Secure and Efficient Data Aggregation Scheme with Fine-Grained Access Control and Verifiability for CWBANs

Xuefeng Fang, Qingqing Gan, Xiaoming Wang

Department of Computer Science, Jinan University, China
xuefeng_f@foxmail.com, gan_qingqing@foxmail.com, wxmsq@eyou.com

Abstract

To protect the patient's privacy in cloud-assisted wireless body area networks (CWBANs), this paper proposes a secure and efficient health data aggregation scheme with fine-grained access control and verifiability. Our scheme can not only make patients get rid of worries about the privacy for their health data, but also achieve secure fine-grained access control by employing ciphertext-policy attribute based encryption (CP-ABE). To enable CP-ABE to be effectively used in CWBANs, we outsource the burdensome computational task of CP-ABE to cloud server, which results in a significant reduction on computing overhead for the sensors or the data sink. In our scheme, the huge amount of health data collected by the sensors are efficiently aggregated with confidentiality at the data sink, then forwarded to the cloud server, which significantly reduces the transmission cost from the data sink to the cloud server. Moreover, our scheme allows the data sink and doctors to check whether the transformation process is performed correctly. As a result, the attacker's malicious behaviors and incorrect data in the transformation can be detected in our scheme. The security analysis and performance evaluation show our scheme is secure and efficient.

Keywords: WBANs, Data aggregation, Confidentiality, Fine-grained access control, Verifiability

1 ntroduction

In recent years, cloud-assisted wireless body area networks (CWBANs) are widely applied in healthcare domains. Patients wear the portable sensors and wearable devices to measure their physiology data, such as temperature, blood pressure, electroc ardio graph and so on. And later the sensor devices send the health data to remote cloud servers for further processing via a data sink (smartphone or other terminals). However, data privacy and security problems have become major concerns for individuals and organizations using such service. Due to the health information transmitted through an open channel, an adversary can easily capture the health information to modify or reveal sensitive information. Failure to obtain correct medical data will result in wrong medical diagnosis and treatment. More importantly, if the health's data is illegally leaked, the privacy of the patients is broken and even the health data can be misused. Therefore, it is important to provide a secure communication environment.

One method for alleviating the aforementioned problems is to transmit and store data in encrypted form. To protect the data privacy, all communications between sensors and cloud server or cloud server and doctors are encrypted. Generally, there are two types of encryption technology: symmetric encryption and asymmetric encryption. Considering the limited power budget and communication ability of body sensors, symmetric encryption can be regarded as a better choice. However, the key-distribution process in symmetric encryption is challenging, which brings considerable storage and computational overhead on body sensors and violates the principle of plugandplay on resource-constrained WBANs [6]. What's more, symmetric encryption severely limits the ability of users to selectively share their encrypted data at a fine-grained level because it involves some challenging issues, such as key-management and access control. But in CWBANs, it is essential to provide a fine-grained access control with confidentiality to ensure the security and privacy of patients, since the patients' health data should be accessed by medical professionals from anywhere via Internet. Here we consider a scenario: a particular patient wants to distribute his sensitive data, such as his disease and family history, to the authorized doctors, while other information such as healthy diet and physical exercise to some professional researchers. In this case, it is imperative to provide a fine-grained access control with confidentiality.

CP-ABE can provide a fine-grained access control with confidentiality, and is widely used for access control of encrypted data stored in cloud. However, it is well known that there are high encryption/decryption cost and relatively large ciphertext size in the existing CP-ABE schemes. Obviously CP-ABE cannot be directly and effectively used in CWBANs since the

*Corresponding Author: Xiaoming Wang; E-mail: wxmsq@eyou.com
DOI: 10.3966/160792642019052003010

energy, storage and computing power of sensors are limited. Therefore, the computational cost and communication cost are two important factors that should be considered when developing CP-ABE schemes in CWBANs. How to build an aggregated mechanism with confidentiality and fine-grained access control for the health data becomes a great challenge.

Moreover, the system may occur malfunction or send the data of incorrect form, thus the data sink and the doctors may have received some wrong data as well as the doctors may make a mistake treatment for the patient based on the incorrect data. These issues could be very serious or even catastrophic. Therefore, we should consider a new requirement for the aggregated scheme: verifiability. The verifiability can guarantee the transformation to be done correctly.

To address the above described research challenges, we present a secure and efficient health data aggregation scheme with fine-grained access control and verifiability for CWBANS. Our contribution can be summarized as follows:

(1) Our scheme can not only make patients dispel worries about the privacy of their health data, but also achieve secure fine-grained access control by employing CP-ABE. In our scheme, we shift the burdensome computational task of CP-ABE from sensors to cloud servers by outsourcing encryption operations, which results in a significant reduction on computing overhead for the sensor or data sink. This enables CP-ABE to be effectively used in CWBANs.

(2) In our scheme, the huge amount of health data collected by the sensors are efficiently aggregated with confidentiality at the data sink and then be sent to the cloud server, which significantly reduces the transmission cost from the data sink to the cloud server. More importantly, the data aggregation is performed directly on blinded data at the data sink without eliminating blindness, thus ensuring the data security on the data sink and minimizing the trust that is usually put on the data sink.

(3) In order to guarantee the correction of the health data transformation, our scheme can achieve verifiability and allow the data sink and the doctors to check whether the transformation is done correctly in CWBANS. As a result, the attacker's malicious behaviors and incorrect data in the transformation can be detected in our scheme.

(4) We analyze the security of our scheme, and obtain the fact that our scheme is secure. Also we evaluate the performance of our scheme and compare our scheme with the previous schemes in terms of encryption computational overhead at sensors, data sink and cloud server. The performance analysis and experiment results show our scheme has higher efficiency.

The rest of the paper is organized as follows. Section 2 overviews the related work. We present preliminaries and the system model in Section 3. Section 4 gives detailed construction of our scheme. In Section 5, we analyze the proposed scheme in terms of security. And performance of our scheme is evaluated in Section 6. Finally, we conclude this paper in Section 7.

2 Related Work

In the literature, lots of user authentication with session key agreement schemes are widely used to realize access control for WBANs [1-7]. In such schemes, a session key is shared between the sensor node and medical doctor, and personal health information can easily be transmitted through open channel by encrypting the message with the session key. Fortino et al. [1-2] introduced SPINE2 for developing WBANs applications on heterogeneous sensor nodes and further proposed BodyCloud for integrating cloud computing into body sensor networks. Wang and Zhang [3] proposed a secure authentication scheme between patients and doctors using bilinear pairing. Later, Jiang et al. [4] proposed an anonymous authentication scheme based on bilinear pairing. Subsequently, many authentication schemes are formulated for WBANs to improve efficiency (e.g. the schemes [5-10, 32]). However, these authentication protocols can only prevent illegal users from accessing system, while cannot achieve fine-grained access control and data privacy. To protect the data privacy, there also exist many efficient and robust researches that are constructed by symmetric encryption (e.g. the schemes [11-13]). However, these schemes cannot realize the function of fine-grained access control. Furthermore, symmetric encryption involves some challenging issues, such as key-management.

To realize fine-grained access control, Bethencourt et al. [14] introduced the concept of attribute-based encryption (ABE) in public key cryptosystem. The proposed ABE can support complex policies to specify that delegated secret key can decrypt corresponding ciphertext, thus providing a fine-grained access control with confidentiality. Subsequently, there has been an increasing interest in applying ABE to secure personal WBANs (e.g. the schemes [15-19, 34-35]). Nevertheless, most of the works have not considered the computation cost on sensors and limited bandwidth of data transmission from data sink to doctors. With the development of cloud computing technology, cloud servers are used to provide clients with more convenient services because it has large computing and storage capacity. By making use of cloud servers to store large amounts of health data and process them for doctor's diagnosis, the schemes [20-23, 33] based on cloud-assisted WBANs (CWBANs) can provide various services for mobile users and patients. However, security and privacy are becoming significant issues. In order to protect data security and privacy, Guan et al. [24] constructed a specific

signature scheme and securely realized the outsourcing operations for encryption and decryption. Although the scheme can protect patient's health data and reduce the computational cost of encryption and decryption, their scheme has not considered the overhead of communication problems. To save communication overhead, Han et al. [25] introduced a privacy-preserving and multifunctional health data aggregation (PPM-HDA) mechanism with fault tolerance for CWBANs, which realizes health data aggregation. However, this scheme does not achieve fine-grained access control. Hu et al. [26] proposed a data communication protocol between sensors and the data sink/data consumers (doctors or nurses) by employing CP-ABE. In their scheme, a sensor encrypts its body data using a random session key by AES and encrypts the session key using CP-ABE, and then sends the encrypted data to data sink at a regular interval. However, it is well known that CP-ABE requires more expensive computational cost since CP-ABE involves expensive pairing operation and the number of such operation grows with the complexity of the access policy. Therefore, this method is not appropriate for resource-constrained sensors with limited energy, storage and computation power. In addition, their scheme needs to send respectively each data collected by each sensor implanted on a patient body to doctors and other experts. This also results in higher communication cost, and may cause unacceptable communication overhead when the data is collected at high frequency. Thus, this scheme is less suitable to WBANs since the available bandwidth of data transmission is absolute limited.

3 Preliminaries and System Model

In this section, we introduce some preliminary knowledge regarding the cryptographic primitives used in this paper, and formalize the system model.

3.1 Preliminaries

Bilinear Maps [14]: Let G_0 and G_1 be two bilinear groups of prime order p, and g be a generator of G_0, a bilinear map: $e: G_0 \times G_0 \to G_1$ with the following properties.

(1) *Bilinear:* A map $e: G_0 \times G_0 \to G_1$ is bilinear if and only if for all $P, Q \in G_0$ and all $a, b \in Z_p$, we have $e(aP, bQ)=e(P, Q)^{ab}$.

(2) *Non-degeneracy:* The generator g satisfies $e(g, g) \neq 1$.

(3) *Computability:* There is an efficient algorithm to compute $e(P, Q)$ for $\forall P, Q \in G_0$.

Paillier Cryptosystem [27]: The Paillier cryptosystem can achieve the homomorphic properties, which is widely desirable in many privacy-preserving applications [28-29]. Concretely, the Paillier cryptosystem is comprised of three algorithms as follows.

(1) *Key Generation*: Given the security parameter κ_1, two large prime numbers (p_1, q_1) are first chosen, where $|p_1| = |q_1| = \kappa_1$. Then, the RSA modulus $\lambda = lcm(p_1 - 1, q_1 - 1)$ and $n = p_1 q_1$ are computed. After defining a function $L(x) = (x-1)/n$, and choosing a generator $g \in Z_{n^2}^*$, $\mu = (L(g^\lambda \bmod n^2))^{-1} \bmod n$ is further calculated. Then the public key is $pk=(n, g)$, and the corresponding private key is $sk = (\lambda, \mu)$.

(2) *Encryption*: Takes a message $m \in Z_n$ and a random number $r \in Z_n^*$ as inputs, the ciphertext can be calculated as $c = E(m) = g^m \cdot r^n \bmod n^2$.

(3) *Decryption*: Given a ciphertext $c \in Z_{n^2}^*$, the corresponding message can be recovered as $m = L(c^\lambda \bmod n^2) \cdot \mu \bmod n$.

Note that, the Paillier cryptosystem is provably secure against chosen plaintext attack, and the correctness and security can be referred to [27]. The property of Paillier cryptosystem we are most interested in the paper is its additive homomorphism. Given C_{m_1} and C_{m_2} as the paillier ciphertexts for m_1 and m_2, the ciphertext for $(m_1 + m_2)$ can be generated by multiplying C_{m_1} and C_{m_2} denoted as $C_{m_1+m_2} = C_{m_1} \cdot C_{m_2}$, while decrypting $C_{m_1+m_2}$ can obtain $(m_1 + m_2)$.

Access Structure [14]: Let $\{P_1, P_2, ..., P_n\}$ be a set of parties. A collection $\Lambda \subseteq 2^{\{P_1, P_2, \cdots, P_n\}}$ is monotone for $\forall B, C$, if $B \subseteq \Lambda$ and $B \subseteq C$, then $C \subseteq \Lambda$. An access structure (respectively, monotone access structure) is a collection (respectively, monotone collection) Λ of nonempty subsets of $\{P_1, P_2, ..., P_n\}$, i.e., $\Lambda \subseteq 2^{\{P_1, P_2, \cdots, P_n\}} \setminus \{\phi\}$. The sets in Λ are called the authorized sets, and the sets not in Λ are called the unauthorized sets.

In ABE schemes, the role of the parties is taken by the attributes. Thus, the access structure Λ will contain the authorized sets of attributes. Note that the access structure used in our scheme is a monotone access structure.

3.2 System Model

The system model is depicted in Figure 1. There are five major entities in this system: trust authority (TA), sensor, data sink, doctor, cloud server.

TA is fully trust and powerful entity located at healthcare center, which is mainly responsible for the management of the healthcare center, e.g., initializing the system, equipping proper body sensor nodes, updating attribute keys for users.

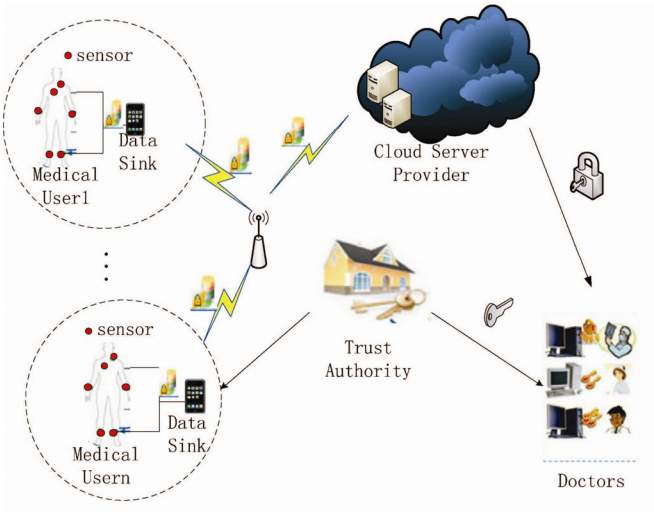

Figure 1. Architecture of wireless body area networks

Sensor is implanted in the deep tissue of a patient body, which periodically collect the patient's health data, and then the data are blinded and forwarded to the data sink.

Data sink aggregates the blinded data received from the sensors implanted in a patient body with confidentiality and then sends the aggregated data to cloud server.

Doctor, who wants to access a patient's health data, will download the patient's data from the cloud server, then decrypt and recover the patient's health records by his private key. To be specific, doctor role can be classified as the professional doctor, nurse, pharmacist, medical researcher and so on. Each role is delegated with one attribute set, and only if his attribute set satisfies the policy, he can decrypt and access the data.

Cloud server, defined as semi-trusted and always online, has abundant storage capacity and computation power.

Based on the system above, we provide an overview of our scheme. Our scheme is comprised of seven algorithms as follows.

(1) $Setup(\chi,\kappa,U,D,w)\rightarrow(PK,MK,SK_i,K)$: Takes as input the security parameters (χ,κ), an attribute universe description U= {1, 2,..., l}, a constant w (the maximum number of the sensors implanted in a patient body is no more than w), and the data type D={D_1, D_2, ..., D_ζ }, where ζ is total types of health data to be collected. It outputs the public parameters PK, a master secret key MK and secret parameters (SK_i, K) where (i=1,2,...,ζ) .

(2) $KeyGen(MK,S,PK)\rightarrow sk_S$: Takes as input the public parameters PK, the master secret key MK and a set of attributes S. It outputs a private key sk_S.

(3) $Blind_{SN}(PK,m_i,SK_i,\gamma_i,TS_i)\rightarrow(s_i,\sigma_i,\eta_i)$: Takes as input the public parameters PK, the secret key SK_i, a random number $\gamma_i\in Z_n^*$, the time stamp TS_i, and a health data m_i. It outputs the blinded data s_i and the verification codes (σ_i,η_i).

(4) $Aggregate(PK,K,s_i,\sigma_i,\eta_i)\rightarrow CT_{AG}$: Takes as input the public parameters PK, the secret key K, the blinded data s_i and the verification codes (σ_i,η_i). It outputs aggregated data CT_{AG} with confidentiality.

(5) $Encrypt_{ABE}(PK,CT_{AG},T)\rightarrow CT$: Takes as input the public parameters PK, the aggregated CT_{AG}, and an access structure T. It outputs a ciphertext CT.

(6) $Decrypt_{ABE}(PK,CT,sk_S)\rightarrow CT_{AG}$: Takes as input the public parameters PK, the private key sk_S and a ciphertext CT. It outputs a message CT_{AG}.

(7) $\mathrm{Recovered}(CT_{AG},sk_S)\rightarrow(m_1,m_2,...,m_w)$: Takes as input the private key sk_S and the ciphertext CT_{AG}. It outputs the health data (m_1, m_2, ..., m_w).

4 Proposed Scheme

In this section, we present the construction of our scheme, which mainly consists of the following seven parts: system initialization, key generation, data blindness, data aggregation, data encryption, data decryption and data recovery.

4.1 System Initialization

The system initialization is performed by TA. Given the security parameters (κ,χ), TA first runs $Setup(\chi,\kappa,U,D,w)$ to initiate the system, and then generates and distributes the public parameters to all the entities in the system. Assuming that the maximum number of the sensors implanted in a patient body is no more than a constant w, and there are total ζ types of health data $D_i(i=1,2,...,\zeta)$ to be collected, where the maximum value of each data type D_i is less than a constant τ .

$Setup(\chi,\kappa,U,D,w)\rightarrow(PK,MK,SK_i,K)$: Takes as input security parameters (χ,κ), an attribute universe description U={1, 2, ..., l}, a constant w and the data type D={D_1, D_2,...., D_ζ }.

It first chooses two large prime numbers (p_1, q_1) with $|p_1|=|q_1|=\kappa$, $n=p_1q_1$, and a super-increasing sequence $\vec{a}$ = (a_1=1, a_2, ..., a_w), where (a_2, ..., a_w) are large primes such that the length $|a_i|\geq\kappa$, $\sum_{j=1}^{i-1}a_j w\tau<a_i$ (i=2,..., ζ), and $\sum_{i=1}^{j-1}a_i w\tau<n$. It defines a function $L(x)=(x-1)/n$, and chooses a generator $\overline{g}\in Z_{n^2}^*$. Then it generates the public key PK_{PC}= {n, $\overline{g}$ } and private key $MK_{PC}=(\vec{a},\lambda,\mu)$, where $\lambda=lcm(p_1-1,q_1-1)$ and $\mu=(L(\overline{g}^{\lambda}\bmod n^2))^{-1}\bmod n$. Next, it chooses a bilinear map $e:G_0\times G_0=G_1$ of prime order p with the generator g, and a secure hash function $H:\{0,1\}^*\rightarrow G_0$. After choosing two random numbers $\alpha,\beta\in Z_p^*$, it has

$PK_{ABE}=\{g,G_0,h=g^{\beta},e(g,g)^{\alpha},H\}$ as the public key and $MK_{ABE}=\{\beta,g^{\alpha}\}$ as the master secret key. Finally, it outputs the system public parameters as $PK=\{PK_{PC},PK_{ABE}\}$ and the corresponding secret key $MK=\{MK_{PC},MK_{ABE}\}$. A random number *K* is chosen and pre-embedded in a data sink. In the same way, the secret parameters $SK_i=\{a_i,K\}(i=1,2,...,\zeta)$ should be pre-embedded in a sensor as the share key.

4.2 Key Generation

$KeyGen(MK,S,PK)\rightarrow sk_S$: The key generation is performed by TA. When a medical doctor registers to TA, the doctor obtains his secret key sk_S such as

$$sk_S=\{\lambda,\mu,\vec{a},V=g^{(\alpha+r)/\beta},\ \forall j\in S: v_j=g^{r}\cdot H(j)^{r_j},v_j^{'}=g^{r_j}\} \quad (1)$$

where *S* is a set of attributes possessed by the doctor, $r,r_j\in Z_p$ are randomly chosen for each attribute $j\in S$.

4.3 Data Blindness

Each sensor implanted in a patient body collects and blinds the patient's health data, then transmits the blinded data to the data sink held by the patient.

$Blind_{SN}(PK,m_i,SK_i,\gamma_i,TS_i)\rightarrow(s_i,\sigma_i,\eta_i)$: The algorithm is performed by the sensor. It chooses a random number $\gamma_i\in Z_n^*$, and blinds the health data m_i using secret parameters $SK_i=(a_i, K)$ pre-embedded in the sensor, and computes the blinded data s_i and the verification codes (σ_i,η_i) such as

$$s_i=a_im_i+\gamma_in \quad (2)$$

$$\sigma_i=H(s_i\,||\,K\,||\,TS_i) \quad (3)$$

$$\eta_i=H(m_i\,||\,a_i) \quad (4)$$

where TS_i is a time stamp, which can resist the potential replay attack, and transmits $(\sigma_i\,||\,s_i\,||\,\eta_i\,||\,TS_i)$ to the data sink.

4.4 Data Aggregation

The data sink aggregates the blinded data received from all sensors implanted in the patient body with confidentiality, and forwards the aggregated data to the cloud server.

$Aggregate(PK,K,s_i,\sigma_i,\eta_i)\rightarrow CT_{AG}$: The algorithm is performed by the data sink. After receiving all $(\sigma_i\,||\,s_i\,||\,\eta_i\,||\,TS_i)$ for *i*=1, 2, ..., *w*, it first checks the validity of the time stamp TS_i and verifies if $\sigma_i=\sigma_i'$, where $\sigma_i'=H(s_i\,||\,K\,||\,TS_i)$. If it does hold, the message s_i is accepted. It aggregates s_i with confidentiality such as.

$$C_i=\overline{g}^{s_i}=\overline{g}^{a_im_i}\cdot\overline{g}^{\gamma_in}\bmod n^2 \quad (5)$$

$$CT'_{AG}=\prod_{i=1}^{w}C_i=\overline{g}^{M}\cdot\gamma^{n}\bmod n^2 \quad (6)$$

$$\eta=H(\eta_1\,||\,\eta_2\,||,..,||\,\eta_w) \quad (7)$$

where $M=\sum_{i=1}^{w}a_i\cdot m_i$, $\gamma=(\prod_{i=1}^{w}\overline{g}^{\gamma_i})$. Let $CT_{AG}=CT'_{AG}\,||\,\eta$, and the data sink sends CT_{AG} to the cloud server.

4.5 Data Encryption

The cloud server encrypts the aggregated data received from the data sink using CP-ABE [14].

$Encrypt_{ABE}(PK,CT_{AG},T)\rightarrow CT$: The algorithm is performed by the cloud server. The aggregated data CT_{AG} is encrypted with an access tree *T* specified by the patient. It first chooses a polynomial q_x for each node x in the tree *T*. These polynomials are chosen as the following way in a top down manner. For each node *x* in the tree, set the degree d_x of the polynomial q_x to be one less than the threshold value k_x of that node, that is, d_x=k_x-1.

Starting with the root node *R*, the algorithm chooses a random $s\in Z_p^*$ and sets $q_R(0)=s$, and d_R random points from Z_p^* to completely define q_R. For any other node *x* in *T*, it sets $q_R(0)=q_{parent(x)}(index(x))$ and chooses d_x points randomly to completely define q_x. Where $index(x)$ denotes a number associated with the node *x*, $parent(x)$ denotes the parent of the node *x* in the tree.

Let *Y* be the set of leaf nodes in *T*. The ciphertext *CT* is then generated by giving the tree access structure *T* as follows:

$$CT=\{T,\overline{C}=C_{AG}\cdot e(g,g)^{\alpha s},C=h^{s},\ \forall y\in Y: C_y=g^{q_y(0)},C'_y=H(att(y))^{q_y(0)}\} \quad (8)$$

where the function $att(y)$ is defined only if *y* is a leaf node and denotes the attribute associated with the leaf node *x* in *T*.

4.6 Data Decryption

The doctor downloads the encrypted data from the cloud server and uses the secret keys corresponding to the matched attributes to recursively decrypt the ciphertext *CT* to obtain the aggregated ciphertext CT_{AG}. The specific processes are as follows.

$Decrypt_{ABE}(PK,CT,sk_S)\rightarrow CT_{AG}$: The doctor obtains the encrypted data *CT* from the cloud server and runs this algorithm to get the aggregated message CT_{AG}. The decryption algorithm is similar to the originally proposed by CP-ABE [14].

We first define a recursive algorithm as following:

Let a node *x* from *T*, and a private key sk_S, which is associated with a set *S* of attributes.

If the node x is a leaf node, let $i = att(x)$, and if $i \in S$, then

$$\begin{aligned} DecryptNode(CT, sk_S, x) &= \frac{e(v_i, C_x)}{e(v_i', C_x')} \\ &= \frac{e(g^r \cdot H(i)^{r_i}, g^{q_x(0)})}{e(g^{r_i}, H(i)^{q_x(0)})} \\ &= e(g,g)^{rq_x(0)} \end{aligned} \quad \textbf{(9)}$$

Otherwise $DecryptNode(CT, sk_S, x) = \perp$.

If the node x is not a leaf node, then for each child node z of the node x, let

$$F_z = DecryptNode(CT, sk_S, z) \quad \textbf{(10)}$$

and let S_x be an arbitrary k_x-sized set of child node z such that $F_z \neq \phi$. If no such set exists then the node was not satisfied and the algorithm returns $\perp$.

Otherwise, computes

$$\begin{aligned} F_x &= \prod_{z \in S_Z} F_z^{\Delta_{i,S_x'(0)}} \\ &= \prod_{z \in S_z} (e(g,g)^{r \cdot q_y(0)})^{\Delta_{i,S_x'(0)}} \\ &= \prod_{z \in S_z} (e(g,g)^{r \cdot q_{parent(z)}(index(z))})^{\Delta_{i,S_x'(0)}} \\ &= \prod_{z \in S_x} e(g,g)^{r \cdot q_x(i) \cdot \Delta_{i,S_x'(0)}} = e(g,g)^{r \cdot q_x(0)} \end{aligned} \quad \textbf{(11)}$$

Where $i = index(z)$ and $S_x' = \{index(z) : z \in S_x\}$, and $\Delta_{i,S_x'(0)}$ is Lagrange coefficient. Finally, the recursive algorithm returns $A = e(g,g)^{rs}$.

Following the doctor obtains the aggregated message:

$$CT_{AG} = \frac{\bar{C}}{e(C,V)/A} \quad \textbf{(12)}$$

4.7 Data Recovery

When the doctor gets the CT_{AG} and performs the data recovery algorithm to the health data (m_1, m_2, ..., m_w) by the following steps.

$Recovered(CT_{AG}, sk_S) \rightarrow (m_1, m_2, ..., m_w)$: When the doctor obtains $CT_{AG} = CT_{AG}' \| \eta$, he gets ($CT_{AG}'$, η) and then the corresponding message M can be recovered as

$$M = D(CT_{AG}') = L(CT_{AG}'^{\lambda} \bmod n^2)\mu \bmod n \quad \textbf{(13)}$$

Subsequently the doctor can recover the health data (m_1, m_2, ..., m_w) by the following steps.

Let X_w=M, i.e.

$$X_w = a_1 m_1 + a_2 m_2 + \cdots + a_w m_w \quad \textbf{(14)}$$

Since any type of the sensor data m_i is less than a constant τ and $\vec{a}$ is a super-increasing sequence, we have

$$a_1 m_1 + a_2 m_2 + \cdots + a_{w-1} m_{w-1} < a_1 \tau + \cdots + a_{w-1} \tau < a_w \quad \textbf{(15)}$$

Therefore,

$$X_{w-1} = X_w \bmod a_w = a_1 m_1 + a_2 m_2 + \cdots + a_{w-1} m_{w-1} \quad \textbf{(16)}$$

$$\frac{X_w - X_{w-1}}{a_w} = \frac{a_w m_w}{a_w} = m_w \quad \textbf{(17)}$$

With the similar procedure, we can also recover each (m_1, m_2, ..., m_w).

In order to verify the correctness of the data (m_1, m_2, ..., m_w), the doctor computes

$$\eta' = H(H(m_1 \| a_i) \| H(m_2 \| a_2), ..., \| H(m_w \| a_w)) \quad \textbf{(18)}$$

and verifies whether $\eta = \eta'$. If it holds, then (m_1, m_2, ..., m_w) is the correctness data collected by sensors. Otherwise (m_1, m_2, ..., m_w) is invalid.

5 Security Analysis

Security is an important aspect in any network. Specifically in the applications of CWBANs, it is critical to maintain the confidentiality and privacy of sensitive medical data. Malicious capture of the private data affects its genuineness and may cause harm to the patient. Our scheme guarantees the following security properties.

(1) Fine-grained access control: Our scheme can realize the fine-grained access control for patients' health data by employing CP-ABE. In our scheme, the data owner can define an access policy according to flexible association of attributes. With the access policy embedded in the ciphertext, a doctor can decrypt the ciphertext to access the data only if his attribute set satisfies the policy. Since CP-ABE is provably secure against the adaptive chosen plaintext attacks (IND-CPA) based on the generic bilinear group model, the correctness and security can be referred to [14]. Therefore, even though adversaries eavesdrop the encrypted data, they still cannot access and read the corresponding contents.

(2) Collusion attack resistance: In our scheme, each doctor's attribute-associated private key sk_S is blinded by the secret numbers ($r, r_j \in Z_p^*$), which is implemented to resist the collusion attack. An adversary cannot combine different sk_S to forge a new private key associated with a larger set of attributes. For instance, assume a doctor with attribute set S_i has been delegated a secret key sk_i and a nurse with attribute set S_j has been delegated a secret key sk_j. According to the *KeyGen* algorithm in our scheme, The doctor and the nurse are unable to utilize sk_i and sk_j to obtain another secret key for the combined attribute set of S_i and S_j. Therefore, our scheme can defend against

collusion attacks.

(3) Data confidentiality: To protect the patient's privacy, the data should be transmitted securely. In our scheme, the patient's health data collected by sensors are blinded and sent to the data sink. Thus the data sink or attacker has no access to the data even if the data sink is compromised physically or virtually since they do not know the blinded keys (r_i, a_i). It eliminates the trust that is usually put on the data sink. Meanwhile, the blinded data are aggregated by using Paillier cryptosystem and transmitted to the cloud server. Note that, Paillier cryptosystem is provably secure against chosen plaintext attack, and the correctness and security can be referred to [27]. Thus, our proposed scheme can ensure data confidentiality thus protect patients' privacy.

(4) Data verifiability: In order to guarantee the correction of the health data transformation, our scheme allows the data sink and the doctor to check whether the transformation is done correctly. To be specific, it contains two phases. Firstly, before the data is aggregated at the data sink, the authentication and validity of the data are checked by verifying whether the formula $\sigma_i = \sigma_i'$ ($\sigma_i' = H(s_i \| K \| TS_i \| \eta_i)$) is satisfied. Because the secret key K is only shared between the sensors and the data sink, only legal sensor can generate a valid authenticated code σ_i, while any attacker cannot generate a valid authenticated code σ_i without the secret key K. Secondly, the data received by the doctor has to be checked by verifying whether the formula $\eta = \eta'$ ($\eta' = H(\eta_1 \| \eta_2 \| ... \| \eta_w)$, $\eta_i = H(m_i \| a_i)$) is satisfied. Since the secret key a_i is only shared between the sensor and the doctor, the doctor can verify the correctness of the data transformation and whether the data comes from the sensor. As a result, our proposed scheme can realize verifiablity for the received data by data sink and doctors, and any attacker's malicious behaviors and incorrect data in transformation can be detected in our scheme.

Based on the analysis above, our proposed scheme is secure in terms of fine-grained access control, collusion attack resistance, data confidentiality and data verifiability.

6 Performance Evaluation

In this section, we evaluate the performance of our scheme in terms of computational cost and communication cost at the sensor, the data sink and the cloud server.

6.1 Computational cost

In our scheme, a sensor is needed to do two multiplication operation and one addition operation in Z_n^* as well as two hash operations to generate a blinded health data s_i and the verification codes (σ_i, η_i). As the computational cost of addition operation and hash operation is negligible, the computational cost of the sensor is relatively lower in our scheme. Notably, lower computational cost is important for the sensor with limited computational power. After receiving the blinded data from w sensors, the data sink first verifies the received data by performing verification algorithm, and then aggregates the blinded data from different sensors, which includes w exponentiation operations in group $Z_{n^2}^*$ and w multiplication operations in group Z_n^*.

As for the cloud server, it encrypts the aggregated data using CP-ABE, if t is the number of attributes appeared in T, it includes one pairing operation and one multiplication operation in group G_T, ($2t$+2) exponentiation operations in group G.

We compare our scheme with schemes [26, 30] in terms of computational cost. The comparison results are shown in Table 1. Denote the computation cost of a multiplication operation in group Z_n^* by C_{mn}, an exponentiation operation in group $Z_{n^2}^*$ by C_{en}, an exponentiation operation in group C_T by C_{et}, a multiplication operation in group G_T by C_{mt}, an exponentiation operation in group G by C_e, and a pairing operation by C_p respectively.

Table 1. Comparison of computational cost

	Scheme [26]	Scheme [30]	Our Scheme
Sensor	$C_{mn} + C_{et} + C_{mt} + C_p + (2t+2) \cdot C_e$	$C_{et} + C_{mt} + C_p + t \cdot C_e$	$2 \cdot C_{mn}$
Data Sink	\	\	$w \cdot (C_{en} + C_{mn})$
Cloud Server	\	\	$C_{et} + C_{mt} + C_p + (2t+1) \cdot C_e$

Table 1 illustrates that our scheme is lower than schemes [26, 30] in terms of the computational cost at the sensor. The reason that our scheme requires a lower computational cost for the sensor is that we shift the burdensome computational task of CP-ABE from the sensor to cloud server by outsourcing encryption operations. Of course, this also results in a higher computational cost at the cloud server in our scheme. However, this computational cost is reasonable for the cloud server side with certain computing power. As our scheme needs to aggregate the blinded data received from the sensors implanted in a patient body at the data sink, our scheme is higher than schemes [26, 30] in terms of the computational cost at the data sink. Furthermore, we conduct the experiments with JPBC libraries [31] running on a 2.4 GHz Intel Core i5 processor running Windows10 OS with 8GB of RAM. The experiment results are shown in Figure 2 and

Figure 3.

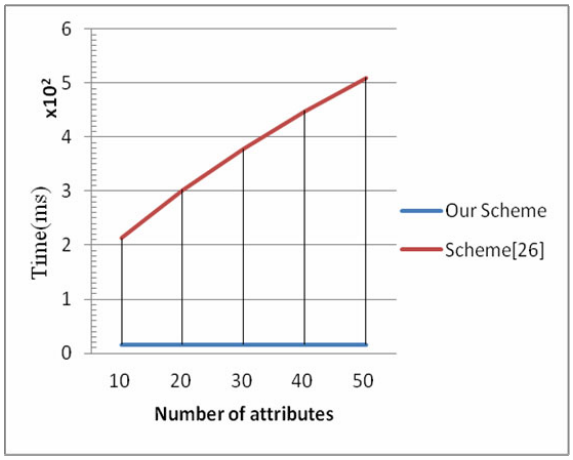

Figure 2. Computational time on sensor

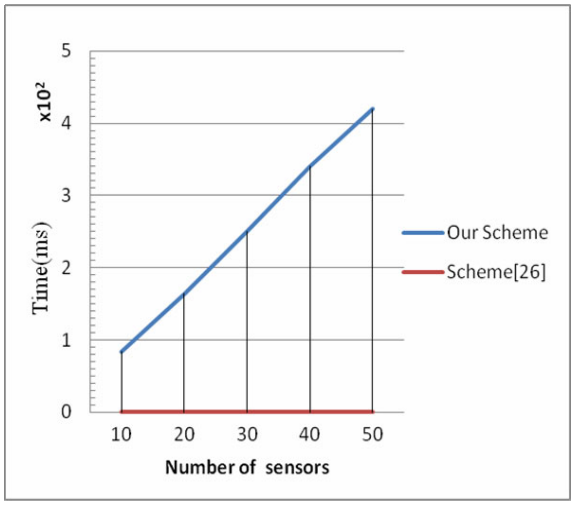

Figure 3. Computational time on data sink

As we analyze, our scheme incurs lower computational cost than [26] at the sensor. However, our scheme needs some computational cost at the data sink, which is reasonable for the data sink with a certain computational power.

6.2 Communication Cost

We first consider from the sensor to the data sink (SN-to-DS) communication, where the sensors generate their health data and deliver these data to the local data sink. If we choose 80-bit security level and let $|T|$=32, then $|G_1|$=512, $|G_0|$=160. In [26], each sensor has to generate the data size is S'_{SN-DS} $=|T|+|\sigma|+|\tilde{C}|+|C|+|C_y|+|C'_y|$=32+160+512+160+2×160×$t$ (t is the number of attributes appeared in T), which is impractical for resource-constrained sensors with limited energy, storage and computation power. Notably, the communication cost of [26] is increasing linear to the size of the attribute universe and the size of sensors. However, in our scheme, each data is transmitted in the form of $\sigma_i \| s_i \| \eta_i \| TS_i$ and its size should be $S_{SN\text{-}DS}$= 160+160+160+32 if we choose 16-bit Z_n^*, 160-bit n, 160-bit hash value, 160-bit G_0 and 32-bit timestamp. Therefore, the communication cost of SN-to-DS is constant in our scheme.

Next, we consider the communication cost between the data sink and the doctor (DS-to-DC). In [26], the data sink passes the encrypted data generated by each sensor to the doctor respectively, so its size is also $S_{DS\text{-}DC}$= $|T|+|\sigma|+|\tilde{C}|+|C|+|C_y|+|C'_y|$=32+160+512+160+2×160×$t$ (t is the number of attributes appeared in T) and increases linear to the size of the attribute universe and the size of sensors. In our scheme, the data sink aggregates the health data and transmits the aggregated data in the form of $CT_{AG} = CT'_{AG} \| \eta$. Therefore, the communication cost between the data sink and the cloud server is $S_{DS\text{-}CS}$=320+ 160($|n^2|$=320), which is constant. And the communication cost between the cloud server and the doctor is similar to [26]. But this communication cost is reasonable for the cloud server with certain energy power. In Figure 4, we further plot the communication overhead in terms of sensor numbers and attribute number t. It is shown that our scheme significantly reduces the communication overhead of SN-to-DS.

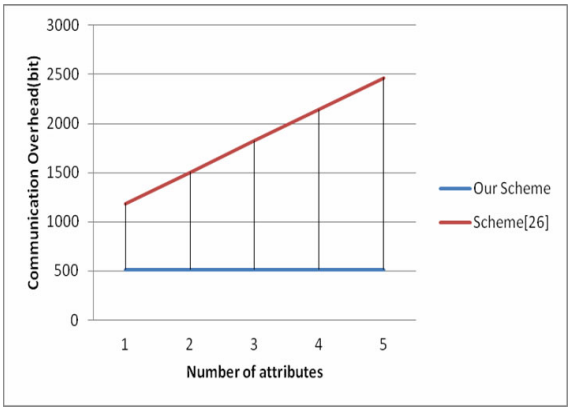

Figure 4. Communication cost of SN-to-DS

From the above analysis, our scheme is indeed efficient in terms of computational and communication cost, which is suitable for the real-time high-frequency data collection in wireless body area networks.

7 Conclusion

In this paper, we consider the problem of medical sensor data transmission in CWBANs. To meet the security requirements of resource-constrained wireless sensor nodes, we propose a secure and efficient health data aggregate scheme with fine-grained access control and verifiability. Our scheme can significantly reduce the computational cost and improve the communication efficiency, satisfying the real-time high- frequency data collection requirements in CWBANs. We have also provided the security analysis to demonstrate our

scheme's privacy-preserving ability. With a lightweight communication and computational cost on both sensors and data sink, our scheme can well suit the practical medical data access control in CWBANs.

Acknowledgments

This work was partially supported by National Natural Science Foundation of China under Grants 61272415; Science and Technology Planning Project of Guangdong Province, China, under Grant 2013B010401015. This work was also supported by the Zhuhai Top Discipline- Information Security.

References

[1] G. Fortino, A. Guerrieri, F. L. Bellifemine, SPINE2: Developing BSN Applications on Heterogeneous Sensor Nodes, *IEEE International Symposium on Industrial Embedded Systems*, Lausanne, Switzerland, 2009, pp. 128-131.

[2] G. Fortino, M. Pathan, G. D. Fatta, BodyCloud: Integration of Cloud Computing and Body Sensor Networks, *Future Generation Computer Systems*, Vol. 35, No. 5, pp. 57-61, June, 2014.

[3] C. Wang, Y. Zhang, New Authentication Scheme for Wireless Body Area Networks Using the Bilinear Pairing, *Journal of Medical Systems*, Vol. 39, No. 11, pp. 136-144, November, 2015.

[4] Q. Jiang, X. Lian, C. Yang, J. Ma, Y. Tian, Y. Yang. A Bilinear Pairing Based Anonymous Authentication Scheme in Wireless Body Area Networks for MHealth, *Journal of Medical Systems*, Vol. 40, No. 11, pp. 231-241, November, 2016.

[5] J. Shen, S. Chang, J. Shen, Q. Liu, X. M. Sun, A Lightweight Multi-layer Authentication Protocol for Wireless Body Area Networks, *Future Generation Computer Systems*, Vol. 78, No. 2, pp. 956-963, February, 2018.

[6] Z. Zhao, An Efficient Anonymous Authentication Scheme for Wireless Body Area Networks Using Elliptic Curve Cryptosystem, *Journal of Medical Systems*, Vol. 38, No. 2, pp. 1-7, February, 2014.

[7] J. Liu, Z. Zhang, X. Chen, K. S. Kwak, Certificateless Remote Anonymous Authentication Schemes for Wireless Body Area Networks, *IEEE Transactions on Parallel and Distributed Systems*, Vol. 25, No. 2, pp. 332-342, February, 2014.

[8] D. He, S. Chan, Y. Zhang, H. Yang, Lightweight and Confidential Data Discovery and Dissemination for Wireless Body Area Networks, *IEEE Journal of Biomedical and Health Informatics*, Vol. 18, No. 2, pp. 440-448, March, 2014.

[9] X. Li, M. H. Ibrahim, S. Kumari, A. K. Sangaiah, V. Gupta, K. K. R. Choo, Anonymous Mutual Authentication and Key Agreement Scheme for Wearable Sensors in Wireless Body Area Networks, *Computer Networks*, Vol. 129, No. 12, pp. 429-443, December, 2017.

[10] H. Xiong, Z. Qin, Revocable and Scalable Certificateless Remote Authentication Protocol with Anonymity for Wireless Body Area Networks, *IEEE Transactions on Information Forensics and Security*, Vol. 10, No. 7, pp. 1442-1455, July, 2015.

[11] D. He, S. Zeadally, K. Kumar, J. H. Lee, Anonymous Authentication for Wireless Body Area Networks with Provable Security, *IEEE Systems Journal*, Vol. 11, No. 4, pp. 2590-2601, December, 2017.

[12] X. Yang, C. Zhao, S. Yang, X. W. Fu, J. McCann, A Systematic Key Management Mechanism for Practical Body Sensor Networks, *IEEE International Conference on Communications*, London, United Kingdom, 2015, pp. 7310-7315.

[13] W. Wu, Y. T. Zhang, An Efficient Biometric-Based Algorithm Using Heart Rate Variability for Securing Body Sensor Networks, *Sensors*, Vol. 15, No. 7, pp. 15067-15089, July, 2015.

[14] J. Bethencourt, A. Sahai, B. Waters, Ciphertext-Policy Attribute-Based Encryption, *IEEE Symposium on Security and Privacy*, Oakland, CA, 2007, pp. 321-334.

[15] H. Qian, J. Li, Y. Zhang, J. Han, Privacy-Preserving Personal Health Record Using Multi-Authority Attribute-Based Encryption with Revocation, *International Journal of Information Security*, Vol. 14, No. 6, pp. 487-497, November, 2015.

[16] H. Wang, D. He, J. Shen, Z. H. Zhang, C. Zhao, M. H. Zhao, Verifiable Outsourced Ciphertext-Policy Attribute-Based Encryption in Cloud Computing, *Soft Computing*, Vol. 21. No. 24, pp. 7325-7335, December, 2017.

[17] D. Meng, E. Luo, G. Wang, A Privacy-Preserving Multi-Authority Attribute-Based Encryption Approach for Mobile Healthcare, *IEEE 13th International Conference on Mobile Ad Hoc and Sensor Systems*, Brasilia, Brazil, 2016, pp. 299-306.

[18] M. Li, S. Yu, Y. Zheng, K. Ren, W. J. Lou, Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption. *IEEE Transactions on Parallel and Distributed Systems*, Vol, 24, No. 1, pp. 11-143, January, 2013.

[19] C. Wang, X. Xu, Y. Li, D. Shi, Integrating Ciphertext-Policy Attribute-Based Encryption with Identity-Based Ring Signature to Enhance Security and Privacy in Wireless Body Area Networks. *International Conference on Information Security and Cryptology*, Beijing, China, 2014, pp. 424-442.

[20] J. Wan, C. Zou, S. Ullah, C. F. Lai, M. Zhou, X. F. Wang, Cloud-Enabled Wireless Body Area Networks for Pervasive Healthcare, *IEEE Network*, Vol. 27, No. 5, pp. 56-61, October, 2013.

[21] J. Zhou, Z. Cao, X. Dong, N. X. Xiong, V. Vasilakos, 4S: A Secure and Privacy-Preserving Key Management Scheme for Cloud-Assisted Wireless Body Area Network in M-Healthcare Social Networks, *Information Sciences*, Vol. 314, No. 9, pp. 255-276, September, 2015.

[22] C. T. Li, C. C. Lee, C. T. Weng, A Secure Cloud-Assisted Wireless Body Area Network in Mobile Emergency Medical

Care System, *Journal of Medical Systems*, Vol. 40, No. 5, pp. 1-15, May, 2016.

[23] J. Li, X. Li, L. Wang, D. B. He, H. Ahwad, X. X. Niu, Fuzzy Encryption in Cloud Computation: Efficient Verifiable Outsourced Attribute-Based Encryption, *Soft Computing*, Vol. 22, No. 3, pp. 707-714, February, 2018.

[24] Z. Guan, T. Yang, X. Du, M. Guizan, Secure Data Access for Wireless Body Sensor Networks, *IEEE Wireless Communications and Networking Conference*, Doha, Qatar, 2016, pp. 1-6.

[25] S. Han, S. Zhao, Q. Li, C. H. Ju, W. L. Zhou, PPM-HDA: Privacy- Preserving and Multifunctional Health Data Aggregation with Fault Tolerance, *IEEE Transactions on Information Forensics and Security*, Vol. 11, No. 9, pp. 1940-1955, September, 2016.

[26] C. Hu, H. Li, Y. Huo, T. Xiang, X. F. Liao, Secure and Efficient Data Communication Protocol for Wireless Body Area Networks, *IEEE Transactions on Multi-Scale Computing Systems*, Vol. 2, No. 2, pp. 94-107, February, 2016.

[27] P. Paillier, Public-key Cryptosystems Based on Composite Degree Residuosity Classes, *International Conference on Theory and Application of Cryptographic Techniques*, Prague, Czech Republic, 1999, pp. 223-238.

[28] V. Kumar, S. Madria, Distributed Attribute Based Access Control of Aggregated Data in Sensor Clouds, *IEEE Symposium on Reliable Distributed Systems*, Montreal, Canada, 2015, pp. 218-227.

[29] X. Zhang, J. Long, Z. Wang, H. Cheng, Lossless and Reversible Data Hiding in Encrypted Images with Public-Key Cryptography, *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 26, No. 9, pp.1622-1631, September, 2016.

[30] F. Xhafa, J. Li, G. Zhao, J. Li, X. Chen, D. S. Wong, Designing Cloud-Based Electronic Health Record System with Attribute-Based Encryption. *Multimedia Tools and Applications*, Vol. 74, No. 10, pp. 3441-3458, October, 2015.

[31] Java Pairing Based Cryptography Library, http://gas.dia.unisa.it/project/jpbc.

[32] F. Wei, P. Vijayakumar, J. Shen, R. Zhang, L. Li, A Provably Secure Password-based Anonymous Authentication Scheme for Wireless Body Area Networks, *Computers and Electrical Engineering*, Vol. 65, No. 1, pp. 322-331, January, 2018.

[33] J. Shen, Z. Gui, S. Ji, J. Shen, H. Tan, Y. Tang, Cloud-Aided Lightweight Certificateless Authentication Protocol with Anonymity for Wireless Body Area Networks, *Journal of Network and Computer Applications*, Vol. 106, No. 3, pp. 117-123, March, 2018.

[34] Y. Tian, Y. Peng, X. Peng, H. Li, An Attribute-based Encryption Scheme with Revocation for Fine-Grained Access Control in Wireless Body Area Networks, *International Journal of Distributed Sensor Networks*, Vol. 10, No. 11, pp. 1-9, November, 2014.

[35] Y. Y. Deng, C. L. Chen, W. J. Tsaur, Y. W. Tang, J. H. Chen, Internet of Things (IoT) Based Design of a Secure and Lightweight Body Area Network (BAN) Healthcare System, *Sensors*, Vol. 17, No. 12, pp. 2919-2936, December, 2017.

Biographies

Xuefeng Fang received the M.Sc. degree in computer engineering at Jinan University, China, in 2017. His research interests include security and privacy in wireless sensor networks.

Qingqing Gan received the M.Sc. degree in software engineering at Jinan University, China, in 2016. Currently, she is a full-time Ph.D. student at Jinan University. Her research interests include security and privacy in cloud computing.

Xiaoming Wang received the B.Sc. degree from Harbin Institute of Technology, China, and the Ph.D degree from Nankai University, China. She is currently working as a Professor in the Department of Computer Science at Jinan University, China. Her research interests include security and privacy in network and distributed systems, such as wireless sensor networks and cloud computing with a focus on security protocol designs and access control.