Secured Data Communication Protocol Using Cp_Abe Algorithm For Modern Patient Health Monitoring System

MRS.R.VADHANI
ASSISTANT PROFESSOR-CSE
SRI VENKATESWARAA COLLEGE OF TECHNOLOGY, TAMIL NADU, INDIA

ABSTRACT:
Wireless Body Area Networks (WBANs) are expected to play a major role in the field of patient-health monitoring in the near future. One of the challenges is to establish secure communication architecture between sensors and users, whilst addressing the prevalent security and privacy concerns. In this paper, we propose a communication architecture for BANs, and design a scheme to secure the data communications between implanted/wearable sensors and the data sink/data consumers (doctors or nurse) by employing Cipher text-Policy Attribute Based Encryption (CP_ABE). Our scheme achieves a role-based access control by employing an access control tree defined by the attributes of the data. These papers design two protocols to securely retrieve the sensitive data from a BAN and instruct the sensors in a BAN. We analyze the proposed scheme, and argue that it provides message authenticity and collusion resistance, and is efficient and feasible. This paper performance in terms of energy consumption and communication/computation overhead.

GENERAL TERMS
Algorithms, Design, Security, Verification

KEYWORDS
Wireless body area networks; access control tree; bilinear map; secure communications; attribute-based cryptosystem

INTRODUCTION:
A body area network (BAN), also referred to as a wireless body area network (WBAN) or a body sensor network (BSN), is a wireless network of wearable computing devices. BAN devices may be with the rapid advancements of wireless communication and semiconductor technologies the area of sensor network has grown significantly supporting a range of applications including medical and healthcare systems. A Wireless Body Area Network is a special purpose sensor network designed to operate autonomously to connect various medical sensors and appliances, located inside and outside of a human body. Introduction of a WBAN for medical monitoring and other applications will offer flexibilities and cost saving options to both health care professionals and patients. A WBAN system can offer two significant advantages compared to current electronic patient monitoring systems. The first advantage is the mobility of patients due to use of portable monitoring devices. Second advantage is the location independent monitoring facility. A WBAN node being an autonomous device can search and find a suitable communication network to transmit data to a remote database server for storage. It is also possible that a WBAN will connect itself to the internet to transmit data in a non-invasive manner.

To overcome the challenges mentioned above, this paper resort to the so-called Cipher text-Policy Attribute-Based Encryption (CP_ABE)[2], which was proposed as a new means of providing role-based access control on encrypted data. ABE has been exploited to secure the communications between a BAN and its external users in [6]and [1], with [6]
focusing on securing the communications between the data controller and an external user via fuzzy ABE and [1] addressing self-protecting electronic medical records (EMRs) on mobile devices and offline communications using the basic ABE. Here, these papers employ CP_ABE such that a sensor can control the access to its data by constructing an access structure defined by a set of attributes. Data are then stored in cipher text format at the data sink and the trust we put on the data sink is thus drastically decreased as the data sink does not have the key to decrypt the stored cipher text. Since CP_ABE belongs to the asymmetric encryption family, which implies a high computational cost, we propose to utilize CP_ABE to encrypt a data encryption key, based on which the data is encrypted by symmetric encryption. More specifically, this paper design four primitive algorithms to implement a secret-sharing based CP_ABE and propose two protocols to securely retrieve the sensitive patient data from a BAN and instructs the sensors in a BAN. This paper also analyze the security strength of our scheme and prove its correctness. The rest of the paper is organized as follows. We present the preliminaries and the system model in Section 2, and develop the main idea of the communication protocols in Section 3. Section 4 analyzes the security of the proposed protocols, followed by a conclusion.

2. PRELIMINARIES AND SYSTEM MODEL

2.1 Preliminaries

This paper introduces some preliminary knowledge regarding the cryptographic primitives used in this paper.

2.1.1 Bilinear Maps

Let G1 and G2 be two bilinear groups of prime order p, and g be a generator of G1. Our proposed scheme makes use of a bilinear map: e : G1 × G1 -> G2 with the following properties:

1. Bilinear: A map e : G1 × G1 -> G2 is bilinear if and only if for all P, Q G1 and all a, b Zp, we have e(P^a, Q^b) = e(P; Q)^{ab}. Here Zp = {0, 1, ..., p-1} is the Galois field of order p.

2. Non-degeneracy: The generator g satisfies e(g, g) ≠ 1.

3. Computability: There exists an efficient algorithm to compute(P, Q) for P, Q G1.

Note that the hardness [7] of the decision version of Bilinear Map, i.e., the decisional bilinear Diffie-Hellman problem (DBDH) forms the basis for the security of our scheme.

2.1.2 Secret Sharing Schemes

Another important cryptographic primitive used by our scheme is secret sharing. Secret sharing schemes were first developed by Shamir [8] and then extensively studied by different researchers [3, 5]. This paper provide a brief overview as follows: In the context of a dealer sharing a secret with a number of participants u1, ..., un, a participant learns the secret if and only if it can cooperate with at least t - 1 other participants (on sharing what they learn from the dealer), where t ≤ n is a predetermined parameter. The secret to be shared by the dealer is denoted by s Zp, where p > n. Before secret sharing, each respondent (participant) ui should obtain its secret key xi Zp, which is only known by ui and the dealer.
The dealer follows a two-step process. First, it constructs a polynomial function \( f(x) \) of degree \( t-1 \), by randomly choosing each \( a_j \) i.i.d. with a uniform distribution from \( \mathbb{Z}_p \). Note that all (additive and multiplication) operations used in (1) and throughout the rest of the paper are modular arithmetic (defined over \( \mathbb{Z}_p \)) as opposed to real arithmetic. Also note that forms the constant component of \( f(x) \) - i.e., \( s = f(0) \). Then, in the second step, the dealer transmits to each user \( u_i \) a shared secret \( s_i \), where

\[
s_i = f(x_i) \quad (2)
\]

We now show how \( t \) or more users can cooperate to recover the \( s \) by sharing the secret shares received from the dealer. Without loss of generality, let \( u_1, \ldots, u_t \) be the cooperating users. These \( t \) users can reconstruct the secret \( s = f(0) \) from \( s_1 = f(x_1), \ldots, s_t = f(x_t) \) by computing

\[
s = f(0) \quad (3)
\]

2.2 System Model

In this paper, we consider a BAN communication system depicted in Fig. 1. There are four major entities in this system: Key Generation Center (KGC), Sensor (implanted and wearable devices), Data Sink (a dedicated BAN data controller or a mobile device such as a smart phone), and Data Consumer (doctors and nurses), whose major functions are summarized in the following four subsections.

### 2.2.1 Key Generation Center (KGC)

The KGC is used to perform system initialization, generate public parameters, and compute a secret key for each data consumer and each sensor based on their attributes. The public parameters should be installed into the sensors before they are deployed (attached to or implanted in a human body) in a BAN. A data consumer should be able to prove to the KGC that it is the owner of a set of attributes.

### 2.2.2 Sensor

A BAN consists of wireless sensors called BAN devices either embedded on/near the surface (i.e., wearable devices) or implanted in the deep tissue (i.e., implanted devices) of a human body. The BAN devices should have certain computational capability to encrypt the patient’s data and store the cipher text into the data sink. When a data consumer needs the data, he should communicate with the data sink to retrieve the (encrypted) data.

### 2.2.3 Data Sink

A data sink, which could be the BAN controller or a mobile device such as a smart phone, is used to store the patient’s data. We apply the attribute-based encryption proposed by Bethen court, Sahai, and Waters [2] to encrypt the data and store the cipher text in the data sink according to the requirements of the BAN.

### 2.2.4 Data Consumer

Data consumers refer to the doctors and nurses or other experts. To decrypt a message, data consumers should have the attributes that satisfy the access tree specified by the data source (the sensor generating the data).

2.3 Access Control Policy – the Access Tree

Our main idea is to design an attribute-based security scheme that views an identity as a set of attributes, and enforces a lower bound on the number of common attributes between a user’s identity and its access...
rights specified for the sensitive data. We use an access tree to control the data consumers’ access to the encrypted data. Fig. 2 illustrates such an access tree structure. In Fig. 2, $num_x$ is the number of child nodes of node $x$, and $k_x [1; num_x]$ is its threshold value, with $k = n$ indicating that node $x$ performs the OR operation over all the subsets of $n$ child nodes of $x$, with each subset supporting an AND operation. Each leaf node $y$ is described by an attribute $att(y)$ and a threshold value $k_y = 1$. When a data item is generated, its associated attributes defining the access right are used to create a tree for access control, which implies that only the users possessing a certain number of the attributes of the data item can decrypt the encrypted data.

To overcome the challenges mentioned above, we resort to the so-called Cipher text-based Policy Attribute-Based Encryption (CP_ABE) [2], which was proposed as a new means of providing role-based access control on encrypted data. ABE has been exploited to secure the communications between a BAN and its external users in [6] and [1], with [6] focusing on securing the communications between the data controller and an external user via fuzzy ABE and [1] addressing self-protecting electronic medical records (EMRs) on mobile devices and offline communications using the basic ABE. In this paper, we employ CP_ABE such that a sensor can control the access to its data by constructing an access structure defined by a set of attributes. Data are then stored in cipher text format at the data sink and the trust we put on the data sink is thus drastically decreased as the data sink does not have the key to decrypt the stored cipher text. Since CP_ABE belongs to the asymmetric encryption family, which implies a high computational cost, we propose to utilize CP_ABE to encrypt a data encryption key, based on which the data is encrypted by symmetric encryption. More specifically, we design four primitive algorithms to implement a secret-sharing based CP_ABE and propose two protocols to securely retrieve the sensitive patient data from a BAN and instructs the patient. The sharing based CP_ABE and propose two protocols to securely retrieve the sensitive patient data from a BAN and instructs the sensors in a BAN. We also analyze the security strength of our scheme and prove its correctness sharing based CP_ABE and propose two protocols to securely retrieve the sensitive. Correctness. The rest of the paper is organized as follows. We present the preliminaries and the system model, and develop the main idea of the communication protocols. analyzes the security of the proposed protocols followed by a conclusion.

3. THE PROPOSED SECURE DATA COMMUNICATION PROTOCOLS:

In this section, we propose the data communication protocols to secure the messages when a data consumer, which could be a doctor or other expert, communicates with the sensors or the data sink, to distribute instructions and commands to the BAN, or retrieve the sensitive data from the BAN.

3.1 Primitive Algorithms

This paper first introduces the following four primitive algorithms that will be utilized by the communication protocols between the data consumers and a BAN. Algorithm 1 presents the system initialization performed by KGC.

Algorithm 2 is executed by KGC to generate private keys for the sensors and data consumers based on their attributes. The encryption procedure is detailed.

Algorithm 3, which encrypts a data encryption key $K$ or an access token $K_1$ with an access tree $T$, all specified by the sensor.

Algorithm 4 implements decryption and authentication, which should be executed by
data consumers since they receive only encrypted data from the BAN.

3.2 System Initialization

Before a BAN is deployed, the following system initialization procedure needs to be carried out:

1. The KGC computes the public parameter PK according to Algorithm 1, and posts PK to all sensors and data consumers.
2. The KGC computes a private key for each sensor and each data consumer based on their possessed attributes according to Algorithm 2.

3.3 Retrieving Data from A BAN

The following procedure illustrates how a data consumer with a set of private keys (corresponding to its attribute set S) obtains the sensitive patient data from the data sink:

1. The sensor selects a random data encryption key K, encrypts K using Algorithm 3, and then encrypts its data M by AES: AES(K;M). One can see that we do not include AES in Algorithm 3 since we use Algorithm 3 to encrypt the data encryption key K, which is used to perform symmetric encryption for the patient data.
2. The sensor sends the encrypted data (the cipher texts of K and M) to the data sink, where ID_s and ID_d are respectively.

Figure 3: Block diagram

Algorithm 1: System Initialization:

1: Selects a prime p, a generator g of G0, and a bilinear map e : G0 × G0 → G1.
2: Defines a Lagrange coefficient \(4i, S\) for \(i \in \mathbb{Z}_p\) and a set S of elements in \(\mathbb{Z}_p\): \(4i, S = Q \sum_{j \in \mathbb{Z}_p, j \neq i} x^{-j} i^{-j}\).
3: Chooses two random exponents \(\alpha, \beta \in \mathbb{Z}_p\).
4: Selects a hash function \(H : \{0, 1\}^* \rightarrow G0\). The function \(H\) is viewed as a random oracle.
5: Distributes the following public parameters to all sensors and data consumers: \(PK = G0, g, h = g^\beta, e(g, g) \alpha\)
6: Computes the master key MSK: \((\beta, g\alpha)\).

Algorithm 2: Key Generation (MSK, S):

Inputs: The master key MSK and the set of attributes S possessed by an entity (could be a sensor or a data consumer) requesting a private key.

1: The KGC selects random numbers \(r\) and \(r_j \in \mathbb{Z}_p\) for each attribute \(j \in S\).
2: The private key SK is computed by

\[
SK = D = g^{(\alpha+r)} \beta .
\]
the identity of the sensor and the data sink.

\[
\{(D_j = g^r \cdot H(j)^{g^j}, D_i = g^{i_j}) \mid \forall j \in S\}
\]

1. The data consumer obtains the encrypted data from the data sink, and then executes Algorithm 4 to retrieve the data encryption key \(K\).

2. The data consumer decrypts AES(K, M) using the decryption key K.

Note that this procedure implies that a data encryption key K is needed for each data item. In practice, the data generated by the same sensor during a certain time interval can be encrypted by the same data encryption key K to conserve the sensor’s computational power and energy. In such a case, K serves as a session key to encrypt all the data for a particular session.

3.4 Sending Instructions to a BAN:

When a data consumer wants to send instructions or commands to a sensor in a BAN, a direct communication session between the data consumer and the sensor is needed. This procedure requires an access token specified by the sensor to grant the access right to the data consumer possessing certain attributes. It involves two phases, described in the following two subsections.

3.4.1 Communication Establishment Phase:

1. First, the sensor selects an access token \(K_1\), and encrypts \(K_1||\text{date}\) with Algorithm 3. Then the sensor sends the encrypted token together with its hash \(h = H(K_1||\text{date})\) to the data sink:

2. The sensor updates \(K_1||\text{date}\) and the corresponding ciphertext at the data sink at a certain time interval, for example, once per day.

3. When a data consumer obtains the encrypted access token...
Encryption(PK; K1||date; T), he decrypts the ciphertext according to Algorithm 4. The sensor receives the proof and then verifies whether or not \( h' = h \). If succeeds, the sensor generates a new access token \( K'1 \) and encrypts \( K'1 ||\text{date} \) using the same access tree with Algorithm 3. The sensor sends the encrypted \( K'1 ||\text{date} \) and \( h = H(K'1||\text{date}) \) to the data consumer as a challenge, and then to the data sink to overwrite the previously encrypted access token.

Sensor -> Data Consumer and Data sink :
(IDs; Encryption(PK; K'1||date; T); H(K'1||date))

(9)

5. The data sink replaces the previously encrypted access token with the new one.

6. The data consumer decrypts Encryption(PK, K'1||date, T), and then sends the salted hash \( h' = H(K'1||\text{date}) \) to the sensor:

Data Consumer → Sensor : (IDd, IDs, AES(K'1,I), h = H(K'1||I||IDd)). (10)

2. The sensor decrypts the message and obtains \( I' \). Then it computes \( h' = h \), the message integrity is proven…

4. ANALYSIS OF THE PROPOSED SCHEME

In this section, we prove the correctness of the scheme, and analyze its security from the aspects of resistance to possible major attacks and authenticity.

4.1 The Correctness of the Proposed Scheme

In this subsection, we show that our proposed scheme is indeed feasible and correct. Algorithm 4 can verify whether the

\[
\begin{align*}
&11: \quad \text{Let } S_x \text{ be an arbitrary } k_x \text{-sized set of child nodes of } x \text{ such that } F_x \neq \bot \text{ if } z \in S_x. \\
&12: \quad \text{if } S_x \text{ exists then} \\
&\quad \quad F_x = e(g, g)^{r_{q(x)}} \Delta_x s_x(d) = e(g, g)^{r_{q(x)}(d)} = e(g, g)^{r_{q(x)}} \\
&\quad \quad \text{where } i = \text{index}(z) \text{ and } S'_{-z} = \{\text{index}(z): z \in S_x\}. \\
&13: \quad \quad \quad \text{Return } F_x \\
&14: \quad \quad \quad \text{else} \\
&15: \quad \quad \quad \quad \text{Return } F_x = \bot \\
&16: \quad \quad \quad \quad \text{end if} \\
&17: \quad \quad \end{align*}
\]

end function

18: end function

19: A = DecryptNode(CT, SK, R)

20: if A \neq \bot then

21: \quad e(C, D)/A = e(g, g)^{\alpha_s};

22: end if

23: The decryption is performed as follows:

\[
K' = e(H(K'1||I), g) = e(H(K|e(g, g)^{\alpha_s}), g)
\]
then 25: The message \( K' \) is valid.

26: end if

3.4.2 Communication Phase

This phase contains the following two steps.

1. The data consumer sends the instruction \( I \) to the sensor by using the shared secret \( K'1 \):

Data Consumer → Sensor : (IDd, IDs, AES(K'1,I), h = H(K'1||I||IDd)). (10)

2. The sensor decrypts the message and obtains \( I' \). Then it computes \( h' = H(K'1||I'||IDd) \). If \( h' = h \), the message integrity is proven…
received data encryption key has been forged or falsified. From Algorithm 4, we have
\[ K' = / = /e(C, D)/A \]
\[ = /e(h^s, g/e(g, g)^s) \]
\[ = Ke(g, g)^s/e(g, g)^s \]
\[ = Ke(g, g)^s/e(g, g)^s/(e(g, g)^s, g^s) \]
\[ = Ke(g, g)^s/e(g, g)^s \]
\[ = Ke(g, g)^s/e(g, g)^s/(e(g, g)^s, g^s) \]
\[ = Ke(g, g)^s/e(g, g)^s \]
\[ = Ke(g, g)^s/e(g, g)^s \]
\[ = Ke(g, g)^s/e(g, g)^s \]
\[ = Ke(g, g)^s/e(g, g)^s \]
\[ = Ke(g, g)^s/e(g, g)^s \]

Thus if \( e(H(k'), g) = e(H(K)|E(g, g)^s, g), K' \) is valid. When a data consumer receives a valid \( K' \), he could decrypt the ciphertext using \( K' \) to obtain the message \( M \).

4.2 Security Analysis

In this subsection, we analyze the security strength of the proposed scheme by examining how it can counter possible major attacks.

4.2.1 Collusion Attack Resistance

In our application of CP_ABE, the set of attributes composes the identity. In order to provide different users with different access rights, the scheme provides an access tree structure for each encrypted data item, and requires only a subset of the attributes for decryption.

4.2.2 Data Encryption Key Authentication

Assume that a data consumer wants to get the data encryption key \( K \) from a sensor. Before \( K \) is stored in the data sink, the sensor has encrypted it with Algorithm 3. When the data consumer intends to obtain \( K \) from the data sink, he needs to get his private key.

4.2.3 Two Phase Commitment

This two-phase commitment can protect the session from the following two vulnerable scenarios: i) an attacker may get a chance to obtain the access token since the attacker has the time to do the crack off-line (the access token refreshes at a certain time period); and ii) the data consumer may accidentally leak its access token to an attacker. The second phase of authentication can effectively correct the corresponding errors by generating a new access token.

5. CONCLUSION AND FUTURE WORK

A WAN is expected to be a very useful technology with potential to offer a wide range of benefits to patients, medical personnel and society through continuous monitoring and early detection of possible problems. The future market of WBAN is growing rapidly in the field of medical as well as in entertainment industry. We believe that WBAN will allow dramatic shift in the way people think about and manage their health. This provide more proactive preventive healthcare that will not only improve the quality of life, but also will reduce healthcare costs.

6. REFERENCE:


