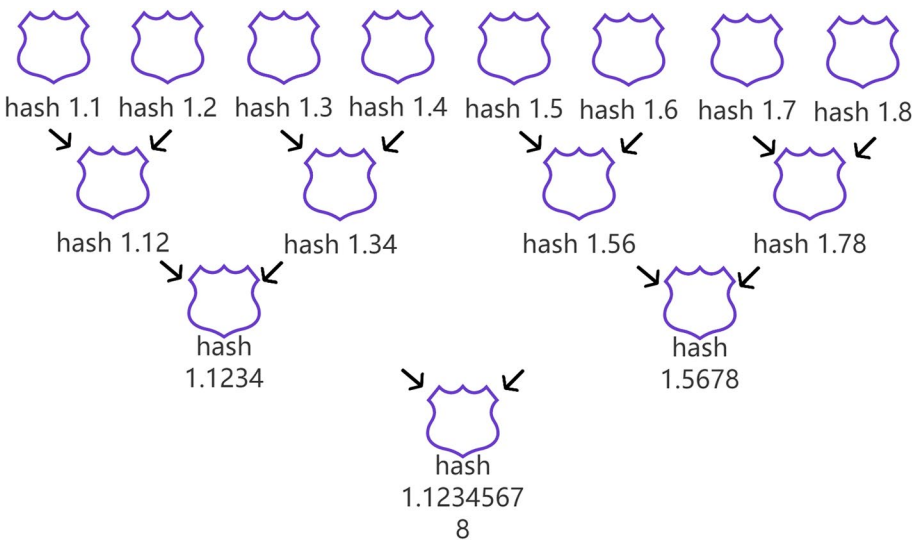

Fig. 5 The root of the hash tree

(5) The doctor uploads the record number, three ciphertexts, and signatures to the cloud storage.

(6) Other users can verify the signature using the doctor's public key to authenticate the data.

(7) The doctor uploads the record number and hash values of the three ciphertexts to the blockchain as an immutable record.

This provides confidentiality through encryption, integrity through signatures, and immutability through blockchain hashes. The three encryption keys allow selective sharing of information.

The process of medical record verification is depicted in Fig. 7 and is illustrated as follows.

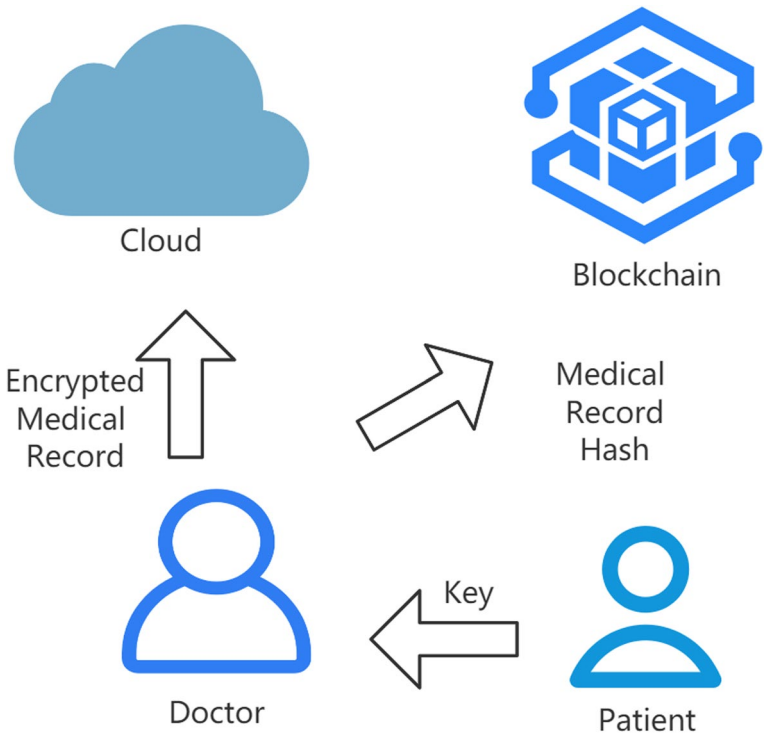

Fig. 6 Submitting medical records

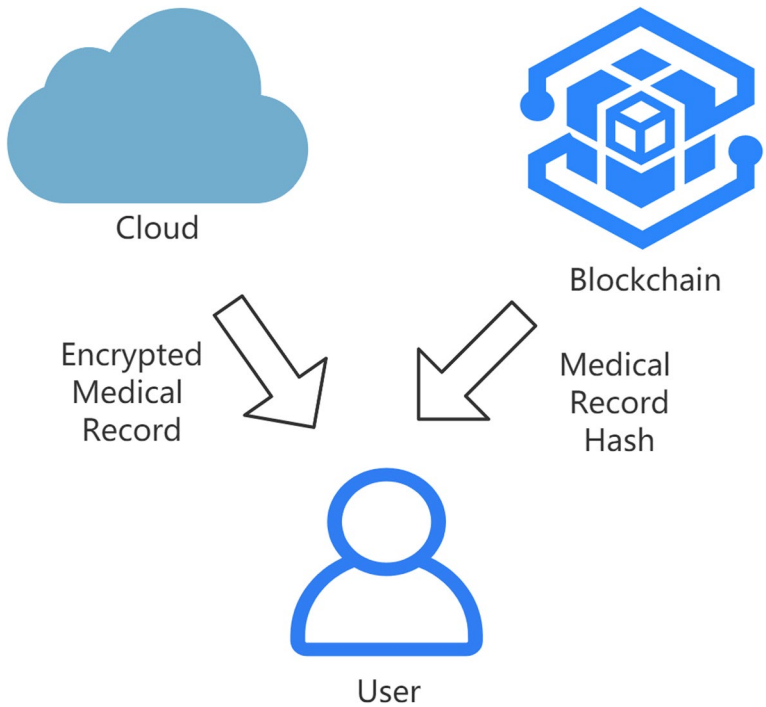

Fig. 7 Process of medical record verification

(1) The user retrieves the encrypted medical record ciphertext from the cloud storage.

(2) The user looks up the hash of the ciphertext stored on the blockchain.

(3) The user hashes the retrieved ciphertext and compares it to the blockchain hash value.

(4) If the hashes match, the medical record is verified as authentic. If they differ, the record is false or corrupted.

This allows the user to verify the integrity of the medical record ciphertext by comparing its hash to the immutable hash recorded on the blockchain. The blockchain hash serves as a tamper-evident seal for the encrypted data.

The process for doctors to query the patient's medical records is depicted in Fig. 8 and is illustrated as follows.

(1) Each user has a unique user ID, and can retrieve all the medical records of the user through index 1.

(2) Doctors only need to use the medical record ID to retrieve specific medical records on the cloud, which can obtain encrypted medical records.

(3) The patient encrypts the decryption key using the doctor's public key.

(4) The patient sends the ciphertext to the doctor.

(5) The doctor uses his private key to decrypt the ciphertext and obtain the medical records.

The process for doctors to inquire about prescriptions is depicted in Fig. 9 and is illustrated as follows.

(1) If the doctor needs to query the prescription of a certain kind of disease, he needs to query index 2 according to the keyword of the disease to obtain the corresponding symptom and the location of the prescription on the cloud.

(2) He downloads the ciphertext of symptoms and prescriptions on the cloud, and request access rights from the users.

Implementation and comparison

We built a blockchain-based medical record system on cloud infrastructure for digital twin. It leverages key techniques for privacy protection, i.e., cloud-based encryption of records for confidentiality, blockchain verification of record hashes for integrity validation and cloud retrieval of encrypted records. The implementation results, outlined in Table 4, demonstrate the system efficiently and securely provides medical record services to users. By encrypting records before cloud storage, verifying record integrity via blockchain, and allowing retrieval of encrypted data from cloud, our solution addresses privacy and security concerns while maintaining usability. Patients and healthcare providers can confidently access accurate, untampered medical histories when needed. The implementation shows how combining these techniques establishes an advanced yet practical electronic health record system optimized for privacy.

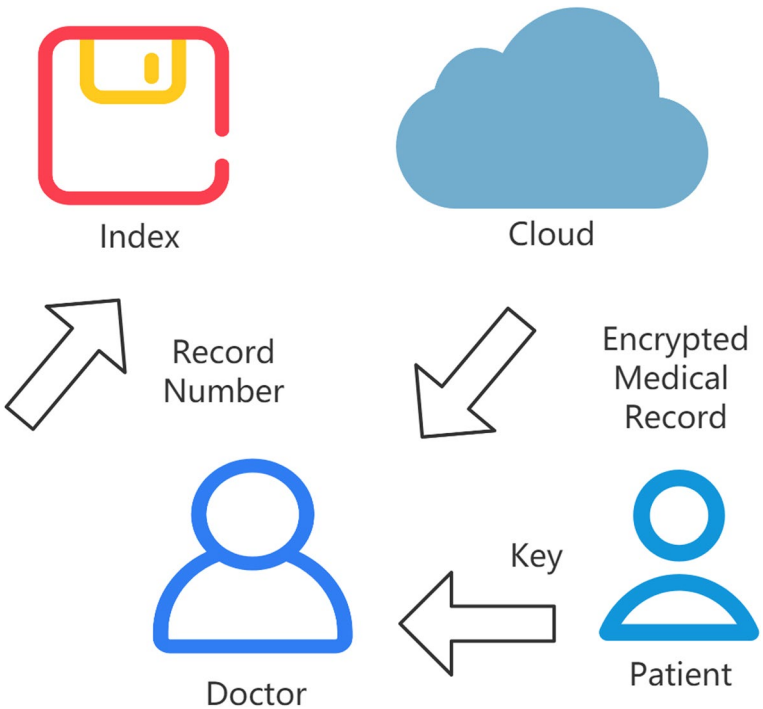

Fig. 8 Query the patient's medical records

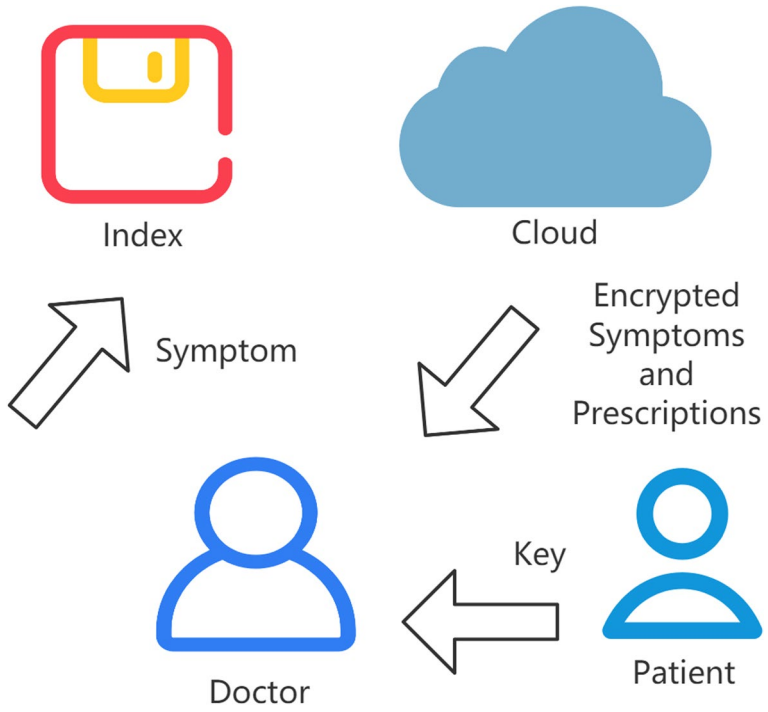

Fig. 9 Inquire about prescriptions

Table 4 Implementation result

Parameters		Results	
Blockchain Nodes	**Medical Record**	**Average Query Time for record**	**Average Query Time for symptom**
10	20	1.5*s*	2.8*s*
100	250	2.2*s*	4.3*s*
200	400	2.8*s*	5.7*s*
500	900	3.5*s*	6.3*s*
1000	1000	4.2*s*	7.2*s*

We evaluated our system against related designs, with results summarized in Table 5. Comparisons with alternative approaches indicate our cloud-blockchain based system provides highly secure medical record services while maintaining moderate efficiency. Specifically, the system offers stronger privacy protections through its encryption of records before cloud storage and blockchain verification of record integrity. Whereas some solutions rely on centralized authorities or less robust security models, our decentralized design leveraging cryptography and blockchain consensus establishes authenticity without weak points of control. However, the additional overhead of encryption, hashing, and blockchain operations results in modest performance impacts for user experience compared to less secure plaintext storage models. Overall, the side-by-side assessment confirms how our solution achieves a favorable balance between security considerations and usability through its combined techniques - outperforming alternatives in the critical domain of privacy while retaining functional practicality.

The blockchain medical record system provides secure cloud-based services for electronic health data management and access. It utilizes encryption of medical records in the cloud for confidentiality, blockchain verification of record hashes to validate integrity, personal record

Table 5 Comparison result

Medical System	System Architecture	Record Verification	Query Security	Query Security	Query Efficiency
Traditional	Server	None	High	Low	High
Blockchain-Based	Distributed	Low	Blockchain	Moderate	Moderate
Ours	Cloud	Blockchain	Moderate	High	Moderate

querying via an encrypted cloud retrieval system and authorized disease or prescription queries to locate relevant health data.

Cryptographic keys are uniquely generated by each user's PUF device, ensuring data security. Private keys allow decrypting records, while public keys enable digital signatures for non-repudiation.

All medical record hashes are recorded on the immutable blockchain. This allows tracing records and detecting tampering, improving security. Blocks contain record IDs, Merkle roots, and prior block hashes.

The encrypted retrieval system leverages cloud computing power for efficient access. Users are assigned unique IDs to query their personal records by ID number. Retrieved records remain encrypted without the user's decryption key.

To access plaintext records, users must exchange keys. Disease queries locate symptom/prescription metadata locations. Users can then retrieve the encrypted health data and request access authorization from involved parties.

Overall, through its combination of encryption, blockchain, and privacy-focused retrieval design, the system provides a secure yet usable platform for electronic healthcare powered by modern distributed technologies.

Conclusion and future work

We present a post-quantum searchable encryption approach to enable a secure and efficient medical record system for digital twins. First, we propose a PUF-based key generation and exchange method. Each record corresponds to a random key uniquely generated by a user's PUF. Public keys encrypt keys for transmission, while private keys allow decryption. Second, we put forth a cloud-based encrypted medical record storage method. Records containing personal, symptom and prescription data are encrypted before storage in the cloud. Third, we design a blockchain-powered verification technique. Hashes of encrypted records are recorded on the immutable blockchain using Merkle trees. Fourth, we introduce an encrypted cloud retrieval system. It allows querying symptoms/prescriptions by person or keyword through the encrypted records. By integrating encryption, blockchain verification and encrypted retrieval, we developed a privacy-preserving blockchain medical record system on cloud infrastructure. Implementation results and comparisons demonstrate it efficiently and securely provides medical services while surpassing alternatives in security.

Additionally, the system can augment other healthcare applications through its utilization of modern cryptographic and distributed technologies. Overall, the work presents an advanced yet usable solution for digital twin medical records. However, the solution discussed does not fully address all potential vulnerabilities. Future work should aim to strengthen security defenses in several key areas.

(1) Regulatory compliance: Healthcare data is highly regulated to protect privacy and security. The system would need to comply with applicable laws and regulations, which is not discussed.

(2) Ethical use of data: The system must have safeguards and transparency around how data is used, shared and potentially monetized. Ethical AI practices are important to address privacy and fairness concerns.

(3) User consent and control: For adoption, users need easy ways to understand and consent to how their data is handled. Strong user consent and data ownership controls are important but not specified.

(4) Interoperability standards: The system must integrate with existing healthcare IT infrastructure, which requires following interoperability standards. Standards compliance is not evaluated.

(5) Earning user trust: For sensitive health data, privacy and security breaches could severely damage trust. More discussion is needed around how to establish and maintain user confidence over time.

(6) Usability testing: The design must be intuitive for non-technical users. Usability and user experience testing results could provide better insights on real-world adoption challenges.

Addressing these social, ethical and regulatory factors is key for any healthcare technology. Future work would benefit from more rigorous analysis of how the proposed system would navigate these important challenges to responsible innovation and deployment at scale.

Authors' contributions

H.Y. wrote the main manuscript text.

Funding

The authors acknowledge National Natural Science Foundation of China (No. 62202316), Characteristic Innovation Projects in Guangdong Provincial Universities (No. 2022KTSCX308), Supporting Project of National Natural Science Foundation of China (No. 6022310037K), Scientific Research Startup Fund for Shenzhen High-Caliber Personnel of Shenzhen Polytechnic (No.6021310026K).

Availability of data and materials

Not applicable.

Declarations

Ethics approval and consent to participate

Not applicable.

Competing interests

The authors declare no competing interests.

Received: 22 July 2023 Accepted: 27 September 2023
Published online: 30 October 2023

References

1. Mihai S, et al (2020) Digital Twins: A Survey on Enabling Technologies, Challenges, Trends and Future Prospects. In: IEEE Communications Surveys & Tutorials, vol 24, no. 4. IEEE, US, p 2255-2291
2. Zhang B, Zhang M, Dong T, Lu M, Li H (2023) Design of Digital Twin System for DC Contactor Condition Monitoring. In: IEEE Transactions on Industry Applications, vol 59, no. 4. IEEE, US, p 3904-3909
3. Wu X, Lian W, Zhou M, Song H, Dong H (2023) A Digital Twin-Based Fault Diagnosis Framework for Bogies of High-Speed Trains. In: IEEE Journal of Radio Frequency Identification, vol 7. IEEE, US, p 203-207
4. Hao H, Wang Y (2023) Smart Curb Digital Twin: Inventorying Curb Environments Using Computer Vision and Street Imagery. In: IEEE Journal of Radio Frequency Identification, vol 7. IEEE, US, p 168-172
5. Telenti A, Steinhubl SR, Topol EJ (2018) Rethinking the medical record. Lancet 391(10125):1013
6. Yang Z, Huang Y, Jiang Y et al (2018) Clinical Assistant Diagnosis for Electronic Medical Record Based on Convolutional Neural Network. Sci Rep 8(1):6329
7. Hechter RC, Lei Q, Yi L et al (2018) Impact of an electronic medical record reminder on hepatitis B vaccine initiation and completion rates among insured adults with diabetes mellitus. Vaccine 37:195–201
8. Delgado MK, Shofer FS, Patel MS et al (2018) Association between Electronic Medical Record Implementation of Default Opioid Prescription Quantities and Prescribing Behavior in Two Emergency Departments. J Gen Intern Med 33(4):1–3
9. Kershaw C, Taylor JL, Horowitz G et al (2018) Use of an electronic medical record reminder improves HIV screening. BMC Health Serv Res 18(1):1–8
10. Vandeloo K, Mcquaid R, Burhunduli P et al (2020) Determinants of Suicide Risk Preceding Psychiatric Admission: A Retrospective Electronic Medical Record Study. Biol Psychiatry 87(9):S269–S270
11. Tsao Y-C, Thanh V-V (2021) Toward blockchain-based renewable energy microgrid design considering default risk and demand uncertainty. Renew Energy 163:870–881
12. Chen B, Wu L, Wang H et al (2020) A Blockchain-Based Searchable Public-Key Encryption With Forward and Backward Privacy for Cloud-Assisted Vehicular Social Networks. IEEE Trans Veh Technol 69(6):5813–5825
13. Sidorov M, Khor JH, Nhut PV, et al (2020) Public Blockchain-enabled Wireless LoRa Sensor Node for Easy Continuous Unattended Health Monitoring of Bolted Joints: Implementation and Evaluation. IEEE Sensors J PP(99):1
14. Hamdaoui B, Alkalbani M, Znati T et al (2020) Unleashing the Power of Participatory IoT with Blockchains for Increased Safety and Situation Awareness of Smart Cities. IEEE Netw 34(2):202–209
15. Gupta R, Kumari A, Tanwar S, et al (2020) Blockchain-envisioned Softwarized Multi-Swarming UAVs to Tackle COVID-19 Situations. IEEE Netw PP(99):160–167
16. Ramezan G, Leung CS (2020) An Analysis of Proof-of-Work based Blockchains under An Adaptive Double-spend Attack. IEEE Trans Ind Inform PP(99):1
17. Musigmann B, Gracht HVD, Hartmann E (2020) Blockchain Technology in Logistics and Supply Chain Managemen, A Bibliometric Literature Review From 2016 to January 2020. IEEE Trans Eng Manag PP(99):1-20
18. Chen R, Tu IP, Chuang KE, et al (2020) Endex: Degree of Mining Power Decentralization for Proof-of-Work Based Blockchain Systems. IEEE Netw PP(99):1-6
19. Schneider S, Leyer M, Tate M (2020) The Transformational Impact of Blockchain Technology on Business Models and Ecosystems: A Symbiosis of Human and Technology Agents. IEEE Trans Eng Manag PP(99):1-12
20. Fraga-Lamas P, Fernandez-Carames TM (2020) Fake news, disinformation, and Deepfakes: leveraging distributed ledger technologies and blockchain to combat digital deception and counterfeit reality. IT Prof 22(2):53–59
21. Sanz Rodrigo M, Rivera D, Moreno JI, Àlvarez-Campana M, López DR (2023) Digital Twins for 5G Networks: A Modeling and Deployment Methodology. In: IEEE Access, vol 11. IEEE, US, p 38112-38126
22. Dai Y, Zhang Y (2022) Adaptive Digital Twin for Vehicular Edge Computing and Networks. In: Journal of Communications and Information Networks, vol 7, no. 1. IEEE, US, p 48-59
23. Wang B, Zhang C, Zhang M, Liu C, Xie Z, Zhang H (2022) Digital Twin Analysis for Driving Risks Based on Virtual Physical Simulation Technology. In: IEEE Journal of Radio Frequency Identification, vol 6. IEEE, US, p 938-942
24. Azfar T, Weidner J, Raheem A, Ke R, Cheu RL (2022) Efficient Procedure of Building University Campus Models for Digital Twin Simulation. In: IEEE Journal of Radio Frequency Identification, vol 6. IEEE, US, p 769-773
25. Tang Q, Wu B, Chen W, Yue J (2023) A Digital Twin-Assisted Collaborative Capability Optimization Model for Smart Manufacturing System Based on Elman-IVIF-TOPSIS. In: IEEE Access, vol 11. IEEE, US, p 40540-40564
26. Mertz L (2018) Hospital CIO Explains Blockchain Potential: An Interview with Beth Israel Deaconess Medical Center's John Halamka. IEEE Pulse 9(3):8–9
27. Lijing Z, Licheng W, Yiru S (2018) MIStore: a Blockchain-Based Medical Insurance Storage System. J Med Syst 42(8):149
28. Tian H, He J, Ding Y (2019) Medical Data Management on Blockchain with Privacy. J Med Syst 43(2):1-10
29. Lee TF, Li HZ, Hsieh YP (2020) A blockchain-based medical data preservation scheme for telecare medical information systems. Int J Inf Secur 2020:1-13
30. Shen M, Deng Y, Zhu L et al (2019) Privacy-Preserving Image Retrieval for Medical IoT Systems: A Blockchain-Based Approach. IEEE Netw 33(5):27–33
31. Cheng X, Chen F, Xie D et al (2020) Design of a Secure Medical Data Sharing Scheme Based on Blockchain. J Med Syst 44(2):52
32. Firdaus A, Anuar NB, Razak MFA et al (2018) Root Exploit Detection and Features Optimization: Mobile Device and Blockchain Based Medical Data Management. J Med Syst 42(6):112
33. Lo YS, Yang CY, Chien HF, et al (2019) Blockchain-Enabled iWellChain Framework Integration With the National Medical Referral System: Development and Usability Study. J Med Internet Res 21(12):1-12
34. Huang H, Zhu P, Xiao F et al (2020) A Blockchain-based Scheme for Privacy-Preserving and Secure Sharing of Medical Data. Comput Secur 99:102010
35. Cheol CM, Ming-Yen H (2023) Boudier-Reveret Mathieu. Blockchain Technology: Efficiently Managing Medical Information in the Pain Management Field. Pain Med 1(7):7
36. Li H, Liu D, Dai Y et al (2015) Engineering searchable encryption of mobile cloud networks: when QoE meets QoP. IEEE Wirel Commun 22(4):74–80
37. Cui B, Liu Z, Wang L (2016) Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage. IEEE Trans Comput 65(8):1
38. Sen Poh G, Chin JJ, Yau WC et al (2017) Searchable Symmetric Encryption: Designs and Challenges. ACM Comput Surv 50(3):1–37
39. Wu Y, Lu X, Su J et al (2016) An Efficient Searchable Encryption Against Keyword Guessing Attacks for Sharable Electronic Medical Records in Cloud-based System. J Med Syst 40(12):258
40. Ma M, He D, Kumar N et al (2018) Certificateless Searchable Public Key Encryption Scheme for Industrial Internet of Things. IEEE Trans Ind Inform 14(99):759–767
41. Zhou R, Zhang X, Du X, et al (2018) File-Centric Multi-Key Aggregate Keyword Searchable Encryption for Industrial Internet of Things. IEEE Trans Ind Inform 2018:1
42. Lu Y, Li J, Wang F (2020) Pairing-Free Certificate-Based Searchable Encryption Supporting Privacy-Preserving Keyword Search Function for IIoTs. IEEE Trans Ind Inform PP(99):1
43. Li H (2019) Jing T (2019) A Lightweight Fine-Grained Searchable Encryption Scheme in Fog-Based Healthcare IoT Networks. Wirel Commun Mob Comput 7:1–15
44. Zamani M, Safkhani M, Daneshpour N, et al (2020) A New Searchable Encryption Scheme with Integrity Preservation Property. Wirel Pers Commun 2020:1-24
45. Padhya M, Jinwala DC (2019) MULKASE: a novel approach for key-aggregate searchable encryption for multi-owner data. Front Inf Technol Electron Eng 20(12):1717–1748

46. Cao L, Kang Y, Wu Q et al (2020) Searchable encryption cloud storage with dynamic data update to support efficient policy hiding. China Commun 17(6):153–163
47. Li H, Tian H, Zhang F et al (2019) Blockchain-based searchable symmetric encryption scheme. Comput Electr Eng 73:32–45
48. Ayad I, Hai J, Yassin AA, et al (2014) Towards Efficient Yet Privacy-Preserving Approximate Search in Cloud Computing. Comput J 57(2):241-254
49. Miao Y, Ma J, Liu X, et al (2018) Lightweight Fine-Grained Search over Encrypted Data in Fog Computing. IEEE Trans Serv Comput 2018:1
50. Zarezadeh M, Mala H, Ashouri-Talouki M (2019) Multi-keyword ranked searchable encryption scheme with access control for cloud storage. Peer Peer Netw Appl 13(1):1–12

Publisher's Note