Access Control for Wireless Body Area Networks

Gang Shen[1], Wenxiang Song[1], Yumin Gui[2(✉)], and Hanjun Gao[3]

[1] School of Computer Science, Hubei University of Technology, Wuhan 430068, China
shengang@hbut.edu.cn, 547521741@qq.com

[2] Department of Ophthalmology, Wuhan Puren Hospital, Wuhan 430080, China
5537468@qq.com

[3] China Nuclear Power Operation Technology Corporation, LTD.,
Wuhan 430070, China
gaohj@cnnp.com.cn

Abstract. Wireless body area network (WBAN) is a network providing healthcare, which is becoming more and more popular. However, the crucial issues of security and privacy in WBAN should still be considered. In this paper, we propose a secure access control scheme for WBAN, which is based on ciphertext policy attribute-based encryption (CP-ABE). Specifically, if the physician has attributes that satisfy the access structure set by the patient, he/she can decrypt the patient's physiological data. A secure two-party protocol is adopted to protect data from internal attacks. In addition, our scheme can implement the strategy that physicians at different levels can only access the corresponding information of patient, which is conducive to improving the efficiency of access. Security analysis indicates that proposed scheme can resist various security threats and achieve privacy preservation of patients' sensitive information. Compared with related schemes, our scheme is more secure and efficient.

Keywords: Wireless body area networks · Access control · Sensitive information · Privacy protection

1 Introduction

WBAN, a special wireless sensor network, is mainly formed by various low-energy, low-cost, heterogeneous, tiny sensors worn on the body. As a popular technology, WBAN has been widely used in e-health to monitor the patients physical health in real time [11]. The sensors in WBAN, such as electrocardiograph (ECG), electroencephalography (EEG), blood pressure, are used to collect and monitor the patients' various physiological signals. The physiological information processed by the sensor network will be transmitted to the remote health care servers or the personal server device via Internet [9].

WBAN plays a very important role in today's medical services because it can bring people the following benefits [1]: i) provide remote health monitoring

D. Wang et al. (Eds.): SPNCE 2020, LNICST 344, pp. 244–254, 2021.
https://doi.org/10.1007/978-3-030-66922-5_16

for patients; ii) achieve real-time diagnosis; iii) give much physical mobility for patients; iv) reduce expenses to medical server; v) store patients' medical data for real-time accessing. However, the disclosure of physiological information could bring a potential threat to patient's privacy [7], e.g., the patient's health status or personal information could be inferred by physiological information. In addition, if the patient's physiological information is maliciously modified, it may cause his/her condition to be misdiagnosed. Therefore, privacy-preserving technique must be employed in WBAN communications. To solve the privacy problem, many related schemes have been proposed for WBAN [8,12,14,15]. Zhang et al. [15] use the biometric signal as the key to encrypt the medical data, and the receiver can decrypt the data by using the same key. Li et al. [8] present an anonymous mutual authentication and key agreement scheme for WBAN. To protect the patient's identity privacy, location privacy and sensor deployment privacy, Zhou et al. [14] propose a secure and privacy-preserving key management scheme for cloud-based WBAN. They embed the symmetric structure of human body into the symmetric key mechanism of Blom by using blind technology and improved secret sharing technology. Tian et al. [12] introduce the scheme of access control of key policy attribute-based encryption (KP-ABE) [4] in WBANs. In their schemes, the ciphertext can be decrypted if the attribute set related to the ciphertext meet the access structures associated with user's key. However, comparing KP-ABE and CP-ABE [2], the latter is more suitable for data sharing systems. The reason is that data users have the right to decide access policies in CP-ABE [3,6,13]. Additionally, Hur [5] provides a CP-ABE scheme for a secure data sharing system, which solves the key escrow problem by using a secure two-party computation (2PC) protocol.

The above mentioned schemes cannot satisfy the requirements of resisting internal attacks and hierarchical access at the same time. Therefore, we propose a secure user access control scheme for WBAN in this paper. Specifically, the main **contributions** of this work are as threefold.

(1) Firstly, we propose a scheme based on CP-ABE, which employs the 2PC protocol mentioned in scheme [5] to ensure the confidentiality of patient's physiological information. Security analysis indicates that the proposed scheme can resist not only external attacks but also internal attacks.
(2) Secondly, in order to improve the diagnosis efficiency, the proposed scheme can realize hierarchical access, that is, physicians at different levels can only access the corresponding information of patient.
(3) Finally, the performance and security of the proposed scheme are analyzed. The results show that the proposed scheme is efficient and secure, and is suitable for WBAN.

The remaining part of the paper is organized as follows. We introduce some preliminary knowledge in Sect. 2. In Sect. 3, we propose the concrete scheme. The security analysis is described in Sect. 4. We also discuss the performance evaluation in Sect. 5. Finally, we draw our conclusions in Sect. 6.

2 Preliminaries

2.1 System Model

The entities in our scheme are as follows: a key generation center (KGC), a data server (DS), a physiological data owner (PDO) and a set of physicians, as shown in Fig. 1. We assume that KGC and DS could become the internal attackers under the influence of adversary.

(1) Key generation center (KGC): KGC is an honest-but-curious institution which generates parameters for CP-ABE. It is responsible for publishing, revoking, and updating physician's attribute key, and granting differential access permissions to physicians according to their attributes.
(2) Data server (DS): DS is an incompletely trusted institution for key generation, which is responsible for providing stored data access to external users.
(3) Physiological data owner (PDO): PDO has physiological data, and can upload the data into the DS for monitoring. In addition, PDO is responsible for dividing the information into different levels and defining access policy.
(4) Physicians: Physicians include resident physician, physician-in-charge, associate chief physician and chief physician. Physicians with different titles can access the corresponding level of physiological information on DS.

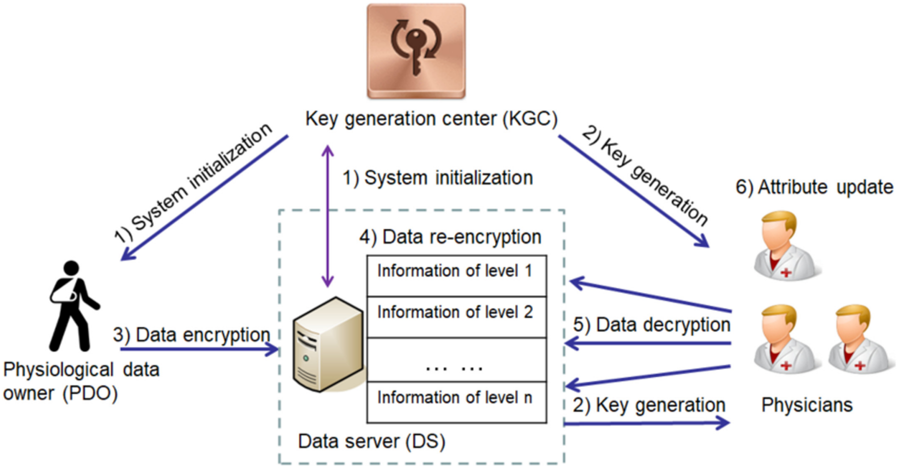


Fig. 1. System model.

2.2 Design Goals

Based on the aforementioned system model, we design a secure user access control scheme that has the following two desirable objectives.

(1) *Security.* The adversary cannot eavesdrop on the patient's information from the transmitted data, thus ensuring the patient's privacy.
(2) *Efficiency.* In the proposed scheme, physicians at different levels can only obtain corresponding information, which improves the efficiency of the system to a certain extent.

2.3 CP-ABE Scheme

CP-ABE scheme [2] consists of the following four algorithms:

(1) Setup: The public parameters PK and master key MK are generated by this algorithm.
(2) Encryption: Input a plaintext M, the public parameters PK and an access structure $\mathbb{T}$, output the ciphertext CT.
(3) Key generation: Input a set of attributes S, the master key MK, and the public parameters PK, output a decryption key SK.
(4) Decryption: Input the ciphertext CT, the parameters PK and the decryption key SK, output the plaintext M.

2.4 Access Tree

The access tree $\mathbb{T}$ is used to represent the structure of access control. The parameters in the tree are presented in Table 1. Ciphertext is associated with $\mathbb{T}$, and each non-leaf node of $\mathbb{T}$ denotes a threshold gate. Let $\mathbb{T}_x$ be an subtree of $\mathbb{T}$ and A be a set of attributes that satisfies $\mathbb{T}_x$. $\mathbb{T}_x(A)$ can be calculated using the following recursive process.

(1) $\mathbb{T}_x(A)$ will be calculated when x is a non-leaf node. Only if at least t_x children return 1, $\mathbb{T}_x(A)$ returns 1.
(2) When x is a leaf node, then $\mathbb{T}_x(A)$ returns 1 if and only if $\lambda_x \in A$.

Table 1. Notation description

Notation	Description
$\mathbb{T}$	Access structure
x	Non-leaf node
num_x	The number of children of node x
t_x	Threshold value
λ_x	The attribute associated with the leaf node x
$p(x)$	The parent of the node x in $\mathbb{T}$
$index(x)$	Return a number associated with node x
$\mathbb{T}_x$	The subtree of $\mathbb{T}$ rooted at the node x
A	A set of attributes, and $\mathbb{T}_x(\gamma) = 1$

3 The Proposed Concrete Scheme

The proposed concrete scheme includes six phases: system initialization, key generation, data encryption, data re-encryption, data decryption and attribute update.

3.1 System Initialization

In the proposed scheme, the PDO first divides his/her physiological data PF into n parts of different levels, that is $PF = \{PF_1, PF_2, \cdots PF_n\}$ [10]. Next, each physiological data PF_i is encrypted by using a symmetric key sk_i. That is, the information of level i is $CPF_i = Enc_{sk_i}(PF_i)$, where $Enc(\cdot)$ is a symmetric encryption algorithm. PDO encrypts a set of symmetric keys $\{sk_1, sk_2, \cdots, sk_n\}$ with the CP-ABE scheme and store them in DS with $\{CPF_1, CPF_2, \cdots, CPF_n\}$. Therefore, the physicians at different levels can obtain different levels of physiological information about PDO.

We assume the system is bootstrapped by KGC. Given a security parameter κ, KGC generates $(q, g, \mathbb{G}_1, \mathbb{G}_2, e)$ by running $\mathcal{G}(\kappa)$, where $g \in \mathbb{G}_1$. We define the Lagrange coefficients $\varDelta_{i,\varPhi}$ as $\varDelta_{i,\varPhi}(x) = \Pi_{j\in\varPhi, j\neq i}\frac{x-j}{i-j}$, where $i \in \mathbb{Z}_q^*$ and a set $\varPhi$ of elements in $\mathbb{Z}_q^*$. We also choose two hash functions $H_0 : \{0,1\}^* \rightarrow \mathbb{G}_1$ and $H_1 : \mathbb{G}_2 \rightarrow \mathbb{Z}_q^*$. Then, the pairs of master public and private key of KGC and DS are given, respectively. KGC picks a random number $\beta \in \mathbb{Z}_q^*$ as its master private key, and calculates the master public key $v = g^\beta$, so its pairs of master public and private key is $(PK_K = v, MK_K = \beta)$. DS selects a random number $\alpha \in \mathbb{Z}_q^*$, and the pairs of master public and private key is $(PK_D = e(g,g)^\alpha, MK_D = g^\alpha)$. DS also picks $\gamma \in \mathbb{Z}_q^*$, and publishes $PK_D^{'} = g^\gamma$ as another master public key. Finally, the system parameters $\{\mathbb{G}_1, g, H_0, H_1\}$ are published, $\{\alpha, \beta, \gamma\}$ are kept.

3.2 Key Generation

Each physician runs following steps to obtain secret key set:

(1) To authenticate the user, the 2PC protocol will be used. KGC first chooses a random number $r_k \in_R \mathbb{Z}_q^*$ as the secret of the physician. Then, 2PC protocol returns the output $w = (\alpha + r_k)\beta$ to DS. DS randomly selects $\tau \in_R \mathbb{Z}_q^*$ and computes $X = g^{w/\tau} = g^{(\alpha+r_k)\beta/\tau}$, and then sends it to KGC. After receiving X, KGC computes $Y = X^{1/\beta^2} = g^{(\alpha+r_k)/\tau\beta}$, and sends it to the DS. DS outputs a personal key component $D = g^{(\alpha+r_k)/\beta}$ by computing Y^τ.

(2) We suppose that physician's attribute set is A as input by KGC. The output is that a group of attribute keys and secret value r_k identified by the group. For each attribute $j \in A$, KGC picks random $r_j \in \mathbb{Z}_q^*$. Then, it computes physician's attribute keys as follows:

$$SK_{K,p} = (\forall j \in A : D_j = g^{r_k} H_0(j)^{r_j}, D_j' = g^{r_j}). \qquad (1)$$

(3) The physician's personal key $SK_{D,p} = D$ is outputted by DS. Whole secret key set of physician is as:

$$\begin{aligned} SK_p &= (SK_{D,p}, SK_{K,p}) \\ &= (D = g^{(\alpha + r_k)/\beta}, \forall j \in A : D_j = g^{r_k} H_0(j)^{r_j}, D'_j = g^{r_j}). \end{aligned} \quad (2)$$

Additionally, the DS also outputs another secret $SK_p^{'} = H_0(ID_p)^{\gamma}$, which will be used to distribute the selective attribute group key, where ID_p denotes the identity of physician.

3.3 Data Encryption

We assume that the symmetric key is $sk_i \in \mathbb{G}_2$. Before sk_i is send to the DS for sharing, it will be encrypted under $\mathbb{T}$ of defining by PDO, who can obtain the ciphertext as follows:

(1) Choose a polynomial q_x for each node x in $\mathbb{T}$. Let the degree of q_x be d_x, where $d_x = t_x - 1$ and t_x is the threshold value.
(2) PDO picks a random $s \in \mathbb{Z}_q^*$ and sets $q_R(0) = s$ for the root node R. It sets $q_x(0) = q_{p(x)}(index(x))$ for any other x, and selects d_x to define q_x.
(3) The ciphertext CT is constructed as:

$$\begin{aligned} &\mathrm{CT} = (\mathbb{T}, C_1 = sk_i \cdot e(g,g)^{\alpha}), C_2 = v^s, \forall y \in B : C_y = g^{q_y(0)}, \\ &C'_y = H_0(\lambda_y)^{q_y(0)}). \end{aligned} \quad (3)$$

where B is a group of leaf nodes in $\mathbb{T}$.
(4) Send encrypted physiological data CT to DS.

3.4 Data Re-encryption

The proxy re-encryption protocol is used by DS to achieve user revocation. The protocol is executed as follows:

(1) DS Chooses $K_{\lambda_y} \in \mathbb{Z}_q^*$, and re-encrypts CT as CT′:

$$\begin{aligned} &\mathrm{CT}' = (\mathbb{T}, C_1 = sk_i \cdot e(g,g)^{\alpha}), C_2 = v^s, \forall y \in B : C_y = g^{q_y(0)}, \\ &C'_y = (H_0(\lambda_y)^{q_y(0)})^{K_{\lambda_y}}). \end{aligned} \quad (4)$$

(2) DS selects random $\rho \in_R \mathbb{Z}_q^*$, and $\forall physician \in \mathbb{G}_1$, and computes $x_k = H_1(e(H_0(ID_p)^{\rho}, PK_D^{'}))$.
(3) DS constructs the function of polynomial as:

$$f^y(x) = \prod_{i=1}^{m}(x - x_i) = \sum_{i=0}^{m} \alpha_i x^j (modq). \quad (5)$$

(4) A random $r \in \mathbb{Z}_q^*$ is chosen by DS who constructs HM_y, and generates a message of head as:

$$HM = (g^{\rho}, \forall y \in B : HM_y). \quad (6)$$

where $HM_y = \{K_{\lambda_y} \cdot g^{ra_0}, g^{ra_1}, ..., g^{ra_m}\}$. The DS responds with (HM_y, CT') to physician after receiving data request query from the physician.

3.5 Data Decryption

If a physician is associated with an attribute λ_y, he/she can obtain attribute group key K_{λ_j} from HM_j as follows:

(1) Computes x_k, then computes K_{λ_j}.
(2) Then physician uses the attribute group keys to update its secret key as follows:

$$SK_p = (D = g^{(\alpha+r_k)/\beta}, \forall j \in \Lambda : D_j = g^{r_k} H_0(j)^{r_j}, D'_j = (g^{r_j})^{1/K_{\lambda_j}}). \quad (7)$$

where Λ denotes a set of attributes.
(3) Suppose x is a leaf node, and $\lambda_k \in \Lambda$, then physician computes

$$DecryptNode(CT', SK_p, x) = e(g,g)^{r_k q_x(0)}. \quad (8)$$

(4) Suppose x is a non-leaf node. The physician computes F_z as the output of $DecryptNode(CT', SK_p, z)$ for all x's children nodes z:

$$F_x = e(g,g)^{r_k q_x(0)}. \quad (9)$$

(5) Let $DecryptNode(CT', SK_p, R)$ is a function of the root node R of $\mathbb{T}$. Then, $DecryptNode(CT', SK_p, z) = e(g,g)^{r_k s}$. The sk_i can be recovered by calculating as $CT' = sk_i$.
(6) Finally, the physician can decrypt the information of level i ($PF_i = Dec_{sk_i}(CPF_i)$) by using the secret key sk_i.

3.6 Attribute Update

If physician can improve his/her access level by updating the attributes. Specifically, KGC update the physician's attribute set A to A'. Then, the physician's new key becomes SK'_p.

4 Security Analysis

In this section, we will conduct the security analysis of the proposed scheme.

4.1 Resist Internal Attacks

In the proposed scheme, KGC and DS cannot decrypt the physiological data alone even if they get the ciphertext. The reason is that KGC and DS do not know each other's master secrets due to the 2PC protocol, so they cannot generate physician's secret keys independently [5]. Therefore, the proposed scheme can resist internal attacks.

4.2 Resist External Attacks

In addition, data confidentiality against the outside adversary can be also guaranteed. The physician cannot obtain the desired value $e(g,g)^{r_k s}$ if the set of attributes do not meet $\mathbb{T}$ in the ciphertext. In order to decrypt a node x holding an attribute λ_x, the physician must obtain pair (C'_x, D'_x) from the ciphertext and its private key, respectively. C'_x is blinded, which means the physician cannot get the value $e(g,g)^{r_x q_x(0)}$, the updated attribute group key cannot be obtained by the revoked physician. Users whose attributes cannot meet the access policy will be not able to decrypt the ciphertext. Therefore, the proposed scheme can resist external attacks.

4.3 Collusion Resistance

In this scheme, since the value is randomized from the private key of particular user, value $e(g,g)^{\alpha s}$ cannot be recovered by the attackers of collusion.

5 Performance Evaluation

We first compare our scheme with scheme [12] in terms of the main characteristic. Then the performance of the computational cost of data encryption and decryption is analyzed.

5.1 Comparative Analysis

Tian et al. [12] propose a scheme of KP-ABE for access control in WBAN, in which the ciphertext can be decrypted if his/her attributes related to the ciphertext meet the access structures. However, our scheme is based on CP-ABE. Since data owners master the access policy in CP-ABE, it is more suitable for practical application than KP-ABE. For example, PDO can define the access policies based on the attributes owned by the physician's level. When the physician's attributes meet the access structure of the encrypted data, the physician can decrypt the patient's physiological data. Therefore, the access control based on CP-ABE is more efficient and flexible. Additionally, our proposed scheme also uses a 2PC protocol in phase of key generation to resist the internal attacks. We present the main performance comparison in Table 2. Compared with the schemes [12], the proposed scheme can better realize both the efficiency of user access control, and realize hierarchical access of patient's physiological data.

5.2 Performance Evaluation

In this paper, the evaluations are conducted on Intel Core i7-6700 @3.10 GHz with 8 GB RAM. The computation costs of our scheme are showed in Table 3, where k_1 denotes the number of attributes associated with physician's private key, k_2 denotes the number of physicians in an attribute group and k_3 denotes the

Table 2. Performance comparison

Characteristics	[12]	Proposed scheme
Security of system entities	No-mentioned	Honest-but-curious
Type of ABE	KP-ABE	CP-ABE
Hierarchical access	No	Yes
Data confidentiality	Yes	Yes
User revocation	Yes	Yes
Collusion attack resistance	Yes	Yes
Data re-encryption	No	Yes
Attribute updated	Yes	Yes
Resist internal attacks	No	Yes

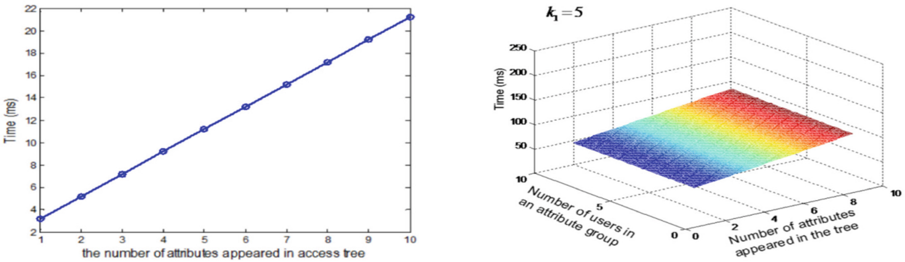
Table 3. Comparison of computational costs

	Encryption	Decryption
Time	$(2k_3+1)T_{eG_1}+T_{eG_2}$	$k_1k_2T_{eG_1}+T_{eG_2}logk_3+(2k_1+2)T_p$

number of attributes appeared in $\mathbb{T}$. In addition, T_{eG_1}, T_{eG_2} and T_P represent an exponentiation operation in $\mathbb{G}_1$, an exponentiation operation in $\mathbb{G}_2$ and a bilinear pairing operation, respectively.

Figure 2 shows the computational costs of data encryption and decryption, respectively. We can see that the proposed scheme is efficient for reducing the computational costs of data encryption and decryption.

In our scheme, the patient's physiological information is divided into n parts and encrypted as $\{CPF_1, CPF_2, \cdots, CPF_n\}$. We assume that the time taken for decrypting a physiological information is t. In the traditional ABE scheme, the time for a physician to obtain patient information is nt, while in our scheme, the time for a physician to obtain patient information is t. Therefore, our scheme can greatly improve the diagnostic efficiency.



(a) Computational costs of encryption.

(b) Computational costs of decryption.

Fig. 2. Computational costs.

6 Conclusion

In this paper, we propose a secure access control scheme based on CP-ABE for WBAN. Specifically, the system employs the CP-ABE and a secure 2PC protocol to resist the internal attacks. Additionally, the physicians at different levels can only access the corresponding information of patient, which realize hierarchical access to improve the diagnosis efficiency. Security analysis and experimental results demonstrate that the proposed scheme can realize secure and efficient user access control in WBAN.

Acknowledgment. We are grateful to the anonymous reviewers for their invaluable comments. The Ph.D research startup foundation of Hubei University of Technology under Grant No. BSQD2019023.

References

1. Ali, M., Sadeghi, M., Liu, X.: Lightweight fine-grained access control for wireless body area networks. Sensors **20**(4), 1–22 (2020)
2. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. IEEE Symposium on Security and Privacy, pp. 321–334 (2007)
3. Bobba, R.: Attribute-sets: a practically motivated enhancement to attribute-based encryption. Cryptology ePrint Archive, pp. 587–604 (2009)
4. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: Proceedings of ACM Conference on Computer and Communications Security, pp. 89–98 (2006)
5. Hur, J.: Improving security and efficiency in attribute-based data sharing. IEEE Trans. Knowl. Data Eng. **25**(10), 2271–2282 (2013)
6. Ibraimi, L., Petkovic, M., Nikova, S., Hartel, P., Jonker, W.: Mediated ciphertext-policy attribute-based encryption and its application. In: Youm, H.Y., Yung, M. (eds.) WISA 2009. LNCS, vol. 5932, pp. 309–323. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-10838-9_23
7. Kargl, F., Lawrence, E., Fischer, M., Lin, Y. Y.: Security, privacy and legal issues in pervasive eHealth monitoring systems. In: Proceedings of International Conference on Mobile Business, pp. 296–304. IEEE (2008)
8. Li, X., Ibrahim, M.H., Kumari, S., Sangaiah, A.K., Gupta, V., Choo, K.K.R.: Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks. Comput. Netw. **129**(2), 429–443 (2017)
9. Meharouech, A., Elias, J., Mehaoua, A.: Future body-to-body networks for ubiquitous healthcare: a survey, taxonomy and challenges. In: Proceedings of International Symposium on Future Information and Communication Technologies for Ubiquitous Healthcare, pp. 1–6. IEEE (2015)
10. Shen, G., Su, Y., Zhang, M.: Secure and membership-based data sharing scheme in V2G networks. IEEE Access **6**(1), 58450–58460 (2018)
11. Salayma, M., AI-Dubai, A., Romdhani, I., Nasser, Y.: Wireless body area network (WBAN): a survey on reliability, fault tolerance, and technologies coexistence. ACM Comput. Surv. **50**(1), 31–338 (2017)
12. Tian, Y.: An attribute-based encryption scheme with revocation for fine-grained access control in wireless body area networks. Int. J. Distrib. Sens. Netw. **2014**(11), 1–9 (2014)

13. Yu, S., Wang, C., Ren, K, Lou, W.: Attribute based data sharing with attribute revocation. In: Proceedings of ACM Symposium on Information Computer and Communication Security, pp. 261–270 (2010)
14. Zhou, J., Cao, Z., Dong, X., Xiong, N., Vasilakos, A.V.: 4S: a secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks. Inf. Sci. **314**, 255–276 (2015)
15. Zhang, Z., Wang, H., Vasilakos, A.V., Fang, H.: ECG-cryptography and authentication in body area networks. IEEE Trans. Inf Technol. Biomed. **16**(6), 1070–1078 (2012)