BLOCKCHAIN ENFORCED ATTRIBUTE BASED ACCESS CONTROL WITH ZKP FOR HEALTHCARE SERVICE

Dongju Lee[1] and Hyunsung Kim[1,2]

[1]Department of Computer Engineering, Kyungil University, Korea
[2]Department of Mathematical Sciences, University of Malawi, Malawi

ABSTRACT

The relationship between doctors and patients is reinforced through the expanded communication channels provided by remote healthcare services, resulting in heightened patient satisfaction and loyalty. Nonetheless, the growth of these services is hampered by security and privacy challenges they confront. Additionally, patient electronic health records (EHR) information is dispersed across multiple hospitals in different formats, undermining data sovereignty. It allows any service to assert authority over their EHR, effectively controlling its usage. This paper proposes a blockchain enforced attribute-based access control in healthcare service. To enhance the privacy and data-sovereignty, the proposed system employs attribute-based access control, zero-knowledge proof (ZKP) and blockchain. The role of data within our system is pivotal in defining attributes. These attributes, in turn, form the fundamental basis for access control criteria. Blockchain is used to keep hospital information in public chain but EHR related data in private chain. Furthermore, EHR provides access control by using the attributed based cryptosystem before they are stored in the blockchain. Analysis shows that the proposed system provides data sovereignty with privacy provision based on the attributed based access control.

KEYWORDS

Healthcare service, Blockchain, Access control, Authentication, Non-interactive zero-knowledge proof.

1. INTRODUCTION

The evolution of high-speed Internet and sensor technology has made it possible for remote healthcare services to effectively manage healthcare needs from any location, at any time [1-3]. With the development of information communication technology, healthcare is transitioning from traditional hospital-centric care to patient-centric remote treatment, focusing on improving convenience and accessibility. Through smart healthcare services, patients' health status can be monitored in real-time, offering advantages in terms of time efficiency and enhancing their quality of life. Patients appreciate the efficiency of accessing healthcare services, irrespective of where they are located. This flexibility eliminates the constraints of time and space, enabling direct consultations with their attending physician.

Nevertheless, safeguarding data privacy and security is crucial during data collection and transmission in healthcare services, given their susceptibility to diverse attacks [4-10]. Successful attacks by malicious actors could result in unintended actions through wireless body area networks (WBAN) or Internet of things (IoT), posing life-threatening risks to patients. Consequently, the development of data privacy and security mechanisms becomes imperative for ensuring the safety of healthcare applications.

In recent times, there has been significant progress in the utilization of blockchain technology, with broader implications across diverse sectors like healthcare, WBAN, and IoT [11-15]. Preventing unauthorized data tampering is a key outcome, enhancing both system integrity and immutability. Furthermore, it could decentralize the security and privacy requirements. A decentralized blockchain-based authentication system for IoT was put forth by Hammi et al., suggesting innovative approaches to security [13]. Khashan & Khafajah introduced an authentication architecture for heterogeneous IoT, blending both centralized and blockchain-based elements [14]. They argued that their architecture provides authentication, secure identity management, data integrity, data freshness, key refreshment and non-repudiation. Liu et al. proposed a blockchain enforced privacy preserving authentication and key agreement and access control (BP-AKAA) for industrial IoT [15].

While medical information exchanged between patients and doctors is typically perceived as patient-owned and managed, it is often stored and managed within the hospital's database [16-18]. Accessing such information requires patients to visit the hospital in person, and even then, access is often restricted. This limitation on accessing one's information diminishes their right to self-determination. Moreover, integrating information becomes challenging when patients see multiple doctors across various hospitals. Since medical data is hospital-dependent and centrally managed, any security breach compromises the patient's electronic health records, leaving them reliant solely on the hospital's data management [19-21]. To cope with the centralized problem, Chen et al. proposed a medical data-sharing mechanism based on attribute-based access control and privacy protection [22]. They used the K-anonymity and searchable encryption techniques for security and privacy reasons. However, it provides a detailed attribute-based access control yet requires a secure channel for the registration of the participants. Azbeg et al. proposed a healthcare system that integrates IoT with blockchain named BlockMedCare [23]. Within BlockMedCare, security is established through the utilization of a re-encryption proxy in conjunction with blockchain, ensuring the safe storage of hash data. However, it does not consider data sovereignty, which involves the rights and obligations regarding the ownership, control, and access to data [24]. Data sovereignty is an emphasis on ensuring that data remains within the jurisdiction and control of the entity that owns it. This concept becomes particularly relevant in cross-border data transfers, where data may move across different legal jurisdictions, raising concerns about compliance with local regulations, privacy laws, and security standards [25]. As observed in the analysis of relevant research, suggestions have been made for decentralized environments in healthcare or security techniques utilizing ZKP. However, secure access control methods in decentralized environments ensuring data sovereignty have yet to be explored.

The purpose of this paper is to propose a blockchain-enforced attribute-based access control in healthcare services for the decentralized security and privacy and data sovereignty. The proposed system employs attribute-based access control, ZKP and blockchain. The definition of attribute within our system can be determined by considering the role of data, which serves as the foundational criterion for access control. Blockchain is used to keep hospital information in the public chain but EHR related data in the private chain. Furthermore, EHR provides access control by using the attributed based cryptosystem before they are stored in the blockchain. The main contributions of this paper are as follows:

- Attribute-based access control with blockchain is proposed to provide data sovereignty of EHR for healthcare services. This method is both time-efficient and energy-saving, aligning perfectly with the limited resources of IoT devices. By doing so, it is possible to reduce misuse of patient data and ensure data sovereignty.

- This paper effectively devises a new authentication scheme based on ZKP and blockchain. Through this functionality, system participants can register using the Internet, guaranteeing secure communication and data exchange across all connected hospitals.
- The blockchain keeps an access control list (ACL) and logs for the patient's EHR-related data. By providing a specific definition of access control details in ACL, it is possible to guarantee patient sovereignty over their information, and through detailed log management, patients can verify how their data is being utilized.
- A doctor collaboration scheme is additionally devised for the patient to freely visit any second hospital and to be treated for the healthcare service securely. However, the patient does not need to consider their EHR data but the main doctor could provide a delegation service to the second hospital doctor.
- The performance and security analyses are presented. Through our approach, the results and comparisons with related schemes demonstrate a substantial potential to enhance patient data sovereignty and privacy. Furthermore, the results illustrate the resilience of our security system, showcasing its ability to withstand attacks and meet the security demands inherent in IoT systems.

The paper is organized as follows: The relevant existing security primitives to understand this paper are presented with the related works in Section 2. The proposed security system with related phases is explained in Section 3. Section 4 provides performance and security analysis with proper comparisons among related works. Section 5 concludes the research.

2. PRELIMINARY AND RELATED WORKS

In this section, a succinct explanation is given concerning the cryptographic primitives utilized in the context of this paper. Furthermore, we provide a detailed analysis of some related works, which are used for the comparisons of analysis.

2.1. Blockchain

The concept of blockchain involves creating a distributed ledger where data blocks are organized into a chain format, following a strict chronological order. [26]. This introduces a fresh trust paradigm within the open network, allowing system participants to establish trust even in decentralized settings. In blockchain systems, the security of the ledger relies on the interconnected structure of hash values and the consensus algorithm. The hash value of the previous block header is included in the latest block. As a result of this synchronized updating process, any attempt to effect unauthorized changes within the blockchain network faces significant barriers. Specifically, without controlling more than 51% of the total computational power of the system, adversaries are unable to execute alterations effectively. This inherent security feature underscores the robustness and resilience of blockchain technology against malicious attacks. Ethereum, HyperLedger Fabric, and Corda R3 are among the diverse platforms available. Within the healthcare environment leveraging blockchain technology, it's crucial to offer varying levels of control to system participants. This is only possible with permission frameworks like HyperLedger Fabric or Corda. In contrast to Ethereum, both Fabric and Corda offer more detailed access control, allowing participants to have their permissions tailored to reading, creating, updating, and deleting rights, thereby enhancing privacy protection. Within this study, HyperLedger Fabric was employed as the chosen blockchain platform. Fabric introduces a novel blockchain architecture with a focus on enhancing resiliency, flexibility, scalability, and confidentiality. [27]. Within a public blockchain system, individuals are able to participate freely, without any requirement for a specific identity. Conversely, a private blockchain restricts access

to only identified participants. Through this method, communication is restricted to trusted participants, promoting a secure mode of interaction.

2.2. Zero-Knowledge Proof

Goldwasser et al. proposed the concept of ZKP [28]. ZKP enables privacy-preserving authentication. In this paper, we will use one discrete logarithm-based ZKP to realize certificateless key generation and privacy protected authentication which was used in [23] as Definition 1.

Definition 1. Proof of knowledge of a discrete logarithm (PoK).

Within the given public parameters (G, g, p, $H(\cdot)$), G denotes a multiplicative cyclic group characterized by a prime order p, with g acting as a generator of G, and $H(\cdot)$ representing a cryptographically secure one-way hash function. For $Y \in G$, a representation of Y in relation to g involves an element $x \in Z_p$, which satisfies the relation $R=\{(x, Y) \in Z_p \times G: g^x = Y\}$. The prover P endeavors to persuade a skeptical yet honest verifier $\mathcal{V}$ that he (or she) possesses knowledge of a representation of a given Y, all the while safeguarding the secrecy of the underlying secret x.

- P chooses $v \leftarrow Z_p^*, R \leftarrow \{0,1\}^*$ to compute $V=g^v$, $c=H(g, Y, V)$ and $y = v - cx (mod\ p)$. P sends the proof $\Psi_{PoK} = <Y, V, r>$ to the verifier.

- $\mathcal{V}$ computes c first. If the condition $V = g^r \cdot Y^c$ holds, $\mathcal{V}$ accepts this proof, otherwise rejects.

2.3. Attribute-based Data Encryption

Waters introduced a ciphertext-policy attribute-based encryption scheme that is both expressive and efficient, providing provable security. This scheme comprises the following algorithms [29]:
- $Setup(\lambda, U) \rightarrow (MPK, MSK)$: a central authorization entity utilizes a security parameter λ and an attribute universe U as input, executing the algorithm to generate the system's public and private key (MPK, MSK).

- $E_{MPK}(MSG) \rightarrow CT$: the encryption algorithm requires the message MSG to be encrypted and the system's public key, which incorporates an attribute access structure, as input. It then produces ciphertext CT, ensuring that only a user whose attribute set meets the access structure criteria can successfully decrypt it.
- $KeyGen(MPK, MSK, S) \rightarrow DK$: the key generation algorithm requires the system's public and private keys along with a user attribute set S, as input. It then generates a decryption (private) key DK for the user.
- $D_{MPK}(CT) \rightarrow MSG$: the decryption algorithm requires a ciphertext related to an access structure and the system key, which corresponds to a set of attributes, as input. If the attribute set meets the access structure, the algorithm will produce valid plaintext MSG.

2.4. Attribute-based Access Control

Attribute-based encryption is an encryption technique in which only a user having an attribute value suitable for the encrypted data may decrypt data. Hu et al. defined a high-level ABAC as follows [30]:

- A logical access control methodology where authorization to perform a set of operations is determined by evaluating attributes associated with the subject, object, quested operations, and, in some cases, environment conditions against policy, rules, or relationships that describe the allowable operations for a given set of attributes.
- Attributes are characteristics that define specific aspects of the subject, object, environmental conditions, and/or requested actions predefined and preassigned by an authority. Attributes typically consist of three components: an optional category that denotes the type of information conveyed by the attribute, a name, and a value.
- A subject is generally an individual, process, or device that is responsible for actively transmitting information between objects or initiating changes in the system's state. This entity has the potential to represent either the user, the requester, or a mechanism acting in the interest of either the user or the requester. A subject within a system can encompass non-human entities like systems or processes, not necessarily limited to human actors. Typically, subjects undertake actions representing a particular individual or organization. Subjects have the potential to be assigned attributes that detail various aspects such as their name, organization affiliation, citizenship, etc.
- An object is an inert entity within the information system framework, encompassing devices, files, records, tables, processes, programs, networks, and domains, which either contain or receive information. When a subject gains access to an object, it inherently means gaining access to the information stored within it. This object can encompass various entities, including resources or requested entities, as well as anything that a subject may interact with, such as data, applications, services, devices, and networks.
- An operation involves the execution of a function in response to a subject's request on an object within the system. The range of operations encompasses actions such as read, write, edit, delete, author, copy, execute, and modify.
- Policy is the representation of rules or relationships that define the set of allowable operations a subject may perform upon an object in permitted environment conditions.

2.5. Related Works

This subsection aims to examine works in the realm of IoT or healthcare that have implemented blockchain technology to establish decentralized security architecture and offer access control [13-15, 23]. These works are utilized for comparison with the proposed system in the analysis section.

To decentralize the authentication system, Hammi et al. proposed a decentralized system called bubbles of trust, which plans to ensure a robust identification and authentication of devices [13]. Utilizing blockchains, their system establishes secure virtual zones wherein entities can mutually identify and trust one another. It provides a good design concept for the decentralization of security and privacy systems. However, it does not provide any cross-domain security concept nor data sovereignty and access control.

For the heterogeneous and scalable IoT systems, Khashan & Khafajah proposed a hybrid centralized and blockchain-based authentication architecture for heterogeneous IoT systems based on a lightweight cryptographic methods [14]. They argued that centralized authentication schemes is inappropriate for cross-domain authentication and limit the scalability of IoT networks. So, edge servers were deployed to provide centralized authentication based on blockchain networks in their architecture. They argued that their architecture provides authentication, secure identity management, data integrity, data freshness, key refreshment and non-repudiation and is strong against various attacks. However, their architecture does not provide any details on the data management for the system and thereby it does not consider any data sovereignty.

Liu et al. proposed a blockchain-enforced privacy-preserving authentication and key agreement and access control (BP-AKAA) for industrial IoT [15]. It is purposed to solve trust issues between mutually untrusted subnets through third-party trusted servers. BP-AKAA is based on attribute-based access control, non-interactive ZKP and blockchain for device to device communication security. They argued that BP-AKAA solved the untrust issue of cross-domain authentication with the assistance of distributed blockchain. Despite its advantages, BP-AKAA lacks data sovereignty for network participants since the encrypted data cannot be controlled by its owner. Additionally, it fails to offer comprehensive insights into attribute usage for secure data management.

Azbeg et al. introduced BlockMedCare, a healthcare system combining IoT and blockchain technologies, designed to facilitate remote patient monitoring. This system aims to address the needs of patients with chronic diseases that necessitate ongoing supervision. [23]. BlockMedCare's security framework relies on a combination of re-encryption proxy and blockchain technology, facilitating the storage of hash data. To address blockchain scalability concerns, the implementation incorporated an off-chain database utilizing the InterPlanetary File System (IPFS) for data storage. As a use case, they applied BlockMedCare to diabetes management and showed the execution results with good security and performance aspects. However, BlockMedCare does not consider doctor collaborations between different hospitals or data sovereignty.

Although various researches have been conducted, there has been no researches that can guarantee open channel registration, data sovereignty, decentralized security framework and cross-domain collaboration framework for healthcare applications.

3. BLOCKCHAIN-ENFORCED ATTRIBUTE- BASED ACCESS CONTROL

In this section, a blockchain-enforced attribute-based access control in healthcare service is proposed. It uses blockchain, ZKP, and attribute-based access control to protect the authentication privacy for healthcare services. Blockchain keeps some healthcare service information for decentralization purposes. It keeps hospital information and public key information in the public chain but EHR related data, ACL and log data in private chain, which could be further controlled based on the access control scheme.

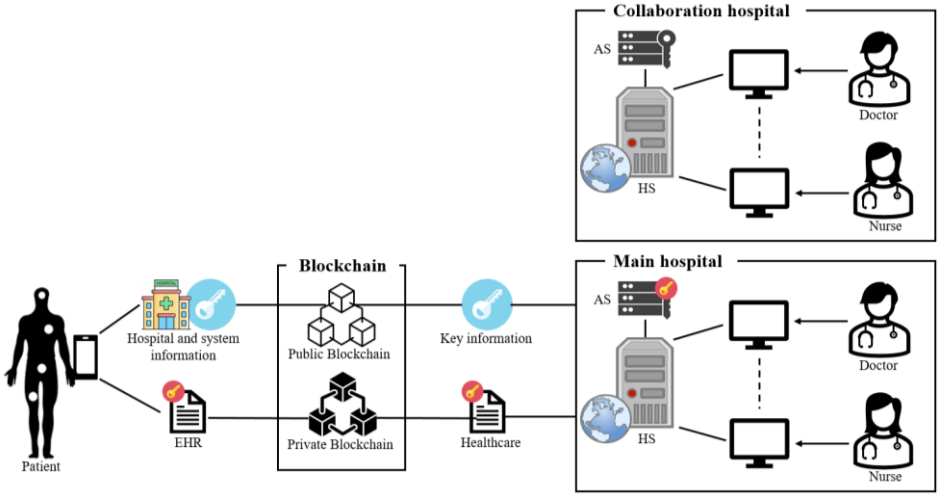

Figure 1. Overview of the proposed security system

3.1. System Model

Figure 1 depicts the system model for attribute-based access control enforced by blockchain. The configuration relies on a blockchain data structure comprising both public and private chains. The designated roles for each entity are defined as follows:

(1) Hospital server (HS): HS acts as the central nexus for remote healthcare services, functioning as the focal point for all aspects of patient care. It is responsible for the registration of system components and oversees the coordination between patients and medical staff. The objective is to provide secure and privacy-assured remote healthcare services by collaborating with in-hospital AS.
(2) Attribute server (AS): AS serves as the key generation center responsible for all processes related to keys, especially attribute keys. It collaborates with HS to generate keys, publish public key information on the blockchain, and securely transmit private key information to system participants through HS.
(3) Patient: The entity is the subject of remote healthcare services. At intervals determined by the doctor for remote healthcare services, EHR is stored on the blockchain using attribute keys.
(4) Doctors and nurses: They offer remote medical consultation services to patients located at a distance. The access scope of EHR may be limited based on system access permissions. It verifies the health information of patients stored on the blockchain and conducts appropriate remote consultations.
(5) Blockchain: Public blockchain stores hospital details and public key information for the system configuration. Private blockchain keeps patient's EHR, ACL and logs data on them.

Table 1. Notations

Notation	Description
k	A security parameter
MPK_{AS}, ASK_{AS}	The master public key, the attribute secret key
RPK_{AS}, RSK_{AS}	The public and private key of AS
ISK_X, IPK_X	Private identity key and public identity key of
AUK_X	X
ID_X, PW_X	Attribute key of X
$KDF(\cdot)$	Identifier and password of X
Ψ_{PoK}	A key derivation function
g	A ZKP of knowledge of a discrete algorithm
G, G_T	A generator of G
H_1, H_2	Two multiplicative groups of prime order p
C	Secure hash functions
TS	Cipher text
$e(\cdot)$	Timestamp
$H_1(\cdot)$	Bilinear pairing
$H_2(\cdot)$	A hash function mapping $\{0, 1\}^* \rightarrow G$
$E_X(\cdot)$	A hash function mapping $\{0, 1\}^* \rightarrow Z_p^*$
$\|\|$	Attribute-based data encryption with the key X
.	String concatenation operation
	Point multiplication operation

(6) Main hospital and collaboration hospital: Main hospital provides remote medical consultation services for patients. However, in cases where collaborative treatment with a doctor from another hospital, which is a cross-domain situation, is required for the patient, it

addresses such requirements by coordinating with a collaboration hospital using the cross-domain collaboration phase.

The data structure of the proposed system is formulated upon hybrid principles of both public and private blockchain technology. In our system, there exist five ledgers tasked with storing hospital particulars, public key data, patient EHR, ACL, and logs. The initial two ledgers are designated for the public blockchain, while the remaining three serve the private blockchain. The data logs are typically public under most circumstances. Nevertheless, logs pertaining to access to EHR may be considered confidential in certain instances, especially focused on healthcare applications. Consequently, we store such logs within the private blockchain. Public blockchains store information intended for sharing among all system participants. This information requires integrity assurance and is organized to facilitate easy verification by system participants.

- Hospital particulars ledger: Various information about hospitals that needs to be shared with patients is stored. Specifically, it provides detailed information about physicians and maintains information about collaborating hospitals and physicians. This allows patients to conveniently select their primary care doctors even from remote locations and make informed decisions about collaboration.
- Public key data ledger: This ledger stores public key information required for initialization and registration. It aims to maintain cryptographic shared information for ensuring secure healthcare services. Only participants registered on the hospital server can generate relevant data but everybody could access the information.

Within the private blockchain, access is restricted solely to entities possessing requisite attributes, as authenticated by the blockchain. This private ledger securely maintains EHRs, ACLs and logs ensuring privacy and security through suitable protective measures. Further elucidation of the configuration of ledgers is provided below:

- EHR ledger: EHRs represent standard personal private data, affording individuals complete ownership rights. EHRs are encrypted by attribute-based encryption as mentioned in EHR generation and retrieval phase, which not only can protect data privacy but also can improve the efficiency of data access. Only authorized users with the proper attributes can access this ledger by smart contracts. The sharing of EHRs is guaranteed even if patients are incapacitated.
- ACL ledger: Management of comprehensive details concerning patient EHR ledger access is conducted. All data presented in this ledger is under the patient's right to ensure data sovereignty. Particularly, even in instances necessitating cross-domain collaboration medical care, the primary doctor can introduce new ACLs with the patient's authorization only.
- Logs ledger: All records related to the patient's EHR ledger are stored. By regularly checking this ledger, patients can determine whether there has been any infringement on their data sovereignty regarding their EHR data.

This system considers the practical Byzantine fault tolerance (PBFT) algorithm for the consensus used in the public blockchain. Nonetheless, the system offers flexibility through pluggable consensus mechanisms, allowing for the integration of alternative algorithms like Raft or Kafka to align with the specific needs of the healthcare application. To simplify matters, in the proposed system, HS holds the authority to make decisions regarding all transactions within the private blockchain. The notations used in this paper are summarized in Table 1.

3.2. System Procedure

The proposed system has four phases: system initialization, registration, authentication, EHR generation and retrieval and cross-domain collaboration.

3.2.1. System Initialization

HS sends a system security initialization request to AS. AS chooses a security parameter $k \in N$ and generates two multiplicative cyclic groups G and G_T of a prime order p. Let g be a generator of G, and $e(\cdot)$: $G_T = G \times G$ be a bilinear map. Let $D = (G, G_T, g, p, e(\cdot))$ be a bilinear group. AS selects two one-way hash functions: $H_1(\cdot)$: $\{0, 1\}^* \rightarrow G$ and $H_2(\cdot)$: $\{0, 1\}^* \rightarrow Z_p^*$. A key derivation function (KDF) is selected for generating symmetric encryption keys. AS chooses its private key, $RSK_{AS}=\alpha \leftarrow Z_p^*$ and proceeds to calculate the public key $RPK_{AS}=g^{\alpha}$. AS selects $t_i \leftarrow Z_p^*$ for each attribute $a_i \in U_A$ to compute attribute public keys $T_i=\{g^{ti}\}$, where U_A is the attribute universe with N attributes. AS releases the master public key $MPK_{AS}=(D, H_1, H_2, KDF(\cdot), RPK)$ onto the blockchain for public access, while safeguarding the attribute secret key $ASK_{AS}= (\{t_i\}_{i\in[1, N]}, RSK_{AS})$ within a trusted platform module (TPM) to maintain confidentiality. After publishing MPK_{AS}, AS informs HS to proceed with the next process.

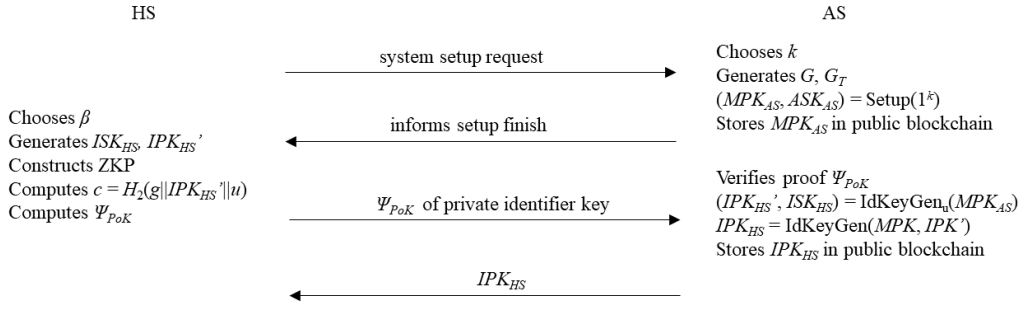

Figure 2. System initialization phase

HS gets MPK, chooses a random number $ISK_{HS}=\beta$, which is an identifier private key, and computes its incomplete public key $IPK_{HS}'=g^{\beta}$. Then, it constructs a zero-knowledge proof (ZKP), $\Psi_{PoK} = <IPK_{HS}', u, \xi>$, of its private identifier key as follows: HS selects $\mu \leftarrow Z_p$ to compute $u = g^{\mu}$, $c = H_2(g||IPK_{HS}'||u)$ and $\xi = \mu - c\beta \ (mod\ p)$. Then, HS sends Ψ_{PoK} to AS. AS verifies the ZKP as follows: AS computes $c = H_2(g||IPK_{HS}'||u)$ and checks if $u = g^{\xi}\cdot(IPK_{HS}')^{c}$. If that passes, AS issues a complete public key $IPK_{HS}=(g^{\beta'})^{\gamma'}$ with a newly selected random number γ'. Then, AS sends the public key back to HS. Figure 2 shows the process.

3.2.2. Registration

[Patient Registration] This process is conducted between the patient and HS. First of all, a patient generates an identifier ID_{PT} and their private identifier key $ISK_{PT} = \lambda = H_2(ID_{PT}||PW_{PT})$ with a password PW_{PT}. Then, he (or she) computes an incomplete public identifier key $IPK_{PT}'=g^{\lambda}$. He (or she) constructs a zero-knowledge proof $\Psi_{PoK\_P} = <IPK_{PT}', U, \xi>$ of his (or her) private identifier key as follows: he (or she) selects $\sigma \leftarrow Z_p^*$ to compute $U=g^{\sigma}$, $c=H_2(g||IPK_{PT}'||U)$ and $\xi=\sigma-c\lambda \ (mod\ p)$. After that, he (or she) sends Ψ_{PoK_P} to HS for registration. After HS receives Ψ_{PoK_P}, HS sends it to AS. AS verifies this proof as follows: it computes $c' = H_2(g||IPK_{PT}'||U)$ and checks if U is equal to $g^{\xi}\cdot(IPK_{PT}')^{c}$. If that passes, AS chooses $l \leftarrow Z_p^*$, computes $IPK_{PT} =(g^{\lambda})^{l}$, stores IPK_{PT} in the public blockchain and sends (IPK_{PT}, IPK_{PT}') to patient via HS.

[Doctors and Nurses Registration] First of all, doctor (or nurse) generates an identifier ID_{DO} and a private identifier key $ISK_{DO} = \varphi = H_2(ID_{DO}||PW_{DO})$ with a password PW_{DO}. Then, he (or she) computes an incomplete public identifier key $IPK_{DO}' = g^{\varphi}$. He (or she) constructs a ZKP $\Psi_{PoK\_D} = <IPK_{DO}', V, r>$ of his (or her) private identifier key and sends it to HS as follows: He (or she)

selects $v \leftarrow Z_p^*$ to compute $V = g^v$, $c = H_2(g||IPK_{DO}'||V)$ and $r = v - c\varphi \ (mod\ p)$. After that, he (or she) sends Ψ_{PoK_D} to HS. HS sends it to AS for verification. AS verifies this proof as follows: it computes $c = H_2(g||IPK_{DO}'||V)$ and checks if V is equal to $g^r \cdot (IPK_{DO}')^c$. If that passes, AS computes $IPK_{DO} = (g^v)^\omega$ with $\omega \leftarrow Z_p^*$, stores IPK_{DO} in the public blockchain and sends (IPK_{DO}, IPK_{DO}') to doctors (or nurses) via HS.

3.2.3. Authentication

Authentication is used between patient and doctor (or nurse) for the rich hospital service except EHR check. HS with blockchain works as a central credential check between two entities.

First of all, patient constructs a ZKP signature Ψ_{PoK_A} on a self-selected random number $r \leftarrow Z_p^*$ and $R = g^r$ and sends this proof with a medical service request to the doctor as follows: Let *req* be the patient's medical service request message and TS_{PT} be a timestamp of patient. Patient encrypts *req* using his (or her) AUK_{PT} (attribute key) as $C_{req} = E_{AUKPT}(req)$. Patient computes $f = H_1(TS_{PT}||C_{req}||R)$, $p_1 = f^r$ and $Z = f^\lambda$ with the secret identifier key λ. Patient computes $c = H_2(f||AUK_{PT}||Z)$ and $y = r + c\lambda \ (mod\ p)$ and sends $\Psi_{PoK\_A} = <IPK_{PT}, Z, y>$ along with $\{TS_{PT}, C_{req}, R, p_1\}$ to the doctor. After doctor receives Ψ_{PoK_A}, doctor sends it for verifying the proof to HS. Then, HS verifies this proof as follows: it computes $f' = H_1(TS_{PT}||C_{req}||R)$ and $c' = H_2(f||AUK_{PT}||Z)$ with the blockchain-stored keys of the patient AUK_{PT} and IPK_{PT}. After that, it checks if the following equation holds $f'^y = p_1 \cdot Z^{c'}$. If the validation check holds, it sends an acknowledgement $Ack \in G$ to doctor. Then, doctor accesses to blockchain which stored AUK_{PT} and patient's medical information. Using AUK_{PT}, doctor checks *req'* by decrypting C_{req} as $req' = D_{AUKDO}(C_{req})$. After confirming the request, doctor generates an appropriate response message *Rep* on the patient's request based on the information stored in blockchain. Finally, doctor sends *Rep* to the patient.

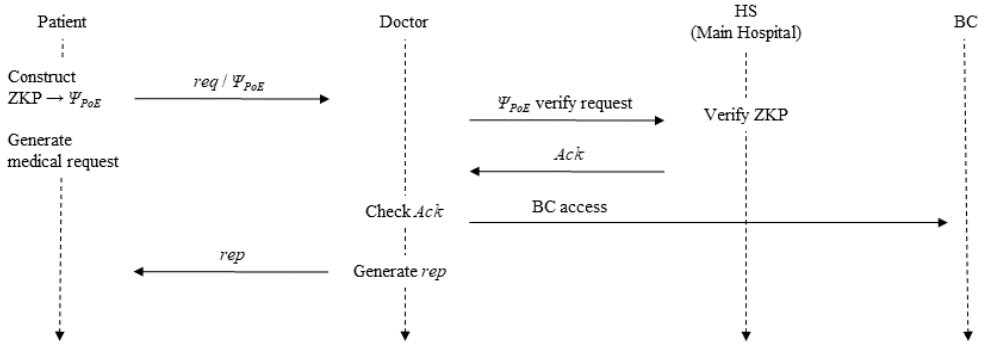

Figure 3. Authentication phase

3.2.4. EHR Generation and Retrieval

Patients should store *EHR* data periodically to blockchain and doctors should check the information. The proposed system uses blockchain to store the patients' *EHR* data. Attribute-based encryption with access control is used to protect patient's data. There should be many required data fields for a patient to present their medical information to doctors. However, we will just simplify the data as *EHR* only for the patient. The patient's *EHR* must be stored in a private blockchain, which should not leak any privacy- related information to anybody without their privilege. For this, the proposed system uses an attribute-based encryption with AUK_{PT}. The patient computes $C_{EHR} = E_{AUKPT}(EHR)$ and stores it in the blockchain. Only the privileged entity with proper attribute key could access the *EHR* but not the others.

Whenever doctor needs to check any patient's medical status in remote environment, he (or she) needs to access the blockchain to reach *EHR* data to check patient's health status, which requires privilege to access the contents of patient's encrypted data C_{EHR}. Doctor uses his (or her) attribute key, AUK_{DO} to decrypt the encrypted data C_{EHR} as $EHR' = D_{AUKDO}(C_{EHR})$.

3.2.5. Cross-Domain Collaboration

In case where collaborative treatment with a doctor from another hospital, which is a cross-domain situation, is required for the patient, it addresses such requirements by coordinating with a collaboration hospital using the cross-domain collaboration phase.

The phase is to give EHR data access rights to the collaboration doctor in different hospital domain from a main hospital doctors via a patient's request. So, main hospital doctor should write a proper request to the collaboration doctor in a different hospital or the same hospital only if any patient's request their healthcare service. If the main hospital sends a verification method with a request for medical cooperation to the collaboration hospital, the collaboration hospital will verify it via HS and approve or refuse the request for medical cooperation as follows: First, doctor (or nurse) of main hospital constructs a ZKP signature Ψ_{PoE} on a self-selected random number $r \leftarrow Z_p^*$ and $R = g^r$ using its secret identifier key and sends it with a medical cooperation request to the doctor of collaboration hospital as follows: Let MD be a main hospital's doctor, CD be a collaboration hospital's doctor and TS_{DO} be a timestamp of MD. MD encrypts *req*, which should clearly be mentioned on the patient's detailed information, data access right clarification by considering the attribute, and the allowed time period of data access, using his (or her) AUK_{MD} *as* $C_{req} = E_{AUKMD}(req)$. MD computes $f = H_1(TS_{DO}||C_{req}||R)$, $p_1 = f^r$ and $Z = f^\lambda$ with the secret identifier key λ. MD computes $c = H_2(f||AUK_{MD}||Z)$ and $y = r + c\lambda \ (mod\ p)$ and sends $\Psi_{PoK\_A} = <IPK_{MD}, Z, y>$ along with $\{TS_{DO}, C_{req}, R, p_1\}$ to CD. Then, CD sends it to HS for the verification and establishes a temporal ACL to access the patient's EHR information. HS verification process is the same as the authentication phase. Only if the verification is successful, HS sets up ACL of CD for the patient's data access right for the proper time periods mentioned in the *req*. CD can access the patient's EHR data freely as the method mentioned in the EHR retrieval phase.

4. IMPLEMENTATION

Instead of utilizing actual systems and physical hardware, this methodology simulates the interaction among diverse components, without necessarily replicating the entire network stack. This creates an entirely controlled and reproducible environment for conducting experiments. As there is no direct reliance on hardware or genuine networks, adjusting the scale of the network by modifying parameters such as the total number of transactions, rate control, virtual machine count, block size, number of rounds, etc., becomes more feasible. Various software platforms are available for assessing Blockchain among which we have employed Hyperledger fabric.

Table 2 shows the requirements and specifications for the functionality implementation of the proposed system. Five numbers of virtual machines have been deployed to put system entities roles in our implementation. They are for HS, AS, patient and two doctors. PBFT is used for the public blockchain consensus and virtual machine 1 works as the authority for the private blockchain.

Table 2. Requirements and specification for the implementation

Requirements	Specification
Operating system	Ubuntu Linux 18.04(64bits)
Virtual machine 1	Ubuntu Linux 18.04(8GB RAM, 64bits)
Virtual machine 2	Ubuntu Linux 18.04(8GB RAM, 64bits)
Virtual machine 3	Ubuntu Linux 18.04(8GB RAM, 64bits)
Virtual machine 4	Ubuntu Linux 18.04(8GB RAM, 64bits)
Virtual machine 5	Ubuntu Linux 18.04(8GB RAM, 64bits)
cURL tool	Version 8.7.1
Javascript	1.8.5
Node JS	Version 16.13.2
NPM	Version 8.1.2
VS code	Version 1.85
Hypherledger fabric	2.0.1

```
func main() {
    http.HandleFunc("/check", checkHandler)
    http.HandleFunc("/register", registerHandler)
    log.Println("[SYS] UCARE KEY server was starting")
    tempfunc()
    log.Fatal(http.ListenAndServe(":9999", nil))
}


func registerKey(id string, key string) {
    keyDatabase[id] = key
    logging("[KEY-SV] Public key was stored. : "+id)
}
```

```
map[dev의 사:-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAi7VjcC+ek9o08u1dqxNY
zWvVdXzD6Iu9FOLq/sf5rM/BSHFn9mgkZx9Ui0LTXCADGb+cdhIS15siM4pnq+mP
bPAgldx7zyzQy6JOOAkZ2tR7/gK7vkWVyL3/9t/JP8+JQ8TOTvCSQSCbnsoWtk0j
1mmE24qLze7+QF/t2o4hEvd+TUBMAIP9oe25sZ3xP3y12NSQJ7z22g//AY485Ysy
QqdqMuD1k2uk3l8xP7VdhJlN4frs8SctASWHsx3foristyxpRyBAQHsjAL5lrKjn
qLYBV9W8tPt0XtFbkgduy08ab6bN16sTym9/z2WbjntdQ3fKrrfRHbqr2RG7XsfO
pQIDAQAB
-----END PUBLIC KEY----- dev환자:-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAy4+BfIl/DlgL/AP+GVq7
k/Iwm0ZqmLokThIVRbTLYtJTacqlhxLF2iqG6Abi7S7MvVSPERsxmYUDMz0gidYD
qjlYnR0SzpqkdflUrQfjCyYT15RI7JtUe+9tDTDohqkOA47s9F4PU/BsTxYfW2Au
pEc+fifWVoCRqxb9inCkzzGHrzt7AQ2gPEYFuucd8JEc3k+ItYPteuOc6iB7rb8Y
tIXdwYlEWq1TKkbpFfcp4POBnlxMrXWH3pwgTL01q/dGaN5eWVCt99b7v5cppKlk
XC59f9Z8LIoV9+WUNpcASBjU2xi8xJfqxdescfX12e2KOGj9pV3ZMf5UetBqQF8+
DQIDAQAB
-----END PUBLIC KEY-----]
```

Figure 4. Parts of AS code

```
function decryptFile(encrypt, origin){
  const key = Buffer.from(sessionkey, 'hex');
  const cipher = crypto
  const input = fs.creat
  const output = fs.crea
  input.pipe(cipher).pip
  output.on('finish', (
    console.log('파일 복
    sessionkey = 'none';
    setTimeout(function(
      fs.unlink(encrypt,
        if (err) {
          console.error(
        } else {
          console.log('파일이 삭제되었습니다:', filePath);
        }
      });
    }, 60*60*1000);
  });

}
```

```
sessionkey = 'none';
setTimeout(function(){
  fs.unlink(encrypt, ()=>{
    if (err) {
      console.error('파일 삭제 중 에러 발생:', err);
    } else {
      console.log('파일이 삭제되었습니다:', filePath);
    }
  });
}, 60*60*1000);
```

Figure 4. Part of EHR generation and retrieval

In this simulation, we tested secure registration via patient's ZKP on the open channel and confirmed blockchain transactions ensuring EHR security through attribute-based encryption. We verified EHR validation through the main doctor (virtual machine 4) and tested the process for

collaborative patient care with the collaborating doctor (virtual machine 5). Throughout these processes, we validated the proper generation of log records for accessing patient EHR-related information. Figures 3 and 4 shows parts of codes for the proposed system.

5. SECURITY AND PERFORMANCE ANALYSIS

The focus of this section is to conduct a thorough analysis of the proposed system, assessing both its security and performance while making appropriate comparisons. We introduce an attack model and security analysis focused on the presence of attacks.

5.1. Security Analysis

This subsection provides security analysis based on the required security features and attacks for the healthcare applications after introducing attack model. Table 3 shows comparisons of security perspectives between related works.

Table 3. Security feature comparison

Feature	[13]	[14]	[15]	[23]	Proposed
Cryptography	Asymmetric	Symmetric & Asymmetric	Asymmetric	Symmetric & Asymmetric	Symmetric & Asymmetric
Authentication	No				
type	Decentralized blockchain based	Decentralized blockchain based	Decentralized blockchain based	Decentralized blockchain based	Decentralized blockchain based
Data sovereignty	No	No	No	No	Yes
Data integrity	Yes	Yes	Yes	Yes	Yes
Non-repudiation	Yes	Yes	Yes	Yes	Yes
Data freshness	Yes	Yes	Yes	Yes	Yes
Attack resistance	Moderate	Strong	Strong	Moderate	Strong

[13] Hammai et al., [14] Khashan & Khafajah, [15] Liu et al., [23] Azbeg et al.

5.1.1. Attack Model

We adopt the Dolev-Yao threat model that has the assumption that the communicating entities are not fully trustworthy and data sharing is performed over insecure public channels [31].

Furthermore, we consider the following powers adversaries have:

- An attacker can control any internet connection between parties.
- There exists a safe stage in a which security module can be computed in the absence of attacks.
- An attacker cannot control all the behavioral models associated with patient’s device.

There is no supplemental knowledge an attacker can obtain from physically accessing network participants, preserving the confidentiality of the system's information.

- The blockchain technology utilized for constructing the public ledger adheres to standard security requirements already established for conventional blockchain applications.
- The cryptographic hash function chosen demonstrates resilience against collision, preimage, and second preimage attacks, ensuring robust security measures.

5.1.2. Data Sovereignty

To access data stored in the proposed system, any entity should have access rights in ACL and could be the classified the accessibility of the data depending on their role in the system, which was defined as an attribute. Furthermore, the main doctor could allow the accessibility to the cross-domain doctor based on the patient's request. In addition to that, the proposed system keeps a log blockchain to keep track the data usage of any patient's data. EHR data are encrypted based on the attribute-based cryptosystem, which could be accessed to someone only has right to access the data. Thereby, the proposed system provide data sovereignty.

To ensure data sovereignty, an analysis of unauthorized data access and safety in data breach scenarios is conducted. An attacker with the power of attack model gains unauthorized access to the remote healthcare application through various means, such as exploiting vulnerabilities in the application's authentication system or stealing login credentials through phishing attacks. Using sophisticated hacking tools, the attacker bypasses any weak encryption or access controls in place, gaining unrestricted access to the medical system. Patients may suffer from identity theft, financial fraud, or discrimination based on their health conditions due to the exposure of their sensitive data. The healthcare provider faces severe reputational damage and legal consequences for failing to protect patient information, leading to a loss of trust among patients and stakeholders. However, the proposed system could cope with these attacks based on the robust authentication and the attribute-based access control. Furthermore, there is no way that the attacker could access to the contents of the encrypted EHR without having the legitimate entity's proper attributes. Furthermore, any access trial for the EHR could be recorded their logs in the log ledger.

5.1.3. Data Confidentiality

By incorporating blockchain into the proposed system, each participating entity can be assigned a unique public key, minimizing the likelihood of collisions. This capability is a significant advantage of blockchain technology, as it eliminates the need for the costly traditional public key infrastructure typically used for key distribution. The public key is accompanied by the attribute key, enabling the simultaneous assurance of confidentiality and access control for EHR. This combination can then be utilized for session key exchange, establishing a secure channel between entities. Furthermore, the proposed security system uses an attribute-based cryptosystem to keep data confidential and all healthcare related data are kept in the private blockchain. Thereby, the proposed system provides data confidentiality.

Potential attack scenario for data confidentiality in the healthcare application is that an attacker gains access to the remote healthcare application through a compromised user account or by exploiting a vulnerability in the application's authentication system. Once inside, the attacker employs various techniques to exfiltrate sensitive patient data stored in the blockchain. However, the proposed system could cope with this trial with authentication mechanism and the attribute-based data encryption applied to the EHR.

5.1.4. Data Integrity and Non-repudiation

Prevention of data modification is ensured by hashing and storing all registration and secret construction transactions in the blockchains. Due to the utilization of tamper-proof blockchain technology in the proposed system, every activity is maintained as immutable transaction records. Furthermore, each transactions are recorded their logs in blockchain. It is impossible for different entities to dispute or alter the activities or messages they have executed or transmitted. Each message is signed using its corresponding attribute private key, which is linked to its public key.

Consequently, the system has the capability to identify it automatically. Moreover, each transaction is signed using the private key and mapped with its identity on the blockchain network. Addition to that, each message should use ZKP, which has the relationship with the entities public key stored in the public blockchain and has the difficulty of discrete logarithm as described in Definition 1. Thereby, the system provide non-repudiation feature.

To compromise the integrity of patient data and undermine the non-repudiation mechanisms, an attacker targets a remote healthcare application, allowing for unauthorized modifications to EHR and denying responsibility for such actions. For that, attacker could apply for exploiting vulnerabilities, data tampering, masquerading as authorized entity and fabricating logs. However, the proposed system uses blcockchain architecture to cope from these attacks.

5.1.5. Data Freshness

The freshness of data guarantees that any received message is current, preventing adversaries from reusing or replaying it. Within this context, the adversary has the capability to replay the intercepted messages on the blockchain in the future, posing a threat of attack. In order to safeguard the system against potential replay attacks, it is necessary to authenticate the freshness of the message by associating it with a specific timeframe. However, blockchain systems encounter difficulties due to a shortage of randomness, making the generation of nonce values a challenging task. Moreover, systems relying solely on a timestamp for verification are exceptionally susceptible to time synchronization attacks. Such vulnerabilities can result in significant security risks, including denial of service attacks. As shown in our proposed system, we combined timestamp with nonce values. When any entity receives a message, it first verifies its ZKP based on them. If the knowledge of proof is not validated, the message is rejected. Consequently, an adversary is unable to replay a past message, ensuring that the message's freshness remains intact at all times.

To compromise the this feature, an attacker targets a remote healthcare application to compromise the freshness of patient data, leading to outdated or inaccurate information being used for medical decision-making and treatment. The attacker could intercepting communication, delaying data transmission, exploiting stale data or manipulating treatment plans. To cope with these trials, the proposed system uses session dependent nonce values in ZKP and timestamp in blockchain.

5.1.6. Sybil Attack Prevention

Sybil attack is a type of security threat in which an individual or group creates multiple nodes, accounts, or devices to take control or exploit a blockchain network. Remember that nodes validate transactions on a blockchain and run consensus. Every registered entity is required to store its public key information in a public blockchain, making it challenging for an attacker to fabricate multiple false identities. Additionally, blockchain employs a strategy of increasing costs to create a new identity, thus demanding a substantial investment to introduce a considerable number of pseudonymous false nodes. Suppose an adversary intercepts a communication message exchanged between entities and proceeds to tamper with the message by inserting malicious code. In the proposed system, ZKP should be verified by the counterpart, which has the difficulty of discrete logarithms in Definition 1. As a result, whether in centralized or decentralized communication scenarios, the data flowing through the network is immune to tampering and safeguarded against diverse attacks.

An attacker conducts a Sybil attack against a remote healthcare application to compromise the integrity of patient data, manipulate medical records, and disrupt healthcare services. There are

attack trials including creation of fake identities, infiltration of patient data and manipulation of EHRs. To mitigate the risk of Sybil attacks, the proposed system uses public key ledger to cope from the fake identities attack, EHR ledger encrypted with the attribute-based encryption for infiltration of patient data and manipulation of EHRs.

5.1.7. Man-in-the-Middle Attacks Prevention

Suppose an adversary is able to eavesdrop on transmitted messages and successfully retrieve the public parameters using a man-in-the-middle attack. In the proposed system, ZKP with nonce and timestamp is independently produced by each entity, and the data are encrypted using an attribute key. Decrypting the ciphertext is the initial step for a node to read a message. The adversary is unable to know the key related information nor nonce, which has a difficulty of discrete logarithm problem. Thus, the proposed system is protected against eavesdropping and man-in-the-middle attacks.

An attacker conducts a man-in-the-middle (MITM) attack against a remote healthcare application to intercept and manipulate sensitive patient data exchanged between the application and its users, such as healthcare providers and patients. They could try to intercept of communication, spoofing legitimate communication, data manipulation, eavesdropping on sensitive information and injection of malicious content. However, the proposed system only exchanges messages for registration and authentication, which is secured based on ZKP. It is infeasible the attacker gain any useful information from the communication. Furthermore, the patient’s health-related information is not communicated over insecure channels but personally stored in the private blockchain directly by the patient.

5.1.8. System-Level Attacks Prevention

System-level attacks target vulnerabilities inherent in the system architecture, including memory modules, system applications, and design flaws, within healthcare systems. Exploiting these vulnerabilities allows attackers to illicitly seize control and access sensitive data. Within the realm of healthcare systems, two primary types of system-level attacks exist: exploits of weak authentication schemes and privilege escalation attacks on healthcare devices.

Weak authentication schemes: Weak authentication refers to a situation where the authentication mechanism's strength is comparatively low in relation to the value of the assets being protected. In a recent research endeavor, researchers examined instances of weak password-based authentication in healthcare devices, with particular emphasis on external and internal defibrillators. Consequently, individuals possessing privileges have the capability to modify or remove the password file and install additional software onto the device. Additionally, researchers conducted reverse engineering of the healthcare authentication system, developing a compact utility to either alter or retrieve a user's password. Hence, the suggested system integrates ZKP alongside a public key cryptosystem to establish robust authentication among entities, thus addressing such potential attacks. Additionally, employing attribute-based access control could afford greater granularity in regulating the usage of patient data.

Privilege escalation attacks: A privilege escalation attack exploits vulnerabilities in the operating system or application, including bugs, design flaws, or configuration errors, to gain unauthorized access to healthcare devices and data normally restricted by permission or authorization protocols. These attacks may be instigated by malicious users, such as patients or physicians, who have legitimate access to healthcare systems and engage in activities like calibration failures or data tampering. By adopting attribute-based access control, the proposed system copes from these attacks simply.

5.2. Performance Analysis

Based on phases and participants, Table 4 depicts comparison of computation overheads between Liu et al.'s scheme and the proposed one because the other three related works are unclearly defined on their operations and also were not focused on the healthcare application nor not using attribute-based access control. For the sake of simplicity and without sacrificing generality, our focus was directed towards computationally intensive operations such as hash operation (H), bilinear map (E), pairing operation (P) and blockchain consensus BC_c. But the other operations were ignored, which are cost-lightened operations.

Table 4. Computation overhead comparison

Phases	Liu et al. in [15]	Proposed
Initialization	AS: (N+1)E	AS: (N+1)E
RS registration	RS:1E+1H+[1E+1H]	HS:1E+1H+[1E+1H]
	AS:[2E+1H]+1E	AS:[2E+1H]+1E
DU registration	DU:1E+1H+[1E+1H]|2E	PT:1E+1H+[1E+1H]|2E
	RS:[2E+1H]+1E+BC_c	HS:[2E+1H]+1E+BC_c
	AS: 3E	AS: 3E
Authentication	DU:[3E+2H]	PT:[1E+1H]
	BC:[4E+2H]+BC_c	BC:[2E+1H]+BC_c
Access control	DU:5E	PT:5E
	DUP:4P	MD:4P
EHR generation	-	PT:1E
		BC:[4E+2H]+BC_c
Collaboration	-	CD:[1E+1H]
		BC:[2E+1H]+BC_c

In comparison to Liu et al.'s scheme, the computational burden during the authentication phase of the proposed system is reduced, as we have streamlined the computational overhead of Zero-Knowledge Proofs (ZKP) more than Liu et al.'s scheme. However, we provide EHR generation and retrieval and cross-domain collaboration.

On the other hand, focusing on the communication overhead. The proposed system requires less size of messages due to now using the proof of equality used in Liu et al.'s scheme. Thereby, the proposed system has better performance than Liu et al.'s scheme. Additionally, the proposed system offers greater functionality compared to other related works, as indicated in Table 3.

Table 5. Storage overhead comparison

Data type	Liu et al. in [15]	Proposed
Attribute key	AS: (N+1)$\|Z_p^*\|$	AS: (N+1)$\|Z_p^*\|$
System key	RS:1$\|Z_p^*\|$	RS:1$\|Z_p^*\|$
UPK	DU:1$\|Z_p^*\|$+4|G|+|UAtS|	DU:1$\|Z_p^*\|$+4|G|+|UAtS|
USK	BC:(N+N_u+N_s)|G|	BC:(N+N_u+N_s)|G|+|Hosp| +|EHR|+|ACL|+|LOG|

N_u-the number of users, N_s-the number of RSs, N_a-the number of attributes in a set
|UAtS|-the cost for storing attribute set, BC-blockchain, DU-data units, |Hosp|-the cost for hospital information
|HER|-the cost for storing EHR, |ACL|-the cost for storing ACL, |LOG|-the cost for storing logs

The storage overhead of the proposed system is detailed in Table 5. In Liu et al.'s scheme and the proposed system, the storage overhead of AS is minimal (N+1)$|Z_p^*|$, while that of BC depends on (N + Nu + Ns)|G|. Similarly, each RS's storage overhead is limited to one its secret key in Z_p^*. Moreover, the storage overhead of DU remains constant regardless of the number of attributes, making it suitable for resource-constrained devices. The storage overhead of the proposed system is similar to Liu et al.'s scheme except additional blockchain overhead, which is |Hosp|+|EHR|+|ACL|+|LOG|. The overhead is related to the healthcare application, which is to provide data sovereignty.

Table 6. Communication overhead comparison

Phases	Liu et al. in [15]	Proposed
Initialization	1D+2|H|+(N+1)|G|+|KDF|	1D+2|H|+(N+1)|G|+|KDF|
RS registration	1$\|\Psi_{PoK}\|$+1|G|+|Txt|	1$\|\Psi_{PoK}\|$+1|G|+|Txt|
DU registration	1$\|\Psi_{PoK}\|$+1|G|+|Txt|	1$\|\Psi_{PoK}\|$+1|G|+|Txt|
Authentication	1$\|\Psi_{PoK}\|$+4|G|+|Txt|	1$\|\Psi_{PoK}\|$+1|G|+|Txt|
EHR generation and retrieval	-	1$\|S_{att}\|$
Cross domain collaboration	-	1$\|\Psi_{PoK}\|$+1|G|+|Txt|

D-a set of (G, G_T, g, p, $e(\cdot)$), |H|-one hash function, |Txt|-communication overhead for a blockchain transaction

Liu et al.'s scheme uses two types of ZKP messages, proof of knowledge (Ψ_{PoK}) and proof of equality (Ψ_{PoE}). Ψ_{PoK} requires one element of G and one element of Z_p^* but Ψ_{PoE} needs three more elements of G than Ψ_{PoK}. Contrast to that the proposed system only requires to use Ψ_{PoK} for both of registration and authentication. The proposed system requires to use EHR generation and retrieval and cross domain collaboration for healthcare application, which is the core parts of the proposed system. EHR generation and retrieval requires one attribute-based encryption or decryption operation S_{att}. Cross domain collaboration requires the same communication overhead as the registration or authentication. Thereby, the communication overhead of the proposed system is lighter than Liu et al.'s scheme as shown in Table 6.

6. CONCLUSIONS AND FUTURE WORK

This paper has proposed a blockchain-enforced attribute-based access control with ZKP for healthcare service. The previous medical systems have a problem that they keep scattered data between hospitals, which is difficult to the patients to keep their data sovereignty. The proposed system employed attribute-based access control, ZKP and blockchain for the healthcare services security provision. Blockchain is used to keep hospital information in public chain but EHR related data with ACL in private chain. Furthermore, EHR provides access control by using the attributed based cryptosystem before they are stored in the blockchain. The envisaged applicability of the proposed system extends to diverse medical systems utilizing private data. In the future, we plan to complete the implementation of the system and add some more security and privacy mechanisms for the further requirements from the medical system.

Personal data treatment is the main security and privacy concern of healthcare applications. Any utilization or handling of personal data must adhere to the regulations outlined in the General Data Protection Regulation (GDPR). Adopted on April 14, 2016, the GDPR officially took effect on May 25, 2018, marking a significant milestone in data protection regulations. Patient data, for the most part, is considered special personal data, and the GDPR prohibits the processing of health information unless specific exceptions specified in Article 9 are met. The data must adhere to the standards outlined by the GDPR to ensure regulatory compliance. The proposed system

aims to attain data sovereignty and privacy but adjustments are required to ensure alignment with GDPR regulations. Moreover, reshaping the proposed system is essential for enhancing both its feasibility and efficiency by using detailed network evaluation based on the Hypherledger Caliper. Ultimately, the development of a system that can guarantee patient data sovereignty and provide security and privacy necessitates integration with real hospital environments.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

ACKNOWLEDGEMENTS

The corresponding author is Hyunsung Kim. Seil Kim collaborated with the authors to put his efforts to collect various resources for the healthcare applications. This research was funded by R&E program funded by Kyungil University and Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2017R1D1A1B04032598).

REFERENCES

[1] Ashok, K. & Gophikrishnan, S. (2024). Q-learning model for blockchain security in Internet of medical things networks. *International Journal of Computer Networks & Communications*, *16*(1), 33-50.

[2] Ryu, H. & Kim, H. (2021). Privacy-Preserving Authentication Protocol for Wireless Body Area Networks in Healthcare Applications. *Healthcare*, *9*, 1114.

[3] Azdad, N., & Elboukhari, M. (2024). A novel medium access control strategy for heterogeneous traffic in wireless body area networks. *International Journal of Computer Networks & Communications*, 16(2), 117-128.

[4] Parihar, A., Prajapati, J. B., Prajapati, B. G., Trambadiya, B., Thakkar, A. & Engineer, P. (2024). Role of IoT in healthcare: Applications, security & privacy concerns. *Intelligent Pharmacy*, In Press, https://doi.org/10.1016/j.ipha.2024.01.003.

[5] Kim, H. (2017). Data centric security and privacy research issues for intelligent Internet of things. *ICSES Interdisciplinary Transactions on Cloud Computing, IoT Big Data*, *1*, 1-2.

[6] Nezhad, M. Z., Bojnordi, A. J. J., Mehraeen, M., Bagheri, R. & Rezazadeh, J. (2024). Securing the future of IoT-healthcare systems: A meta-synthesis of mandatory security requirements. *International Journal of Medical Informatics*, *185*, 105379.

[7] Antolis, K. & Jaksetic, D. (2023). Patients' perception of data security in healthcare. *In Proc. Of 2023 IEEE International Mediterranean Conference on Communications and Networking*, Croatia, https://doi.org/10.1109/MeditCom58224.2023.10266639.

[8] Letafati, M. & Otoum, S. (2024). Digital healthcare in the metaverse: insights into privacy and security. *IEEE Consumer Electronics Magazine*, *13*(3), 80-89.

[9] Khan, A. A., Bourouis, S., Kamruzzaman, M. M., Hadjouni, M., Shaikh, Z. A., Laghari, A. A., Elmannai, H. & Dhahbi, S. (2023). Data security in healthcare industrial Internet of things with blockchain. *IEEE Sensors Journal*, *23*(20), 25144-25151.

[10] Mlato, S., Gabriel, Y., Chirwa, P. & Kim, H. (2024). Multi-server user authentication scheme for privacy preservation with fuzzy commitment. *International Journal of Computer Networks & Communications*, *16*(2), 87-106.

[11] Yao, P., Yan, B., Yang, T., Wang, Y., Yang, Q. & Wang W. (2024). Security-enhanced operational architecture for decentralized industrial Internet of things: a blockchain-based approach. *IEEE Internet of Things Journal*, *11*(6), 11073-11086.

[12] Chu, Y., Kim, S., Song, Y., Yoon, Y. & Jin, Y. (2024). Blockchain-based REC system for improving the aspects of procedural complexity and cyber security. *IEEE Access*, *12*, 40657-40667.

[13] Hammi, M. T., Hammi, B., Bellot, P. & Serhrouchni, A. (2018). Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. *Computers & Security*, *78*, 126–142.

[14] Khashan, O. A. & Khafajah, N. M. (2023). Efficient hybrid centralized and blockchain-based authentication architecture for heterogeneous IoT systems. *Journal of King Saud University-Computer and Information Sciences*, *35*, 726-739

[15] Liu, S., Chen, L., Yu, H., Gao, S. & Fang, H. (2023). BP-AKAA: Blockchain-enforced privacy-preserving authentication and key agreement and access control for IIoT. *Journal of Information Security and Applications*, *73*, 103443.

[16] Wang, K., Xie, S. & Rodrigues, J. (2022). Medical data security of wearable tele-rehabilitation under Internet of things. *Internet of Things and Cyber-Physical Systems*, *2*, 1-11.

[17] Kim, H. (2019). Research issues on data centric security and privacy model for intelligent Internet of things based healthcare. *ICSES Transactions on Computer Networks and Communications*, *5*(2), 1-3.

[18] Sharma, P., Borah, M. D. & Namasudra, S. (2021). Improving security of medical big data by using blockchain technology. *Computers & Electrical Engineering*, *96*, 107529.

[19] Semantha, F. H., Azam, S., Shanmugam, B., Yeo, K. C. & Beeravolu, A. R. (2021). A conceptual framework to ensure privacy in patient record management system. *IEEE Access*, *9*, 21506669.

[20] Butpheng, C., Yeh, K. H. & Xiong, H. (2020). Security and privacy in IoT-cloud-based e-health systems-a comprehensive review. *Symmetry*, *12*(7), 1191.

[21] Amato, F., Casola, V., Cozzolino, G., Benedictis, A. D., Mazzocca, N. & Moscato, F. (2021). A security and privacy validation methodology for e-health systems. *ACM Transactions on Multimedia Computing, Communications, and Applications*, *17*(2s), Article No. 67, 1-22.

[22] Chen, Y., Meng, L., Zhou, H. & Xue, G. (2021). A blockchain-based medical data sharing mechanism with attribute-based access control and privacy protection. *Wireless Communications and Mobile Computing*, *2021*, 6685762.

[23] Azbeg, K., Ouchetto, O. & Andaloussi, S. J. (2022). BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security. *Egyptian Informatics Journal*, *23*, 329-343.

[24] Lohmoller, J., Pennekamp, J., Matzutt, R., Schneider, C. V., Vald, E., Trautwein, C. & Wehrle, K. (2024). The unresolved need for dependable guarantees on security, sovereignty, and trust in data ecosystems. *Data & Knowledge Engineering*, *151*, 102301.

[25] Mackey, T. K., Calac, A. J., Keshava, B. S. C., Yracheta, J., Tsosie, K. S. & Fox, K. (2022). Establishing a blockchain-enabled indigenous data sovereignty framework for genomic data. *Cell*, *185*(15), 2626-2631.

[26] Wang, Q. & Liu, Y. (2023). Blockchain for public safety: a survey of techniques and applications. *Journal of Safety Science and Resilience*, *4*(4), 389-395.

[27] Jena, S. K., Kumar, B., Mohanty, B., Singhal, A. & Barik, R. C. (2024). An advanced blockchain-based Hyperledger fabric solution for tracing fraudulent claims in the healthcare industry. *Decision Analytics Journal*, *10*, 100411.

[28] Goldwasser, S., Micali, S. & Rackoff, C. (1985). The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, *18*(1), 186-208.

[29] Waters, B. (2011). Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. *In Proc. of International Workshop on Public Key Cryptography*, 53-70.

[30] Hu, V. C., Ferraiolo, D., Kuhn, R., Friedman, A. R., Lang, A. J., Cogdell, M. M., Schnitzer, A., Sandlin, K., Miller, R. & Scarfone, K. (2013). Guide to Attribute Based Access Control (ABAC) Definition and Considerations (Draft). *NIST Special Publication*, 800-162.

[31] Dolev, Y. & Yao, A. (1983). On the security of public key protocol. *IEEE Transactions on Information Theory*, *29*(2), 198-208.

AUTHORS

Dongju Lee is B.E. degree student in Computer Science at Kyungil University, Korea. He has been a member of Information Security Laboratory in Kyungil University from 2023. He has been a research member of "Research on Data Centric Security and Privacy Model for Intelligent Internet of Things" project funded by National Research Foundation of Korea. His research interests are in Cryptography, Information Security, Cryptographic Protocol, Privacy, Internet of Things, Blockchain and Cryptanalysis.

Hyunsung Kim received the M.Sc. and Ph.D. degrees in computer engineering from Kyungpook National University, Korea, in 1998 and 2002, respectively. He is a Professor at the School of Computer Science, Kyungil University, Korea from 2012. Furthermore, he is currently a visiting professor at the Department of Mathematical Sciences, Chancellor College, University of Malawi, Malawi from 2015. He also was a visiting researcher at Dublin City University in 2009. From 2000 to 2002, he worked as a senior researcher at Ditto Technology. He had been an associate professor from 2002 to 2012 with the Department of Computer Engineering, Kyungil University. His research interests include cryptography, VLSI, authentication technologies, network security, ubiquitous computing security, blockchain, and security protocol.