Biometric-based key management for satisfying patient's control over health information in the HIPAA regulations

Quy-Anh Bui[1], Wei-Bin Lee[1], Jung-San Lee[1*], Hsiao-Ling Wu[1,2], Jo-Yun Liu[1]
[1] Department of Information Engineering and Computer Science, Feng Chia University, Taichung 40724, Taiwan
[e-mail: quanganhit@gmail.com; m0502598@fcu.edu.tw;leejs@fcu.edu.tw; ycchen.blythe@mail.fcu.edu.tw]
[2] Department of information management, Chaoyang University of Technology, Taichung, 41349, Taiwan
[e-mail: wuhsiaoling590@gmail.com]
*Corresponding author : Jung-San Lee

Received April 5, 2019; revised July 28, 2019; accepted August 29, 2019; published January 31, 2020

Abstract

According to the privacy regulations of the health insurance portability and accountability act (HIPAA), patients' control over electronic health data is one of the major concern issues. Currently, remote access authorization is considered as the best solution to guarantee the patients' control over their health data. In this paper, a new biometric-based key management scheme is proposed to facilitate remote access authorization anytime and anywhere. First, patients and doctors can use their biometric information to verify the authenticity of communication partners through real-time video communication technology. Second, a safety channel is provided in delivering their access authorization and secret data between patient and doctor. In the designed scheme, the user's public key is authenticated by the corresponding biometric information without the help of public key infrastructure (PKI). Therefore, our proposed scheme does not have the costs of certificate storage, certificate delivery, and certificate revocation. In addition, the implementation time of our proposed system can be significantly reduced.

Keywords: Health Insurance Portability and Accountability Act (HIPAA), electronic health information control, patient's privacy/security

1. Introduction

The technology advances as the time goes. The medical data of a patient is stored in electronic form for convenience, consisting of diagnosis, treatment, and medical image. It might cause serious effect on health status if there exists an unauthorized modification. Also, the medical information includes individual strings such as name, gender, address, and ID card number. All these information are significant to a patient. Therefore, patient control over health information is one of the major concern issues in the privacy regulations of health insurance and accountability act (HIPAA) [1]. Privacy regulations provide the various rights for patients to assure that a patient can control their electronic protected health data anytime and anywhere. For examples, Guo et al. have introduced attribute-based access control for patient to manage their healthy data [2], and the authorized groups being able to read the medical record of patient are recorded in smart contract for medical research [3]. According to the description of the privacy regulations of the HIPAA, patient's health information control means that everyone, who wants to access a patient's health information, must have access permission of the patient.

To prevent unauthorized data access as well as to guaranty the confidentiality of a patient's health information, cryptographic systems [4] can be applied to encrypt the medical data. In such a way, the decrypted key must be exactly provided to legally authorized users for carrying out the activities, which predefined based on their role, job function or responsibility. In 2008, Lee et al. [5] proposed a smart card-based key management solution by integrating various cryptographic techniques to solve the above problems. Then, several methods are proposed to deal with key management concern issues [6]-[10].

The methods in [5]-[10] allow that a patient provides his/her access authorization directly to an authorized user by presenting and enabling a smart card. In this consent case, the patients can correctly control the access to their health information. However, patients sometimes cannot directly provide their access authorization to medical staff, but the patient's health information still is used or disclosed for performing certain activities such as the payment or treatment under the supervision of a third party. In this case, the patient can not completely control their health data. It severely affects the data access control and the confidentiality of a patient's medical information. To ensure the patient can monitor their health information even in the exception case, the methods in [5], [10] allow that a patient authorizes healthcare institutes to access his/her medical information within a contract time period. In addition, the method in [10] also allows that a patient is able to revoke the authorization at any time. However, the disadvantage of these methods is that the authorized users can access the patient's medical information to use and disclosure as whatever they like before the valid time period expires. Therefore, patients will lose control of their health information during the valid time period of the authorization.

Due to the extraordinary evolution of information technology in the recent decade, real-time communication has become very popular in our life, especially in the health care environment. Telemedicine [11] helps doctors remotely diagnose and treat the sickness of patients like face-to-face communication [12]. In telemedicine, doctors sometimes need the related medical information of the patients to diagnose the illness of the patients under online video communication. In order to ensure the privacy of the patient's information that was defined in the HIPAA regulations, remote access authorization from the patients to doctors becomes an

urgent requirement for patients to control their health information. Unfortunately, those methods in [5]-[10] are not suitable for this case, that is authorizing healthcare institutes to access a patient's health information in telemedicine.

In this paper, we employ real-time communication technology to design new biometric-based key management scheme for achieving remote authorization in telemedicine. To make the proposed system can be work in practice, several well-established cryptographic mechanisms are applied to protect the medical data. For legally authorized users, the patient will provide the decryption key for each encryption medical record. Only authorized users have decrypted key to decrypt the emcryption medical files. Hence, patients' control over their health information is more strengthening and the patient's privacy in the HIPAA regulations to be guaranteed.

The remainder of this paper is organized as follows. Section II briefly introduces the related works to understand our design easily. In section III, the proposed method is described in details. Section IV provides privacy, security, and feasibility analyses to prove that the proposed scheme satisfies the requirements of HIPAA regulations. Finally, the conclusions and future works are listed in section V.

2. Related Works

In this section, we briefly introduce five related technologies, i.e., 1) RSA and unbalanced RSA cryptosystem, 2) Shamir's identity-based signature, 3) fuzzy extractor scheme, 4) Liu et al.'s real-time communication scheme, and 5) healthcare certificate authority and healthcare virtual smart card in Taiwan.

2.1 RSA and Unbalanced RSA

RSA and unbalanced RSA are public-key cryptography algorithms, which are used in encrypting a secret message. The security of RSA and unbalanced RSA is based on the difficulty of factoring large integers. Due to the key size of unbalanced RSA is bigger than that of RSA, unbalanced RSA is more robustness than RSA for resisting rapidly increasing computing power.

2.1.1 RSA

A public-key cryptography algorithm, called RSA scheme [4], was proposed by Ron Rivest, Adi Shamir and Leonard Adleman in 1978. This algorithm quickly become one of the most used mainstays for internet security. In the RSA scheme, a public/private key pair is easily generated when two large prime numbers are obtained. The public key can be published while the private key must be kept secretly. A secret message can be protected by using the public key, and the encrypted message can be decrypted by the correspoding private key. The RSA algorithm can be illustrated as three parts that including key generation, encryption, and decryption.

1. Key generation:

   Two large different prime numbers p, and q, with the same length size are choosed. Then, a user computes $n = p.q$ and $\phi(n) = (p-1)(q-1)$. The user selects a random integer e such that $gcd(e, \phi(n)) = 1$, where $1 < e < \phi(n)$ and $gcd(.)$ is the greatest common divisor. Subsequently, the user chooses a unique integer d such that $d = e^{-1}$

mod $\phi(n)$. Finally, (e, n) is the public key and (d, p, q) is the corresponding private key and.

2. Encryption:

   Assume that M is a message; it can be encrypted into ciphertext C by using a public key e as

$$C = M^e \bmod n.$$

3. Decryption:

   The ciphertext C can be decrypted by using the correspoding private key d as

$$M = C^d (\bmod n).$$

2.1.2 Unbalanced RSA

A variant RSA cryptosystem, called unbalanced RSA scheme [13], was proposed by Shamir in 1995. The difference between unbalanced RSA and traditional RSA is the size of two prime numbers, i.e., p and q. In traditional RSA, $|p|=|q|$ and $|p.q|$=512-bits. In unbalanced RSA, $|p| \neq |q|$ and $|p.q|$=5000-bits. Therefore, the unbalanced RSA has higher security than RSA.

The key generation of the unbalanced RSA is shown as below.

1. The user computes the value $t = G(i)$, where $G(.)$ is a public function which is used to convert any user's identity i into a unique 5000-bits.
2. The user chooses a random prime number p with 500-bits, and the other prime number q with the size to be restricted in the range $[\alpha, \alpha + 2^{50}]$ where $\alpha \leq t / p$. Then, the modulus N can be generated as $N = p.q$.
3. The user computes the public key $s = N - t$. Then, the user can publish s.

When having the user's identity i and the public key s, anyone can recover the modulus N by computing $N = G(i) + s$.

2.2 Shamir's identity-based signature scheme

In 1998, Shamir proposed a signature scheme based on the RSA cryptosystem. The procedures of this signature scheme are performed as follows:

A user obtains a unique number g from key generation server as $g = i^d \bmod n$, where i is the user's identification.

To sign the signature on the message m, the user chooses a random number r to compute the parameters t and s as $t = r^e \bmod n$, $s = g \cdot r^{h(t,m)} \bmod n$, where $h(.)$ is a one-way hash function. The signature is (s, t).

The verification condition of the signature scheme is $s^e = i \cdot t^{h(t,m)} \bmod n$.

2.3 Fuzzy extractor scheme

In 2008, Dodis et al. proposed a fuzzy extractor scheme to transform biometric data into a cryptographic key [14]. In this scheme, a random secret string R and a random helper string P are extracted from a biometric data w in a noise-tolerant way. If any biometric w' is similar to original biometric w, the random secret string R can be recovered exactly from it with the

helper string P. The secure sketches and fuzzy extractors are constructed by using three metrics that include hamming distance, set difference, and edit distance. The fuzzy extractor has two functions:

1. Generation function $Gen(.)$ is defined as $Gen(w) = (R, P)$, where the input w is the biometric information, and the outputs R and P are the secret and the helper strings.
2. Reproduction function $Rep(.)$ is defined as $\text{Rep}(w', P) = R$, where w' is another biometric information. The biometric w' must be sufficiently close to the original biometric w. In other words, the Hamming distance between w' and w is smaller than a threshold value.

2.4 Liu et al.'s real-time communication scheme

In 2018, Liu et al. proposed a new scheme to create a secure communication channel over a public network [15]. This scheme is divided into two-phase: the initialization phase and the authentication and key agreement phase. In the initialization phase, both communication partners will use real-time online communication to identify and confirm each other in front of the camera. An unbalanced RSA key pair is generated from their biometric without the help of public key infrastructure (PKI). They exchange some information over a public network for recovering and verifying each other's public key in the authentication and key agreement phase. Finally, a session key, which is used to protect the secret message, will be randomly generated. Interested readers may refer to [15] for more details.

2.5 Healthcare certificate authority and healthcare virtual smart card in Taiwan

In order to provide and manage public keys and certificates of all participants in the healthcare environment, Taiwan's government root certification authority (GRCA) [16] has established the healthcare certificate authority (HCA). Therefore, HCA is responsible for the management of public keys and certificates of the healthcare institutes, medical care personnel, and patients. Additionally, as the advantages of the virtual smart card such as contactless and biometric identification functions like fingerprint or iris recognition. It can increase resistance to the physical and the logical attack. Therefore, the virtual smart card is widely used to store sensitive data. In Taiwan, the virtual smart card is begun used from August 2018 in the healthcare environment [17]. It is evident that a virtual smart card, which is based on smartphone technology, can help us to accomplish some significant requirements of security and privacy issues.

3. Proposed Scheme

In the proposed scheme, there are three roles in the healthcare environment, i.e., users (doctors and patients), a personal health record server (PHR), and a governmental healthcare office (SG). All doctors and patients have a smart device with a camera such as a smartphone, laptop. The personal health record server (PHR) is a data center; it is responsible for storing the patient's encrypted health information record. The governmental healthcare office (SG) is a trusted server; it is responsible for managing all participants' keys. Besides, we assume that $E_{CK}(.)$ and $D_{CK}(.)$ are an encryption function and the corresponding decryption function with a symmetric key CK, and $H(.)$ is a public one-way hash function such as SHA-256. The proposed scheme is divided into three phases: the initialization phase, the medical information package phase, and the fetch phase. Notations and the details of our proposed scheme are described in **Table 1** and subsections 3.1, 3.2 and 3.3.

Table 1. Notions of the Proposed Scheme

Notations	Description
Gen(.)	The generator of Fuzzy Extractors
Ren(.)	The reputation of Fuzzy Extractors
E_{CK}(.)	The function of symmetric encryption with a content key, *CK*
D_{CK}(.)	A function of symmetric decryption with a content key, *CK*
H(.)	One-way hash function
G(.)	The public function used to convert any data into a unique 5000-bits long.
β	Biometric of users
γ	Helper string for Fuzzy Extractors
δ	Extracted string for fuzzy Extractors
p,*q*	The prime numbers of *RSA*
n	A modus of *RSA*
α	A security parameter
T	Timestamp

3.1 Initialization phase

To obtain services from a healthcare provider, each user first must register their biometric information at the SG server for obtaining a key pair of RSA through a virtual private network VPN. In this paper, the user's face is used as the biometric information to generate the key pair of RSA, and the procedures are performed as the following steps.

Step 1: The user captures face to produce biometric β_u by using his/her camera.

Step 2: The user sends the biometric β_u and the identification id_u to the SG server.

Step 3: After checking the validity of data, the SG server generates extracted string id_u and helper string γ_u by using fuzzy extractor function *Gen*(.), i.e.,

$$(\delta_u, \gamma_u) = Gen(\beta_u). \quad (1)$$

Step 4: The SG server computes a unique fixed length parameter τ_u by using a random bit generator function *G*(.), i.e.,

$$\tau_u = G(\delta_u). \quad (2)$$

Step 5: The SG server chooses two random prime numbers (p_u, q_u) , where q_u in $[\alpha_u \alpha_u + 2^{\alpha}]$, $\alpha_u = \tau_u / p_u$, and α is a security attribute.

Step 6: The SG server computes a parameter n_u as

$$n_u = p_u.q_u. \quad (3)$$

Step 7: The SG server chooses a key pair of RSA, (e_u, d_u) [15], where $1 < e_u < \varphi(n_u) = (p_u - 1)(q_u - 1)$, gcd($e_u, \varphi(n_u)$) = 1, and $e_u.d_u = 1 \bmod \varphi(n_u)$.

Step 8: The SG server computes a public number N_u as [15]

$$N_u = n_u - \tau_u. \quad (4)$$

Step 9: The SG server sends the parameters $(d_u, e_u, n_u, \gamma_u, N_u)$ to the user's smartphone, where d_u must be kept secretly and $(e_u, n_u, \gamma_u, N_u)$ can be published.

Therefore, doctor and patient can obtain their RSA key pair, i.e., $(d_d, e_d, n_d, \gamma_d, N_d)$ and $(d_p, e_p, n_p, \gamma_p, N_p)$.

3.2 Medical information package phase

For simplicity, we assume that *M* is the electronic health information of a patient and the data index id_M refers to *M*. To ensure the privacy of patients, *M* must be encrypted. Therefore, when *M* is created by physicians, the patient's smartphone must be enabled by entering his/her password or verifying the biometric information to create an encryption key k_M. Then, the enabled smartphone will perform the following steps to package *M*.

Step 1: Generates a secrete extracted string δ_M and a helper string γ_M from the patient's biometric β_p as

$$(\delta_M, \gamma_M) = Gen(\beta_p). \tag{5}$$

Step 2: Generates an encryption key k_M as

$$k_M = H(id_p \| id_M \| \delta_M), \tag{6}$$

where id_p is the patient's identification.

Step 3: Creates a checksum of *M* as

$$cs_M = H(M). \tag{7}$$

Step 4: Encrypts the patient's medical data *M* as

$$C_M = E_{k_M}(M, cs_M). \tag{8}$$

Step 5: Encrypts the helper string γ_M as

$$C_{\gamma_M} = \gamma_M{}^{e_p} \bmod n_p. \tag{9}$$

Step 6: Stores $(id_M, C_M, C_{\gamma_M})$ into database of *PHR*.

3.3 Fetch phase

In order to provide the patient's health information safely for an authorized user, this phase is divided into two sessions, i.e., 1) the authentication and authorization session 2) the decryption session. The detail of each session is described as follows

3.3.1 Authentication and authorization session

In this session, a patient and a doctor will have a conversation using real-time video communication. Once they confirm that their expected communication partner is correct, they will exchange their public keys and start to verify the correctness of the partner's public key by using the partner's face. After authentication each other, a session key will be generated. Authentication and authorization session are produced as the following steps. Note that the Step 3 to Step 10 are similar to [15].

Step 1: The patient sends its parameters (e_p, γ_p, N_p) to the doctor through a public network. The doctor also sends its parameter (e_d, γ_d, N_d) to the patient.

Step 2: After receiving the parameters (e_d, γ_d, N_d) from the doctor, the patient captures the doctor's face to produce the doctor's biometric information β_p' by using the patient's camera.

Step 3: The patient recovers the doctor's secret extracted string δ_d as

$$\delta_d = Rep(\beta_p', \gamma_d). \tag{10}$$

Step 4: The patient computes the doctor's τ_u as

$$\tau_u = G(\delta_d). \tag{11}$$

Step 5: The patient computes the doctor's modus n_d as

$$n_d = \tau_d + N_d. \tag{12}$$

Similarly, when the doctor performs steps 2 to 5, he also reproduces the patient's modus n_p.

Step 6: The patient chooses a random number K_p.

Step 7: The patient encrypts K_p as

$$C_{K_p} = K_p^{e_d} \bmod n_d. \tag{13}$$

Step 8: The patient sends C_{K_p} to the doctor.

Step 9: When receiving C_{K_p} from the patient, The doctor decrypts C_{K_p} as

$$K_p = C_{K_p}^{d_d} \bmod n_d. \tag{14}$$

Step 10: The doctor chooses a random number K_d.

Step 11: The doctor computes the session key k_s *as*

$$k_s = H(K_p \| K_d). \tag{15}$$

Step 12: The doctor encrypts K_d as

$$C_{K_d} = K_d^{e_p} \bmod n_p. \tag{16}$$

Step 13: The doctor encrypts the parameters (id_d, id_M) as

$$C_{DI} = E_{k_s}(id_d, id_M). \tag{17}$$

Step 14: The doctor sends (s, C_{DI}) to the patient.

Step 15: When receiving the (C_{K_d}, C_{DI}) from the doctor, the patient decrypts C_{K_d} as

$$K_d = C_{K_d}^{d_p} \bmod n_p. \tag{18}$$

Step 16: The patient computes session key k_s *as*

$$k_s = H(K_p \| K_d). \tag{19}$$

Step 17: The patient decrypts C_{DI} as

$$(id_d, id_M) = D_{k_s}(C_{DI}). \tag{20}$$

Step 18: The patient generates permission of the patient as

$$per_p = H(id_p \| id_d \| id_M \| T_p)^{d_p} \bmod n_p. \tag{21}$$

Step 19: The patient encrypts the permission per_p as

$$C_{per_p} = E_{k_s}(per_p, id_p, T_p). \tag{22}$$

Step 20: The patient sends C_{per_p} to the doctor as a patient's health information access authorization.

3.3.2 Decryption session

When the doctor receives the permission of the patient, he/she creates a signature on this permission for requestting the patient's health information from the PHR server. The procedures of the doctor and the PHR server are shown as follows:

Step 1: The doctor decrypt C_{per_p} as

$$(per_p, id_p, T_p) = D_{k_s}(C_{per_p}). \tag{23}$$

Step 2: The doctor generates a signture s_d as

$$s_d = H(id_d \,||\, id_M)^{d_d} \bmod n_d. \tag{24}$$

Step 3: The doctor sends (id_M, per_p, id_p, T_p, id_d, s_d) to the PHR server for requesting the patient's health data.

Step 4: When the PHR server receives the request from the doctor, it verifies per_p and s_d as

$$per_p^{e_p} ?= H(id_p \,||\, id_d \,||\, id_M \,||\, T_p) \bmod n_p,$$
$$s_d^{e_d} = H(id_d \,||\, id_M) \bmod n_d \tag{25}$$

Step 5: The PHR server sends the patient's health data (C_M, C_{γ_M}) to the doctor if the above formula is correct; otherwise, this request will be rejected.

Step 6: When the doctor obtains the patient's encrypted data (C_M, C_{γ_M}), he/she needs assistance from the patient. Therefore, the doctor sends the helper string C_{γ_M} to the patient.

Step 7: When receiving C_{γ_M} from the doctor, the patient's enable smartphone will decrypt the encrypted helper string C_{γ_M} as

$$\gamma_M = C_{\gamma_M}^{d_p} \bmod n_p. \tag{26}$$

Step 8: The enable smartphone recovers the extracting string δ_M as

$$\delta_M = Rep(\beta_p', \gamma_M). \tag{27}$$

where β_p' is the patient's biometric information.

Step 9: The enable smartphone recalls the decryption key k_M as

$$k_M = H(id_p \,||\, id_M \,||\, \delta_M). \tag{28}$$

Step 10: The enable smartphone encrypts k_M as

$$C_{k_M} = E_{k_s}(k_M). \tag{29}$$

Step 11: The enable smartphone sends C_{k_M} to the doctor.

Step 12: When receiving the decrypted data C_{k_M}, the doctor can use the session key k_s to

decrypt it, i.e.,

$$k_M = D_{k_s}(C_{k_M}). \tag{30}$$

Step 13: The doctor decrypts C_M as

$$(M, cs_M) = D_{k_M}(C_M). \tag{31}$$

Step 14: The doctor checks the validity of cs_M as

$$cs_M \,?= H(M). \tag{32}$$

When having the patient's health information, the doctor can use M according to the privacy regulations of the HIPAA.

4. Analysis

In this paper, we propose a new biometric-based key management to ensure patients' remote control over health information according to the individual privacy/security rule of HIPAA regulations. In addition, the proposed scheme also allows patients and doctors can safely exchange health information through the public network based on the advantages of real-time online video communication. To ensure the proposed scheme is secure and feasibility, we first focus on analyzing the privacy and security in subsections 4.1, 4.2, and 4.3. Second, the feasibility analysis of the proposed scheme is discussed in subsection 4.4. Finally, we give the comparisons of properties between Liu et al.'s scheme and ours in subsection 4.5.

4.1 Privacy protection issues

In this subsection, we focus on analyzing the privacy protection capability and the patient's health information access processes.

For each patient, we apply the patient's biometric information β_p into Equation (1) to get the secret string δ_M. Then, we apply δ_M, id_p, and id_M into Equation (2) to get an symmetry encryption key k_M, where id_p is a unique identification of patient and id_M is the medical record index. Finally, we employ a symmetry encryption algorithm, advanced encryption standard (AES) [18],[19], to protect the patient's health information record. Thus, the patient's health information is compromised only if the secret string δ_M is broken. When each authorized user wants to decrypt the patient's encrypted medical information record C_M in Equation (8), the secret string δ_M must be recovered. According to Equation (27), we know that the secret key δ_M is recovered from the patient's biometric information β'_p the helper string γ_M is required, i.e., $\delta_M = Rep(\beta'_p, \gamma_M)$. Since γ_M is encrypted by the public key e_p of the patient in Equation (9), the encrypted medical record only can be decrypted by the patient who has the private key d_p.

4.2 Authentication and authorization issues

Real-time online video communication allows patients and doctors to see each other through a camera lens. Therefore, it can help patients and doctors easily to identify and confirm each other as a kind of face-to-face communication. In the initialization phase, the private keys (d_p, d_d) and the public keys (e_p, e_d) are generated based on the users' biometrics. In

the authentication and authorization session, the public keys (e_p, e_d) will be verified with the users' biometrics. If the public key of the doctor (or the patient) is illegal, the doctor (or the patient) never get the correctly secret random K_p (or K_d) in Eqtation (14) (or Equation (18)). Therefore, they cannot correctly compute the session key $k_s = H(K_P||K_d)$ in Equations (15) and (19). Since the signature per_p of the patient is generated in Equation (21), only the authorized doctor who has the correct session key k_s can decrypt it. The patient's signature means a patient's permission, which is used to authorize the doctor to access his/her health information. This permission cannot be modified by anyone because of the property of the hash function.

Regards to non-repudiation, the meaning is that patient and doctor cannot deny their responsibility when a dispute occurs. Firstly, it is hard for patient to deny that he/she has given the aceess right to doctor because the permission of patient $per_p = H(id_p \| id_d \| id_M \| T_p)^{d_p} \bmod n_p$ in Equitation (21) is used for confirmation. In the role of doctor, he/she has no idea to decline having asked the medical record since the requesting message includes the signature of doctor, which is $s_d = H(id_d \| id_M)^{d_d} \bmod n_d$ in Equitation (24). Hence, no one can deny what he/she has done once an argument happens according to formulas (21) and (24).

4.3. Data confidentiality and integrity analysis

The security of encryption/decryption key and integrity of a patient's health information in the proposed scheme will be analyzed in this subsection.

Data confidentiality

In our system, the encryption/decryption key $k_M = H(id_p \| id_M \| \delta_M)$, which is used to encrypt/decrypt the patient's health information C_M in Equations (8) and (31), does not store in any devices. It is only recovered by using the secret extracting string δ_M, the patient-related information id_p, and the medical information index id_M. Although the patient's face can be easy to get by using the common camera, the secret extracting string δ_M cannot be recovered exactly from this biometric when the user does not have the helper string γ_M. The helper string γ_M can be decrypted by the patient, who has the private key d_p. In addition, the session key k_s in Equations (15) and (19), which is used to encrypt secret data, has proof that it is secure enough to resist malicious attacks under BAN Logic.

Data Integrity

By using the cryptographic checksum cs_M in Equation (7) to protect the patient's medical information, the integrity of the patient's data can be made sure. Any effort for altering patient's encryption data by an unauthorized user will cause the heavy change of the checksum in Equation (31). Hence, only the authorized user, who has permission from the patient, can alter the patient's data. According to Equation (8), we know that the patient's record M is encrypted by the patient's secret key k_M. Therefore, the integrity of the patient's data can be guaranteed, and any alteration of data by an unauthorized user can be detected.

Proof with BAN logic $|\equiv$

Burrows et al. presented a formal logic analysis for proving the correctness of the authentication schemes, called the BAN logic model [20]. BAN logic model is designed to

focus on whether exchanged information is trustworthy between two parties. We are going to employ BAN logic to prove the correctness of the mutual authentication of our proposed scheme. We give a formal definition and rules of the BAN logic model in **Table 2** [20], [21] and below.

Table 2. BAN logic notations

Notation	Definition
$P \mid\equiv X$	P believes in X
$P \triangleleft X$	P sees X (receive)
$P \mid\sim X$	P once said X (send)
$\#(X)$	The formula X is fresh
$\{X\}_k$	The formula X is encrypted under the key k
$P \overset{k}{\leftrightarrow} Q$	P and Q may use the shared key k to communicate
$< X >_Y$	The formula X is combined with the formula Y

Rules of BAN logic:

R1. *The message-meaning*

$$\frac{P \mid\equiv Q \overset{Y}{\rightleftharpoons} P, P \triangleleft < X >_Y}{P \mid\equiv Q \mid\sim X}$$

R2. *The freshness*

$$\frac{P \mid\equiv \#(X)}{P \mid\equiv \#(X, Y)} \text{ and } \frac{P \mid\equiv \#(X, Y)}{P \mid\equiv \#(X)}$$

R3. *The nonce-verification*

$$\frac{P \mid\equiv \#(X), P \mid\equiv Q \mid\sim X}{P \mid\equiv Q \mid\equiv X}$$

R4. *The session-key*

$$\frac{P \mid\equiv \#(k), P \mid\equiv Q \mid\equiv X}{P \mid\equiv P \overset{k}{\leftrightarrow} Q}$$

In our scheme, the patient and doctor together coordinate the session key $k_s = H(K_p \| K_d)$. They must believe that this session key is shared between them. Hence, the goals are listed:

G1. Doctor $\mid\equiv$ (Patient $\overset{k_s}{\leftrightarrow}$ Doctor)

G2. Patient $\mid\equiv$ (Patient $\overset{k_s}{\leftrightarrow}$ Doctor)

In the authentication and authorization session phase, the message exchange steps are written in M1 and M2:

M1. Patient → Doctor: C_{K_p} $(C_{K_p} = K_p^{e_d} \bmod n_d)$ (13)

M2. Doctor → Patient: C_{K_d} $(C_{K_d} = K_d^{e_p} \bmod n_p)$ (16)

We can transfer the generic messages into the idealized form as:

I1. Patient → Doctor: $\{< K_p >_{n_d}, K_p\}_{pk_d}$

I2. Doctor → Patient: $\{< K_d >_{n_p}, K_d\}_{pk_p}$

According to steps 1 to 5 of the authentication and authorization session phase, we know that only the patient and doctor compute n_d and n_p. Therefore, we can treat n_d and n_p as the secrets between patient and doctor.

To complete the analysis, we give the following basic assumption:

A1. Doctor $|\equiv$ Patient $\overset{n_d}{\rightleftharpoons}$ Doctor

A2. Doctor $|\equiv \#(n_d)$

A3. Doctor $|\equiv \#(K_d)$

A4. Patient $|\equiv$ Patient $\overset{n_p}{\rightleftharpoons}$ Doctor

A5. Patient $|\equiv \#(n_p)$

A6. Patient $|\equiv \#(K_p)$

Proof G1 and G2:

When the doctor receives $\{< K_p >_{n_d}, K_p\}_{pk_d}$ in I1, he/she uses the private key pk_d^{-1} to decrypt it.

We have

D1. Doctor $\triangleleft$ $< K_p >_{n_d}$

According to A1 and D1, we employ *the message-meaning rule* to obtain

D2. Doctor $|\equiv$ Patient $|\sim$ K_p

Based on *the freshness rule*, A2, we can obtain

D3. Doctor $|\equiv$ $\#(K_p)$

Using *the nonce-verification rule*, D2 and D3, we can infer that

D4. Doctor $|\equiv$ Patient $|\equiv$ K_p

We know that the session key $k_s = H(K_p \,||\, K_d)$ and A3, we can use *the freshness rule* to get

D5. Doctor $|\equiv \#(k_s)$

Applying D4, D5 to *the session-key rule*, we can deduce

G1. Doctor $|\equiv$ (Patient $\overset{k_s}{\longleftrightarrow}$ Doctor)

When the patient receives $\{< K_d >_{n_p}, K_d\}_{pk_p}$ in I2, he/she uses the private key pk_p^{-1} to decrypt it. We have

D6. Patient $\triangleleft < K_d >_{n_p}$

According to A4 and D6, we employ *the message-meaning rule* to obtain

D7. Patient $|\equiv$ Doctor $|\sim$ K_d

Based on *the freshness rule*, A5, we can obtain

D8. Patient $|\equiv \#(K_d)$

Using *the nonce-verification rule*, D7 and D8, we can infer that

D9. Patient $|\equiv$ Doctor $|\equiv K_d$

We know that the session key $k_s = H(K_p \,||\, K_d)$ and A6, we can use *the freshness rule* to get

D10. Patient $|\equiv$ $\#(k_s)$

Applying D9, D10 to *the session-key rule*, we can deduce

G2. Patient $|\equiv$ (Patient $\overset{k_s}{\longleftrightarrow}$ Doctor)

Therefore, we have proved G1 and G2 are correctly under BAN logic model.

4.4. Feasibility analysis

In order to make sure the practicability of the proposed system, we have discussed the used techniques, equipment, and information in this subsection.

Required techniques

In our proposed system, some of the techniques are required, i.e., a one-way hash function, an asymmetric/symmetric cipher, an identification and key generator based on biometric mechanism. All of these techniques have been carefully developed, published, and evaluated by various researchers for the past decades. Moreover, these techniques are still continuously improved for better adaptation to new applications; for instance, the biometric identification mechanism and real-time communication techniques are combined to the remote healthcare business.

Required equipment

To implement our proposed system, each healthcare provider and users need to equip a network and biometric extraction equipment for communication and biometric extraction. Over the past decade, real-time online communication has become very common in our life, such as video conferencing, smart space and collaborative business [22]-[24]. In 2018, Liu et al. already use real-time communication technology and digital devices in their scheme [15]. It allows that confidential and sensitive messages are conveyed between partners through the public network. Hence, all of the equipment required to implement the system is available and practical.

Required information

In the proposed system, the encryption/decryption key of patients and doctors are generated based on their's identification and biometric information. According to the above description, the individual biometric information can be easily obtained by using a digital device with a high-quality camera. We use fuzzy extractor scheme [14] to extract the secret string δ_p in Equation (1) δ_M and in Equation (5) from the biometric information of a user. Fuzzy extractor scheme was proposed in 2008, many various researchers [15], [25] has proved its effectiveness and applied it in many scenarios. Thus, the information, that is used to implement the proposed system, is effectiveness.

4.5 Comparisons of properties between Liu et al.'s scheme and ours

In this subsection, we will discuss the properties of Liu et al.'s scheme and ours. Liu et al. use the biometrics key and real-time communication technologies to construct a secure channel for exchanging secret data. According to the security analyses in their article, we know that their scheme can achieve ten properties. Since our system is based on Liu et al.'s scheme, the security of our system is the same as Liu et al.'s scheme. However, Liu et al.'s scheme cannot directly apply in telemedicine. Therefore, only our system can achieve the property of patients' control over health information. **Table 3** displays the comparisons of properties between Liu et al.'s scheme and ours.

Table 3. Comparisons of properties between Liu et al.'s scheme and ours

	Liu et al.'s scheme [15]	Proposed scheme
P1	Y	Y
P2	Y	Y
P3	Y	Y
P4	Y	Y
P5	Y	Y
P6	Y	Y
P7	Y	Y
P8	Y	Y
P9	Y	Y
P10	Y	Y
P11	N	Y

P1: the property of resisting replay attack
P2: the property of resisting masquerading server attack
P3: the property of resisting user impersonation attack
P4: the property of resisting DoS attack
P5: the property of resisting database capture attack
P6: the property of resisting smart card attack
P7: the property of resisting man-in-the-middle attack
P8: the property of mutual authentication
P9: the property of biometric recognition error
P10: the property of session key agreement
P11: the property of patients' control over health information

5. Conclusions

In this paper, we combine biometric information and real-time communication to propose a new key management scheme for strengthening patients' control over individual health information. Real-time video communication provides that patients and doctors can mutually communicate over a public network anytime and anywhere. In the designed scheme, the user's public key is authenticated by the corresponding biometric information. The PKI and third-party certifier are not involved. Therefore, our proposed scheme has lower cost than previous PKI-based schemes. In addition, the feasibility analysis shows that the scheme can be easily and effectively implemented in the current healthcare environment.

References

[1] Health Insurance Portability Accountability Act of 1996(HIPAA), Centers for Medicare and Medicaid Services,Baltimore, MD, 1996, Available online: Article (CrossRef Link).

[2] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure Attribute-based Signature Scheme with Multiple Authorities for Blockchain in Electronic Health Records Systems," *IEEE Access*, Vol. 6, pp. 11676-11686, Feb. 2018. Article (CrossRef Link)

[3] 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, May 2019. Article (CrossRef Link)

[4] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, vol. 21 no. 2, Feb. 1978. Article (CrossRef Link)

[5] W.B. Lee and C.D. Lee, "A Cryptographic Key Management Solution for HIPAA Privacy/Security Regulations," *IEEE Transactions on Information Technology in Biomedicine*, vol. 12, no. 1, pp. 34-41, Jan. 2008. Article (CrossRef Link)

[6] J. Li, J. Lee, and C. Chang, "Preserving PHI in Compliance with HIPAA Privacy/Security Regulations using Cryptographic Techniques," in *Proc. of International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Harbin*, Aug. 2008. Article (CrossRef Link)

[7] J. Hu, H. H. Chen, and T. W. Hou, "A Hybrid Public Key Infrastructure Solution (HPKI) for HIPAA Privacy/Security Regulations," *Computer Standards & Interfaces*, vol. 32, no 5-6, pp. 274-280, 2010. Article (CrossRef Link)

[8] H. F. Huang, K. C. Liu, and H. W. Wang, "A New Design of Cryptographic Key Management for HIPAA Privacy and Security Regulations," *International journal of innovative computing, information & control*, vol. 5, no. 11(A), pp. 3923-3931, Nov. 2009. Article (CrossRef Link)

[9] H. F. Huang and K. C. Liu, "Efficient Key Management for Preserving HIPAA Regulations," *Journal of Systems and Software*, vol. 84, no. 1, pp. 113-119, Jan. 2011. Article (CrossRef Link)

[10] W.B. Lee, C.D. Lee, K. I. J. Ho, "A HIPAA-compliant Key Management Scheme with Revocation of Authorization," *Computer Methods and Programs in Biomedic*ine, vol. 113, no. 3, pp. 809-814, Mar. 2014. Article (CrossRef Link)

[11] A. Jebrane, N. Meddah, A. Toumanari, and M. Bousseta, "New Real Time Cloud Telemedicine using Digital Signature Algorithm on Elliptic Curves," in *Proc. of International Conference on Advanced Information Technology, Services and Systems*, pp. 324-332, Nov. 2017. Article (CrossRef Link)

[12] D. Anton, G. Kurillo, and R. Bajcsy, "User Experience and Interaction Performance in 2D/3D Telecollaboration," *Future Generation Computer Systems*, vol. 82, pp. 77-88, May 2018. Article (CrossRef Link)

[13] R. L. Rivest, A. Shamir, and L. M. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120-126, Jan 1978. Article (CrossRef Link)

[14] Y. Dodis, R. Reyzin, and A. Smith, "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data," *SIAM Journal on Computing*, vol. 38, no. 1, pp. 97-139, Mar. 2008. Article (CrossRef Link)

[15] X. Liu, W.B. Lee, B.Q. Bui, C.C. Lin, and H.L. Wu, "Biometrics-Based RSA Cryptosystem for Securing Real-Time Communication," *Sustainability*, vol. 10, no. 10, p.3588, Oct. 2018. Article (CrossRef Link)

[16] Government Public Key Infrastructure, Available Online: Article (CrossRef Link).

[17] Could Physical NHI Cards Go the Way of History?, Available Online: Article (CrossRef Link).

[18] A. Biryukov, "Block Ciphers and Stream Ciphers: The State of the Art," *IACR Cryptology ePrint Archive*, 2004. Article (CrossRef Link)

[19] J. Daemen and V. Rijmen, "The Block Cipher Rijndael," in *Proc. of the International Conference on Smart Card Research and Applications*, pp. 277-284, Sep. 1998. Article (CrossRef Link)

[20] S.P. Yang and X. Li, "Defect in Protocol Analysis with BAN Logic on Man-in-the-Middle Attacks," *OALib Journal*, 2007.
[21] M. Burrows, M. Abadi, and R. Needham, "A Logic of Authenticatio," *ACM Transactions on Computer Systems*, vol. 8, no. 1, Feb. 1990. Article (CrossRef Link)
[22] N. Panteli and P. Dawson, "Video Conferencing Meetings: Changing Patterns of Business Communication," *New Technology Work and Employment*, vol. 16, no. 2, pp. 88-99, Dec. 2001. Article (CrossRef Link)
[23] S. Jeong, Y. Jeong, K. Lee, S. Lee, and B.Yoon, "Technology-based New Service Idea Generation for Smart Spaces: Application of 5g Mobile Communication Technology," *Sustainability*, vol. 8, no. 11, p. 1211, Nov. 2016. Article (CrossRef Link)
[24] J. A. Correa-Garcia, M. A. Garcia-Benau, and E. Garcia-Meca, "CSR Communication Strategies of Colombian Business Groups: An Analysis of Corporate Reports," *Sustainability*, vol. 10, no. 5, p. 1602, May 2018. Article (CrossRef Link)
[25] W.B. Lee, Y.T. Lin, M.H. Tsai, and H.B. Chen, "A Novel One-time Password Mutual Authentication Scheme using Biometrics-based Key and Visual Secret Sharing," *Interational journal of Advance Computational Engineering and Networking (IJACEN)*, vol.3, no.5, pp.27-32, 2015. Article (CrossRef Link)

Quy-Anh Bui received the B.S. degree in information technology from the Thai Nguyen University of Information and Communication Technology, Vietnam, in 2009, and the master's degree in information technology from the Manuel S. Enverga University Foundation, Philippines, in 2012. He is currently pursuing the Ph.D. degree with the Department of Information Engineering and Computer Science, Feng Chia University, Taichung, Taiwan. His current research interests include cloud security & digital right management, medical information security.

Wei-Bin Lee received the B.S. degree from the Department of Information and Computer Engineering, Chung Yuan Christian University, Chungli, Taiwan, R.O.C., in 1991, and the M.S. degree in computer science and information engineering and the Ph.D. degree from National Chung Cheng University, Chiayi, Taiwan, R.O.C., in 1993 and 1997, respectively. Since 1999, he has been with the Department of Information Engineering, Feng Chia University, Taichung, Taiwan, R.O.C., where he is currently a Full Professor. Since 2015, he has been with the Department of Information Technology, Taipei City Government, Taiwan, R.O.C., where he is currently a Commissioner. His research interests currently include cryptography, information security management, steganography, and network security. Dr. Lee is an Honorary Member of the Phi Tau Phi.

Jung-San Lee received the BS degree in computer science and information engineering from National Chung Cheng University, Chiayi, Taiwan in 2002. He received his Ph.D. degree in computer science and information engineering in 2008 from National Chung Cheng University, Chiayi, Taiwan. Since 2017, he has worked as a professor in the Department of Information Engineering and Computer Science at Feng Chia University, Taichung, Taiwan. His current research interests include image processing, information security, and watermarking.

Hsiao-Ling Wu received her Ph.D. degree in information engineering and computer science from Feng Chia University, Taichung, Taiwan in 2018. She is also the honorary member of The Phi Tau Phi Scholastic Honor Society of the Republic of China in the same year. She received the BS degree in department of applied mathematics from Feng Chia University, Taichung, Taiwan in 2007. Now she is as a Postdoctoral Fellow in department of information management from Chaoyang University of Technology (CYUT), Taichung, Taiwan. Her current research interests include electronic commerce, information security, image processing, cryptography, and mobile communications.

Jo-Yun Liu is currently pursuing her MS degree in information engineering and computer science in Feng Chia University, Taichung, Taiwan. Her current research interests include information security and healthcare-data protection.