Hindawi
Security and Communication Networks
Volume 2017, Article ID 4364376, 16 pages
https://doi.org/10.1155/2017/4364376

Research Article

LEPA: A Lightweight and Efficient Public Auditing Scheme for Cloud-Assisted Wireless Body Sensor Networks

Song Li,[1] Jie Cui,[1] Hong Zhong,[1] Yiwen Zhang,[1] and Qiang He[2]

[1]*School of Computer Science and Technology, Anhui University, Hefei, Anhui, China*
[2]*School of Software and Electrical Engineering, Swinburne University of Technology, Melbourne, VIC, Australia*

Correspondence should be addressed to Jie Cui; cuijie@mail.ustc.edu.cn

Received 26 March 2017; Accepted 23 May 2017; Published 19 July 2017

Academic Editor: Chang Liu

From smart watch to remote healthcare system, wireless body sensor networks (WBSNs) play an important role in modern healthcare system. However, the weak capacity of devices has limited WBSNs development. Considering the huge processing and storage capacity of the cloud, it can be merged with WBSNs to make up for the deficiencies of weak capacity. Based on this consideration, the concept of cloud-assisted WBSNs has been proposed recently. In contrast to generic data, the data in cloud-assisted WBSNs will be used for providing medical diagnosis, so the integrity of data is very important because any modification will result in severe consequences such as misdiagnosis. The public auditing scheme could provide an efficient solution to check the data integrity remotely without downloading them. However, the traditional public auditing scheme for cloud cannot be used directly due to the high data density and weak processing capacity in WBSNs. So, in this paper, we proposed a lightweight and efficient public auditing scheme, LEPA, for cloud-assisted WBSNs. Compared with similar schemes, the WBSNs' client only needs to do one symmetrical encryption with low computational cost in LEPA. Security proof shows that LEPA can resist two types of adversaries in random oracle model. The efficiency evaluation also shows that LEPA outperforms previous proposals.

1. Introduction

With the technological advances in various fields, the people's life expectancy increased all over the world. In Unites States, the life expectancy has increased to 78.2 years from 69.8 years over the last 50 years [1]. It is expected that the number of people aged 60 years and older will reach about 81 million in 2050. The aging population brings many social and economic challenges. For example, the healthcare of elderly with chronic diseases caused the huge burden on society. To solve these problems, the modern medical system with function of the remote medical clinical diagnostics and real-time health monitoring has gained more and more attention, while the WBSNs (wireless body sensor networks) technique plays a fundamental role in intelligent modern medical system.

The body sensor networks (BSNs) were initially proposed by Zimmerman [2]. Due to the use of wireless communication technique, they are also known as wireless body sensor networks (WBSNs). WBSNs are body-centric networks within of 3–5 m. In general, the WBSNs devices can be classified as wearable devices and implantable devices. The wearable devices can be deployed on clothing or body surface and implantable devices can be implanted into human body to collect the Personal Health Information (PHI) such as electrocardiogram and blood pressure. After being collected, the PHI will be sent to the controller (mobile phone) via wireless technique such as WiFi or Bluetooth. Then controller can process/store the received PHI locally or send it to remote medical service provider which can analyze the user's PHI to give health suggestion. In some emergency situations such as sudden infant death syndrome (SIDS) which was not preventable in the past, the SP can react, process PHI immediately, and inform the medical staff to take emergency measures immediately (Figure 1 shows the typical architecture of WBSNs application for remote medical diagnosis). In addition, WBSNs also can provide other entertainment applications such as motion sensing game or social network.

Considering the eager demand of WBSNs in reality, a number of research institutions have conducted researches on

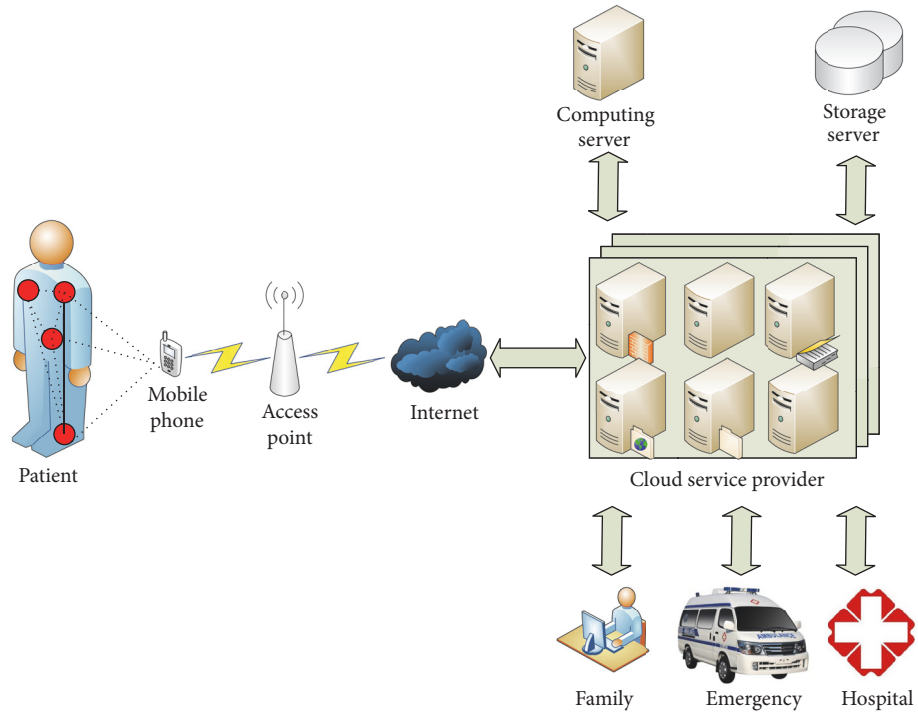

Figure 1: The system model of WBSNs application for remote medical treatment.

the WBSNs system [3–8]. In 2004, [6], the Harvard University launched a system called CodeBlue for emergency care. In 2004 [7], the French CENS Research Institute launched the MARSIAN project. MARSIAN is a wrist ambulatory monitoring and recording system with a smart glove embedded with physiology sensors for the detection of the activity of the autonomic nervous system. In 2005 [8], NASA and Stanford University jointly developed the LifeGuard system for space and terrestrial applications. Recently, some WBSNs based healthcare monitoring and diagnosis architecture also have been proposed [9, 10]. In [9], Wannenburg and Malekian proposed a health monitoring scheme which is capable of measuring the vital physiological parameters and sending biofeedback to user. When an emergency is detected, the medical notification will be sent to medical team. To connect the conventional electromagnetic-based Internet to the biochemical signaling-based bionanonetwork, Chude-Okonkwo et al. proposed an illustrative scenario and system model of an IoBNT for application in an advanced healthcare delivery system in literature [10]. In 2012 [11], to generalize the applications based on WBSNs, the Institute of Electrical and Electronics Engineers (IEEE) released the 802.15.6 standard to support for low energy consumption, short distance, and reliable wireless network communication surrounding the human body area.

For the reason that the WBSNs applications are related to people's life security, the security problem is a very important issue. On the Black Hat conference in 2012, a McAfee expert has proved that, by remotely controlling the insulin pump implanted in the body, hacker can inject an overdose of insulin causing patient death. Besides, the data collected and transmitted in WBSNs are very sensitive because they are used for clinical diagnostics. Therefore, authentication, data confidentiality, integrity, access control, and privacy preserving should be guaranteed while using the WBSNs. In HIPAA (Health Insurance Portability and Accountability Act), there are strict requirements for the patient's identity and data privacy. The standard 802.15.6 also emphasises the security issues in WBSNs. In 802.15.6, the communication is divided into three security levels.

Level 0. It is unsecured level without authentication or encryption. This is the lowest level of security in 802.15.6; the data is transmitted in plaintext and no authentication steps are executed at all.

Level 1 (Only Authentication). Some measures are involved to validate the data, but the data is still transmitted in plaintext without encryption.

Level 2 (Authentication and Encryption). This is the highest level of security in 802.15.6, where the data is transmitted in ciphertext form and authentication is provided.

However, some recent works show that 802.15.6 has security defects [12, 13]. Therefore, the 802.15.6 is not secure enough for reality practice.

With the maturity of the cloud computing technology, WBSNs and cloud computing technique have been merged closely. Compared with WBSNs device, cloud server has more powerful computing and storage capacity which is nicely complementary with WBSNs devices. Based on this consideration, the concept of cloud-assisted WBSNs has

been proposed. Cloud-assisted WBSNs can provide the user with richer experience than traditional WBSNs: user can upload the PHI to cloud storage server to reduce the local storage burden; user also can outsource the large amount of collected PHI to cloud computing server to conduct medical big data analysis. Recently, many cloud-assisted WBSNs systems have been proposed [14–17]. It is noteworthy that the data stored in cloud-assisted WBSNs are the basis of all clinical diagnoses, so the integrity of storing data is a very important issue because any modification on data will result in severe consequences such as misdiagnosis. To solve this problem, the public auditing technique is proposed. The public auditing scheme could provide an efficient solution to check the data integrity remotely without downloading them. Many public auditing schemes for cloud have been proposed [18–28] recently. However, these schemes cannot be used directly in cloud-assisted WBSNs due to the high data density in WBSNs and weak processing capacity of WBSNs devices.

To resolve the drawbacks in the existing schemes, we proposed a lightweight and efficient public auditing scheme for cloud-assisted WBSNs—LEPA in this paper. Based on the lightweight designing concept, we reduced the cryptographic operation of client in our protocol; besides, by transferring the authenticator generation work to service provider, the client (WBSNs devices) in our scheme only needs to do one symmetric encryption.

Based on our scheme, LEPA, a large number of user's physiological data can be uploaded to the remote cloud server to build the user's historical health record. Besides, the user can check the integrity of the data stored in the cloud at any time. Our scheme can be used in the environment below: if a hospital is reluctant to purchase equipment or build its own data center, the hospital can upload patients' data to the remote cloud service provider. However, considering the requirement for the accuracy of medical data, hospital needs to audit the data integrity stored in the cloud at any time. The contributions in this paper can be summarized as follows.

(1) We analyzed the differences between cloud environment and cloud-assisted WBSNs including the traffic characteristic, the capacity of the equipment, and the privacy requirements. Based on these discussions, we think that the existing public auditing schemes are not suitable for the data integrity checking task in cloud-assisted WBSNs.

(2) We proposed a new public auditing scheme LEPA for cloud-assisted WBSNs. Based on the designing concept of lightweight cryptographic protocols, we reduced the operations with expensive time cost such as bilinear mapping and hash to point and improved the efficiency of the system; besides, we translated the tag generation work from client to service provider so as to reduce the computational burden on client kind.

The rest of paper is organized as follows: in Section 2, we introduce some related works including the security researches in WBSNs and storage auditing scheme for cloud environment; in Section 3, some preliminaries are presented; the security requirements and system model are also presented in Section 3; in Section 4, we describe our proposed scheme LEPA in detail; in Section 5, we prove that our scheme is secure under random oracle model and can defend two types of adversaries; performance analysis is presented in Section 6. At last, we conclude our paper in Section 7.

2. Related Works

2.1. The Security Researches in WBSNs. There are many proposals that have been proposed to secure the communication in WBSNs. Generally speaking, these proposals are mainly focused on authentication between sensors or authentication between service provider (SP) and client. Basically, these schemes can be classified as physiological parameter based schemes and cryptography based schemes. Physiological parameter based schemes use the similar biological characteristics (electrocardiogram, blood pressure, etc.) collected from the same individuals to identity the legal devices. These schemes are mainly used to solve the problem of authentication or key agreement between sensors which is also known as intrabody communication. In [29, 30], the authors proposed to use the interpulse interval of electrocardiogram (ECG) and photoplethysmogram (PPG) to generate key for encryption and authentication. In [31, 32], the frequency coefficients of ECG and PPG are proposed to generate key. In [33], Juels and Sudan put forward a method called "fuzzy vault" for biometric authentication. In [34], Venkatasubramanian et al. proposed a fuzzy vault based physiological signal key agreement scheme (PSKA); however, the "fuzzy vault" based scheme needs to add confusion data (chaff point) to achieve the security so the computational cost becomes higher with the increasing of extra chaff points. In [35, 36], two modified fuzzy vault methods were proposed to improve the performance. In [37], Zhang et al. proposed to use a time variation ECG features based scheme to achieve the key extracting. In [38], Mohana and Bai proposed a method to generate 128-bit key from the dynamic behavior of ECG. However, the methods based on the physiological parameter have the problem of poor accuracy because, even in the same individual, the collected signals still have small differences in different body parts. In addition, the physiological signal is time-variant so strict clock synchronization is needed, but the strict clock synchronization is difficult to achieve. Furthermore, it is limited to use between different types of sensors (e.g., between the blood pressure sensor and accelerometer). So the physiological parameter based schemes are difficult to be applied in practical applications.

In contrast to the physiological parameter based schemes, the cryptography based schemes are more mature and flexible which can be applied in both intrabody communication and external-body communication (authentication between service provider and controller). The cryptography based schemes can be divided into three types in general: symmetric cryptography based schemes [39–44], traditional public key infrastructure (PKI) based schemes [45–50], and some special cryptographic methods based schemes such as identity cryptography [51] and certificateless cryptography [52]. Compared with the latter two methods, symmetric cryptography based schemes need relatively low computational cost but support limited security functions and create key distribution problem; PKI based scheme needs relatively higher computational cost compared with symmetric cryptography based

schemes; the special cryptographic methods support richer security service but need the highest computational cost.

In [39–44], the symmetrical cryptography based WBSNs security schemes have been proposed; however, the distribution of secret keys is not efficient. In [45–50], some public key cryptography based schemes are proposed; however, compared with the proposal [39–44], not only is higher computational cost needed, but also the certificate management and storage are not efficient in resource-constraint WBSNs environment. Compared with symmetrical cryptography based schemes [39–44] and PKI based schemes [45–50], certificateless cryptography based schemes [53–58] eliminate both the key distribution problem in symmetrical key based schemes and certificate management in PKI based schemes, so it is more suitable for the application of WBSNs. Liu et al. proposed two certificateless authentication schemes for WBSNs firstly [53]; however, their schemes have been observed to have security defect [54, 55]. In [54], Zhao found that Liu et al.'s scheme [53] cannot withstand the stolen verifier table attack and proposed a new scheme, but, in Zhao's scheme [54], a large number of pseudoidentities should be stored. In [55], Zhao's scheme [54] has proven that the user's pseudoidentities could be traced. In [56], He et al.'s pointed out the security defect of signature forging attack in Liu et al.'s scheme [53] and proposed an improved scheme with proven security. Xiong [57] pointed out that Liu et al.'s scheme [53] cannot resist the attack mounted by the key replacement adversary. They proposed a lightweight and certificateless anonymous authentication scheme for extrabody communication. However, their scheme cannot support revocation of illegal users. To solve this problem, Xiong and Qin [58] proposed another scheme with user revocation based on KUNODE revocation tree, but the high computational and storage cost is needed in their scheme.

The schemes introduced above are mainly focused on the authentication between sensors or authentication between SP and controller. Some other security researches in WBSNs have been presented recently. In [59], Lu et al. proposed a secure and privacy preserving opportunistic computing framework for mobile health emergency based on attribute access control. Once the execution of a task exceeds the energy and computing power available on a single node, other opportunistically contacted nodes can contribute to the execution of the original task by running a subset of task. However, in [60], Lee et al. found that Lu et al.'s scheme [57] has some security flaws such as user anonymity, and they proposed an improved mobile-healthcare emergency scheme based on extended chaotic maps. In [61], Yi et al. proposed medical data analysis scheme with homomorphic encryption to achieve the privacy preserving; however, the security of their scheme is based on the assumption that the distributing servers cannot collude.

The security problems in cloud-assisted WBSNs are also being studied by more and more researchers [62–66]. In [62], Zhou et al. proposed a key management scheme for cloud-assisted WBSNs based on the Blom's symmetrical key. Their schemes could resist two types of adversaries: the time-based adversaries and location-based adversaries. In [63], Han et al. proposed a multivalued and ambiguous encryption scheme to ensure data confidentiality. In [64], Wan et al. proposed a cloud-assisted WBSNs architecture to solve the problems including energy-efficient routing and cloud resource allocation; however, security properties were not achieved in their schemes. In [65], Xie et al. proposed a secure roaming authentication protocol for cloud-assisted WBSNs to achieve the devices authentication in different access point. In [66], Zhu et al. proposed a secure outsourced computing scheme for cloud-assisted WBSNs with 2DNF cryptosystem. However, their scheme could not simultaneously achieve the satisfying security goals and low computation cost. In [67], Gupta et al. proposed a secure IoT based cloud centric architecture to perform predictive analysis of user's activities in sustainable health centers with RSA and DES encryption algorithms.

2.2. Storage Auditing for Cloud Environment. As can be seen from the schemes above, the study of data integrity checking for cloud-assisted WBSNs is relatively limited. However, data integrity checking for cloud-assisted WBSNs is very important because any modification on data will result in severe consequences such as misdiagnosis. In cloud-assisted WBSNs, user's data is stored in remote cloud server instead of storing it locally. Therefore, it is not efficient to download all the data from cloud server to check the integrity. To address this problem, the concept of public auditing was proposed by Shacham and Waters firstly [18]. With public auditing technique, user can check the data integrity remotely without downloading all the stored data. Based on this consideration, many public auditing schemes have been proposed later [19–22]. However, these schemes [18–22] are based on traditional public key based cryptograph (TPKC). In TPKC, a certificate-manager-certified certificate is needed to be bound with user's public key and identity. With the increasing number of users, the certificate management becomes difficult. Besides, the certificate transmitting is not suitable for bandwidth-constrained applications. Considering the large number of users and limited bandwidth/storage resource in WBSNs devices, the TPKC-based schemes are not suitable for cloud-assisted WBSNs.

To address the certificate management problem in TPKC, the identity-based public key cryptography (ID-based PKC) has been proposed by Shamir [51]. In ID-based PKC, the public key is user's identity and the private key is extracted by key generate center (KGC) based on user's public key (identity). Based on the identity-based public key cryptography (ID-based PKC) [51], several ID-based public auditing schemes have been proposed [23–25]. Wang et al. [23] presented the first ID-based public auditing protocol proven to be secure assuming the hardness of the computational Diffie-Hellman problem. Later, Tan and Jia [24] proposed an ID-based public verification scheme with aggregate signature. In [25], Wang proposed an ID-based public auditing scheme for multicloud environment. Though these schemes eliminate the certificate management drawback in TPKC-based schemes [18–22], these schemes suffer from the drawback of key escrow (KGC can get user's private key) which is inherited from ID-based PKC. So these schemes are also not suitable for cloud-assisted WBSNs.

In 2003, Al-Riyami and Paterson [52] presented the concept of certificateless public key cryptography (CLPKC) to resolve the key escrow problem in ID-based PKC. In CLPKC, the key is generally divided into two parts that are generated by the user and KGC, respectively. Therefore, CLPKC technique could resolve the key escrow problem in ID-based PKC and the key management in TPKC. Some CLPKC based authentication schemes have been proposed [26, 27]. Wang et al. presented certificateless public auditing scheme (CLPA) [26] with blockless verifiability and homomorphic authentication firstly. Their scheme could resolve the key escrow problem in ID-based public auditing schemes [23–25] and certificate management problem in TPKC. However, their scheme has proved that it cannot withstand the public key replacement attack which is defined as type I by He et al. [27]. Considering that the CLPA based scheme is suitable for resource-constraint WBSNs environment, He et al. presented another CLPA scheme which can withstand the public key replacement attack in Wang et al.'s scheme [26]. However, we found that He et al.'s scheme [27] has some defects below.

(1) The scheme in [27] is based on the public auditing scheme in [26]. The scheme in [26] is a public auditing scheme for cloud environment. The authenticator generating phase is conducted in client side, considering that the WBSNs client has weak processing capacity; this part of computational work will cause high energy loss and storage burden for WBSNs client. So it is not suitable to transplant the public auditing scheme for cloud to WBSNs environment directly.

(2) Secondly, the public auditing scheme in [27] is used for personal file. File uploading is a discrete event that may happen only once in a few days. However, when the WBSNs user requests medical service, the physiological information is constantly collected (several times in one second) and lasts for a long period of time. Similar to IoT, the density of collected data by sensors is extremely large. Based on (1) and (2), it is better to design a lightweight public auditing scheme to reduce the burden of authenticator generation in user sides.

(3) At last, we know that the cloud server can be divided into public cloud, private cloud, and hybrid cloud. Private cloud is a cloud server for individuals or company; the privacy of data can be guaranteed. But public cloud or hybrid cloud is a cloud service provider with untrusted third party, so if the confidentiality of the data is not protected, the user's sensitive medical information will be disclosed to the cloud service provider. However, in [27], the user's data is uploaded to cloud server directly without encryption. Considering that the cloud server is untrusted, the confidentiality cannot be protected in their scheme.

Based on the discussions above, we can see that, so far, there is still no public auditing scheme suitable for the low-capacity, high data density and privacy preserving requirements in cloud-assisted WBSNs. However, this kind of scheme is necessary in reality before the cloud-assisted WBSNs healthcare systems are widely applied. So this induced the motivation behind proposing our scheme LEPA in this paper.

3. Preliminaries and Formulation

In this section, we introduce the cryptographic technique used to construct LEPA and give a formal definition of cloud-assisted WBSNs public auditing scheme. Besides, the system model and security requirements are also introduced in this section.

3.1. Cryptographic Techniques

Definition 1 (bilinear Pairing). Given an additive group G_1 and a multiplicative group G_2 with the same order q, a bilinear paring refers to a map $e : G_1 \times G_2 \to G_2$ if the following three conditions hold:

(1) *Bilinearity*: $\forall P, Q \in G_1$ and $\forall a, b \in Z_q^*$, $e(a \cdot P, b \cdot Q) = e(P, Q)^{ab}$.

(2) *Nondegeneracy*: $\exists P, Q \in G_1$ such that $e(a \cdot P, b \cdot Q) \neq 1_{G_2}$.

(3) *Computability*: $\forall P, Q \in G_1$ and $\forall a, b \in Z_q^*$, these exists an algorithm to compute $e(a \cdot P, b \cdot Q)$ efficiently.

Definition 2 (ECDLP). $\forall P, s \cdot P \in G_1, s \in Z_q^*$, it is difficult to find out an algorithm A to compute s with input $(P, s \cdot P)$.

Definition 3 (CDLP). $\forall P, s \cdot P, t \cdot P \in G_1, s, t \in Z_q^*$, it is difficult to find out an algorithm A to compute $s \cdot t \cdot P$ with input $(P, s \cdot P, t \cdot P)$.

3.2. System Model. There are five entities in our scheme: key generating center (KGC), cloud server (CS), client, service provider (SP), and third-party auditor (TPA). The relationship among them is shown in Figure 2.

(1) CS. The CS in our scheme is a semitrusted entity with large computing power and storage capacity; the client can upload medical data to the CS for storage. If user wants to check the data integrity stored in CS, the CS can execute interactive protocols (LEPA) with TPA to check if the stored data is well-kept.

(2) KGC. The KGC is also a semitrusted entity, responsible for generating system parameters and extracting key for the other entities.

(3) TPA. The TPA is a semitrusted third party. If the client wants to check the integrity of stored data in CS, he/she can request the service to TPA and then TPA runs an interactive algorithm with CS to achieve the goal of integrity checking. In this process, TPA should not get any information about stored sensitive medical data. The reason of using TPA is that, for a task of data integrity checking, the checking result will be unfair no matter whether it is generated by client or CS: reluctant to take the responsibility of data corruption, the CS may give out an incorrect result; similarly, client also wants to shirk the responsibility of the data corruption to CS.

(4) Client. Client is a cloud-assisted WBSNs service user. He/she uses sensor devices to obtain PHI, uploads PHI to the

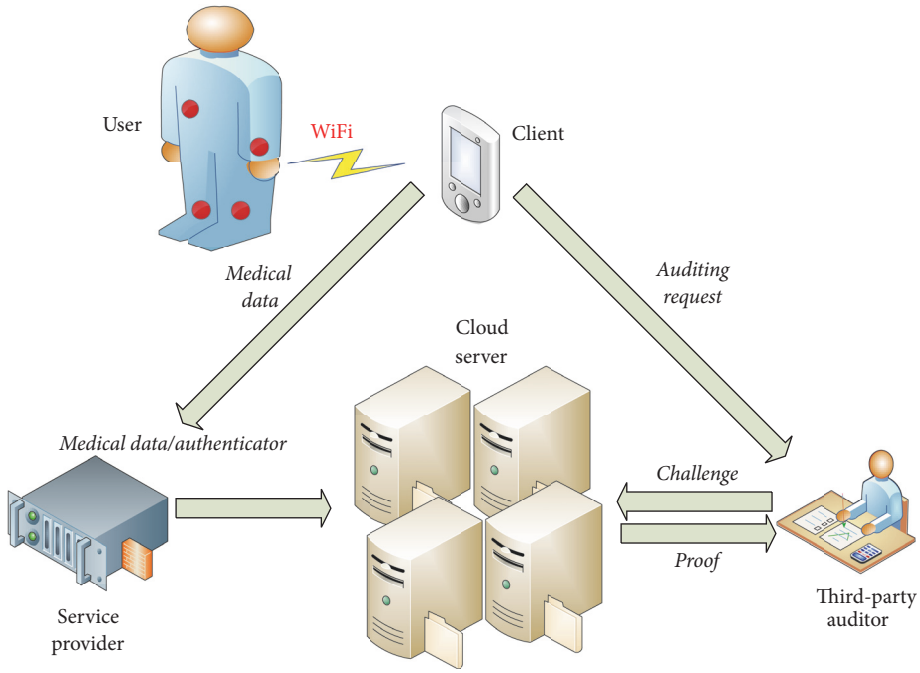

Figure 2: The system model of our public auditing scheme.

CS, and forms historical archives. The client has limited computing and storage capacity compared with CS and SP. The client does not want any part to get his/her PHI except for SP.

(5) SP. SP is a trusted part which can provide medical service for client. The SP has stronger capacity of computing and storage than client. The SP is responsible for generating authenticator and uploading the real-time collected PHI to CS. The SP also needs to analyze PHI and give a diagnostic result to client.

3.3. The Definition of Cloud-Assisted WBSNs Public Auditing Scheme. Here, we give a formal definition of cloud-assisted WBSNs public auditing scheme.

Definition 4 (cloud-assisted WBSNs public auditing scheme). A cloud-assisted WBSNs public auditing scheme is composed of algorithms below.

(1) SysSetup$(1^l) \rightarrow (q, G_1, G_2, P, H, h, e, \mathrm{PK}_{\mathrm{KGC}})$. The *SysSetup* is a probabilistic algorithm which takes a security parameter l as input and generate the published system parameters $(q, G_1, G_2, P, H, h, e, \mathrm{PK}_{\mathrm{KGC}})$. This algorithm is run by KGC.

(2) ParKeyGen$(\mathrm{ID}_{\mathrm{SP}}, \mathrm{PK}_{\mathrm{SP},1}) \rightarrow (\mathrm{PK}_{\mathrm{SP},1}, \mathrm{PK}_{\mathrm{SP},2})$. The *ParKeyGen* is a probabilistic algorithm which takes the SP's identity $\mathrm{ID}_{\mathrm{SP}}$ and SP's partial public key $\mathrm{PK}_{\mathrm{SP},1}$ as inputs, and then KGC generates another partial key $\mathrm{PK}_{\mathrm{SP},2}$ and returns $(\mathrm{PK}_{\mathrm{SP},1}, \mathrm{PK}_{\mathrm{SP},2})$ to SP. This algorithm is run by KGC.

(3) PriKeyGen$(NULL) \rightarrow (\mathrm{SK}_{\mathrm{SP}})$. The *PriKeyGen* algorithm is a probabilistic algorithm which takes *NULL* as input and generates private key for SP. This algorithm is run by SP.

(4) PubKeyGen$(\mathrm{SK}_{\mathrm{SP}}) \rightarrow (\mathrm{PK}_{\mathrm{SP},1})$. The *PubKeyGen* algorithm is a probabilistic algorithm which takes $\mathrm{SK}_{\mathrm{SP}}$ as input and generates partial public key $\mathrm{PK}_{\mathrm{SP},1}$ for SP. This algorithm is run by SP.

(5) Encryption$(m_i) \rightarrow (c_i)$. The *Encryption* algorithm is a probabilistic algorithm which takes the plaintext of medical data m_i as input and generates the ciphertext of medical data c_i as output. This algorithm is run by client.

(6) AuthGen$(\mathrm{SK}_{\mathrm{SP}}, \mathrm{id}_i, \mathrm{PK}_{\mathrm{KGC}}, \mathrm{PK}_{\mathrm{SP},1}, \mathrm{PK}_{\mathrm{SP},2}, \mathrm{ID}_{\mathrm{SP}}, c_i) \rightarrow (\mathrm{auth}_i)$. The *AuthGen* algorithm is a probabilistic algorithm which takes SP's private key $\mathrm{SK}_{\mathrm{SP}}$, the identity id_i of c_i, the SP's public key $(\mathrm{PK}_{\mathrm{SP},1}, \mathrm{PK}_{\mathrm{SP},2})$, and KGC's public key $\mathrm{PK}_{\mathrm{KGC}}$ as inputs and generates the authenticator auth_i for c_i. This algorithm is run by SP.

(7) ProofGen$(\mathrm{Chal}, \mathrm{auth}_i) \rightarrow (\mathrm{Pro}, C)$. The *ProofGen* algorithm is a probabilistic algorithm which takes Chal as the challenge and the generator auth_i as input and generates a proof (Pro, C). This algorithm is run by CS.

(8) ProofVerify$(\mathrm{Pro}, C) \rightarrow$ (*"TRUE" or "FALSE"*). The *ProofVerify* algorithm is a deterministic algorithm which takes (Pro, C) as input and returns *"TRUE"* or *"FALSE."* This algorithm is run by TPA.

3.4. Security Requirements. Here, we give some security requirements for cloud-assisted WBSNs public auditing scheme [27].

Input: a security parameter l
Output: system parameters $(q, G_1, G_2, P, H, h, e, \mathrm{PK}_{\mathrm{KGC}})$.
(1) The KGC chooses a large prime number $q > 2^l$.
(2) The KGC chooses an additive group $\langle G_1, + \rangle$, a multiplicative group $\langle G_2, \cdot \rangle$, a generator P of G_1; Then KGC chooses a bilinear paring $G_1 \times G_1 \to G_2$.
(3) The KGC chooses three hash functions $H : \{(0,1)^*, G_1\} \to G_1$, $h : \{(0,1)^*, G_1, G_1, G_1\} \to Z_q^*$.
(4) The KGC choose a random number $\mathrm{SK}_{\mathrm{KGC}} \in Z_q^*$ as secret key and generates $\mathrm{PK}_{\mathrm{KGC}} = \mathrm{SK}_{\mathrm{KGC}} \cdot P$.
(5) **Returns** $(q, G_1, G_2, P, H, h, e, \mathrm{PK}_{\mathrm{KGC}})$.

Algorithm 1: *SysSetup*.

(1) Publicly Verifiability. TPA should verify the data integrity stored in CS without downloading the entire data and causing additional computational burden on user.

(2) Privacy Preserving. The uploaded data should not be accessed by the CS or TPA even while uploading or auditing.

(3) Storage Correctness. Only the server keeping the user's data can accomplish the publicly verifiability with TPA.

(4) Confidentiality. The data transfer between any two parties should be encrypted.

(5) Batch Auditing. To improve the efficiency, the TPA should execute multiple auditing tasks simultaneously when receiving several requests.

4. Our Proposed Scheme: LEPA

There are eight polynomial-time algorithms in our proposed scheme, LEPA, that is, *SysSetup*, *PriKeyGen*, *PubKeyGen*, *ParKeyGen*, *Encryption*, *AuthGen*, *ProofGen,* and *Proof Verify*. Notations shows the notation list of our scheme.

Our designed protocol's general work flow is as follows: in the *SysSetup phase*, KGC generates a set of system parameters and publishes them; next, SP needs to generate its private key and public key in *PriKeyGen* and *PubKeyGen*, respectively; after these two steps, the SP sends the partial public key generated by himself/herself to KGC and KGC will generate another partial public key for SP in *ParKeyGen* phase; in *Encryption* phase, client encrypts the collected PHI with shared secret key and sends the ciphertext to SP (we assume that a shared secret key has been established, and this part of the work is not considered in this paper because there exist many authentication and key establishment schemes for SP and client in WBSNs [53–58]); after SP receives the PHI, the SP generates an authenticator for the encrypted data (*AuthGen* phase) and uploads the PHI with authenticator to CS; uploaded PHI forms a user's medical history files; client/SP can apply for data from the CS; when the client/SP wants to check the integrity of stored data (whether the data has been lost or damaged for the reason of CS), client/SP requests service to TPA (third-party auditing is to ensure fairness). After TPA receives the request, TPA will send a challenge to the CS, and then CS will respond with a proof to TPA *(ProofGen phase)*. TPA can check the data integrity with proof *(Proof Verify)* and then send the auditing result to the client/SP. The work process of our scheme is shown in Figure 3.

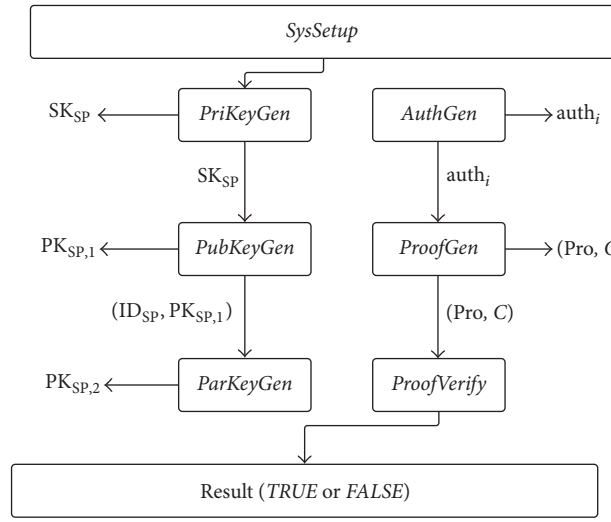

Figure 3: The flow chart of our public auditing scheme.

4.1. The Details of LEPA

SysSetup Phase. The KGC inputs a security parameter l into Algorithm 1 and outputs the system parameters $(q, G_1, G_2, P, H, h, e, \mathrm{PK}_{\mathrm{KGC}})$. KGC publishes these parameters and the other entities including CS, TPA, client, and SP can get them.

PriKeyGen Phase. The SP generated Algorithm 2 to generate private key for himself/herself.

PubKeyGen Phase. The SP executes Algorithm 3 to generate partial public key for himself/herself. Then SP sends $(\mathrm{ID}_{\mathrm{SP}}, \mathrm{PK}_{\mathrm{SP},1})$ to KGC, where $\mathrm{ID}_{\mathrm{SP}}$ is SP's identity.

ParKeyGen Phase. Upon receiving the request $(\mathrm{ID}_{\mathrm{SP}}, \mathrm{PK}_{\mathrm{SP},1})$ from SP, the KGC generates another partial public key for SP with Algorithm 4. Then KGC sends $\mathrm{PK}_{\mathrm{SP},2}$ to SP. After receiving $\mathrm{PK}_{\mathrm{SP},2}$, the SP takes $(\mathrm{PK}_{\mathrm{SP},1}, \mathrm{PK}_{\mathrm{SP},2})$ as his/her public key.

Input: *NULL*
Output: SK_{SP}
(1) The SP chooses a random number $SK_{SP} \in Z_q^*$ as SP's secret key.
(2) **Returns** SK_{SP}

Algorithm 2: *PriKeyGen*.

Input: SK_{SP}
Output: $PK_{SP,1}$
(1) The SP computes $PK_{SP,1} = SK_{SP} \cdot P$ as partial public key.
(2) **Returns** $PK_{SP,1}$

Algorithm 3: *PubKeyGen*.

Input: $(ID_{SP}, PK_{SP,1})$
Output: $PK_{SP,2}$
(1) KGC computes $Q = H(ID_{SP}, PK_{SP,1}) \in G_1$.
(2) KGC computes $PK_{SP,2} = SK_{KGC} \cdot Q$.
(3) **Returns** $PK_{SP,2}$

Algorithm 4: *ParKeyGen*.

Encryption Phase. In this phase, the client generates the ciphertext of collected data m_i (we assume that the established key is *KEY*). The client computes ciphertext c_i with *KEY* (any symmetrical cryptosystem can be taken such as AES). The client sends c_i to SP.

AuthGen Phase. The SP executes Algorithm 5 to generate the authenticator for c_i. After that, the SP sends (auth_i, c_i) to CS. The CS stores the collected data block c_i and its authenticator auth_i.

ProofGen Phase. If SP/client wants to check the integrity of stored data in CS. He/she can send the auditing request to TPA. Then TPA executes Algorithm 6 with CS to get the proof (Pro, C) from CS. The proof will be used for auditing in the next phase.

ProofVerify Phase. Upon receiving the proof (Pro, C) from CS, the TPA executes Algorithm 7 to check the integrity of c_i.

4.2. Correctness Proof. The correctness of TPA can check the integrity of data block $\{(i, r_i)\}_{i \in I}$ with proof (Pro, C) that can be proved by the formula derivation below:

$$
\begin{aligned}
e(\text{Pro}, P) &= e\left(\sum_{i=1}^{k} r_i \cdot \text{auth}_i, P\right) = e\left(\sum_{i=1}^{k} r_i \cdot (\text{SK}_{\text{SP}} \right. \\
&\cdot h(\text{id}_i, \text{PK}_{\text{KGC}}, \text{PK}_{\text{SP},1}, \text{PK}_{\text{SP},2}) \cdot H(\text{ID}_{\text{SP}}, \text{PK}_{\text{SP},1}) \\
&\left. + \text{PK}_{\text{SP},2} \cdot c_i), P\right) = e\left(\sum_{i=1}^{k} r_i \cdot (\text{SK}_{\text{SP}} \right. \\
&\cdot h(\text{id}_i, \text{PK}_{\text{KGC}}, \text{PK}_{\text{SP},1}, \text{PK}_{\text{SP},2}) \cdot H(\text{ID}_{\text{SP}}, \text{PK}_{\text{SP},1}) \\
&\left. + \text{SK}_{\text{KGC}} \cdot H(\text{ID}_{\text{SP}}, \text{PK}_{\text{SP},1}) \cdot c_i), P\right) = e\left(\sum_{i=1}^{k} r_i \right. \\
&\cdot (\text{SK}_{\text{SP}} \cdot h(\text{id}_i, \text{PK}_{\text{KGC}}, \text{PK}_{\text{SP},1}, \text{PK}_{\text{SP},2}) + \text{SK}_{\text{KGC}} \cdot c_i) \\
&\left. \cdot H(\text{ID}_{\text{SP}}, \text{PK}_{\text{SP},1}), P\right) = e\left(H(\text{ID}_{\text{SP}}, \text{PK}_{\text{SP},1}), \sum_{i=1}^{k} r_i \right. \\
&\cdot (\text{SK}_{\text{SP}} \cdot h(\text{id}_i, \text{PK}_{\text{KGC}}, \text{PK}_{\text{SP},1}, \text{PK}_{\text{SP},2}) + \text{SK}_{\text{KGC}} \cdot c_i) \\
&\left. \cdot P\right) = e\left(H(\text{ID}_{\text{SP}}, \text{PK}_{\text{SP},1}), \sum_{i=1}^{k} r_i \cdot \text{SK}_{\text{SP}} \right. \\
&\left. \cdot h(\text{id}_i, \text{PK}_{\text{KGC}}, \text{PK}_{\text{SP},1}, \text{PK}_{\text{SP},2}) \cdot P + \sum_{i=1}^{k} r_i \cdot \text{SK}_{\text{KGC}} \right. \\
&\left. \cdot c_i \cdot P\right) = e\left(H(\text{ID}_{\text{SP}}, \text{PK}_{\text{SP},1}), \sum_{i=1}^{k} r_i \right. \\
&\left. \cdot h(\text{id}_i, \text{PK}_{\text{KGC}}, \text{PK}_{\text{SP},1}, \text{PK}_{\text{SP},2}) \cdot (\text{SK}_{\text{SP}} \cdot P) + \sum_{i=1}^{k} r_i \right. \\
&\left. \cdot c_i \cdot (\text{SK}_{\text{KGC}} \cdot P)\right) = e\left(H(\text{ID}_{\text{SP}}, \text{PK}_{\text{SP},1}), R \right. \\
&\left. \cdot \text{PK}_{\text{SP},1} + \sum_{i=1}^{k} r_i \cdot c_i \cdot \text{PK}_{\text{KGC}}\right) = e(H(\text{ID}_{\text{SP}}, \text{PK}_{\text{SP},1}), \\
&R \cdot \text{PK}_{\text{SP},1} + C \cdot \text{PK}_{\text{KGC}}) = e(h_0, R \cdot \text{PK}_{\text{SP},1} + C \\
&\cdot \text{PK}_{\text{KGC}}) = e(C \cdot \text{PK}_{\text{KGC}} + R \cdot \text{PK}_{\text{SP},1}, h_0).
\end{aligned}
\tag{1}
$$

5. Security Analysis

In this part, we analyze the security of our certificateless public auditing scheme LEPA in the random oracle model; we analyze and prove that the two types of attackers in certificateless cryptography will not succeed. We first introduce the security model in Section 5.1; in Section 5.2, we give proofs of two security lemmas.

5.1. Adversary Model. There are two types of adversaries in certificateless based schemes [24]: type I adversary A_1 and type II adversary A_2. The type I adversary A_1 can access private key of KGC but cannot replace the SP's public key; the

Input: $(SK_{SP}, id_i, PK_{KGC}, PK_{SP,1}, PK_{SP,2}, ID_{SP}, c_i)$
Output: $auth_i$
(1) The SP computes $auth_i = SK_{SP} \cdot h(id_i, PK_{KGC}, PK_{SP,1}, PK_{SP,2}) \cdot H(ID_{SP}, PK_{SP,1}) + c_i \cdot PK_{SP,2}$.
(2) **Returns** $auth_i$

Algorithm 5: *AuthGen*.

Input: *NULL*
Output: (Pro, C)
(1) TPA generates a challenge $Chal = \{(i, r_i)\}_{i \in I}$ where I is a k-element subset of set $[1, n]$ and $r_i \in Z_q^*$ and sends Chal to CS.
(2) The CS computes $Pro = \sum_{i=1}^{k} r_i \cdot auth_i$ and $C = \sum_{i=1}^{k} r_i \cdot c_i$.
(3) **Returns** (Pro, C)

Algorithm 6: *ProofGen*.

Input: (Pro, C)
Output: *"TRUE"* or *"FALSE"*
(1) The TPA computes $h_0 = H(ID_{SP}, PK_{SP,1})$ and $h_i = h(id_i, PK_{KGC}, PK_{SP,1}, PK_{SP,2})$ and $R = \sum_{i-1}^{k} r_i \cdot h_i$.
(2) The TPA checks whether equation $e(Pro, P) = e(C \cdot PK_{KGC} + R \cdot PK_{SP,1}, h_0)$ holds.
(3) **Returns** *result*

Algorithm 7: *Proof Verify*.

type II A_2 can replace the SP's public key but cannot access KGC's private key. Our proof is based on this model and two games are set up between the challenger C and $\{A_1, A_2\}$. The adversary $\{A_1, A_2\}$ cloud accesses the following oracle controlled by C.

Create-User. Upon receiving a request with ID_X, C computes $\{PK_{SP,1}, PK_{SP,2}\}$ and SK_{SP} with algorithms *PriKeyGen*, *PubKeyGen*, and *ParKeyGen*; finally, C returns $\{PK_{SP,1}, PK_{SP,2}\}$ to A_1/A_2.

Public Key Replacement. Upon receiving the query with $\{ID_{SP}, PK'_{SP,1}, PK'_{SP,2}\}$, C replaces $\{PK_{SP,1}, PK_{SP,2}\}$ with $\{PK'_{SP,1}, PK'_{SP,2}\}$.

Tag-Gen. Upon receiving the query with $\{c_i, id_i\}$, C computes $auth_i$ with algorithm *AuthGen* and returns $\{c_i, id_i, auth_i\}$ to A_1/A_2.

5.2. Security Analysis. In this section, we prove that our scheme is secure against two types of adversaries $\{A_1, A_2\}$ in random oracle model.

Lemma 5. *The proposed scheme is secure against type I adversary A_1 if CDH problem is hard in G_1.*

Proof. Suppose A_1 could win the authenticator forging game; then C can construct a polynomial-algorithm to solve the CDH problem with nonnegligible probability ε: given an instance $(P, Q_1 = a \cdot P,\ Q_2 = b \cdot P)$, we set $PK_{SP,1} = Q_1$ here.

h-Query. C maintains a list L_h of tuples $\{id_i, PK_{KGC}, PK_{SP,1}, PK_{SP,2}, u_1\}$ and sets them as empty initially. Upon receiving a request with $\{id_i, PK_{KGC}, PK_{SP,1}, PK_{SP,2}\}$, C checks whether tuple $\{id_i, PK_{KGC}, PK_{SP,1}, PK_{SP,2}\}$ exists. If so, C returns u_1 to A_1; else, C generates a random number $u_1 \in Z_q^*$ and returns u_1 to A_1.

H-Query. C maintains a list L_H of tuples $\{ID_{SP}, PK_{SP,1}, u_2\}$ and sets them as empty initially. Upon receiving a request with $\{ID_{SP}, PK_{SP,1}\}$, C checks whether tuple $\{ID_{SP}, PK_{SP,1}\}$ exists. If so, C returns u_2 to A_1; else, C generates a random number $z_1 \in Z_q^*$ and returns $u_2 = z_1 \cdot Q_2$ to A_1.

Create-User. C maintains a list L_U of tuples $\{ID_{SP}, SK_{SP}, PK_{SP,1}, PK_{SP,2}\}$ and sets them as empty initially. Upon receiving a request with ID_X, C checks whether tuple $\{ID_{SP}, SK_{SP}, PK_{SP,1}, PK_{SP,2}\}$ exists. If so, C returns $\{PK_{SP,1}, PK_{SP,2}\}$ to A_1; else, if $ID_X = ID_{SP}$, C generates a random number $SK_{SP} \in Z_q^*$, requesting H-query with $\{ID_{SP}, PK_{SP,1}\}$; then C computes $PK_{SP,2} = SK_{KGC} \cdot H(ID_{SP}, PK_{SP,1})$ and returns $\{PK_{SP,1}, PK_{SP,2}\}$ to A_1; if $ID_X \neq ID_{SP}$, C chooses a random number w and computes $PK_{SP,2} = w \cdot SK_{KGC} \cdot H(ID_{SP}, PK_{SP,1})$ and returns $\{PK_{SP,1}, PK_{SP,2}\}$ to A_1.

Public Key Replacement. Upon receiving the query with $\{\mathrm{ID}_{\mathrm{SP}}, \mathrm{PK}'_{\mathrm{SP},1}, \mathrm{PK}'_{\mathrm{SP},2}\}$, $\mathrm{PK}'_{\mathrm{SP},1}$ and $\mathrm{PK}'_{\mathrm{SP},2}$ are replaced keys generated by A_1. C looks up L_U and replaces $\{\mathrm{PK}_{\mathrm{SP},1}, \mathrm{PK}_{\mathrm{SP},2}\}$ with $\{\mathrm{PK}'_{\mathrm{SP},1}, \mathrm{PK}'_{\mathrm{SP},2}\}$.

Tag-Gen. Upon receiving the query with $\{c_i, \mathrm{id}_i\}$, C makes h-query with $\{\mathrm{id}_i, \mathrm{PK}_{\mathrm{KGC}}, \mathrm{PK}_{\mathrm{SP},1}, \mathrm{PK}_{\mathrm{SP},2}\}$ and makes H-query with $\{\mathrm{ID}_{\mathrm{SP}}, \mathrm{PK}_{\mathrm{SP},1}\}$. Then $\mathrm{auth}_i = \mathrm{SK}_{\mathrm{SP}} \cdot u_1 \cdot u_2 + c_i \cdot \mathrm{PK}_{\mathrm{SP},2}$ is computed. At last, C returns $\{c_i, \mathrm{id}_i, \mathrm{auth}_i\}$ to A_1.

Eventually A_1 outputs a forgery proof (Pro', C') with challenge $\mathrm{Chal} = \{(i, r_i)\}_{i \in I}$ from TPA; C looks up L_h and L_H, respectively; at last C could get the following equation:

$$\begin{aligned} e(\mathrm{Pro}, P) &= e\left(C \cdot \mathrm{PK}_{\mathrm{KGC}} + R \cdot h_1 \cdot \mathrm{PK}_{\mathrm{SP},1}, h_0\right) \\ &= e\left(C \cdot \mathrm{PK}_{\mathrm{KGC}}, h_0\right) \cdot e\left(R \cdot h_1 \cdot \mathrm{PK}_{\mathrm{SP},1}, h_0\right). \end{aligned} \tag{2}$$

C also can get another equation.

$$\begin{aligned} e\left(\mathrm{Pro}', P\right) &= e\left(C \cdot \mathrm{PK}_{\mathrm{KGC}} + R \cdot h'_1 \cdot \mathrm{PK}_{\mathrm{SP},1}, h_0\right) \\ &= e\left(C \cdot \mathrm{PK}_{\mathrm{KGC}}, h_0\right) \cdot e\left(R \cdot h'_1 \cdot \mathrm{PK}_{\mathrm{SP},1}, h_0\right). \end{aligned} \tag{3}$$

Based on (2) and (3), we could get

$$\begin{aligned} & e\left(\mathrm{Pro} - \mathrm{Pro}', P\right) \\ &= e\left(R \cdot h_1 \cdot \mathrm{PK}_{\mathrm{SP},1} - R \cdot h'_1 \cdot \mathrm{PK}_{\mathrm{SP},1}, h_0\right) \\ &= e\left(R \cdot \left(h_1 - h'_1\right) \cdot \mathrm{PK}_{\mathrm{SP},1}, h_0\right) \\ &= e\left(R \cdot \left(h_1 - h'_1\right) \cdot Q_1 \cdot R, z_i \cdot Q_2\right) \\ &= e\left(R \cdot \left(h_1 - h'_1\right) \cdot a \cdot R \cdot P, z_i \cdot b \cdot P\right) \\ &= e\left(R \cdot \left(h_1 - h'_1\right) \cdot z_i \cdot a \cdot b \cdot R \cdot P, P\right). \end{aligned} \tag{4}$$

Then we could get $\mathrm{Pro} - \mathrm{Pro}' = R \cdot (h_1 - h'_1) \cdot z_i \cdot a \cdot b \cdot R \cdot P$ and output $(R \cdot (h_1 - h'_1) \cdot z_i \cdot R \cdot a \cdot b)^{-1} \cdot (\mathrm{Pro} - \mathrm{Pro}')$ as the solution of CDH instance $(P, Q_1 = a \cdot P,\ Q_2 = b \cdot P)$. □

Lemma 6. *The proposed scheme is secure against type II adversary A_2 if CDH problem is hard in G_1.*

Proof. Suppose A_2 could win the authenticator forging game; then C can construct a polynomial-algorithm to solve the CDH problem with nonnegligible probability ε: given an instance $(P, Q_1 = a \cdot P,\ Q_2 = b \cdot P)$.

Create-User. C maintains a list L_U of tuples $\{\mathrm{ID}_{\mathrm{SP}}, \mathrm{SK}_{\mathrm{SP}}, \mathrm{PK}_{\mathrm{SP},1}, \mathrm{PK}_{\mathrm{SP},2}\}$ and sets them as empty initially. Upon receiving a request with ID_X, C checks whether tuple $\{\mathrm{ID}_{\mathrm{SP}}, \mathrm{SK}_{\mathrm{SP}}, \mathrm{PK}_{\mathrm{SP},1}, \mathrm{PK}_{\mathrm{SP},2}\}$ exists. If so, C returns $\{\mathrm{PK}_{\mathrm{SP},1}, \mathrm{PK}_{\mathrm{SP},2}\}$ to A_1; else, if $\mathrm{ID}_X = \mathrm{ID}_{\mathrm{SP}}$, C generates a random number $\mathrm{SK}_{\mathrm{SP}} \in Z_q^*$, sets $\mathrm{PK}_{\mathrm{SP},1} = Q_1$, requests H-query with $\{\mathrm{ID}_{\mathrm{SP}}, \mathrm{PK}_{\mathrm{SP},1}\}$, and computes $\mathrm{PK}_{\mathrm{SP},2} = \mathrm{SK}_{\mathrm{KGC}} \cdot H(\mathrm{ID}_{\mathrm{SP}}, \mathrm{PK}_{\mathrm{SP},1})$; then C returns $\{\mathrm{PK}_{\mathrm{SP},1}, \mathrm{PK}_{\mathrm{SP},2}\}$ to A_1; if $\mathrm{ID}_X \neq \mathrm{ID}_{\mathrm{SP}}$, C chooses a random number w and computes $\mathrm{PK}_{\mathrm{SP},1} = w \cdot P, \mathrm{PK}_{\mathrm{SP},2} = \mathrm{SK}_{\mathrm{KGC}} \cdot H(\mathrm{ID}_{\mathrm{SP}}, \mathrm{PK}_{\mathrm{SP},1})$ and returns $\{\mathrm{PK}_{\mathrm{SP},1}, \mathrm{PK}_{\mathrm{SP},2}\}$ to A_1.

The other queries are the same as Lemma 5.

Eventually A_2 outputs a forgery proof (Pro', C') with challenge $\mathrm{Chal} = \{(i, r_i)\}_{i \in I}$ from TPA; C looks up L_h and L_H, respectively; at last C could get the following equation:

$$\begin{aligned} e(\mathrm{Pro}, P) &= e\left(C \cdot \mathrm{PK}_{\mathrm{KGC}} + R \cdot h_1 \cdot \mathrm{PK}_{\mathrm{SP},1}, h_0\right) \\ &= e\left(C \cdot \mathrm{PK}_{\mathrm{KGC}}, h_0\right) \cdot e\left(R \cdot h_1 \cdot \mathrm{PK}_{\mathrm{SP},1}, h_0\right). \end{aligned} \tag{5}$$

C also can get another equation:

$$\begin{aligned} e\left(\mathrm{Pro}', P\right) &= e\left(C \cdot \mathrm{PK}_{\mathrm{KGC}} + R \cdot h'_1 \cdot \mathrm{PK}_{\mathrm{SP},1}, h_0\right) \\ &= e\left(C \cdot \mathrm{PK}_{\mathrm{KGC}}, h_0\right) \cdot e\left(R \cdot h'_1 \cdot \mathrm{PK}_{\mathrm{SP},1}, h_0\right). \end{aligned} \tag{6}$$

Based on (5) and (6), we could get

$$\begin{aligned} & e\left(\mathrm{Pro} - \mathrm{Pro}', P\right) \\ &= e\left(R \cdot h_1 \cdot \mathrm{PK}_{\mathrm{SP},1} - R \cdot h'_1 \cdot \mathrm{PK}_{\mathrm{SP},1}, h_0\right) \\ &= e\left(R \cdot \left(h_1 - h'_1\right) \cdot \mathrm{PK}_{\mathrm{SP},1}, h_0\right) \\ &= e\left(R \cdot \left(h_1 - h'_1\right) \cdot Q_1 \cdot R, z_i \cdot Q_2\right) \\ &= e\left(R \cdot \left(h_1 - h'_1\right) \cdot a \cdot R \cdot P, z_i \cdot b \cdot P\right) \\ &= e\left(R \cdot \left(h_1 - h'_1\right) \cdot z_i \cdot a \cdot b \cdot R \cdot P, P\right). \end{aligned} \tag{7}$$

Then we could get $\mathrm{Pro} - \mathrm{Pro}' = R \cdot (h_1 - h'_1) \cdot z_i \cdot a \cdot b \cdot R \cdot P$ and output $(R \cdot (h_1 - h'_1) \cdot z_i \cdot R \cdot a \cdot b)^{-1} \cdot (\mathrm{Pro} - \mathrm{Pro}')$ as the solution of CDH instance $(P, Q_1 = a \cdot P,\ Q_2 = b \cdot P)$.

Through Lemmas 5 and 6, we have proved that our scheme could defend two types of attackers in certificateless public auditing scheme. □

5.3. Security Requirements Discussions

(1) Publicly Verifiability. From the equation of correctness analysis, we can see that, through the *ProofGen* and *ProofVerify*, TPA only needs to verify the proof generated by CS when the user requests public auditing service. Therefore, our scheme satisfies the publicly verifiability requirement.

(2) Privacy Preserving. We can see that our scheme achieves privacy preserving from two aspects: firstly, the medical data storing on CS is encrypted, so CS cannot get any information about the client's PHI; the TPA also cannot get any information with proof generated from CS. So, we can see that our scheme achieves the goal of protecting the client's privacy.

(3) Storage Correctness. When the stored data in CS has been modified, deleted, or corrupted, the TPA can check the result with the algorithm *ProofVerify*. Besides, we can see that any adversaries cannot forge the proof without secret key through Lemmas 5 and 6. So we see that the storage correctness has been achieved in our scheme.

(4) Confidentiality. The data has been encrypted with session key established between client and SP. So the monitor cannot

Table 1: The cryptographic operation in client side.

LEPA	He et al.'s scheme [27]	Yu et al.'s scheme [28]
1Enc	(2PM + 2H + 1h)	(3Exp + 1H)

Enc: symmetrical encryption; PM: point multiplication; H: hash to element; h: hash; Exp: exponentiation.

Table 2: The communication cost comparison.

LEPA	He et al.'s scheme [27]	Yu et al.'s scheme [28]
1 group element and 1 integer	1 group element and 1 integer	(d + 2) group elements and 2 integers

d is the parameter numbers of Ω_j in Yu et al.'s scheme [28].

get any information of client's collected medical data. So we see that the confidentiality has been achieved in our scheme.

(5) Batch Auditing. Through the algorithm of *ProofVerify*, we can see that several blocks of data can be checked in one phase. Therefore, our scheme achieves batch auditing requirement.

6. Performance Analysis

6.1. Computational Cost. We evaluate the performance of our proposed scheme through several experiments with the help of Java Pairing-Based Cryptography (JPBC) library [68]. These experiments are carried out on a machine with Intel Core i5-3337U CPU (1.8 GHz clock speed), 4 GB RAM, and running the Win 8 Operating System. The selected elliptic curve is a supersingular curve, $y^2 = x^3 + x$, with the order of 160 bits, and elements in G_1 is 128 bytes. We compared our scheme with the other two schemes [27, 28] for the reason that these two schemes are similar to our proposed schemes. The comparison is mainly focused on *ProofVerify* and *AuthGen* phase for the reason that these two phases are the two most time-consuming phases.

In Figure 4(a), we can see that, in *AuthGen* phase, our scheme needs less time compared with the other two schemes. We tested [0, 1000] blocks of data. The time cost of the authenticator generating time is linearly increasing. Besides, considering that, in our scheme, the *AuthGen* phase is conducted in SP side (in [27, 28], the *AuthGen* phase is generated by client), the time cost of authenticator generation for client is 0. The client only needs to do one symmetrical encryption such as AES (computational cost in client side is shown in Table 1). For the reason that, in pairing-based cryptographic schemes, the point multiplication operation, hash to point, and bilinear pairing are the main computational expansive operations, the time cost of each algorithm mainly depends on the number of point multiplication operations. However, the symmetrical encryption only needs almost the same computational cost with hash function which is negligible compared with point multiplication and exponentiation. So from Table 1 we can see that the computational cost of our scheme LEPA with 1Enc greatly reduces the computational cost in client side compared with He et al.'s scheme (2PM + 2H + 1h) and Yu et al.'s scheme (3Exp + 1H).

In Figures 4(b) and 5, we tested the *Proof Verify* efficiency of the three schemes. In Yu et al.'s scheme [28], the proof verifying time will be affected with the changing of time period for the reason that the proof verifying parameters are changed in different time period. In Yu et al.'s scheme, each time period corresponds to a tree node and, with the variation of the node depth in tree, the time cost is different. We tested the results in different depth of the node: $d = 1$, 10, and 15. We can see that, in the three conditions (Figures 4(b), 5(a), and 5(b)), our scheme needs the least computation cost. The reason is that, with the increase of data blocks in the verification step, only several integer arithmetic and hash operations are conducted; however, integer multiplication and hash operations are relatively of low computation cost. In scheme [28], one more bilinear pairing operation is needed; the bilinear pairing operation is computation-expensive so Yu et al.'s scheme needs the highest time cost. In scheme [27], with increasing of verifying data blocks, the mapping to point operations and point multiplications are increasing, but the time cost of these two operations is relatively high, so, with the increasing amount of data blocks, the time cost of scheme is growing quickly.

Yu et al.'s scheme needs relatively more bilinear maps (3 bilinear maps) and this part of computational cost makes up a large proportion when verified blocks are few. Therefore, in the initial stage, Yu et al.'s scheme costs more time compared with other two schemes. However, the computational cost of He et al.'s scheme will gradually increase and transcend Yu et al.'s scheme, due to the mapping to point operation and point multiplication operations. The time point of transcending changes with the depth of time node in Yu et al.'s scheme: in Figure 4(b) ($d = 1$), He et al.'s scheme transcend Yu et al.'s scheme in earlier time point; with the increase of the time node depth, the time point of transcending will be delayed: the transcending time was delayed in Figure 5(a) ($d = 10$) compared with Figure 4(b) ($d = 1$). When $d = 15$ (Figure 5(b)), the time of transcending time disappeared (but it will certainly appear at a certain moment in future).

6.2. Communication Cost. The communication cost of scheme is generated in Algorithm 5 *AuthGen*, Algorithm 6 *ProofGen*, and Algorithm 7 *Proof Verify*. The communication cost of Chal is the same in three schemes with the form $\text{Chal} = \{(i, r_i)\}_{i \in I}$; the elements i and r_i are two integers and the size of Chal depends on the number of (i, r_i) in Chal. The number of (i, r_i) in Chal will depend on the number of data blocks to be checked in the cloud server which was decided by the auditor.

However, the communication cost of *Proof* is different in three schemes (a detailed comparison is shown in Table 2): from Table 2, we can see that our scheme has the same communication cost as He et al.'s scheme [27]; in He et al.'s scheme, the form of proof is (m, S) and, in our scheme, the form of proof is (Pro, C), where $\text{Pro} = \sum_{i=1}^{k} r_i \cdot \text{auth}_i$ and $C = \sum_{i=1}^{k} r_i \cdot c_i$. For the reason that $\text{auth}_i = \text{SK}_{\text{SP}} \cdot h(\text{id}_i, \text{PK}_{\text{KGC}}, \text{PK}_{\text{SP},1}, \text{PK}_{\text{SP},2}) \cdot H(\text{ID}_{\text{SP}}, \text{PK}_{\text{SP},1}) + c_i \cdot \text{PK}_{\text{SP},2}$ is a group element,

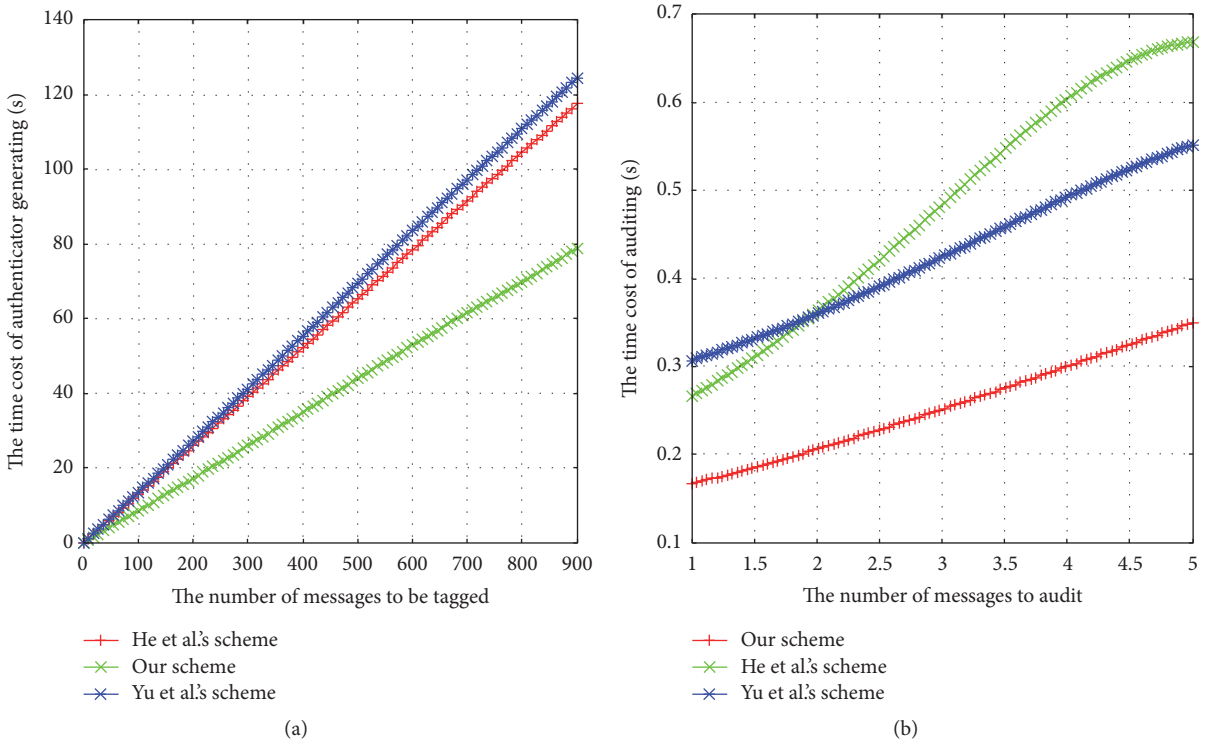

FIGURE 4: (a) The time cost of authenticator generating phase with regard to the number of blocks in seconds; (b) the time cost of proof verifying phase with regard to the number of blocks in seconds ($d = 1$).

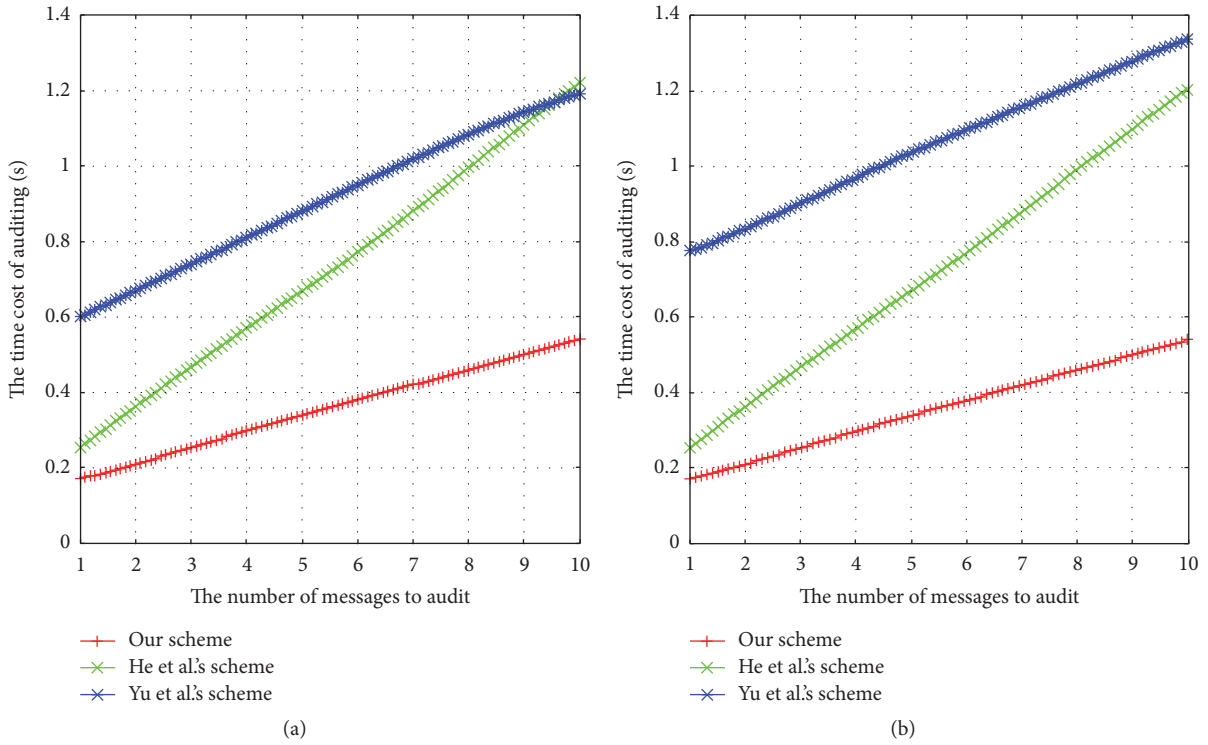

FIGURE 5: (a) The time cost of proof verifying phase with regard to the number of blocks in seconds ($d = 10$); (b) the time cost of proof verifying phase with regard to the number of blocks in seconds ($d = 15$).

Pro $= \sum_{i=1}^{k} r_i \cdot \text{auth}_i$ is also a group element. So we can compute that the communication cost in our scheme is 1 group element and 1 integer. In He et al.'s scheme, $S = \sum_{j=1}^{c} w_i \cdot S_{i_j}$ and $m = \sum_{j=1}^{c} w_i \cdot m_{i_j}$; with the same method we can get that the communication cost in their scheme is 1 group element and 1 integer. For the reason that the communication and computational cost in Yu et al.' scheme [28] are time-varying, the proof in Yu et al.'s scheme will be changing in different time period. The proof in their scheme is $(j, U, \sigma, \mu, \Omega_j)$ about $(d + 2)$ group elements and 2 integers where d is the parameter numbers in Ω_j (the depth of time node). So, from Table 2, we can see that our scheme needs the same communication cost as He al.'s scheme and less communication cost than Yu et al.'s scheme.

7. Conclusion

Considering that there has been no good solution for public auditing in cloud-assisted WBSNs, we propose a lightweight and efficient public auditing scheme, LEPA, for cloud-assisted WBSNs in this paper. With our proposed scheme LEPA, in some healthcare applications of cloud-assisted WBSNs (such as the hospital without private data center that needs to outsource the important medical data into cloud service provider), the sensitive data used for diagnosis could be checked whether it is well-kept in remote cloud server. Through the lightweight designing concepts, we reduce the computational expensive operations such as hash to point or point multiplication in user side. In addition, the authenticator generation is outsourced to service provider and user only needs to do one symmetrical encryption. Compared to related works, the client in our scheme has the least security computational burden. Besides, we give the formal security proof of that our scheme can resist two kinds of adversaries in the random oracle model including public key replacement attacker and master key accessing attacker. Furthermore, we use Java language to implement our scheme. The experimental result shows that our scheme outperforms other similar schemes in both the verification phase and authenticator generating phase. To the best of our knowledge and using the analysis above, we think that the proposed scheme LEPA is the most suitable public auditing scheme for cloud-assisted WBSNs.

Although our proposed scheme LEPA achieves better security properties and efficiency compared with similar works, however, we think that our scheme still has the defects below.

(1) The application model is relatively simple and not suitable for complicated model such as multiuser model. In some application scenarios such as community hospital, the users may be organized as a group to share the data stored in cloud. So it is meaningful to propose a multiuser model based cloud-assisted WBSNs auditing scheme.

(2) Considering that, with the physiological sensors in WBSNs, the physiological information can be collected and these data can be used to achieve biometric authentication, the two-factor based auditing schemes will support stronger security goals.

So, in the future, we plan to extend our scheme, LEPA, to different application scenarios such as mobile WBSN based healthcare system or the multiuser model of cloud-assisted WBSNs environment. Besides, the two-factor based authentication technology with physiological information and modern cryptographic technology will be used together in our future works to enhance the security of cloud-assisted WBSN applications.

Notations

l: A security parameter
q: A large prime number $q > 2^l$
e: A bilinear pairing $e : G_1 \times G_2 \to G_2$
SK_{KGC}: The KGC's secret key
PK_{KGC}: The public key of KGC
ID_{SP}: The identity of SP
$\text{PK}_{\text{SP},1}$: The partial public key generated by oneself
$\text{PK}_{\text{SP},2}$: The partial public key generated by KGC
SK_{SP}: The secret key of SP
auth_i: The authenticator of m_i
(Pro, C): The proof of medical data $c_1, c_2, \ldots, c_i$ generated by SP
Chal: The integrity checking challenge generated by TPA: $\text{Chal} = \{(i, r_i)\}_{i \in I}$
c_i/m_i: The medical data m_i and corresponding ciphertext c_i encrypted by client
h: A hash function: $\{(0,1)^*, G_1, G_1, G_1\} \to Z_q^*$
H: A hash to point function: $\{(0,1)^*, G_1\} \to G_1$.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (no. 61572001, no. 61502008), the Research Fund for the Doctoral Program of Higher Education (no. 20133401110004), the Natural Science Foundation of Anhui Province (no. 1508085QF132), and the Doctoral Research Start-Up Funds Project of Anhui University.

References

[1] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, "Wireless body area networks: a survey," *IEEE Communications Survey & Tutorials*, vol. 16, no. 3, pp. 1658–1686, 2014.

[2] T. G. Zimmerman, "Personal area networks: near-field intrabody communication," *IBM Systems Journal*, vol. 35, no. 3-4, pp. 609–617, 1996.

[3] S. Ivanov, C. Foley, S. Balasubramaniam, and D. Botvich, "Virtual groups for patient WBSNs monitoring in medical environment," *IEEE Transactions on Biomedical Engineering*, vol. 59, no. 11, pp. 3238–3246, 2012.

[4] T. Gao, T. Massey, L. Selavo et al. et al., "The Advanced Health and Disaster Aid Network: a Light-Weight Wireless Medical

System for Triage," *IEEE Transactions on Biomedical Circuits Systems*, vol. 1, no. 3, pp. 203–216, 2007.

[5] E. Jovanov, A. Milenković, C. Otto et al., "A WBAN system for ambulatory monitoring of physical activity and health status: applications and challenges," in *Proceedings of the 27th Annual International Conference of the Engineering in Medicine and Biology Society (IEEE-EMBS '05)*, pp. 3810–3813, September 2005.

[6] K. Lorincz, D. J. Malan, T. R. F. Fulford-Jones et al., "Sensor networks for emergency response: challenges and opportunities," *IEEE Pervasive Computing*, vol. 3, no. 4, pp. 16–23, 2004.

[7] F. Axisa, C. Gehin, G. Delhomme, C. Collet, O. Robin, and A. Dittmar, "Wrist ambulatory monitoring system and smart glove for real time emotional, sensorial and physiological analysis," in *Proceedings of the 26th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC '04)*, pp. 2161–2164, September 2004.

[8] C. Mundt W, K. Montgomery N, and U. Udoh E, "A multi parameter wearable physiologic monitoring system for space and terrestrial applications," *IEEE Transactions on Information Technology in Biomedicine*, vol. 9, no. 3, pp. 382–391, 2005.

[9] J. Wannenburg and R. Malekian, "Body sensor network for mobile health monitoring, a diagnosis and anticipating system," *IEEE Sensors Journal*, vol. 15, no. 12, pp. 6839–6852, 2015.

[10] U. A. K. Chude-Okonkwo, R. Malekian, and B. T. Maharaj, "Biologically inspired bio-cyber interface architecture and model for internet of bio-Nanothings applications," *IEEE Transactions on Communications*, vol. 64, no. 8, pp. 3444–3455, 2016.

[11] K. S. Kwak, S. Ullah, and N. Ullah, "An overview of IEEE 802.15.6 standard," in *Proceedings of the 3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL '10)*, pp. 1–6, IEEE, November 2010.

[12] M. Toorani, "On vulnerabilities of the security association in the IEEE 802.15.6 standard," in *Financial Cryptography and Data Security*, vol. 8976 of *Lecture Notes in Computer Science*, pp. 245–260, Springer, Berlin, Heidelberg, 2015.

[13] M. Toorani, "Cryptanalysis of two PAKE protocols for body area networks and smart environments," *International Journal of Network Security*, vol. 17, no. 5, pp. 629–636, 2015.

[14] G. Fortino and M. Pathan, "Integration of cloud computing and body sensor networks," *Future Generation Computer Systems*, vol. 35, no. 5, pp. 57–61, 2014.

[15] M. Chen, "NDNC-BAN: supporting rich media healthcare services via named data networking in cloud-assisted wireless body area networks," *Information Sciences*, vol. 284, no. 10, pp. 142–156, 2014.

[16] O. Diallo, J. J. P. C. Rodrigues, M. Sene, and J. Niu, "Real-time query processing optimization for cloud-based wireless body area networks," *Information Sciences*, vol. 284, pp. 84–94, 2014.

[17] G. Fortino, G. Di Fatta, M. Pathan, and A. V. Vasilakos, "Cloud-assisted body area networks: state-of-the-art and future challenges," *Wireless Networks*, vol. 20, no. 7, pp. 1925–1938, 2014.

[18] H. Shacham and B. Waters, "Compact proofs of retrievability," in *Advances in Cryptology—ASIACRYPT 2008: Proceedings of the 14th International Conference on the Theory and Application of Cryptology and Information Security, Melbourne, Australia, December 2008*, vol. 5350 of *Lecture Notes in Computer Science*, pp. 90–107, Springer, Berlin, Germany, 2008.

[19] Z. Hao, S. Zhong, and N. Yu, "A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability," *IEEE Transactions on Knowledge and Data Engineering*, vol. 23, no. 9, pp. 1432–1437, 2011.

[20] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward secure and dependable storage services in cloud computing," *IEEE Transactions on Services Computing*, vol. 5, no. 2, pp. 220–232, 2012.

[21] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," *Institute of Electrical and Electronics Engineers. Transactions on Computers*, vol. 62, no. 2, pp. 362–375, 2013.

[22] K. Huang, M. Xian, S. Fu, and J. Liu, "Securing the cloud storage audit service: defending against frame and collude attacks of third party auditor," *IET Communications*, vol. 8, no. 12, pp. 2106–2113, 2014.

[23] H. Wang, J. Domingo-Ferrer, Q. Wu, and B. Qin, "Identity-based remote data possession checking in public clouds," *IET Information Security*, vol. 8, no. 2, pp. 114–121, 2014.

[24] S. Tan and Y. Jia, "NaEPASC: a novel and efficient public auditing scheme for cloud data," *Frontiers of Information Technology & Electronic Engineering*, vol. 15, no. 9, pp. 794–804, 2014.

[25] H. Wang, "Identity-based distributed provable data possession in multi-cloud storage," *IEEE Transactions on Services Computing*, vol. 8, no. 2, pp. 328–340, 2015.

[26] B. Wang, B. Li, H. Li, and F. Li, "Certificateless public auditing for data integrity in the cloud," in *Proceedings of the 1st IEEE International Conference on Communications and Network Security (CNS '13)*, pp. 136–144, National Harbo, Md, USA, October 2013.

[27] D. He, S. Zeadally, and L. Wu, "Certificateless public auditing scheme for cloud-assisted wireless body area networks," *IEEE Systems Journal*, no. 99, pp. 1–10, 2015.

[28] J. Yu, K. Ren, and C. Wang, "Enabling cloud storage auditing with verifiable outsourcing of key updates," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 6, pp. 1362–1375, 2016.

[29] C. C. Y. Poon, Y.-T. Zhang, and S.-D. Bao, "A novel biometrics method to secure wireless body area sensor networks for telemedicine and M-health," *IEEE Communications Magazine*, vol. 44, no. 4, pp. 73–81, 2006.

[30] S.-D. Bao, Y.-T. Zhang, and L.-F. Shen, "Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems," in *Proceedings of the 2005 27th Annual International Conference of the Engineering in Medicine and Biology Society (IEEE-EMBS '05)*, pp. 2455–2458, September 2005.

[31] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "EKG-based key agreement in body sensor networks," in *Proceedings of the 2008 IEEE INFOCOM Workshops*, pp. 1–6, IEEE Xplore, April 2008.

[32] S. Cherukuri, K. K. Venkatasubramanian, and S. K. S. Gupta, "Biosec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body," in *Proceedings of the 32nd International Conference on Parallel Processing (ICPP '03)*, pp. 432–439, October 2003.

[33] A. Juels and M. Sudan, "A fuzzy vault scheme," in *Proceedings of the IEEE International Symposium on Information Theory*, pp. 408–415, July 2002.

[34] K. K. Venkatasubramanian, A. Banerjee, and S. K. Gupta, "SKA: usable and secure key agreement scheme for body area networks," *IEEE Transactions on Information Technology in Biomedicine*, vol. 14, no. 1, pp. 60–68, 2010.

[35] F. Miao, S.-D. Bao, and Y. Li, "A modified fuzzy vault scheme for biometrics-based body sensor networks security," in *Proceedings of the 53rd IEEE Global Communications Conference (GLOBECOM '10)*, pp. 1–5, December 2010.

[36] H. Liu, D. Sun, K. Xiong, and Z. Qiu, "A new fuzzy vault method using cubic spline interpolation," in *Proceedings of the 2010 International Conference on Artificial Intelligence and Computational Intelligence (AICI '10)*, pp. 103–106, October 2010.

[37] Z. Zhang, H. Wang, A. V. Vasilakos, and H. Fang, "ECG-cryptography and authentication in body area networks," *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, no. 6, pp. 1070–1078, 2012.

[38] J. Mohana and V. T. Bai, "128 bit key generations from the dynamic behavior of ECG for securing wireless body area network," *ARPN Journal of Engineering and Applied Sciences*, vol. 10, no. 18, pp. 8048–8051, 2015.

[39] F. Hu, M. Jiang, M. Wagner, and D.-C. Dong, "Privacy-preserving telecardiology sensor networks: Toward a low-cost portable wireless hardware/software codesign," *IEEE Transactions on Information Technology in Biomedicine*, vol. 11, no. 6, pp. 619–627, 2007.

[40] P. Kumar, Y. Lee D, and D. Lee Y, "Secure health monitoring using medical wireless sensor networks," in *Proceedings of the Sixth International Conference on Networked Computing and Advanced Information Management*, pp. 491–494, 2010.

[41] S. Raazi, H. Lee, S. Lee, and Y.-K. Lee, "BARI+: a biometric based distributed key management approach for wireless body area networks," *Sensors*, vol. 10, no. 4, pp. 3911–3933, 2010.

[42] A. B. Waluyo, I. Pek, X. Chen, and W. S. Yeoh, "Design and evaluation of lightweight middleware for personal wireless body area network," *Personal and Ubiquitous Computing*, vol. 13, no. 7, pp. 509–525, 2009.

[43] X. Yi, J. Willemson, and F. Nait-Abdesselam, "Privacy-preserving wireless medical sensor network," in *Proceedings of the 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom '13)*, pp. 118–125, July 2013.

[44] H. Zhao, J. Qin, and J. Hu, "An energy efficient key management scheme for body sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 11, pp. 2202–2210, 2013.

[45] D. He, S. Chan, and S. Tang, "A novel and lightweight system to secure wireless medical sensor networks," *IEEE Journal of Biomedical and Health Informatics*, vol. 18, no. 1, pp. 316–326, 2014.

[46] Y. M. Huang, M. Y. Hsieh, H. C. Chao, S. H. Hung, and J. H. Park, "Pervasive, secure access to a hierarchical sensor-based healthcare monitoring architecture in wireless heterogeneous networks," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 4, pp. 400–411, 2009.

[47] X. H. Le, M. Khalid, R. Sankar, and S. Lee, "An efficient mutual authentication and access control scheme for wireless sensor networks in healthcare," *Journal of Networks*, vol. 6, no. 3, pp. 355–364, 2011.

[48] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "Sage: a strong privacy-preserving scheme against global eavesdropping for ehealth systems," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 4, pp. 365–378, 2009.

[49] K. Malasri and L. Wang, "Design and implementation of a secure wireless mote-based medical sensor network," *Sensors*, vol. 9, no. 8, pp. 6273–6297, 2009.

[50] J. Misic and V. Misic, "Enforcing patient privacy in healthcare WSNs through key distribution algorithms," *Security & Communication Networks*, vol. 1, no. 5, pp. 417–429, 2008.

[51] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology: Proceedings of (CRYPTO '84)*, vol. 196 of *Lecture Notes in Computer Science*, pp. 47–53, Springer, Berlin, Germany, 1985.

[52] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Advances in Cryptology-ASIACRYPT*, vol. 2894 of *Lecture Notes in Computer Science*, pp. 452–473, Springer, 2003.

[53] J. Liu, Z. Zhang, X. Chen, and 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, 2014.

[54] 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, 2014.

[55] C. Wang and Y. Zhang, "New authentication scheme for wireless body area networks using the bilinear pairing," *Journal of Medical Systems*, vol. 39, no. 11, article 136, 2015.

[56] D. He, S. Zeadally, N. Kumar, and J.-H. Lee, "Anonymous authentication for wireless body area networks with provable security," *IEEE Systems Journal*, vol. 99, pp. 1–12, 2016.

[57] H. Xiong, "Cost-effective scalable and anonymous certificateless remote authentication protocol," *IEEE Transactions on Information Forensics & Security*, vol. 9, no. 12, pp. 2327–2339, 2014.

[58] H. Xiong and 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, 2015.

[59] R. Lu, X. Lin, and X. Shen, "SPOC: a secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 3, pp. 614–624, 2013.

[60] C.-C. Lee, C.-W. Hsu, Y.-M. Lai, and A. Vasilakos, "An enhanced mobile-healthcare emergency system based on extended chaotic maps," *Journal of Medical Systems*, vol. 37, no. 5, article 9973, pp. 1–12, 2013.

[61] X. Yi, A. Bouguettaya, D. Georgakopoulos, A. Song, and J. Willemson, "Privacy protection for wireless medical sensor data," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 3, pp. 369–380, 2016.

[62] J. Zhou, Z. Cao, X. Dong, N. Xiong, and A. 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, pp. 255–276, 2015.

[63] N. D. Han, L. Han, D. M. Tuan, H. P. In, and M. Jo, "A scheme for data confidentiality in cloud-assisted wireless body area networks," *Information Sciences*, vol. 284, no. 5, pp. 157–166, 2014.

[64] J. Wan, C. Zou, S. Ullah, C.-F. Lai, M. Zhou, and X. Wang, "Cloud-Enabled wireless body area networks for pervasive healthcare," *IEEE Network*, vol. 27, no. 5, pp. 56–61, 2013.

[65] Q.-Q. Xie, S.-R. Jiang, L.-M. Wang, and C.-C. Chang, "Composable secure roaming authentication protocol for cloud-assisted body sensor networks," *International Journal of Network Security*, vol. 18, no. 5, pp. 816–831, 2016.

[66] H. Zhu, L. Gao, and H. Li, "Secure and privacy-preserving body sensor data collection and query scheme," *Sensors*, vol. 16, no. 2, article 179, 2016.

[67] P. K. Gupta, B. T. Maharaj, and R. Malekian, "A novel and secure IoT based cloud centric architecture to perform predictive analysis of users activities in sustainable health centres," *Multimedia Tools and Applications*, pp. 1–24, 2016.

[68] A. de Caro and V. Iovino, "jPBC: Java pairing based cryptography," in *Proceedings of the 16th IEEE Symposium on Computers and Communications (ISCC '11)*, pp. 850–855, July 2011.