Received: 29 August 2022 | Revised: 22 September 2022 | Accepted: 25 September 2022
DOI: 10.37917/ijeee.19.1.8 Vol. 19| Issue 1| June 2023

Open Access

Iraqi Journal for Electrical and Electronic Engineering
Original Article

Secure Electronic Healthcare Record based on Distributed Global Database and Schnorr Signcryption

Mohammad Fareed *[1, 2], Ali A Yassin [1]
[1]Department of Computer Science, Education College for Pure Science, University of Basrah Basrah 61004, Iraq
[2]Communication Media and Commission

Correspondence
*Mohammad Fareed
Department of Computer Science
Education College for Pure Science,
University of Basrah, Basrah, 61004, Iraq.
Email: pedupg.m.fareed@uobasrah.edu.iq

Abstract
Preserving privacy and security plays a key role in allowing each component in the healthcare system to access control and gain privileges for services and resources. Over recent years, there have been several role-based access control and authentication schemes, but we noticed some drawbacks in target schemes such as failing to resist well-known attacks, leaking privacy-related information, and operational cost. To defeat the weakness, this paper proposes a secure electronic healthcare record scheme based on Schnorr Signcryption, crypto hash function, and Distributed Global Database (DGDB) for the healthcare system. Based on security theories and the Canetti-Krawczyk model (CK), we notice that the proposed scheme has suitable matrices such as scalability, privacy preservation, and mutual authentication. Furthermore, findings from comparisons with comparable schemes reveal that the suggested approach provides greater privacy and security characteristics than the other schemes and has enough efficiency in computational and communicational aspects.

KEYWORDS: Authentication, Schnorr Signcryption, Healthcare system, DGDB, CK model.

I. INTRODUCTION

Healthcare data are critical and sensitive in our lives. Health records of patients were stored on paper in the past, making them more susceptible to damage and difficult to retrieve information. Subsequently, electronic storage of healthcare data was necessary to reduce the hurdles between various healthcare providers in terms of data exchange and protection. With the rapid increase in information technology and the Internet used in the current era, it has become necessary to transform healthcare records from traditional to electronic to adapt to modern life. The advanced age of electronic health records (EHR) leads to access to vast data inside EHR. Such an increase in EHR requires matchless data protection in healthcare. However, the health data must be stored securely and shared only with authorized parties. In some systems, centralization saves all data on the same server. This mechanism is not secure because the server keeps the data and faces security risks and malicious attacks. On the other side, we see the decentralized method to save data in shared servers because it is more secure, safe to exchange and upgrade data, and suitable for massive data. Here, we will focus on patients' privacy, secure exchange, and retrieving data of EHR among authorized and trusted parties. For example, the accuracy of diagnosing a patient's case by a specialized doctor depends on the retrieved EHR. In addition, some of the methods used in data sharing through decentralization, in terms of data encryption or accuracy, are not considered sufficient to maintain patients' privacy. Therefore, developing a secure data sharing and distribution mechanism has become necessary through Distributed Global Database (DGDB).

This paper proposes a secure scheme based on DGDB for securely exchanging health data while preserving its privacy against recognized malicious attacks by using decentralized data storage. The contributions of this research can be summarized as follows:

1- We propose a DGDB-based authentication scheme. The proposed mechanism provides a powerful distributed data storage between health care centers and secures data exchange by encrypting transmitted data used by the Key Distribution Center(KDC).

2- Officially, we confirm the system's security using the security analysis tool Scyther Tool.

3- Similar systems are compared in the comparison table to prove the proposed system's efficiency.

The rest of the paper is structured as follows: Section two discusses the latest related work. Section three presents the primitive tools, while the section four refers to the proposed scheme. Section five focuses on security analysis. Finally, section six concludes this paper. Fig.1. shows the proposed decentralization model.

II. Related Works

Decentralized technology can robustly and effectively solve complicated issues like securing healthcare data, transactions, and storage. In addition, this technique enables an encrypted method for healthcare data [1]. This paper comprises a state-of-the-art and the most recent study of applying related work decentralized mechanism for preserving privacy in the healthcare models. In 2019, Mubarakali et al. [2] used blockchain technology to make practical and secure transactions for health records. The authors used to ensure that everyone who had access to the data did so privately. Their study focuses on Blockchain technologies that have been used over time to stay in touch with the healthcare industry. In the quest for the healthcare field, the people were far more willing to access and exchange their data safely through cloud technology without putting their privacy at risk. This work also found a quick and easy way to keep the patients' private information saved in the intellectual health care system. Their work builds the system in a way that does not compromise privacy; a trusted third party does the computing of patient data. Omar et al. [3] increased the emerging interest in healthy data in the cloud due to malicious attackers. The healthcare centers have suffered severe consequences from the attacks on health data; the effect of attacks has decreased with the decentralization of the cloud's data. Confidential health data is computed, managed, and processed by decentralized data of the peer-to-peer (P2P) system. Blockchain technology depends on main features such as decentralized, shared properties, secured exchanged data. Although the malicious attack impacts have been controlled by proposing diverse solutions based on a decentralized approach, these solutions have failed to ensure the complete privacy of patient-centric systems. Consequently, there paper refers to create healthcare framework to manage data of patient using the blockchain technology. This method used cryptographic tools for encrypting medical data.

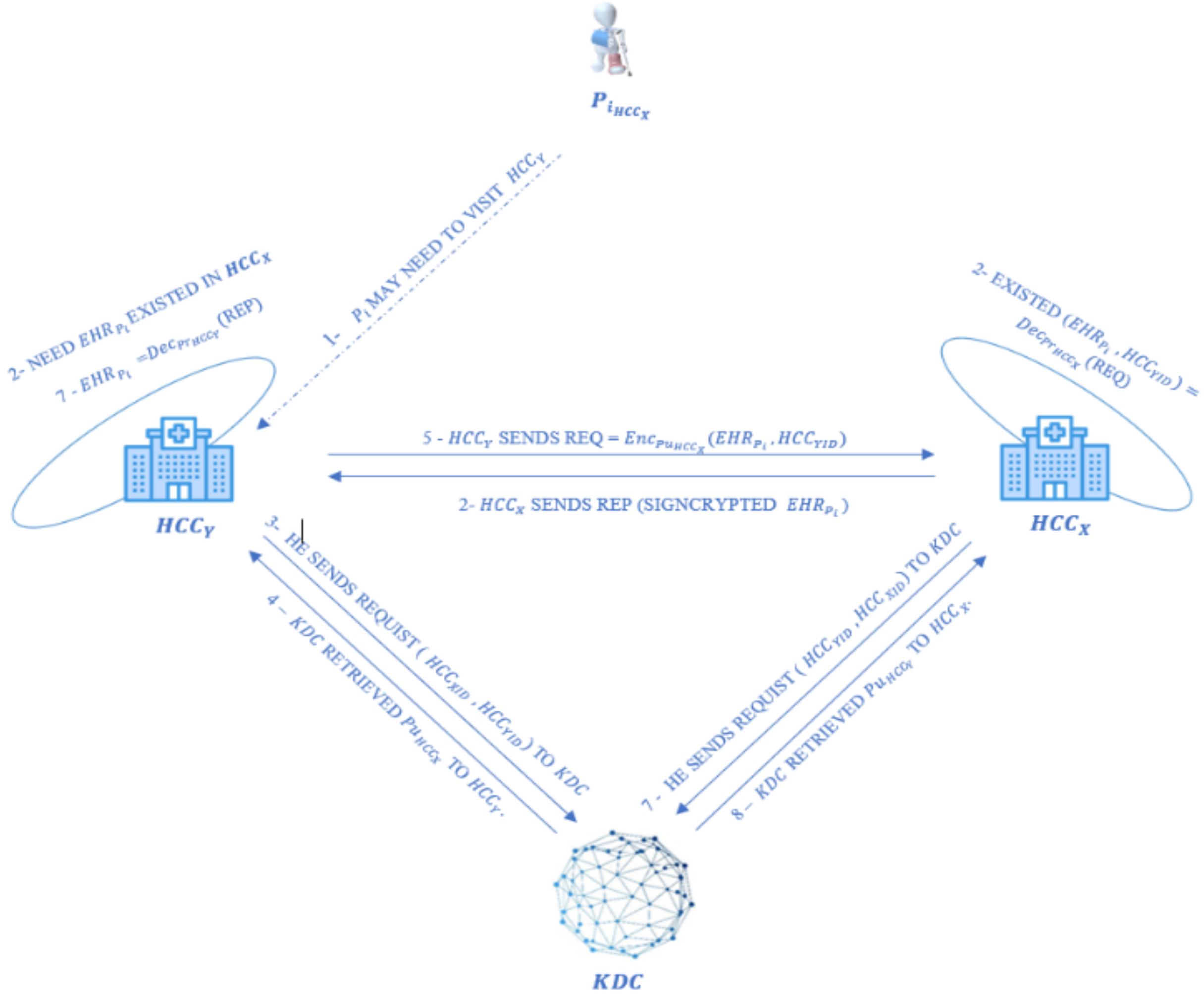
$P_{i_{HCC_X}}$
1- P_i MAY NEED TO VISIT HCC_Y
2- NEED EHR_{P_i} EXISTED IN HCC_X
7 - EHR_{P_i} $=Dec_{Pr_{HCC_Y}}$ (REP)
2- EXISTED (EHR_{P_i} , HCC_{YID}) = $Dec_{Pr_{HCC_X}}$ (REQ)
5 - HCC_Y SENDS REQ = $Enc_{Pu_{HCC_X}}(EHR_{P_i}, HCC_{YID})$
2- HCC_X SENDS REP (SIGNCRYPTED EHR_{P_i})
HCC_Y
HCC_X
3- HE SENDS REQUIST (HCC_{XID} , HCC_{YID}) TO KDC
4 – KDC RETRIEVED Pu_{HCC_X} TO HCC_Y.
7 - HE SENDS REQUIST (HCC_{YID} , HCC_{XID}) TO KDC
8 – KDC RETRIEVED Pu_{HCC_Y} TO HCC_X.
KDC

Fig.1. Proposed decentralization model

Additionally, Nguyen et al. [4] recommended a narrative framework used to transferred data of EHRs via a mobile cloud server relied on blockchain and a shared data. Blockchain technology has been used in the past to establish a system for managing safe access to EHRs for patients and health care professionals. In addition, the Ethereum blockchain was used in a specialized data exchange function with Amazon cloud computing to propose a hypothetical smartphone implementation. According to the research's conclusions, virtual clouds may be used effectively to safely transfer sensitive health data to prevent future attacks. Moreover, lightweight network access architectures are more efficient through security research and device optimization. In 2020, Islam and Shin [5] un-crewed aerial vehicles and the nearest storage portal were used to providing consumers with health data (HD) in a blockchain-based, secure healthcare system (UAV). The UAV initially created a partnership with the body sensor hives (BSH) using a token and a transfer key for small-power, safe communication. After extracting the HD, the UAV uses a two-phase authentication mechanism to decode the encrypted HD (BSH authenticated). The UAV sends the HD to the nearest server for long-term storage upon successful certification. A protection evaluation was conducted to exhibit the feasibility of the healthcare system that are used currently. Analysis and implementation were subsequently used to evaluate the overall performance of the conceptual design. As a result, the new approach encourages more extensive BSH aid and maintains stability according to the evaluation of protection and efficiency. In 2019, Tripathi et al. [6] reported the healthcare industry had been one of the most popular uses of the Internet of Things (IoT) and its applications. However, widespread use was not easy to accomplish, primarily due to the individuals involved and the need to ensure the privacy and security of the information. Blockchain technology has emerged to address this issue as a realistic means of improving data security.

However, their method suffers from several issues and concerns relating to data and user solidity, availability, and secrecy that must be addressed. Studies of the conventional approach, expert views, and customer expectations were explored concerning technical and social barriers to SHS implementation. In the SHS platform based on blockchain was established to retain the system's inherent security and legality. Finally, we have explored the many research paths and applications for blockchain in healthcare. In 2018, Almadhoun et al. [7] suggested a large-scale, blockchain-based secure system for IoT nodes and provided an architecture that ensures end-users secure data exchange. In 2020, Zhihua et al. [8] offered a new alternative for dispersed IoT systems through decentralized blockchain technology. In 2021, Hasan et al. [9] proposed that electronic healthcare records are advantageous over handwritten documents. Still, they also have several drawbacks, including security, privacy, and the general shift of patient data from a central database to a decentralized database. In this paper, we propose secure scheme overcome the weaknesses and security issues above mentioned and we refer to main comparison with related work in Table 2.

III. Primitive Tools

A. Schnorr Signcryption

- Initialization

p = prime number (large), public variable.

q = a prime factor of $p - 1$(large), public variable.

g = integer number with order $q \; mod \; p$, in [1,.., $p - 1$], public variable.

$hash$ = a hash function

KH = a one-way hash function key = $KHk(m) = hash(k, m)$

(E, D) = algorithms used to encrypt and decrypt a private key.

- Keygen sender

The pair of keys (X_a, Y_a):

X_a = sender private key, randomly from [1, .., q-1].

Y_a = sender public key =g^{-X_a} mod p

- Keygen receiver

The pair of keys (X_b, Y_b):

X_b = receiver private key, chosen randomly [1,.., q-1]

Y_b = receiver public key = $g^{-X_b} \; mod \; p.$

- Signcryption

Signcrypt a message m to receiver of the following operations:

$k \; = \; hash({Y_b}^X) \; mod \; p.$

Split k in $k1$ and $k2$ of appropriate length.

Calculate $r \; = \; KH_{k2}(\, m) \; = \; hash(h2, m)$

Calculate $s \; = \; x + (r * X_a) \; mod \; q$

Calculate $c \; = \; E_{k1} \; (m)$ = the encryption of m with the key $k1$.

Sender sends to receiver the values (r, s, c).

- Usigncryption

Unsigncrypt m from sender, receiver has does the following operations:

Calculate $k \; using \; r, s, g, p, Ya \; and \; Xb$, $hash(g^s . {Y_a}^r)^{-X_b} mod \; p)$

Split k in $k1$ and $k2$ of appropriate length.

Calculate m using the decrypt algorithm $m \; = \; D_{k1}(c)$.

Accept m is a valid message only if $KH_{k2}(m) \; = \; r$.

B. SHA-256 hash function:

The SHA-256 created by the National Security Agency is a variation of this algorithm (NSA). In addition, popular encryption protocols like SSL, TLS, and SSH and open-source operating systems like Unix/Linux all make use of SHA-256 [11].

The hash algorithm is incredibly secure, and its workings are unknown to the general public. However, due to the usage of digital signatures, it is utilized by the United States government to ensure that sensitive information is protected. In addition, it is used to validate passwords since the hash values may be saved and compared to the user input to check whether it is correct or not, which eliminates the need to record specific passwords.

A hash value is practically impossible to decipher since the original data is so difficult to find. In addition, the sheer amount of possible combinations makes a brute force approach impossible. Because of this, it is quite difficult to come up with two data items (known as collisions) that have the same hash. Any text is signed using an SHA-256, and the output is 256 bits long.

C. CK threat model:

With the Canetti-Krawczyk model (CK), we can formally develop and analyze the proposed scheme. The proposed system should have many essential security properties [12].

In this paper, we used the following features:

- Scalability.
- Privacy preservation.
- Mutual authentication
- Attack resistance.
- Communication security.
- Secure $DGDB$.

IV. The Proposal Scheme

The EHR is controlled by health centers instead of the patients, making it difficult to obtain medical advice from different health centers. Thus, patients need to concentrate on getting their health information and medical records back in order. The development of distributed global database technology (DGDB) has made it easier for people to obtain information within medical records. The technology offers patients access to extensive, consistent reports, with free access to EHRs from treatment websites or mobile applications. We will report how we built a security framework for EHRs with multiple authorities to meet the need for DGDB in shared EHRs. This method protects patients' privacy and ensures that EHRs remain unchanged.

This section proposes a secure $DGDB$ authentication scheme in a healthcare system consisting of two components; healthcare center (HCC_i) and key distribution center (KDC). Table I contains the necessary symbols used in this paper. Additionally, our work depends on the initialization phase, registration phase, and the $DGDB$ phase. The initialization phase employs KDC to generate and exchange private and public keys, which use signing/verifying and encrypting/decrypting among the main components of the EHRs message. The registration phase registers a new HCC_i, which generates the primary keys for the HCC_i. The $DGDB$ phase is responsible for exchanging, authenticating, and verifying the EHR of the system's components. These main phases are explained in detail below.

TABLE I
NOTATIONS.

Notation	Descriptions
HCC	Healthcare centers
$DGDB$	Distributed Global Database
EHR_{P_i}	The patient's electronic health record
P_i	patient
KDC	Key Distribution Center
Pu_{HCC_i}	The public key of the health center
Pr_{HCC_i}	The private key of the health center
$SENC(.)$	Signcryption function
$USENC(.)$	Usigncryption function
$\oplus$	Exclusive-Or
$\|$	Concatenation

A. Initialization Phase

Step 1. In the initialization phase, the KDC creates a table containing all public keys for the HCC_i.

Step 2. Key Initialization

- p = a large prime number, public to all
- q = a large prime factor of $p-1$, public to all
- g = an integer with order q $modulo$ p, in [1,… , $p-1$], public to all
- $hash$ = a one-way hash function
- KH = a keyed one-way hash function = $KHk(m) = hash(k, m)$
- (E, D) = the algorithms which are used for encryption and decryption of a private key cipher. Alice sends a message to Bob.

B. Registration Phase

The HCC_i achieves registration in the system through the following steps:

Step1. The HCC_i registers its information in the system (e.g. Healthcare center name (HCC_{HN_i}), Address (AD_i), Phone No. (PN_i), Email (EM_i).

Step2. HCC_i Initializes the database to save the patient's EHR.

Step3. Public and private keys are generated (Pr_{HCC_i}, Pu_{HCC_i}) for the signing/encrypting (signcryption) data from the HCC_i as shown below:

- $Pr_{HCC_i} = X_a$; where X_a is a private key of HCC_i, chosen randomly from 1 to $q-1$.
- $Pu_{HCC_i} = Y_a ==g^{-X_a}$ mod p; it represents the public key of HCC_i.

Step 4. Finally, HCC_i sends (Pu_{HCC_i},HCC_{HN_i}) to the KDC.

C. Distributed Global Database (**DGDB**) Phase

In this phase, we give details regarding the patient's need to visit a healthcare center that is different from their primary center; the patient's EHR is included. The following steps describe the primary tasks of this phase:

Step 1. EHR_{P_i} is stored in the HCC_X.

Step 2. P_i needs to visit a specific healthcare center that is not his primary healthcare center.

Step 3. There is a HCC_Y that is near P_i.

Step 4. P_i needs to visit the nearby HCC_Y.

Step 5. HCC_Y requires the EHR_{P_i} from the HCC_X.

Step 6. HCC_Y calculates $R_{HCC_X} = (HCC_{XID})$ and sends it to KDC to receive the public key for HCC_X.

Step 7. KDC receives R_{HCC_X} to retrieve the Pu_{HCC_X} and calculate $HPu_{HCC_X} = hash(Pu_{HCC_X})$.

Step 8. KDC sends (Pu_{HCC_X}, HPu_{HCC_X}) to HCC_Y.

Step 9. HCC_Y receives (Pu_{HCC_X}, HPu_{HCC_X}) and calculate $H'Pu_{HCC_X} = hash(Pu_{HCC_X})$.

Step10. HCC_Y compares ($H'Pu_{HCC_X}$, HPu_{HCC_X}) if true, then computes $Q = SENC_{Pu_{HCC_X}}(\text{query}_{P_i})$ then go to Step 12.

Step11. Otherwise terminate this phase.

Step12. HCC_Y sends Q to HCC_X to receive EHR_{P_i} .

Step13. HCC_X receives and decrypts Q based on $USENC_{Pr_{HCC_X}}(Q)$ and finds the EHR_{P_i} on the local database;

if a match is found, it then calculates $R_{\ HCC_Y} = (HCC_{YID})$ and sends it to KDC.

Step14. KDC receives the $R_{\ HCC_Y}$ to retrieve the Pu_{HCC_Y}, and calculate $HPu_{HCC_Y} = hash(Pu_{HCC_Y})$.

Step15. HCC_X receives $(Pu_{HCC_Y}, HPu_{HCC_Y})$ and calculate $H'Pu_{HCC_Y} = hash(Pu_{HCC_Y})$.

Step16. HCC_X compares $(H'Pu_{HCC_Y}, HPu_{HCC_Y})$ if so, then computes $REP\_EHR_{\ P_i} = SENC_{Pu_{HCC_Y}}(EHR_{P_i})$ then go to next step, otherwise terminate this phase.

Step 17. HCC_X sends $REP\_EHR_{\ P_i}$ to HCC_Y.

Step 18. HCC_Y receives $REP\_EHR_{\ P_i}$ and decrypts based on EHR_{P_i} $=USENC_{Pr_{HCC_Y}}(REP\_EHR_{\ P_i})$.

Step13. HCC_Y updates EHR_{P_i} and sends $U\_EHR_{\ P_i} = SENC_{Pu_{HCC_X}}(EHR_{P_i})$ to HCC_X.

Step14. HCC_X decrypts and saves $EHR_{P_i} = USENC_{Pr_{HCC_X}}(U\_EHR_{\ P_i})$ to their local database. Fig.2. shows the DGDB authentication.

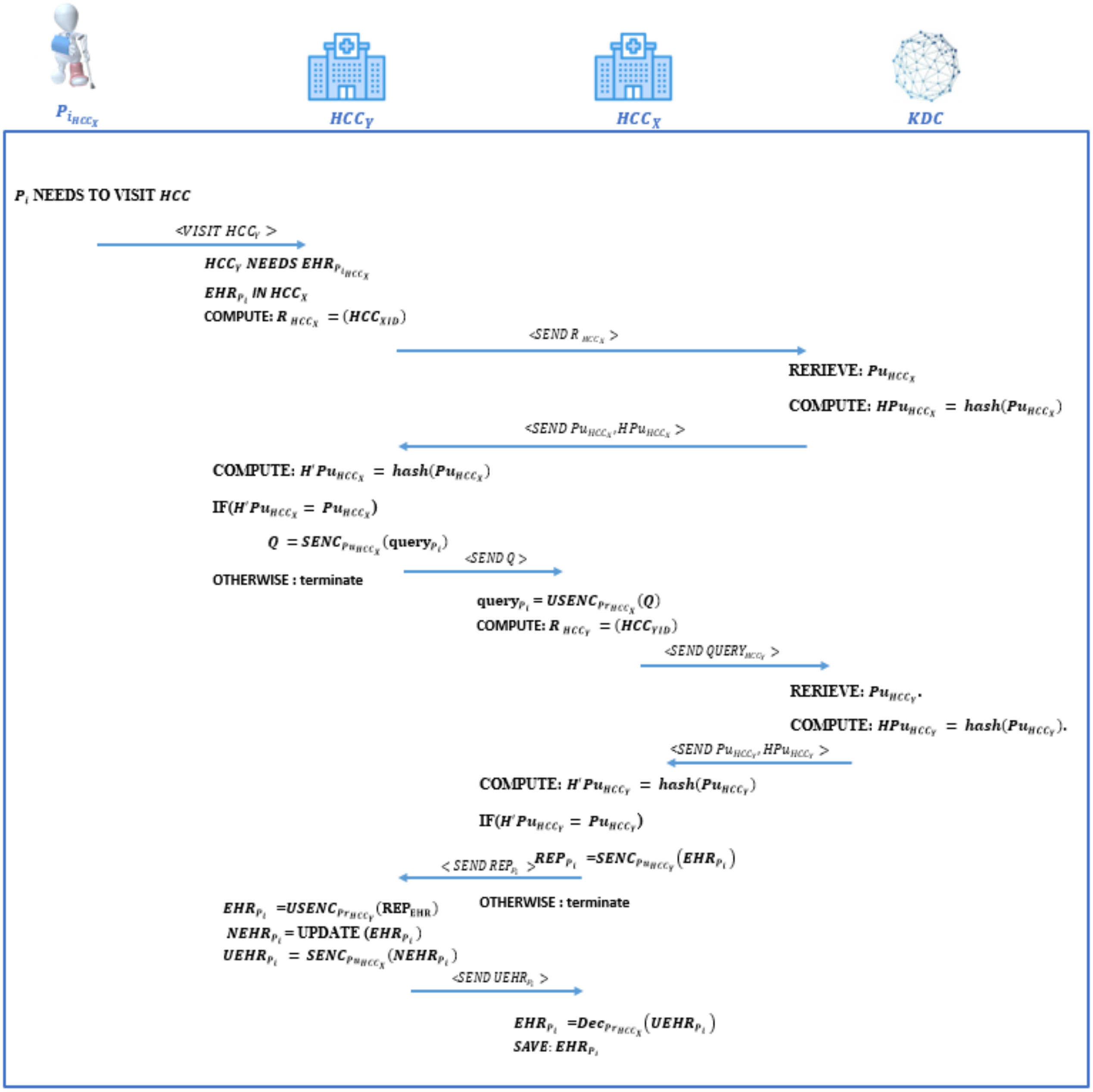
$P_{i_{HCC_X}}$
HCC_Y
HCC_X
KDC
P_i NEEDS TO VISIT HCC
<VISIT HCC_Y >
HCC_Y NEEDS $EHR_{P_{i_{HCC_X}}}$
EHR_{P_i} IN HCC_X
COMPUTE: $R_{\ HCC_X} = (HCC_{XID})$
<SEND $R_{\ HCC_X}$ >
RERIEVE: Pu_{HCC_X}
COMPUTE: $HPu_{HCC_X} = hash(Pu_{HCC_X})$
<SEND Pu_{HCC_X}, HPu_{HCC_X} >
COMPUTE: $H'Pu_{HCC_X} = hash(Pu_{HCC_X})$
IF($H'Pu_{HCC_X} = Pu_{HCC_X}$)
$Q = SENC_{Pu_{HCC_X}}(\text{query}_{P_i})$
<SEND Q >
OTHERWISE : terminate
$\text{query}_{P_i} = USENC_{Pr_{HCC_X}}(Q)$
COMPUTE: $R_{\ HCC_Y} = (HCC_{YID})$
<SEND $QUERY_{HCC_Y}$ >
RERIEVE: Pu_{HCC_Y}.
COMPUTE: $HPu_{HCC_Y} = hash(Pu_{HCC_Y})$.
<SEND Pu_{HCC_Y}, HPu_{HCC_Y} >
COMPUTE: $H'Pu_{HCC_Y} = hash(Pu_{HCC_Y})$
IF($H'Pu_{HCC_Y} = Pu_{HCC_Y}$)
< SEND REP_{P_i} >
$REP_{P_i} = SENC_{Pu_{HCC_Y}}(EHR_{P_i})$
OTHERWISE : terminate
$EHR_{P_i} = USENC_{Pr_{HCC_Y}}(REP_{EHR})$
$NEHR_{P_i} = \text{UPDATE}\ (EHR_{P_i})$
$UEHR_{P_i} = SENC_{Pu_{HCC_X}}(NEHR_{P_i})$
<SEND $UEHR_{P_i}$ >
$EHR_{P_i} = Dec_{Pr_{HCC_X}}(UEHR_{P_i})$
SAVE: EHR_{P_i}

Fig. 2. DGDB Authentication

V. Security Analysis

This section uses the CK thread model to analyze the proposed system security [13-18]. Then, we show how the proposed protocol improves privacy and security compared to the related works.

There are types of security considerations that must be considered while designing a secure system. Therefore, a particular function was used to assess the solution against other available decentralized options. Results of the comparison are reported in Table II; furthermore, it can be seen from the Table of benefits that our system provides identity anonymity and authentication and superior privacy protection and communication security.

- **Scalability**: Decentralized authentication requires scalability as one of the most important security features. Due to the time delay characteristics of decentralized authentication, considerable resources and time are consumed if $HCCs$ complete patient authentication through transactions. In the system designed in this paper, $HCCs$ only needs to complete the corresponding public keys on the KDC during the healthcare phase, then search the keys on the KDC to complete the identity authentication. For scalability requirements, this solution can be well adapted.
- **Privacy preservation:** Basic privacy protection refers to preserving data stored in $HCCs$. Since all data stored is encrypted, an attacker is unable to read it when he accesses the system. Therefore, only public keys for $HCCs$ are stored, in addition to the keys in the KDC.
- **Communication security:** The data transmitted through the communication media is secure, because when the HCC_X sends a request to the KDC, the encrypted data is under the $KDC's$ public key. Additionally, when the HCC_X sends data to another HCC, it encrypts the data with the public key of the receiving center.
- **Mutual authentication:** HCC_X is authenticated by HCC_Y based on Pu_{HCC} , Pr_{HCC} and crypto-hash function, which is a message from $HCC_X\ to\ HCC_Y$ vice versa. The HCC_X in the proposed system could authenticate only the legal HCC_Y because an adversary would need to use the private key (Pr_{HCC_Y}), then the received information is decrypted based on [EHR_{P_i} = $Dec_{Pr_{HCC_Y}}$(REQ_EHR)]; if it is identical, then HCC_Y is a trusted party. HCC_Y , after updating the received EHR_{P_i} requests the Pu_{HCC_X} from KDC and resends $NEWEHR_{P_i}\ =\ ENC_{Pu_{HCC_X}}$(UPDATE ($EHR_{P_i}$)) to HCC_X . HCC_X received and computed $NEHR_{P_i}$ = $Dec_{Pr_{HCC_X}}$(U_EHR) if the result is actual, then HCC_X can now be considered a trusted party.
- **Secure $\boldsymbol{DGDB}$:** Decentralized data storage, as patients' $EHRs$ are stored only in the HCC where they are registered. Furthermore, all parties through which data is exchanged are reliable, as explained in the mutual authentication, resulting in speed and security in response and privacy preservation.
- **Attack resistance**: We could argue that any attack is positive if an adversary locates any technique to run several malicious attacks, such as impersonation, Man-In-The-Middle (MITM), and insider attacks [20]. Most of all, an impersonation attack has a direct relationship with mutual authentication; the adversary needs a private key (Pr_{HCC}), then the decrypted based on [EHR_{P_i} = $Dec_{Pr_{HCC}}$(REQ_EHR)]. So, the proposed system could prevent impersonation attacks. Additionally, the MITM attack works in the same manner as active eavesdropping; when the HCC_X sends data to another HCC, it encrypts the data with the public key of the receiving center. Therefore, our proposed system resists MITM, dictionary, impersonate, sniffing, hijacking, and eavesdropping attacks because an adversary cannot access any benefits from exchanged parameters between $HCC_X\ and\ HCC_Y$.

TABLE II
PRIVACY AND SECURITY FEATURE COMPARISON.

-	[18]	[19]	[7]	[8]	[20]	Proposed
Mutual authentication	O	O	O	O	O	O
Privacy preservation	O	O	X	X	X	O
Scalability	-	-	O	O	O	O
Communication security	O	O	O	O	O	O
Secure $DGDB$	X	X	X	X	X	O
Attack resistance	X	X	X	X	X	O

VI. Performance Evaluation

- Computation Result

There are three phases in the proposed protocol: The initialization phase, registration phase, and $DGDB$ phase. With the proposed protocol, we will focus on the calculation needs of the DGDB phase, since this is the most commonly utilized phase. To facilitate computation analysis, we define the computational requirements of a Schnorr Signcryption T_{SENC}, Schnorr verification T_{USENC}, respectively, and a one-way hash function as T_h, but do not consider the overhead of the exclusive-or operations as $\boldsymbol{T_\oplus}$ which requires a comparatively relatively low overhead than any other operations [21]. Table IV shows the computational overhead based on Table III.

TABLE III
COMPUTATION COST RESULT.

Operation	General Meaning	Time
$T_\oplus$	Exclusive-OR operation	*negligible*
T_m	Mathematical operation	0.005
T_h	One-way hash function	0.08
$T_{SENC}(2T_h + 2T_m)$	Schnorr Signcryption	0.17
$T_{USENC}(1T_h + 1T_m)$	Schnorr Usigncryption	0.085

TABLE IV
COMPUTATION COST RESULT.

Operation	Explain operation	Time
T_h	KDC decryption	0.08
T_{SENC}	HCC_Y to HCC_X	0.17
T_{USENC}	HCC_X decryption	0.085
T_h	KDC decryption	0.08
T_{SENC}	HCC_X to HCC_Y	0.17
T_{USENC}	HCC_Y decryption	0.085
T_{SENC}	HCC_Y to HCC_X	0.17
T_{USENC}	HCC_X decryption	0.08
TOTAL		0.84

- Communication Cost

We used seven different lengths for our communication analysis. Symmetric key encryption (256 bits) and a Schnorr Signcryption (512 bits) are all supported. The communication cost is shown in Table V.

TABLE V
COMMUNICATION COST.

Message	Operation	Time
Message1	T_h	256 *bits*
Message2	T_{SENC}	512 *bits*
Message3	T_{USENC}	512 *bits*
Message4	T_h	256 *bits*
Message5	T_{SENC}	512 *bits*
Message6	T_{USENC}	512 *bits*
Message7	T_{SENC}	512 *bits*
Message8	T_{USENC}	512 *bits*
TOTAL		4096

VII. CONCLUSION

This article presented a multi-factor authentication scheme based on DGDB and Schnorr Signcryption to enhance the security performance of components of the healthcare security system to achieve preserve-privacy, access control, and authority. Accordingly, the suggested healthcare system verified its ability to securely manage patients' medical information and react quickly to an emergency without depending on patient location. Furthermore, the proposed scheme is secure against well-known attacks such as MITM, Insider, and Reply, and it has many positive metrics such as mutual authentication, scalability, and privacy preservation. Finally, the proposed scheme achieves good computation and communication cost results compared with other related works.

CONFLICT OF INTEREST

The authors have no conflict of relevant interest to this article.

REFERENCES

[1] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, "A survey on privacy protection in blockchain system," *Journal of Network and Computer Applications,* vol. 126, pp. 45-58, 2019.

[2] A. Mubarakali, S. C. Bose, K. Srinivasan, A. Elsir, and O. Elsier, "Design a secure and efficient health record transaction utilizing block chain (SEHRTB) algorithm for health record transaction in block chain," *Journal of Ambient Intelligence and Humanized Computing,* pp. 1-9, 2019.

[3] A. Al Omar, M. Z. A. Bhuiyan, A. Basu, S. Kiyomoto, and M. S. Rahman, "Privacy-friendly platform for healthcare data in cloud based on blockchain environment," *Future generation computer systems,* vol. 95, pp. 511-521, 2019.

[4] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for secure EHRs sharing of mobile cloud based e-health systems," *IEEE access,* vol. 7, pp. 66792-66806, 2019.

[5] A. Islam and S. Y. Shin, "A blockchain-based secure healthcare scheme with the assistance of unmanned aerial vehicle in Internet of Things," *Computers & Electrical Engineering,* vol. 84, p. 106627, 2020.

[6] G. Tripathi, M. A. Ahad, and S. Paiva, "S2HS-A blockchain based approach for smart healthcare system," in *Healthcare*, 2020, vol. 8, no. 1: Elsevier, p. 100391.

[7] R. Almadhoun, M. Kadadha, M. Alhemeiri, M. Alshehhi, and K. Salah, "A user authentication scheme of IoT devices using blockchain-enabled fog nodes," in *2018 IEEE/ACS 15th international conference on computer systems and applications (AICCSA)*, 2018: IEEE, pp. 1-8.

[8] Z. Cui *et al.*, "A hybrid blockchain-based identity authentication scheme for multi-WSN," *IEEE Transactions on Services Computing,* vol. 13, no. 2, pp. 241-251, 2020.

[9] Q. Hasan, A. A. Yassin, and O. Ata, "Electronic health records system using blockchain technology," 2021.

[10] M. Al-Zubi and A. A. Abu-Shareha, "Efficient signcryption scheme based on El-Gamal and Schnorr," *Multimedia Tools and Applications,* vol. 78, no. 9, pp. 11091-11104, 2019.

[11] M. Lamberger and F. Mendel, "Higher-Order Differential Attack on Reduced SHA-256," *IACR Cryptology ePrint Archive,* vol. 2011, p. 37, 01/01 2011.

[12] X. Li, J. Ma, and S.-J. Moon, *On the Security of the Canetti-Krawczyk Model*. 2005, pp. 356-363.

[13] M. Burrows, M. Abadi, and R. M. Needham, "A logic of authentication," *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences,* vol. 426, no. 1871, pp. 233-271, 1989.

[14] I. Khan, S. A. Chaudhry, M. Sher, J. I. Khan, and M. K. Khan, "An anonymous and provably secure biometric-based authentication scheme using chaotic maps for accessing medical drop box data," *The Journal of Supercomputing,* vol. 74, no. 8, pp. 3685-3703, 2018.

[15] M. N. Aman, K. C. Chua, and B. Sikdar, "A light-weight mutual authentication protocol for IoT systems," in

GLOBECOM 2017-2017 IEEE Global Communications Conference, 2017: IEEE, pp. 1-6.

[16] Z. Xu, C. Xu, H. Chen, and F. Yang, "A lightweight anonymous mutual authentication and key agreement scheme for WBAN," *Concurrency and computation: Practice and experience,* vol. 31, no. 14, p. e5295, 2019.

[17] B. A. Alzahrani, A. Irshad, A. Albeshri, and K. Alsubhi, "A provably secure and lightweight patient-healthcare authentication protocol in wireless body area networks," *Wireless Personal Communications,* vol. 117, no. 1, pp. 47-69, 2021.

[18] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Transactions on Information Forensics and Security,* vol. 10, no. 12, pp. 2681-2691, 2015.

[19] C.-C. Chang and H.-C. Tsai, "An anonymous and self-verified mobile authentication with authenticated key agreement for large-scale wireless networks," *IEEE Transactions on Wireless Communications,* vol. 9, no. 11, pp. 3346-3353, 2010.

[20] H. I. Nasser and M. A. Hussain, "Provably curb man-in-the-middle attack-based ARP spoofing in a local network," *Bulletin of Electrical Engineering and Informatics*, vol. 11, no. 4, 2022.

[21] Mustafa H. Alzuwaini, and Ali A. Yassin, " An Efficient Mechanism to Prevent the Phishing Attacks " *Iraqi Journal for Electrical & Electronic Engineering*, vol. 17, Issue 1, pp. 125-135, 2021.