INVITED PAPER  
Special Section on Security, Privacy and Anonymity of Internet of Things

Remote Data Integrity Checking and Sharing in Cloud-Based Health Internet of Things

Huaqun WANG\textsuperscript{1,†††}, Keqiu LI\textsuperscript{††b}, Nonmembers, Kaoru OTA\textsuperscript{†††c}, Member, and Jian SHEN\textsuperscript{1d}, Nonmember

SUMMARY  
In the health IoT (Internet of Things), the specialized sensor devices can be used to monitor remote health and notify the emergency information, e.g., blood pressure, heart rate, etc. These data can help the doctors to rescue the patients. In cloud-based health IoT, patients’ medical/health data is managed by the cloud service providers. Secure storage and privacy preservation are indispensable for the outsourced medical/health data in cloud computing. In this paper, we study the integrity checking and sharing of outsourced private medical/health records for critical patients in public clouds (ICS). The patient can check his own medical/health data integrity and retrieve them. When a patient is in coma, some authorized entities and hospital can cooperate to share the patient’s necessary medical/health data in order to rescue the patient. The paper studies the system model, security model and concrete scheme for ICS in public clouds. Based on the bilinear pairing technique, we design an efficient ICS protocol. Through security analysis and performance analysis, the proposed protocol is provably secure and efficient.

key words: remote data integrity checking, public cloud, data sharing

1. Introduction

IoT can be used in the healthcare applications. It plays a significant role from managing chronic diseases at one end of the spectrum to preventing disease at the other, such as clinical care and remote monitoring. In the life of every people, the generated medical data and the health data is very large. In the medical research, the researchers will process massive medical data. Massive data processing and information security risk call for the new computation model as an alternative to conventional computing. As a new computation model, cloud computing has become a reality along with the development of network and computer technology. Cloud computing provides a flexible, dynamic, resilient and cost effective infrastructure for the business environments. For the patients and hospital, the remote medical/health data integrity checking and sharing can be performed by the patients and hospital. Since the medical/health data is outside the control of patients and hospital, cloud service providers are more responsible for the security of application services, especially in public clouds. Based on public cloud server’s benefits and security risks, the paper focuses on privacy-preserving remote medical/health data integrity checking and sharing for critical patients in public clouds.

Throughout the paper, “privacy-preserving ICS” is simplified as “ICS”, “public cloud server” is simplified as “PCS”.

1.1 Motivation

Along with the development of IoT, it is widely used in the field of healthcare. By using the IoT, massive health data is generated. On the other hand, when the patient goes to the hospital, the medical data is also generated. These generated medical/health data can be used in order to rescue the patients. In the cloud-based health IoT, the medical/health data is stored in public clouds. In public clouds, the hospitals and patients access PCS via Internet. To protect the hospital’s benefits, it is important to prevent unauthorized entities to check these data integrity. If the malicious competitors can check these data integrity, they can evaluate these data size. Then, the competitors can evaluate the hospital’s daily business volume. Then, the competitors can take measures to prevail the hospital. In order to protect these data, the remote data integrity checking can only be performed by the hospital besides of the patient. Usually, in order to protect the patients’ privacy, only the patient can retrieve his own medical/health data. Unfortunately, the critical patients may be in a coma before reaching the hospital. In this case, the hospital and the patient’s relatives should be able to cooperate to share the patient’s medical/health data in order to rescue him. This real social requirement motivates us to study privacy-preserving remote medical/health data integrity checking and sharing for critical patients in public clouds.

1.2 Related Work

The rapidly developed IoT has been widely applied in the medical/health field [1], [2]. Based on the special properties of medical/health data, when IoT is used in the medical/health field, some security risks emerge [3], [4]. In 2015, Wu et al. proposed employment of the regenerating codes.
and symmetric-key encryption with a Blom based key management [5]. Their scheme can repair the lost fragment and protect data secrecy. When the medical/health data is stored on the PCS, the remote data integrity checking and sharing become an urgent security problem which needs to be solved. In 2014, Wang et al. proposed the fair remote retrieval of outsourced private medical records in electronic health networks [6]. Lu et al. proposed privacy preserving opportunistic computing framework for mobile-health care emergency [7]. In 2016, He et al. introduced a novel network security architecture for cloud computing considering characteristics of cloud computing [8]. Their scheme can protect external and internal traffics in cloud computing. It can also attain flexible scalability with respect to virtual middle box load and achieve fault-tolerant among virtual middle box failure.

Since these privacy-aware medical/health data is stored on the untrusted third party PCS, it is important to keep these data uncorrupted and privacy-preserving. As an efficient remote data integrity checking model, the concept of provable data integrity (PDP) was proposed by G. Atieniese et al. in 2007 [9]. They also designed two concrete statically secure PDP schemes. Since PDP is a very efficient remote data integrity checking model, many researchers proposed a variety of PDP security models and concrete schemes [10]–[14].

Privacy-preservation is an important security issue in cloud computing. In 2013, Wang et al. proposed the privacy-preserving public auditing in cloud computing [15]. Nabeel et al. proposed privacy preserving policy based content sharing in public clouds [16]. Guo et al. proposed the variable threshold-value authentication architecture for wireless mesh networks [17]. In the medical/health data cloud storage, privacy preservation is especially important. Only the patient and the authorized entities can get the patient’s medical/health data. PDP protocols are classified into two categories: private PDP and public PDP. Some private information is necessary to perform private PDP. The private information is not needed for public PDP.

1.3 Our Contribution and Organization

In this paper, we propose the novel concept of ICS. Then, we give the formal system model and security model of ICS. By using the bilinear pairings, an efficient ICS protocol is designed. Through security analysis and performance analysis, our ICS protocol is provably secure and efficient.

The rest of the paper is organized as follows. Section 2 introduces the preliminaries and Sect. 3 describes our pairing-based ICS protocol and analyzes its security. Section 4 gives the performance analysis of our ICS protocol. Finally, Sect. 5 concludes this paper.

2. Preliminaries

ICS system model and security model are proposed in this section. After that, bilinear pairings and some corresponding difficult problems are also described below.

2.1 System Model and Security Model

ICS system consists of four different network entities: Patient, Hospital, AuthSet, PCS. They can be identified below.

1. Patient, whose medical/health data will be uploaded to PCS for maintenance and computation, is individual human being;
2. Hospital, which diagnoses the patients and generates the medical/health data for the patients, can be physicians or medical institutions;
3. AuthSet, which is the patient’s authorized entity set, can cooperate with the hospital to share the patient’s medical/health data;
4. PCS, which is managed by cloud service provider, has significant storage space and computation resource to maintain the patients’ data.

Definition 1 (ICS). A ICS protocol is a collection of seven polynomial time algorithms (SetUp, EncTagGen, CheckTagSign, GenProof, GenRetr, CheckProof, Retrieval) among PCS, Hospital, Patient, and AuthSet such that:

1. \(\text{SetUp}(\text{params}, \text{sk}, \text{pk})\) is a probabilistic system parameters and key generation algorithm to setup the protocol where \(k\) is a security parameter, \(\text{sk}\) is the secret key and \(\text{pk}\) is the public key. params is the public system parameters. \(\text{ID}_j\) gets its private/public key pair \((x_j, X_j)\) and a symmetric encryption key \(sk_j\). The hospital’s private/public key pair are \((y, Y)\). PCS’s private/public key pair are \((z, Z)\). The patient \(\text{ID}_j\) prepares the warrant \(\omega_j\) and the corresponding certificate \(\text{Sign}(\omega_j)\). \(\text{ID}_j\) creates \(sk_j\)’s secret shares and distributes the shares among AuthSet.
2. \(\text{EncTagGen}(x_j, sk_j, Y, M_j)\rightarrow \{T_{i,j}\}\) is run by the patient \(\text{ID}_j\) to generate the verification metadata, where \(M_j\) is \(\text{ID}_j\)’s medical/health data and \(T_{i,j}\) is \(\text{ID}_j\)’s i-th block’s tag.
3. \(\text{CheckTagSign}(F_{i,j}, T_{i,j}, z, X_j, Y_j, Z_j, \omega_j, \text{Sign}(\omega_j))\rightarrow \{\text{success}, \text{failure}\}\) is run by PCS to check whether the medical/health block-tag pair \((F_{i,j}, T_{i,j})\) and the warrant-signature pair \((\omega_j, \text{Sign}(\omega_j))\) are valid or not.
4. \(\text{GenProof}(F, \text{chal}_p, \Sigma)\rightarrow V_p\) is run by PCS to generate the proof of integrity. \(F\) is the stored file and \(\Sigma\) is the stored tags. \(\text{chal}_p\) is the challenge from the verifier.
5. \(\text{GenRetr}(F, \text{chal}_r, \Sigma)\rightarrow V_r\) is run by PCS to generate the retrieval response.
6. \(\text{CheckProof}(x_j, y, X_j, Y_j, Z_j, \text{chal}_p, V_p)\rightarrow \{\text{success}, \text{failure}\}\) is run by the patient \(\text{ID}_j\) or the hospital to check the data integrity.
7. \(\text{Retrieval}(x_j, sk_j)\) or \((y, sk_v\text{'s valid share set}),X_j, Y_j, Z_j, \text{chal}_r, V_r\rightarrow M_j\) is run by the patient \(\text{ID}_j\) or the cooperation of hospital and AuthSet to retrieve \(\text{ID}_j\)’s remote medical/health data \(M_j\).

The following definitions 2, 3, 4 define the security against the malicious PCS forgery, restrictive remote medical/health data integrity checking and restrictive retrievability.
Definition 2 (Integrity Against Malicious PCS). ICS protocol satisfies the integrity if any PPT (probabilistic polynomial time) adversary \( A \) (i.e., malicious PCS) can win the ICS game only with negligible probability. ICS game between the challenger \( C \) and the adversary \( A \) is described below:

1. Setup: In this phase, the system parameters are created. Let the patient set be \( \mathcal{P} \). The patient ID\(_j\)’s private/public key pair \((x_1, X_1)\), the hospital’s private/public key pair \((y, Y)\) and PCS’s private/public key pair \((z, Z)\) are created where ID\(_j\) \( \in \mathcal{P} \). Let ID\(_j\)’s symmetric encryption/decryption key be \( sk_j \). The private keys \( x_j, y \) are kept secret. The parameters \((x, X_1, y, Z, \text{params, } ID_j \in \mathcal{P})\) are sent to \( A \).

2. First-Phase Queries: \( A \) adaptively queries \( C \) below:
   - Hash query. Input the hash queries adaptively, \( C \) responds the corresponding hash values to \( A \).
   - Tag query. Input the medical/health block \( F_{i,j} \) for the patient ID\(_j\), \( C \) calculates the tag \( T_{i,j} \leftarrow \text{TagGen}(x_j, F_{i,j}) \) and sends it to \( A \). Without loss of generality, let \( \{F_{i,j}, T_{i,j}\} \) be the queried block-tag pair set and \( \mathcal{I}_1 = \{i, j\} \) in First-Phase Queries.

3. Challenge: \( C \) generates a data integrity challenge \( \text{chal}_p \) which defines the challenged block-tag pair index collection \( \mathcal{I}_2 = \{\{i, j\}, \{i_2, j_2\}, \cdots, \{i_c, j_c\}\} \), where \( \mathcal{I}_o \not\subseteq \mathcal{I}_1 \) and \( c \) is a positive integer. \( C \) is queried to prove the proof of integrity checking for the medical/health blocks \( F_{i_o,j_o}, \cdots, F_{i_c,j_c} \).

4. Second-Phase Queries: Similar to First-Phase Queries. Let the queried medical/health block-tag pair set be \( \{F_{i,j}, T_{i,j}\} \) and \( \mathcal{I}_2 = \{i, j\} \) in Second-Phase Queries. The restriction is that \( \mathcal{I}_o \not\subseteq \mathcal{I}_2 \).

5. Forge: Finally, \( A \) forges a data integrity proof \( \text{V}_p \) for the medical/health blocks indicated by \( \text{chal}_p \) and returns \( \text{V}_p \) to \( C \).

In the above ICS game, we say \( A \) wins if
\[
\Pr \left[ \text{CheckProof}(y, X_1, Y, Z, \text{chal}_p, \text{V}_p, \text{ID}_j \in \mathcal{P}) \right] \Rightarrow \text{"success"} \geq \frac{1}{p(k)}
\]
where \( p(k) \) is a polynomial of the security parameter \( k \).

Definition 3 (Restrictive Integrity Checking). In the remote medical/health data integrity checking, only the following restrictive entities have the ability to perform the data integrity checking protocol:

1. The hospital can perform the remote medical/health data integrity checking for all the patients.
2. The individual patient can perform the integrity checking only for his own remote medical/health data.
3. Except the hospital, patient and PCS, the other entity cannot perform the remote medical/health data integrity checking.

Definition 4 (Restrictive Retriviality). In the remote medical/health data retrievability, the patient ID\(_j\) creates the retrievability control set \( \mathcal{R} = \{R_{1,j}, R_{2,j}, \cdots, R_{h,j}\} \). It satisfies the following requirements:

1. The patient ID\(_j\) can retrieve his own remote medical/health data by himself, i.e., \( \{ID_j\} \in \mathcal{R} \).
2. For the other retrievability control set \( \mathcal{R} \), the entities in \( R_{i,j} \) can cooperate to retrieve ID\(_j\)’s remote medical/health data under the help of the hospital.
3. For any entity set \( \mathcal{R} \), if \( R_{j} \not\subseteq \mathcal{R} \) for every \( 1 \leq i \leq h_j \), the entities in \( S_A \) cannot retrieve ID\(_j\)’s remote medical/health data even if they collude.

A secure ICS protocol also needs to guarantee that after validating the PCS-generated proof, the verifier can also be convinced that all of his outsourced data has been kept intact with a high probability. The following security definition gives the security property.

Definition 5 ((\( \rho, \delta \)) Security). An ICS protocol is \((\rho, \delta)\)-secure if PCS corrupted \( \rho \) fraction of the whole medical/health data, the probability that the corrupted blocks are detected is at least \( \delta \).

2.2 Bilinear Pairings and Difficult Problems

Let \( G_1 \) and \( G_2 \) be two cyclic multiplicative groups with the same prime order \( q \). Let \( \tilde{\epsilon} : G_1 \times G_1 \rightarrow G_2 \) be a bilinear map. \( \tilde{\epsilon} \) can be constructed by the modified Weil or Tate pairings on elliptic curves [18], [19]. The group with such a map \( \tilde{\epsilon} \) is called a bilinear group, on which the Computational Diffie-Hellman (CDH) problem is assumed hard while the Decisional Diffie-Hellman (DDH) problem is easy [20].

Definition 6 (Gap Diffie-Hellman (GDH) Group). Let \( g \) is the generator of \( G_1 \). Given \( g, g^a, g^b, g^c \in G_1 \) while \( a, b, c \in \mathbb{Z}_q^* \) are unknown, it is recognized that there exists an efficient algorithm to determine whether \( ab \equiv c \mod q \) holds by verifying \( \tilde{\epsilon}(g^a, g^b) = \tilde{\epsilon}(g, g^c) \) in polynomial time (DDH problem), while there exist no efficient algorithms to compute \( g^{ab} \in G_1 \) with non-negligible probability within polynomial time (CDH problem). An algorithm \( A \) is said to \((t, \epsilon)\)-break the CDH problem on \( G_1 \) if \( A \) runs in time at most \( t \), and the following CDH advantage is at least \( \epsilon \).

\[
\text{Adv}^{CDH}_A = \Pr[A(g, g^a, g^b) \rightarrow g^{ab} : \forall a, b \in \mathbb{Z}_q^*] \geq \epsilon
\]
The probability is taken over the choice of \( a, b \) and \( A \)’s coin tosses. A group \( G_1 \) is a \((t, \epsilon)\)-GDH group if the DDH problem on \( G_1 \) is efficiently computable and no algorithm \((t, \epsilon)\)-breaks the CDH problem on \( G_1 \).

Definition 7 (Bilinear Diffie-Hellman Problem (BDHP) assumption). Given \( g, g^a, g^b, g^c \) for unknown \( a, b, c \in \mathbb{Z}_q^* \), it is difficult to compute \( W = \tilde{\epsilon}(g, g)^{abc} \in G_2 \).
3. Our Proposed Pairing-Based ICS Protocol

3.1 ICS Protocol Construction

Our ICS protocol consists of seven phases: (SetUp, EncTagGen, CheckTagSign, GenProof, GenRetr, CheckProof, Retrieval) among PCS, Hospital, Patient, and AuthSet. Suppose there are \( n_p \) patients whose set is denoted as \( \mathcal{P} \), i.e., \( \mathcal{P} = \{D_{1j}, D_{2j}, \ldots, D_{nj}\} \). Suppose the patient \( ID_j \) will upload \( n_j \) block-tag pairs. Denote the corresponding block-patient index set as \( \mathcal{B} \times \mathcal{P} = \{(i, j), 1 \leq j \leq n_p, 1 \leq i \leq n_j\} \). Let \( n \) denote the whole block number, i.e., \( n = \sum_{i=1}^{n_p} n_j \). Let \( f \) and \( \Omega \) be two pseudo-random functions, and let \( \pi \) be a pseudo-random permutation. Let \( H, h \) be two cryptographic hash functions. They are described below:

\[
\begin{align*}
  f : \mathbb{Z}_q^* \times \{1, 2, \ldots, n\} & \rightarrow \mathbb{Z}_q^*, \\
  \Omega : \mathbb{Z}_q^* \times (\mathcal{B} \times \mathcal{P}) & \rightarrow \mathbb{Z}_q^* \\
  \pi : \mathbb{Z}_q^* \times \{1, 2, \ldots, n\} & \rightarrow \mathcal{B} \times \mathcal{P} \\
  H : \mathbb{G}_2 \times \{0, 1\}^* & \rightarrow \mathbb{G}_1^*, \quad h : \mathbb{Z}_q^* \rightarrow \mathbb{G}_1^*
\end{align*}
\]

Let \( g \) be a generator of \( \mathbb{G}_1 \). Without loss of generality, we only consider the patient \( ID_j \) in the concrete scheme construction. Denote \( ID_j \)'s medical/health data as \( M_j \). The patient \( ID_j \) picks a random \( x_j \in \mathbb{Z}_q^* \) as his private key and computes \( X_j = g^{x_j} \) as his public key. On the other hand, \( ID_j \) picks a random \( s_j \in \mathbb{Z}_q^* \) as its symmetric encryption/decryption key. The hospital picks a random number \( y \in \mathbb{Z}_q^* \) as its private key and computes \( Y = g^y \) as its public key. PCS picks a random number \( z \in \mathbb{Z}_q^* \) as its private key and computes \( Z = g^z \) as its public key. The phases of our proposed ICS protocol are described below.

SetUp: The patient \( ID_j \) delegates his remote medical/health data retrieval capability to the authorized entity set AuthSet. Suppose that \( n_s \) entities share \( ID_j \)'s symmetric key and \( th_j \) entities can retrieve \( ID_j \)'s remote medical/health data by cooperating with the hospital. Let the authorized entity set be \( \text{AuthSet}_j = \{D_{j1}, D_{j2}, \ldots, D_{jth_j}\} \) and \( D_{jj} \in \mathbb{Z}_q^* \) (it can be realized by using the hash function \( \mathbb{H} : \{0, 1\}^* \rightarrow \mathbb{Z}_q^* \)). Let \( \text{Sign}, \text{Verify} \) be secure signature/verification algorithm pairs. In order to restrict the authorized entities' behaviors, for every entity \( D_{jj} \), \( ID_j \) creates the warrant \( \omega_j \) and \( \text{Sign} (\omega_j) \) by using his own private key \( x_j \). The warrant \( \omega_j \) describes the rules which must be obeyed by \( D_{jj} \). For the symmetric encryption key \( s_j \), \( ID_j \) generates the corresponding shares below.

1. Pick the random \( a_{1j}, a_{2j}, \ldots, a_{nj} \in \mathbb{Z}_q^* \) and get the following polynomial with the order \( th_j - 1 \):

\[
F_j(x) = s_j + \sum_{i=1}^{th_j-1} a_{ij}x^i
\]

2. Compute the share \( ss_{jj} = F_j(D_{jj}) \) for every entity \( D_{jj} \). Then, \( ID_j \) sends \( (ss_{jj}, \omega_j, \text{Sign}(\omega_j)) \) to \( D_{jj} \).

3. Every entity \( D_{jj} \) verifies whether the warrant-signature pair \( (\omega_j, \text{Sign}(\omega_j)) \) is valid. If it is valid, \( D_{jj} \) keeps the warrant-signature pair \( (\omega_j, \text{Sign}(\omega_j)) \) and the corresponding secret share \( ss_{jj} \) of the symmetric encryption/decryption key \( s_j \) of the patient \( ID_j \).

Finally, \( ID_j \) picks a public random element \( u_j \in \mathcal{G}_1^* \). The final system parameters are

\[
\text{params} = \{(G_1, G_2, \hat{\epsilon}, f, \Omega, h, x_j, Y, Z, u_j, q, ID_j \in \mathcal{P}) \}
\]

EncTagGen \((x_j, s_j, M_j, \Omega, Y, Z)\): After finishing the medical/health advices, the patient \( ID_j \) gets his own medical/health data \( M_j \). Taking use of the symmetric encryption algorithm, \( ID_j \) gets the ciphertext \( F_j = E_{sk_j}(M_j) \). Then, \( F_j \) is divided into \( n_j \) blocks, i.e., \( F_j = (F_{1j}, F_{2j}, \ldots, F_{nj}) \). For the block \( F_{ij} \), the patient \( ID_j \) computes \( t_{ij} = H(\hat{\epsilon}(Y, Z)^{t}, \omega_j) \) and \( \hat{W}_{ij} = \Omega_j(i, j) \); then, it outputs the block-tag pair \( (F_{ij}, t_{ij}) \).

When the above procedures are performed \( n_j \) times, all the block-tag pairs are created. At last, the patient \( ID_j \) uploads his block-tag pairs collection \( \{(F_{ij}, t_{ij}), 1 \leq i \leq n_j\} \) and the warrant-signature pairs \( (\omega_j, \text{Sign}(\omega_j)) \) to PCS. PCS stores the block-tag pairs and the warrant-signature pairs \( (\omega_j, \text{Sign}(\omega_j)) \). The patient deletes these block-tag pairs \( \{(F_{ij}, t_{ij}), 1 \leq i \leq n_j\} \) from its local storage.

CheckTagSign \((z, F_{1j}, F_{2j}, \ldots, F_{nj}, t_{1i}, t_{2i}, \ldots, t_{ni})\): Upon receiving \( (\omega_j, \text{Sign}(\omega_j)) \), PCS verifies its validity by using the corresponding verification algorithm \( \text{Verify} \). If it is invalid, output “failure”. Otherwise, for every \( 1 \leq i \leq n_j \), PCS computes \( t_{ij} = H(\hat{\epsilon}(X_j, Y)^{t}, \omega_j) \) and \( \hat{W}_{ij} = \Omega_j(i, j) \). Then, it verifies whether the following formula holds: \( \hat{e}(T_{ij}, g) = \hat{\epsilon}(h(W_{ij})^{F_{ij}}, X_j) \). If it holds, then PCS accepts it. Otherwise, PCS rejects it and responds “failure”.

GenProof \((F, \text{chal}_p, \Sigma)\): Let the challenge be \( \text{chal}_p = (c, k_1, k_2) \) where \( 1 \leq c \leq n \), \( k_1 \in \mathbb{Z}_q^* \), \( k_2 \in \mathbb{Z}_q^* \). Let \( F \) be the set of the blocks. Let \( \Sigma \) be the set of the tags. The hospital queries PCS for medical/health data integrity proof of \( c \) file blocks. \( k_1 \) is used as the random key of the pseudo-random permutation \( \pi \). \( k_2 \) is used as the random key of the pseudo-random function \( f \). PCS performs the procedures below.

1. For \( 1 \leq i \leq c \), PCS computes the indexes and coefficients below: \( (I_{ij}, j) = \pi_k(i), a_i = f_{k_2}(i) \)

2. The set \( \{(I_{ij}, j), 1 \leq i \leq c\} \) is divided into many subsets \( S_j \) based on the different patients. For the same patient \( ID_j \), let \( S_{ij} \) be the subset \( \{(I_{ij}, j), j \text{ is constant}, 1 \leq i \leq c\} \). Thus, \( S_{ij} \) describes the challenged medical/health data blocks of the patient \( ID_j \). Denote \( S = \{S_{ij}, 1 \leq i \leq c\} \).

Note: For the different \( i \), maybe, the mapped \( j \) are the same, i.e., there exist more challenged blocks for the patient \( ID_j \). Of course, maybe, there doesn’t exist challenged blocks for some patients.

3. For \( 1 \leq i \leq c \), compute
\[
T = \prod_{i=1}^{c} T_{i,j}^{a_i}, \quad \hat{F}_j = \sum_{(i,j) \in S_j} a_i F_{i,j,}n
\]

4. Denote \( \hat{F} = \{ \hat{F}_j, S_j \in S \} \). Output \( V = (\hat{F}, T) \) to the hospital.

GenRetr(\( F, cha_r, \Sigma \)): Suppose the patient ID\( j \) wants to retrieve his own medical/health data blocks \((I_1, j), (I_2, j), \ldots, (I_c, j)\). ID\( j \) sends the challenge \( cha_l = (\{I_1, j), (I_2, j), \ldots, (I_c, j, k_2\}) \) where \( k_2 \in Z^*_2 \). Upon receiving the retrieval challenge \( cha_l \), from the patient ID\( j \), PCS performs the procedures below:

1. For \( 1 \leq i \leq c \), compute the coefficients: \( a_i = f_{k_2}(i) \).
2. For \( 1 \leq i \leq c \), compute \( T = \prod_{i=1}^{c} T_{i,j}^{a_i} \).
3. Output \( V_r = (F_{i,j}, F_{i,j}, \ldots, F_{i,j}, T) \) to ID\( j \).

When the hospital and AuthSet cooperate to query PCS to retrieve the patient ID\( j \)'s medical/health data, they sends the challenge \( cha_l = (\omega_j, \text{Sign}(\omega_j), (I_1, j), (I_2, j), \ldots, (I_c, j, k_2)) \) to PCS. PCS verifies the warrant-signature pair \((\omega_j, \text{Sign}(\omega_j))\). If it is valid and the query complies with the warrant \( \omega_j \), PCS performs the same procedures as ID\( j \)'s retrieval query. Otherwise, rejects it.

CheckProof(\( y, X_j, Y, Z, cha_l, V_r, ID_j \in \mathcal{P} \)): Upon receiving the response \( V_r \) from PCS, the hospital performs the procedures below:

1. For \( 1 \leq i \leq c \), compute the indexes and coefficients below: \((I_1, j), a_i = f_{k_2}(i)\).
2. For \( 1 \leq i \leq c \), compute \( \hat{t}_j = H(\hat{t}(X_j, Y, \omega_j)); \)
3. Check whether the following formula holds.

\[
\hat{e}(T, g) = \prod_{I_i} \hat{e} \left( \prod_{(I_i, j) \in S_i} h(\Omega_{I_i}(I_i, j))^{a_i} u_i^{I_i,j}, X_j \right)
\]

(1)

If (1) holds, then the hospital outputs “success”. Otherwise, the hospital outputs “failure”.

Retrieval(\( x_j, sk_j \) or \( y, sk_j \)'s valid share set), \( X_j, Y, Z, cha_l, V_r \)): The two cases can be considered. (1) The patient ID\( j \) retrieves his own medical/health data. (2) The hospital and AuthSet cooperate to retrieve ID\( j \)'s medical/health data.

The first case, ID\( j \) retrieves his own medical/health data below:

1. For \( 1 \leq i \leq c \), compute the coefficients: \( a_i = f_{k_2}(i) \).
2. Compute \( \hat{F}_j = \sum_{i=1}^{c} a_i F_{i,j} \), \( t_j = H(\hat{t}(X_j, Y, \omega_j)) \).
3. Check whether the following formula holds.

\[
\hat{e}(T, g) = \hat{e} \left( \prod_{i=1}^{c} h(\Omega_{I_i}(I_i, j))^{a_i} u_i^{I_i,j}, X_j \right)
\]

(2)

If the formula (2) holds, the patient ID\( j \) accepts the blocks \( F_j = \{ F_{i,j}, F_{i,j}, \ldots, F_{i,j} \} \). Then, the corresponding plaintext \( M_j = D_{sk_j}(F_j) \) can be retrieved by using the symmetric encryption key \( sk_j \). Otherwise, the patient ID\( j \) rejects the response.

The second case, in the authorized set AuthSet, suppose that \( th_j \) entities agree to retrieve the patient ID\( j \)'s medical/health data. Let the \( th_j \) entities be \( D_{i,j_1}, D_{i,j_2}, \ldots, D_{i,j_{th_j}} \). Under the help of the hospital, they cooperate to perform the steps below:

1. For \( 1 \leq i \leq c \), compute the coefficients: \( a_i = f_{k_2}(i) \). After that, it computes \( \hat{F}_j = \sum_{i=1}^{c} a_i F_{i,j} \), \( t_j = H(\hat{t}(X_j, Y, \omega_j)) \).
2. Check whether the following formula holds.

\[
\hat{e}(T, g) = \hat{e} \left( \prod_{i=1}^{c} h(\Omega_{I_i}(I_i, j))^{a_i} u_i^{I_i,j}, X_j \right)
\]

(3)

If the formula (3) holds, they accept the blocks \( F_j = \{ F_{i,j}, F_{i,j}, \ldots, F_{i,j} \} \) by using their own shares, these \( th_j \) entities can compute \( sk_j \).

\[
sk_j = \sum_{i=1}^{th_j} \left( \prod_{j \in \mathcal{E}_j} -D_{j,k_i} -D_{j,k_i} \right) x_{j_i}
\]

The corresponding plaintext \( M_j = D_{sk_j}(F_j) \) can be retrieved by using the symmetric encryption key \( sk_j \). Otherwise, they reject the response.

3.2 Security Analysis

The correctness analysis and security analysis of our proposed ICS protocol are given by the lemmas and theorems below:

**Theorem 1.** If the patient ID\( j \), hospital and PCS are honest and follow the proposed procedures, then any block-tag pair can pass PCS’s tag checking, i.e., CheckProof satisfies the correctness.

*Proof.* Since \((\text{Sign}, \text{Verify})\) is secure signature-verification algorithm pair, and \((\omega_j, \text{Sign}(\omega_j))\) is valid warrant-signature pair, thus, \((\omega_j, \text{Sign}(\omega_j))\) can pass the verification. According to the phases of EncTagGen and CheckTagSign, the following formulas hold:

\[
\begin{align*}
\hat{t} = H(\hat{t}(X_j, Y, \omega_j)) = H(\hat{t}(X_j, Y, \omega_j)) = t \\
\hat{W}_{i,j} = \Omega_{I_i}(I_i, j) = \Omega_{I_i}(I_i, j) = W_{i,j} \\
\hat{e}(T_{i,j}, g) &= \hat{e}(h(W_{i,j})u_i^{I_i,j}, g) \\
&= \hat{e}(h(W_{i,j})u_i^{I_i,j}, g) = \hat{e}(h(W_{i,j})u_i^{I_i,j}, X_j)
\end{align*}
\]

**Theorem 2.** If hospital and PCS are honest and follow the proposed procedures, the response \( V_r \) can pass the hospital’s data integrity checking, i.e., CheckProof satisfies the correctness.

*Proof.* Let the challenge be \( cha_l = (c, k_1, k_2) \). According to the phases of EncTagGen and GenProof, we know that \( \hat{t} = \)
\[ H(\hat{e}(X_j, Z)^r, \omega_j) = H(\hat{e}(Y, Z)^{y_j}, \omega_j) = t_j, \ \hat{W}_{i,j} = \Omega_i(i, j) = \Omega_i(i, j) = W_{i,j}. \]  
Thus, 
\[ \hat{e}(T, g) = \hat{e} \left( \prod_{i=1}^c T_{i,j}^{a_i} \right) \]
\[ = \hat{e} \left( \prod_{S_i \subseteq S, (i,j) \in S} T_{i,j}^{a_i} \right) \]
\[ = \hat{e} \left( \prod_{S_i \subseteq S, (i,j) \in S} (h(W_{i,j})u_j^F_{i,j})_{\alpha_{x_i}}, g \right) \]
\[ = \prod_{S_i \subseteq S} \hat{e} \left( \prod_{(i,j) \in S_i} (h(W_{i,j})u_j^F_{i,j})_{\alpha_{x_i}}, g_{x_i} \right) \]
\[ = \prod_{S_i \subseteq S} \hat{e} \left( h(\Omega_i(i, j))^\alpha_{x_i}, X_{j} \right) \]

\[ \hat{e}(T, g) = \prod_{(i,j) \in S} \hat{e} \left( h(\Omega_i(i, j))^\alpha_{x_i}, X_{j} \right) \]

Thus, the proposed ICS protocol satisfies restrictive proof of integrity.

\[ \square \]

**Theorem 3.** If the patient ID (or hospital and AuthSet) and PCS are honest and follow the proposed procedures, IDj (or hospital and AuthSet) can retrieve the queried medical/health data, i.e., Retrieval satisfies the correctness.

**Proof.** When the patient IDj queries to retrieve his own medical/health data, the verification formula (2) holds based on the theorem 2. Then, it is straightforward to get the medical/health data by decrypting the ciphertext using his own symmetric encryption key skj.

When the hospital and AuthSetj cooperate to retrieve IDj’s medical/health data, by Lagrange interpolation formula, the skj can be obtained below:

\[ sk_j = \sum_{i=1}^{t_{j1}} \left( \sum_{j_{1,1} \in R} \frac{-D_{j_{1,1}}}{D_{j_{1,1}} - D_{j_{1,2}}} \right) s_{j_{1,2}} \]

After that, since \( t_j = H(\hat{e}(X_j, Z)^r, \omega_j) = H(\hat{e}(Y, Z)^{y_j}, \omega_j) \), they can also get IDj’s medical/health data by performs the similar procedures as the patient IDj.

\[ \square \]

**Theorem 4 (Possession Against Malicious PCS).** On the GDH group G1, based on the difficulty of CDH problem, the proposed ICS protocol is existentially unforgeable in the random oracle model. That is, the proposed ICS protocol satisfies the security property of provable data integrity against malicious PCS.

**Proof.** It is similar with the Ref. [10]. We omit it due to the page limits.

\[ \square \]

**Theorem 5 (Restrictive Proof of Possession).** For the remote medical/health data, the proposed ICS protocol satisfies restrictive proof of integrity.

**Proof.** From the theorem 2, the hospital can perform all the patients’ medical/health data integrity checking. For the patient IDj, he can compute the parameter tj and Wj. Based on the two parameters, IDj can perform the proof of his own medical/health data integrity below: \( \hat{e}(T, g) = \hat{e} \left( \prod_{(i,j) \in S} h(\Omega_i(i, j))^\alpha_{x_i}, X_{j} \right) \).

Except for the hospital, the patients and PCS, the third party has no ability to get tj based on the difficulty of BDHP. Thus, the third party can not also compute \( \Omega_i(i, j) \). Finally, the third party can not perform the verification equation:

\[ \hat{e}(T, g) = \prod_{(i,j) \in S} \hat{e} \left( h(\Omega_i(i, j))^\alpha_{x_i}, X_{j} \right) \]

Thus, the proposed ICS protocol satisfies restrictive proof of integrity.

\[ \square \]

**Theorem 6 (Restrictive Retrievability).** For the remote medical/health data, the proposed ICS protocol satisfies the property of restrictive retrievability.

**Proof.** From the theorem 3, the patients have the ability to retrieve their own medical/health data. In the patient IDj’s authorized entities, if at least \( t_{j1} \) entities agree to retrieve IDj’s remote medical/health data, these authorized entities and the hospital have the ability to cooperate to retrieve IDj’s remote medical/health data.

On the contrary, if less than \( t_{j1} \) authorized entities agree to retrieve IDj’s data, they only succeed with negligible probability. According to the process of symmetric encryption key distribution, the function \( F_j \) has the order \( t_{j1} - 1 \). It can be determined by at least \( t_{j1} \) points. Less than \( t_{j1} \) authorized entities can provide less than \( t_{j1} \) points. \( F_j \) can not be determined and the symmetric encryption key skj can not also be determined. Thus, they have no ability to retrieve IDj’s remote medical/health data.

\[ \square \]

**Theorem 7.** The proposed ICS protocol is \( \left( \frac{d}{n}, 1 - \left( \frac{n - d}{n} \right)^c \right) \)-secure since the probability \( P_R \) of detecting the corruption satisfies:

\[ 1 - \left( \frac{n - d}{n} \right)^c \leq P_R \leq 1 - \left( \frac{n - c + 1 - d}{n - c + 1} \right)^c \]

where PCS has stored \( n = n_1 + n_2 + \cdots + n_p \) block-tag pairs for \( n_p \) patients, PCS has corrupted \( d \) block-tag pairs, and the challenge is \( \text{chal}_p = (c, k_1, k_2) \).

**Proof.** It is similar with Ref. [9]. We omit it due to the page limits.

\[ \square \]

4. Performance

We implemented our ICS scheme in order to demonstrate the effectiveness of our scheme. We used the C programming language with the GMP (GMP-5.0.5), Miracl and PBC (pbc-0.5.13) libraries. In the implementation, PCS ran on the laptop with the following features:

- CPU: Intel Core i7-3517U @ 1.90GHz
- Physical Memory: 4GB DDR3 1600MHz
6. Conclusions

In this paper, we propose the concept of ICS protocol for critical patients in cloud-based health internet of things. This paper formalizes the system model and security model of ICS protocol. Based on the pairing, a concrete ICS protocol is designed. The proposed ICS protocol is provably secure and efficient by security analysis and performance analysis.

Acknowledgments

The work of H. Wang was supported in part by the National Natural Science Foundation of China under Grant (61272522), in part by the Natural Science Foundation of Liaoning Province under Grant (2014020147), and in part by the Program for Liaoning Excellent Talents in University under Grant (LR2014021), and in part by the CICAET fund and the PAPD fund. This work of K. Li was partly supported by the National Science Foundation for Distinguished Young Scholars of China (61225010), and the State Key Program of National Natural Science of China (61432002).

References


Huaquun Wang received the BS degree in mathematics education from the Shandong Normal University, Jinan, China, in 1997, the MS degree in applied mathematics from the East China Normal University, Shanghai, China, in 2000, and the PhD degree in cryptography from Nanjing University of Posts and Telecommunications, Nanjing, China, in 2006. Since then, he has been with Dalian Ocean University, Dalian, China, as a Full Professor. His research interests include cryptography, network security, and cloud computing security. Dr. Wang has published more than 50 papers. He has served in the program committee of several international conferences and the editor board of international journals.

Keqiu Li received the bachelor’s and master’s degrees from the Department of Applied Mathematics, Dalian University of Technology in 1994 and 1997, respectively. He received the PhD degree from the Graduate School of Information Science, Japan Advanced Institute of Science and Technology in 2005. He also has a two-year postdoctoral experience in the University of Tokyo, Japan. He is currently a professor in the School of Computer Science and Technology, Dalian University of Technology, China. He has published more than 100 technical papers, such as IEEE TPDS, ACM TOIT, and ACM TOMCCAP. He is an associate editor of IEEE TPDS and IEEE TC. His research interests include internet technology, data center networks, cloud computing and wireless networks. He is a senior member of the IEEE.

Kaoru Ota received M.S. degree in Computer Science from Oklahoma State University, USA in 2008 and Ph.D. degree in Computer Science and Engineering from The University of Aizu, Japan in 2012. She is currently an Assistant Professor with Department of Information and Electronic Engineering, Muroran Institute of Technology, Japan. From March 2010 to March 2011, she was a visiting scholar with BBCR group at University of Waterloo, Canada. Also she was a Japan Society of the Promotion of Science (JSPS) research fellow with Kato-Nishiyama Lab at Graduate School of Information Sciences at Tohoku University, Japan from April 2012 to April 2013. She has joined JSPS A3 foresight program as one of primary researchers since 2011 which is supported by Japanese, Chinese and Korean government. Dr. Ota’s research results have been published in 90 research papers in international journals, conferences and books. She is the Best Paper Award Winner of ICA3PP 2014, GPC 2015 and IEEE DASC 2015. She serves a Guest Editor of IEEE Wireless Communications, IEICE Transactions on Information and Systems and serves Editor of Peer-to-Peer Networking and Applications (Springer), Ad Hoc & Sensor Wireless Networks, International Journal of Embedded Systems (InderScience). Her research interests include wireless sensor networks, vehicular ad hoc networks, and ubiquitous computing.

Jian Shen received the B.E. degree from Nanjing University of Information Science and Technology, Nanjing, China, in 2007 and the M.E. and Ph.D. degrees in Computer Science from Chosun University, Gwangju, Korea, in 2009 and 2012, respectively. Since late 2012, he has been a faculty member in the School of Computer and Software at Nanjing University of Information Science and Technology, Nanjing, China. His research interests include computer networking, security systems, mobile computing and networking, ad-hoc networks and systems, and ubiquitous sensor networks.