Secure Data Communication using File Hierarchy Attribute Based Encryption in Wireless Body Area Networks

Balaji Chandrasekaran, Student member, ACM, Ramadoss Balakrishnan, Member, IEEE and Yasuyuki Nogami, Member, IEEE

***Abstract*—Wireless Body Area Networks (WBANs) play an important role in healthcare system by enabling medical experts to guide patients remotely. The unauthorized access of medical data from WBAN controller as well as the unreliable data communication may leads to risk for patients life. Currently, Chunqiang Hu et al., [1] proposed a data communication protocol by using Ciphertext-Policy Attribute-Based Encryption (CP-ABE) for a single file. The major limitation of Chunqiang Hu et al., [1] is that as the number of files increases, CP-ABE will suffer from parameters such as message size, energy consumption and computation cost. This paper proposes a more secure and efficient data communication scheme for WBANs by using an efficient File Hierarchy CP-ABE (FH-CP-ABE). The proposed scheme uses integrated access structure which is a combination of two or more access structures with hierarchical files encrypted. We evaluate the performance analysis of the proposed data communication protocol in terms of message size, energy consumption, computation cost and compared with Chunqiang Hu et al., [1].**

***Index Terms*—Computer Communication Networks, Data Encryption, Electronic Health Record, Health Communication, Task Performance and Analysis.**

I. Introduction

Recently, Wireless body area networks (WBANs) [1], [2], [3] have been gaining more attention in modern E-healthcare systems by providing an appropriate way for monitoring the human body using intelligent light-weight wearable or implantable sensors. Accordingly, medical specialists can utilize this real time information from WBAN to provide timely advices and medical treatments to patients. Figure 1 shows the system model for WBAN in a healthcare system. The system consists of four parts namely Key Authority, Wearable and implanted sensors, WBAN Controller and a Data Consumer.

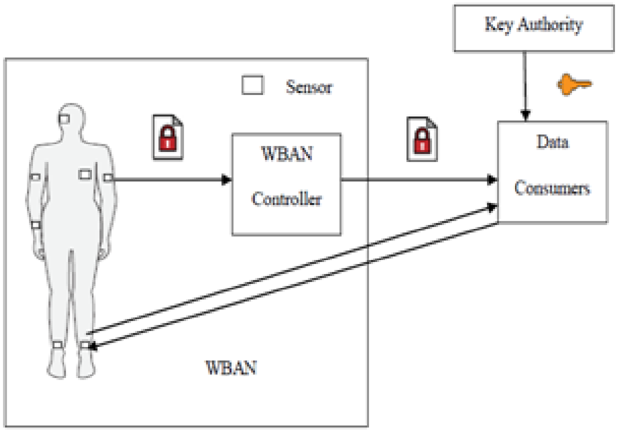

Fig. 1. System model for WBAN in a healthcare system

The critical functions of key authority include system initialization, public parameters generation, and assigning secret key for each of the data consumer. The generated public parameters are installed in to the sensors before they are implanted or hooked up in the human body. A WBAN consists of wireless sensors which are used to monitor vital human body actions (e.g., motion sensors) and parameters (e.g., body temperature, blood pressure, pulse (heart rate), and breathing rate (respiratory rate) [4]. Implanted devices endure from resource constraints such as battery power, storage etc. On the contrary, wearable devices have fewer resource constraints. The sensor devices encrypt patient’s data and store the ciphertext in the WBAN controller. WBAN controller is typically used to store the patient’s ciphertext data. When an authorised data consumer (doctors, nurses, healthcare experts) needs to access the data, the person should communicate with the WBAN controller to retrieve the ciphertext data. Despite of the uses, WBANs also raises some major privacy and security concerns, mainly unauthorized data access and message modification. Chunqiang Hu et. al [1] addressed solutions to these problems by proposing a Secure and Efficient Data Communication Protocol by using CP-ABE for a single file. The major limitation of Chunqiang Hu et. al [1] is, as the number of files increases, CP-ABE will suffer from parameters such as larger message size, high communication

Manuscript received January 17, 2018; revised March 3, 2018. Date of publication April 5, 2018.

B. Chandrasekaran (corresponding author) and R. Balakrishnan are with the Department of Computer Applications, National Institute of Technology, Tiruchirappalli, TamilNadu, India (e-mails: cbalaji1988@gmail.com, brama@nitt.edu).

Y. Nogami is with the Graduate School of Natural Science and Technology, Okayama University, Okayama, Japan (e-mail: yasuyuki.nogami@okayama-u.ac.jp).

Digital Object Identifier (DOI): 10.24138/jcomss.v14i1.446

overhead, high energy consumption and high computation cost. Thus the main motivation of this paper is to significantly improve these parameters when the number of files increases.

A. Our Contributions

The contributions of this paper are highlighted as follows:

1. We propose an efficient scheme for secure data communications in WBANs using FH-CP-ABE for multiple hierarchical files in a single encryption.
2. We evaluate the performance analysis of the proposed scheme in terms of message size, energy consumption, computation cost and compared with [1].

B. Paper Organization

The rest of this paper is organized as follows. Section II deals with the preliminaries. Section III presents the proposed scheme using FH-CP-ABE. Section IV presents the performance analysis of the proposed scheme. Section V concludes the paper.

II. Preliminaries

A. Bilinear Map

Let G_1, $G_2$and G_T are three cyclic groups of prime order q. G_1 and G_2 are a source group and G_T is a target group. Let g_1 and g_2 are generators of G_1 and G_2 respectively. A bilinear map e is defined as $e: G_1 \times G_2 \rightarrow G_T$ which has the following properties [5]:

1. *Bilinearity:* $e(g_1^a, g_2^b)$= $e(g_1, g_2)^{ab}$, where $a, b \in \mathbb{Z}_p$.
2. *Computability:* The bilinear map e is efficiently computable by $G_1 \times G_2$ for any pairs.
3. *Non-degeneracy:* $e(g_1, g_2) \neq 1$. It means all pairs of source group do not map to the identity of the target group.

Note: If $G_1 = G_2$, then it is a symmetric map, otherwise it is an asymmetric map.

B. Decisional Bilinear Diffie-Hellman (DBDH) assumption

Let $\mathrm{a, b, c, z} \in \mathbb{Z}_p$be chooses at random. DBDH problem in group G of prime order q and g is the generator of the group is a problem that no polynomial time adversary is able to distinguish the tuple $(g^{\mathrm{a}}, g^{\mathrm{b}}, g^{\mathrm{c}}, \mathrm{e}(g,g)^{\mathrm{abc}})$ from the tuple $(g^{\mathrm{a}}, g^{\mathrm{b}}, g^{\mathrm{c}}, \mathrm{e}(g,g)^{\mathrm{z}})$ with a non-negligible advantage [6].

$$\left(\left|Pr\left[\mathcal{A}\left(g, g^{\mathrm{a}}, g^{\mathrm{b}}, g^{\mathrm{c}}, \mathrm{e}(g,g)^{\mathrm{abc}}\right) = 0\right] - Pr\left[\mathcal{A}\left(g, g^{\mathrm{a}}, g^{\mathrm{b}}, g^{\mathrm{c}}, \mathrm{e}(g,g)^{\mathrm{z}}\right) = 0\right]\right| \geq \varepsilon\right)$$

III. Proposed Scheme

The bilinear map $e: G_1 \times G_1 \rightarrow G_T$, G_1be the source group of prime order p and G_T be the target group. Let g be the generator of the groupG_1. Let Lagrange Co-efficient $\Delta_{k,S}$= $\prod_{l \in S, l \neq k}(x - l)/(k - l)$, $k \in \mathbb{Z}_p$ and an attribute set $S = \{S_1, S_2, \dots, S_m \in \mathbb{Z}_p\}$. Let $H_1: \{0,1\}^*$ be the hash functions for the group G_1. An attribute universe set is defined as $\tilde{A} = \{a_1, a_2, \dots, a_n\}$. In this section, we propose a more efficient Secure and Efficient Data Communication Protocol for WBANs by using an efficient File Hierarchy CP-ABE (FH-CP-ABE) [7]. We use the integrated access structure which is a combination of two or more access structures with the hierarchical files encrypted. The proposed scheme has two kinds of data communications. First, the data communication between data consumer and WBAN controller. It consists of four algorithms, namely, *setup, key generation, encryption and decryption*. Second, the data communication between data consumer and sensors. It consists of three steps, namely, initialization, connection establishment and communication. The steps for data communication between data consumer and WBAN controller are detailed as follows:

$Setup(1^{\lambda})$: This algorithm is executed by the key authority and it takes as input a security parameter λ and chooses $\eta, \varkappa \in_{randomly} \mathbb{Z}_p$. It generates public key (PK) and master secret key (MSK) as the output which is calculated in equation (1) as follows:

$$\{PK = \{G_1, g, g^{\varkappa}, e(g,g)^{\eta}\}, MSK = \{\, g^{\eta}, \varkappa\}\} \qquad (1)$$

$Key\ Generation(PK, MSK, S)$: This algorithm is executed by the key authority and it takes as input, public key (PK), master secret key (MSK) and an attribute set $S (S \subseteq \tilde{A})$. Choose $r_{sn} \in_{randomly} \mathbb{Z}_p$ and $CK_{sign} = r_{sn}$and compute the verification key,$CK_{ver} = g^{r_{sn}}$. Choose $r, r_j \in_{randomly} \mathbb{Z}_p$ for each user and each attribute $j \in S$. It produces secret key (SK) as the output which is calculated in equation (2) as follows:

$$SK = \begin{Bmatrix} D = g^{\eta + \varkappa . r} \\ \forall j \in S: D_j = g^r . H_1(j)^{r_j}, D'_j = g^{\varkappa . r_j} \end{Bmatrix} \qquad (2)$$

It sends the SK and r_{sn} to the owner of the attribute set S and distribute CK_{ver} for others.

$Encryption(PK, ck, T)$: This algorithm is executed by the sensor. Let us assume that the data owner shares k files, i.e.,$M = \{m_1, m_2, \dots, m_k\}$ with k access level and corresponding content keys $ck = \{ck_1, ck_2, \dots, ck_k\}$. It takes as input the public key (PK), content keys (ck) and hierarchical access structure T. It produces as output the ciphertext CT, which can be calculated as the follows:

1. The level nodes $(x_i, y_i), (i \in [1, k])$ are set by the data owner in access structure T with k access levels and its hierarchy is sorted from highest to lowest, i.e., (x_1, y_1) is the highest hierarchy and (x_k, y_k) is the lowest hierarchy. For k chosen numbers $\alpha_1, \alpha_2, \dots, \alpha_k \in_{randomly} \mathbb{Z}_p$,

$$\widetilde{C_\iota} = ck_i e(g,g)^{\eta\alpha_i}, C'_i = g^{\alpha_i}, \forall i = 1,2, \dots, k \qquad (3)$$

2. In access structure T, for each node (x,y), a polynomial $q_{(x,y)}$has to be selected. The node information of polynomial$q_{(x,y)}$ for root node R is randomly chosen as top to bottom fashion. The degree of the polynomial is $deg_{(x,y)}$,$deg_{(x,y)} = k_{(x,y)} - 1, 0 < k_{(x,y)} \leq num_{(x,y)}$, where $k_{(x,y)}$ is the threshold value of node (x,y) and $num_{(x,y)}$ is the number of children for node (x,y) in T. The threshold value $k_{(x,y)}$ can be calculated as follows:

$$k_{(x,y)} = \begin{cases} num_{(x,y)}, & (x,y)\ is\ a\ non-leaf\ node(AND\ gate) \\ 1, & (x,y)\ is\ a\ non-leaf\ node(OR\ gate) \\ 1, & (x,y)\ is\ a\ leaf\ node \end{cases}$$

3. The data owner starts from the root node R and sets the polynomial $q_R(0) = q_{(x_1,y_1)} = \alpha_1$ and the degree $deg_{(x_1,y_1)}$ of the root node. For rest of the nodes,

$$q_{(x,y)}(0) = \begin{cases} q_{(x_i,y_i)}(0) = \alpha_i, & (x,y)\ is\ a\ level\,node \\ q_{parent(x,y)}(index(x,y)), & otherwise \end{cases}$$

Where $\mathrm{parent(x,y)}$ be the parent of node $\mathrm{(x,y)}$ and $\mathrm{index(x,y)}$ return the unique value associated with node $\mathrm{(x,y)}$. Let Y be set of leaf node in access structure T and for each node in Y the data owner computes,

$$C_{(x,y)} = g^{q_{(x,y)}(0)}, C'_{(x,y)} = H_1(att(x,y))^{q_{(x,y)}(0)} \qquad (4)$$

Where $\mathrm{att(x,y)}$ are the attributes linked with the leaf node in T.

4. Let X be the set of transport node (i.e. one of the children containing at least one threshold gate) and $TN - TG(x,y)$ be the threshold gate set of transport nodes of(x,y) children, i.e., $TN - TG(x,y) = \{child_1, child_2, \dots, child_j, \dots\}$ and for each nodes in X the data owner computes,

$$\hat{C}_{(x,y),j} = \{e(g,g)^{\eta\cdot\left(q_{(x,y)}(0)+q_{child_j}(0)\right)} \times H_1(e(g,g)^{\eta\cdot q_{(x,y)}(0)})\}, \qquad (5)$$
$$\forall j = 1,2,\dots.$$

5. The final output of encryption algorithm is:

$$\mathrm{CT} = \begin{Bmatrix} \mathrm{T}, \widetilde{\mathrm{C}_\imath}, \mathrm{C}'_\mathrm{i}, \mathrm{C}_{(\mathrm{x,y})}, \mathrm{C}'_{(\mathrm{x,y})}, \hat{\mathrm{C}}_{(\mathrm{x,y}),\mathrm{j}}, \\ \mathrm{sig} = (\mathrm{H}_1(\mathrm{ck_i}))^{\mathrm{r_{sn}}} \end{Bmatrix}, \qquad (6)$$
$$\forall \mathrm{i} = 1,2,\dots,\mathrm{k}\ \text{and}\ \forall \mathrm{j} = 1,2,\dots$$

$Decrypt(PK, CT, SK)$: A user decrypts the ciphertext CT with the help of public key (PK) and secret key (SK). First we define the recursive operation $DecryptNode\ (CT, SK, (x,y))$. If the recursive operation takes as input a leaf node (x,y), it should be computed as,

$$DecryptNode(CT, SK, (x,y)) = $$
$$\begin{cases} null, & i = att(x,y) \notin S \\ DecryptNode(CT, SK, (x,y)), & otherwise \end{cases}$$

$$DecryptNode(CT, SK, (x,y)) = \frac{e(D_i, C_{(x,y)})}{e(D'_i, C'_{(x,y)})} = e(g,g)^{r\varkappa q_{(x,y)}(0)} \qquad (7)$$

If the recursive operation takes as input a non leaf node (x,y)it should be computed as follows:

The operation $DecryptNode(CT, SK, z)$ runs if and only if all the elements in set z are the children of (x,y) and the result will be stored as F_z. It can be calculated as follows:

$$F_z = \begin{cases} null, & set\ does\ not\ exist \\ F_{(x,y)}, & otherwise \end{cases} \qquad (8)$$

Let $S_{(x,y)}$ be the $k_{(x,y)} - sized$ child nodes of set $z.F_{(x,y)}$can be calculated as follows:

$$F_{(x,y)} = \prod_{z\in S_{(x,y)}} F_z^{\Delta_{i,S'_{(x,y)}}(0)}, S'_{(x,y)}=\{index(z): z \in S_{(x,y)}\},$$
$$i = index(z) = \prod_{z\in S_{(x,y)}} (e(g,g)^{r\varkappa q_z(0)})^{\Delta_{i,S'_{(x,y)}}(0)} =$$
$$\prod_{z\in S_{(x,y)}} (e(g,g)^{r\varkappa q_{(x,y)}(i)})^{\Delta_{i,S'_{(x,y)}}(0)} = e(g,g)^{r\varkappa q_{(x,y)}(0)} \qquad (9)$$

Thus the decryption step can be detailed as follows:

1. If the attribute set S satisfies the partial or whole T, then $AS_i = DecryptNode(CT, SK, (x_i, y_i))$=
$$e(g,g)^{r\varkappa q_{(x_i,y_i)}(0)} = e(g,g)^{r\varkappa\alpha_i}, i \in [1,k]$$
2. Next, compute $F_i = \frac{e(C'_i, D)}{AS_i} = e(g,g)^{\eta\alpha_i}, i \in [1,k]$
3. Then compute the content keys (ck) as follows:

$$\frac{\widetilde{C_\imath}}{F_i} = \frac{ck_i e(g,g)^{\eta\alpha_i}}{e(g,g)^{\eta\alpha_i}} = ck_i, i \in [1,k]$$

The computed $\mathrm{ck_i}$ is valid if $\mathrm{e(sig, g)} = \mathrm{e(H_1(ck_i), g^{r_{sn}})}$.

4. Finally, we decrypt the k file $\{m_1, m_2, \dots, m_k\}$ with the help of k content keys $ck_i, i \in [1,k]$ using symmetric technique.

As like as in [1], we follow the same procedure for data communication between data consumer and sensors. For real time applications, we recommend to change the revocation time periodically. Periodically updating the secret key is highly secure for real time applications.

A. *Proposed Scheme: Proof of Security*

Theorem 1: Under Decisional Bilinear Diffie-Hellman (DBDH) assumptions, no polynomial time attacker can selectively break the proposed system.

Proof: The security game is based on the hardness of the DBDH assumption. Suppose attacker atk can win the FH-CP-ABE game with advantage ε. We construct a simulator sim that can distinguish a DBDH tuple from a random tuple with advantage$\frac{\varepsilon}{2}$. Let G_1 be the source group and G_T be the target group. Let g be the generator of the groupG_1. The challenger chooses the fair binary coin ɦ $\in \{0,1\}$, $g \in G_1, R \in G_T$ and $a, b, c \in \mathbb{Z}_p$. If ɦ $= 0$, then the challenger defines T to be $e(g,g)^{abc}$. Otherwise, he sets $T = e(g,g)^z\ or\ R$.

The challenger then gives the simulator the DBDH details and then simulator sim now plays the role of challenger in the security game.

Init: During the init phase, simreceives the challenge access structure $\mathcal{A}^*$ from attacker atk.

Setup: To provide a public key PK to atk, sim randomly chooses $\eta' \in \mathbb{Z}_p$and note $\eta = \eta' + ab$. It calculates $e(g_1, g_2)^{\eta}$ as: $e(g,g)^{\eta} = e(g,g)^{\eta'}.e(g,g)^{ab}$. Finally, sim sends public key PK to atk.

Phase 1*:* During this phase, atk submits an attribute set $\mathcal{W}_j \in \mathcal{A}$ such that $\mathcal{W}_j \notin \mathcal{A}^*$, to sim. Simulator sim chooses $r' \in_{randomly} \mathbb{Z}_p$ and sets $r = r' - a$. It can be obtained as follows:

$$D = g^{\eta+\varkappa.r} = g^{\eta}.g^{\varkappa.r} = g^{(\eta'+ab)}.g^{\varkappa(r'-a)} = g^{(\eta'+r'b)}.$$

For each attribute in $\mathcal{W}_j$, sim has to choose $r_j \in_{randomly} \mathbb{Z}_p$. It computes the rest of the secret key as follows:$D_j = g^{r'-a}.H_1(j)^{r_j} = \frac{g^{r'}}{g^a}.H_1(j)^{r_j}, D_j' = g^{br_j}$. Finally, sim sends the SK to atk.

Challenge: The attacker atk submits two equal length messages m_1 and m_2 along with a challenge access structure $\mathcal{A}^*$. sim randomly generates a bit $\hat{\hbar} \in \{0,1\}$ and computes CT^* as $C' = g^a = g^c$,$\tilde{C} = m_{\hat{\hbar}}.e(g,g)^{\eta\alpha} = m_{\hat{\hbar}}.T.e(g,g)^{\eta'\alpha}$. Finally, sim sends the CT^* to atk.

Phase 2*:* Same as the Phase 1.

Guess: The attacker atk outputs a guess $\hat{\hbar}'$of $\hat{\hbar}$. If $\hat{\hbar} = \hat{\hbar}'$, simulator$sim$ guess that $T = e(g,g)^{abc}$. Otherwise, T is a random target group element in G_T.

The advantage of the attacker is ε, when $T = e(g,g)^{abc}$. The advantage of the attacker is $\frac{1}{2}$, when T is a random target group element in G_T. Finally, the advantage of the simulator in this security game is $\frac{\varepsilon}{2}$.

IV. Performance Analysis

This section deals with the performance analysis of the proposed scheme in terms of message size, energy consumption on communications and computation cost.

A. Message Size

The total message size of proposed decryption scheme during communication between data consumer and the BAN controller connection can be computed as

$$size = |ID_s| + |ID_d| + |Encryption(CK)| = \\ |ID_s| + |ID_d| + |T| + |\widetilde{C}_\iota| + |C_i'| + |C_{(x,y)}| + |C'_{(x,y)}| + |\hat{C}_{(x,y),j}| + |sig| = \\ 1 + 1 + 4 + k|p| + k|p| + |p| + |p| + j|p| + k|p| = \\ (3k + j + 2)|p| + 6.$$

It is sufficient forID_s,ID_d and T to have one byte, one byte and four bytes respectively for a WBAN. The elliptic curve is defined over $\mathbb{F}_p$. The message size of the proposed data consumer and the WBAN controller communication is $(16k + 2)$ $bytes$. Similarly, total message size of proposed decryption for communication between data consumer and the sensor connection can be computed as

$$size = |ID| + |Encryption(CK \parallel date)| + |Hash(CK \parallel date)| = \\ |ID| + |T| + |\widetilde{C}_\iota| + |C_i'| + |C_{(x,y)}| + |C'_{(x,y)}| + |\hat{C}_{(x,y),j}| + |sig| \\ + |Hash(CK \parallel date)| = \\ 1 + 4 + k|p| + k|p| + |p| + |p| + j|p| + k|p| + 16k = \\ (3k + j + 2)|p| + 16k + 5.$$

The message size of the proposed data consumer and the sensor communication is $(32k + 2)$ $bytes$.

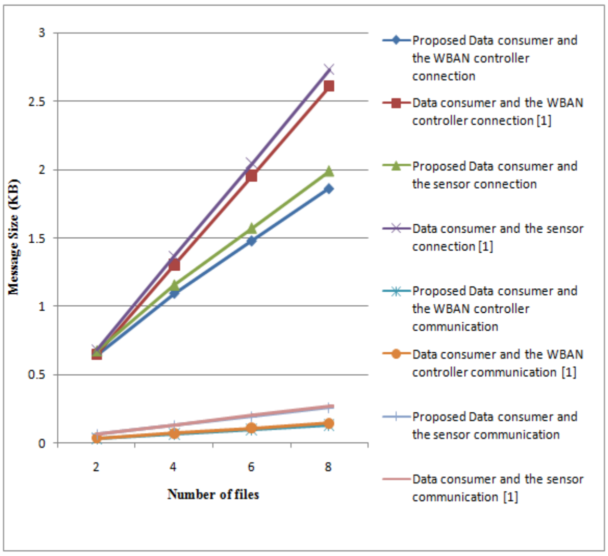

Fig. 2. Message size versus Number of files

TABLE I
Message Size

	Proposed Scheme in $bytes$	Chunqiang Hu et al., [1] in $bytes$
Data consumer and the WBAN controller connection	$((3k + j + 2)\,|p| + 6)$	$(5\,|p| + 6)\,k$
Data consumer and the sensor connection	$((3k + j + 2)\,|p| + 16k + 5)$	$(5\,|p| + 21)\,k$
Data consumer and the WBAN controller communication	$(16k + 2)$	$18k$
Data consumer and the sensor communication	$(32k + 2)$	$34k$

The number of files is k.
The prime order of the group is p.
The Number of transport nodes which carry any information about level node is j.

Table I shows the message size of the proposed scheme and Chunqiang Hu et al., [1]. Figure 2 illustrates the relationship between the message size and the number of files of the proposed scheme and [1]. For this experiment, the security level $p = 64\, bytes$ and number of files $\mathrm{k} = \{2,4,6,8\}$. It clearly shows that, as the number of files are increased, the message size of the proposed scheme is significantly getting reduced when compared with [1]. In this experiment we consider communications between data consumer and WBAN controller/sensors. In the proposed scheme, we observe that the message size has a linear relationship with the number of files for establishing a connection between data consumer and WBAN controller/sensors. We can also find that the proposed scheme shows a drastic improvement when compared with the schemes in [1]. Once the connection is established, the message size of the proposed scheme shows slight improvement when compared with the schemes in [1].

B. *Energy Consumption on Communications*

As noted in [8], a Chipcon CC1000 radio which is used in Crossbow MICA2DOTmotes [9] utilizes $28.6\ \mu J$ to receive one byte and $59.2\ \mu J$ to transmit one byte. For the proposed data consumer and the WBAN controller connections, the total energy consumption in mJ of one data transmission is

$$\big((3k+j+2)\,|p|+6\big)(28.6+59.2)\,/\,1000 = \big((0.2634k+0.0878j+0.1756)\,|p|+0.5268\big) \tag{10}$$

After the connection establishment, the energy consumption in mJ is

$$(16k+2)(28.6+59.2)\,/1000 = (1.4048k+0.1756) \tag{11}$$

The total energy consumption in mJ for the proposed communication for N transmissions is

$$\Big(\big((0.2634k+0.0878j+0.1756)\,|p|+0.5268\big) + (1.4048k+0.1756)\,(N-1)\Big) = \big((1.4048k+0.1756)N+(0.2634k+0.0878j+0.1756)\,|p| - 1.4048k+0.3512\big) \tag{12}$$

For the proposed data consumer and the sensor connections, the total energy consumption in mJ of one data transmission is

$$\big(2\,\big((3k+j+2)\,|p|+16k+5\big)\,(28.6+59.2)\,/1000\big) = \big((0.5268k+0.1756j+0.3512)\,|p|+2.8096k+0.878\big) \tag{13}$$

After the connection establishment, the energy consumption in mJ is

$$(32k+2)\,(28.6+59.2)\,/1000 = (2.8096k+0.1756) \tag{14}$$

The total energy consumption in mJ for the proposed communication for N transmissions is

$$\Big(\big((0.5268k+0.1756j+0.3512)\,|p|+2.8096k+0.878\big) + (2.8096k+0.1756)\,(N-1)\Big) = \big((2.8096k+0.1756)N + (0.5268k+0.1756j+0.3512)\,|p|+0.7024\big) \tag{15}$$

The total energy consumption of some of the other schemes such as certificate-based scheme, Merkle hash tree based scheme, and ID-based scheme are $146.99N\ mJ$, $144.56N\ mJ$ and $111.02N\ mJ$ respectively [9]. Table II shows the energy consumption for communications of the proposed scheme and Chunqiang Hu et al., [1]. Figure 3 illustrates the energy consumption for communications of the proposed scheme and [1] when the number of transmissions $N = 100$, security level $p = 64\ bytes$ and number of files $\mathrm{k} = \{2,4,6,8\}$. It clearly shows that the proposed scheme has lower energy consumption than the schemes in [1] once the connection is established.

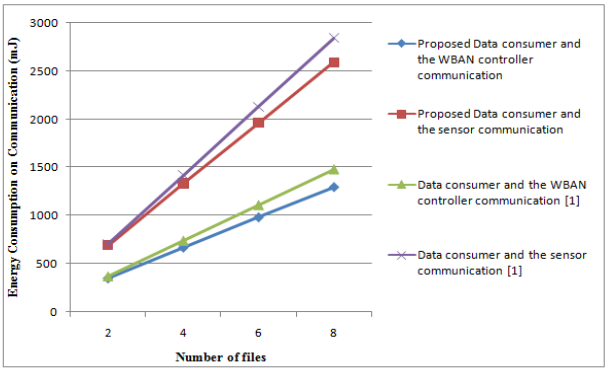

Fig. 3. Energy consumption on communications with regard to the number of files

TABLE II
ENERGY CONSUMPTION FOR COMMUNICATIONS

	Proposed Scheme in mJ	Chunqiang Hu et al., [1] in mJ
Data consumer and the WBAN controller communication	$\big((1.4048k+0.1756)N$ $+\big((0.2634k+0.0878j$ $+0.1756)\,\lvert p\rvert\big)$ $-1.4048k+0.3512\big)$	$(1.5804N$ $+0.439\,\lvert p\rvert$ $-1.0536)k$
Data consumer and the sensor communication	$\big((2.8096k+0.1756)N$ $+\big((0.5268k+0.1756j$ $+0.3512)\,\lvert p\rvert\big)$ $+0.7024\big)$	$(2.9852N$ $+0.878\,\lvert p\rvert$ $-0.7024)\,k$

The number of files is k.
The prime order of the group is p.
The Number of transport nodes which carry any information about level node is j.
The number of transmissions is N.

C. *Computation Cost*

As noted in [10], the computation cost of Tate pairing on a 32-bit ST22 smartcard microprocessor running at 33 MHz is $752\ ms$ approximately. We examine the computation overhead of the proposed scheme on a 32-bit Intel PXA255 processor running at 400 MHz. The computation cost of Tate pairing on a 32-bit Intel PXA255 is $\big((33/400)\times 752 \approx 62.04\big)\ ms$. For establishing connection, the computation cost of the proposed data consumer and the WBAN controller communications is obtained by $(3k+j+2)$ Tate pairing. The total computation cost for establishing connection is $\big((3k+j+2)\ 62.04\big)\ ms$. After connection establishment, the data consumers do not require to compute Tate pairing again until the content key is renewed. For establishing connection, the computation cost of theproposed data consumer and the sensor communications is obtained by $(6k + 2j + 4)$ Tate pairing. The total computation cost for establishing connection is $((6k + 2j + 4)\ 62.04\ )\ ms$. After connection establishment, the data consumers do not require to compute Tate pairing again until the token is updated.

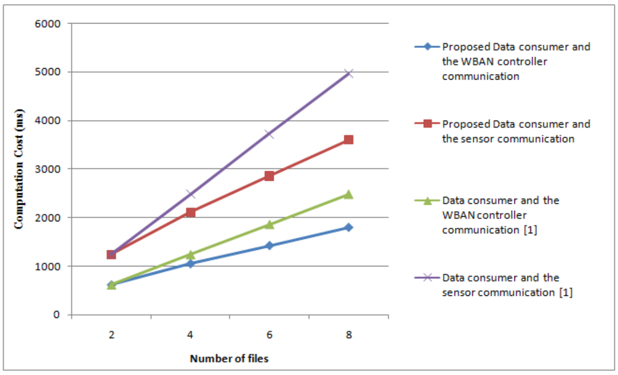

Fig. 4. Computation cost with regard to the number of files

TABLE III
COMPUTATION COST

	Proposed Scheme in ms	Chunqiang Hu et al., [1] in ms
Data consumer and the WBAN controller communication	$((3k + j + 2)\ 62.04)$	$(5k \times 62.04)$
Data consumer and the sensor communication	$((6k + 2j + 4)\ 62.04)$	$(10k \times 62.04)$

The number of files is k.
The prime order of the group is p.
The Number of transport nodes which carry any information about level node is j.

The computation cost of some of the other schemes such as certificate-based scheme, Merkle hash tree based scheme, and ID-based scheme are $36.96N\ ms$, $18.48N\ ms$ and $124.08N\ ms$ respectively [9]. Table III shows the computation cost of the proposed scheme and Chunqiang Hu et al., [1]. Figure 4 illustrates the computation cost of the proposed scheme and [1] when the number of files are increased. It clearly shows that the proposed scheme has a lower computation cost than the schemes in [1]. When we consider the energy consumption incurred by both computation and communications, our proposed scheme is relatively efficient when the number of files k is increased.

V. Conclusions and Future Works

In this paper, we proposed an efficient data communication for WBANs by using a File Hierarchy CP-ABE (FH-CP-ABE). The proposed scheme uses integrated access structure to solve the problem of multiple hierarchical files sharing in WBAN. This enables sensors to share multiple files in a single encryption. As a result, the consumers can decrypt all authorization files by computing secret key once. Performance analysis of the proposed scheme is evaluated in terms of parameters such as message size, energy consumption and computation cost. The results show that the proposed scheme is more efficient than schemes in [1]. In future, we would like to extend this scheme to include policy updating and multi-authority CP-ABE in WBAN.

Acknowledgment

This work was supported by the Ministry of Human Resource Development (MHRD) under the Government of India.

References

[1] Hu, C., Li, H., Huo, Y., Xiang, T. and Liao, X. "Secure and efficient data communication protocol for wireless body area networks." IEEE Transactions on Multi-Scale Computing Systems, 2.2 (2016): 94-107.

[2] Li, Fagen, and Jiaojiao Hong. "Efficient Certificateless Access Control for Wireless Body Area Networks." IEEE Sensors Journal 16.13 (2016): 5389-5396.

[3] M. Rushanan, A. D. Rubin, D. F. Kune, and C. M. Swanson, “Sok: Security and privacy in implantable medical devices and body area networks,” in Proc. IEEE Symp. Security Privacy, 2014, pp. 524–539.

[4] Al Ameen, Moshaddique, Jingwei Liu, and KyungsupKwak. "Security and privacy issues in wireless sensor networks for healthcare applications." Journal of medical systems 36, no. 1 (2012): 93-101.

[5] B. Chandrasekaran and R. Balakrishnan, "Efficient pairing computation for Attribute Based Encryption using MBNR for Big Data in cloud," 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), Bangalore, 2016, pp. 243-247.

[6] Sahai, Amit, and Brent Waters. "Fuzzy identity-based encryption." In Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 457-473. Springer, Berlin, Heidelberg, 2005.

[7] Wang, S., Zhou, J., Liu, J.K., Yu, J., Chen, J. and Xie, W.,"An efficient file hierarchy attribute-based encryption scheme in cloud computing." IEEE Transactions on Information Forensics and Security 11.6 (2016): 1265-1277.

[8] Wander, A.S., Gura, N., Eberle, H., Gupta, V. and Shantz, S.C.,"Energy analysis of public-key cryptography for wireless sensor networks." Pervasive Computing and Communications, 2005. PerCom 2005. Third IEEE International Conference on. IEEE, 2005, pp. 324-328.

[9] K. Ren, W. Lou, K. Zeng and P. J. Moran, "On Broadcast Authentication in Wireless Sensor Networks," in IEEE Transactions on Wireless Communications, vol. 6, no. 11, pp. 4136-4144, November 2007.

[10] Bertoni, G., Chen, L., Fragneto, P., Harrison, K. and Pelosi, G., "Computing tate pairing on smartcards." White Paper STMicroelectronics (2005).Available:http://www.st.com/stonline/products/families/smartcard/ches2005 v4. Pdf

Balaji Chandrasekaran received the B.E degree in Computer Science and Engineering from J.J College of Engineering and Technology, Anna University, Chennai in 2009 and the M.E degree in Software Engineering from Anna University, Tiruchirappalli in 2011. Currently, he is a PhD researcher in the Department of Computer Applications at National Institute of Technology, Tiruchirappalli, India. His research interests include: Cryptography, Cloud Computing, and Information Security. He is a student member of ACM.

Ramadoss Balakrishnan received the M.Tech degree in Computer science and Engineering in 1995 from the Indian Institute of Technology, Delhi and the PhD degree in Applied Mathematics in 1983 from Indian Institute of Technology, Bombay. Currently he is working as a Professor of Computer Applications at National Institute of Technology, Tiruchirapalli. His research interests include: Software Testing Methodologies, Security and Privacy in Big Data and Cloud, software Metrics, Data Warehouse – EAI, Data Mining, WBL, and XML. He is a recipient of Best Teacher Award at National Institute of Technology, Tiruchirapalli, India during 2006-2007. He is a member of IEEE, Life Member (LM) of ISTE, New Delhi, Life Member (LM), Computer Society of India.

Yasuyuki Nogami graduated from Shinshu University in 1994 and received the PhD degree in1999 from Shinshu University. He is now an associate professor of Okayama University. His main fields of research are finite field theory and its applications such as recent public key cryptographies. He is now studying about elliptic curve cryptography, pairing-based cryptography, Lattice-based cryptography, pseudo random number generator, Advanced Encryption Standard, and homomorphic encryptions. Recently, he is a member of security research group in Okayama University and particularly focusing on IoT security from the viewpoints of software and hardware implementations. He is a member of IEICE and IEEE.