SPECIAL SECTION ON HEALTHCARE INFORMATION TECHNOLOGY

FOR THE EXTREME AND REMOTE ENVIRONMENTS

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 18, 2018, accepted January 5, 2019, date of publication January 9, 2019, date of current version March 29, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2891775

Achieve Privacy-Preserving Priority Classification on Patient Health Data in Remote eHealthcare System

GUOMING WANG[1], RONGXING LU[2], (Senior Member, IEEE), AND YONG LIANG GUAN[1], (Senior Member, IEEE)

[1]School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore 639798
[2]Faculty of Computer Science, University of New Brunswick, NB, Canada

Corresponding author: Guoming Wang (wang0947@e.ntu.edu.sg)

ABSTRACT The wireless body area network (WBAN) has attracted considerable attention and becomes a promising approach to provide a 24-h on-the-go healthcare service for users. However, it still faces many challenges on the privacy of users' sensitive personal information and the confidentiality of healthcare center's disease models. For this reason, many privacy-preserving schemes have been proposed in recent years. However, the efficiency and accuracy of those privacy-preserving schemes become a big issue to be solved. In this paper, we propose an efficient and privacy-preserving priority classification scheme, named PPC, for classifying patients' encrypted data at the WBAN-gateway in a remote eHealthcare system. Specifically, to reduce the system latency, we design a non-interactive privacy-preserving priority classification algorithm, which allows the WBAN-gateway to conduct the privacy-preserving priority classification for the received users' medical packets by itself and to relay these packets according to their priorities (criticalities). A detailed security analysis shows that the PPC scheme can achieve the priority classification and packets relay without disclosing the privacy of the users' personal information and the confidentiality of the healthcare center's disease models. In addition, the extensive experiments with an android app and two java server programs demonstrate its efficiency in terms of computational costs and communication overheads.

INDEX TERMS Priority, remote eHealthcare, privacy, sensor, smart phone.

I. INTRODUCTION

With the pervasiveness of smartphones and the wireless body area network (WBAN), the remote eHealthcare system has received considerable attention and become more popular. A variety of WBAN schemes and applications have been proposed [1]–[4] in recent years, including energy-efficient medium access protocol for WBAN using the listen-before-transmit manner [2], data forwarding framework between biosensors and the gateway considering the presence of body shadowing [3], prioritized adaptive resource allocation algorithm for WBAN based on patients' medical situation [4]. Considering the limited resource of the sensors, the collected data streams can not be transmitted directly to the healthcare center. As shown in Fig. 1, the sensors in each user's wearable health system periodically collect the users' physiological data, send these raw data to the his/her smartphone for preprocessing. The smartphone assembles a medical packet containing the user's preprocessed physiological data, and sends it to a WBAN-gateway nearby. The medical packets from different users will be randomly aggregated in WBAN-gateways. Then the WBAN-gateways relay all the medical packets to the remote healthcare center.

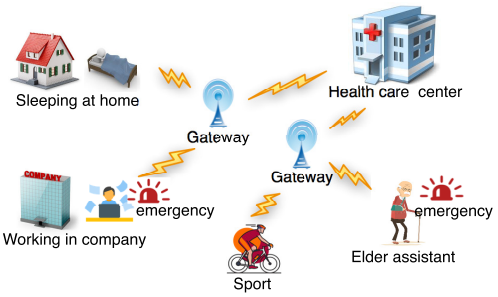

FIGURE 1. Wearable health monitor system.

While the WBAN remote healthcare system is popular and vital, most of the remote healthcare systems require users

to submit sensitive physiological data, personal information like age, name, gender, medical history, which seriously raises concerns about leaking and misusing of users' sensitive privacy data. On the other hand, the disease models are precious intellectual properties of the healthcare center. The healthcare center is not willing to reveal the disease models to the users or the WBAN-gateways. Some attackers may crack the users' smartphones or the WBAN-gateways, and steal the sensitive users' personal information and the healthcare center's intellectual properties. Therefore, a variety of privacy-preserving schemes have been proposed in remote eHealthcare system [5]–[8]. However, the privacy-preserving healthcare schemes based on the encrypted data have some issues like accuracy and efficiency to be solved. We outline the challenges for privacy-preserving remote eHealthcare system would face as below:

- Challenges on security and privacy. As discussed above, all the users' physiological data, personal information and the healthcare center's disease models need to be encrypted. An attacker should not recover the sensitive plaintext by observing the ciphertext, i.e., secure under ciphertext-only attack. Moreover, it is reasonable to assume in some scenarios, the attacker knows some users' information or some disease models. Even in this context, the attacker can not recover other plaintext of the corresponding encrypted data. In other words, the system should be secure under know-plaintext attack.
- Challenges on accuracy. To achieve the security requirements of the remote eHealthcare system, some privacy-preserving schemes based on the encrypted data need to standardize the users' personal information and healthcare center's disease model first. The standardization techniques may compromise the computational accuracy. What's more, some randomization techniques like the differential privacy [9] add some random values to the computational results, which may cause medical disaster in some scenarios [10]. Therefore, the privacy-preserving remote eHealthcare system should be accurate for medical analysis.
- Challenges on efficiency. Most of the privacy-preserving schemes based on the encrypted data are involved with large computational overhead. Recent studies propose some privacy-preserving schemes with multi parties [11], which derives large communication cost. On the other hand, the non-interactive privacy-preserving schemes are always associated with time-consuming techniques, such as fully homomorphic encryption [12]. Thus, the privacy-preserving remote eHealthcare system needs to solve the efficiency issues.

In this paper, aiming at solving the above challenges, we propose an efficient and privacy-preserving priority classification (PPC) on patient health data in remote eHealthcare system, which allows authenticated users to periodically send medical packets to the healthcare center through WBAN-gatways. The WBAN-gateways relay these aggregated medical packets in a non-interactive privacy-preserving way based on the packets' priorities (criticalities). The main contributions of this paper are as following:

- First, we propose the PPC scheme, an efficient privacy-preserving non-interactive priority classification scheme for users' medical packets in WBAN-gateways. Particularly, The WBAN-gateways derive the priorities of the medical packets and relay the packets in a priority heap.
- Second, we develop an android app and two java server programs to evaluate the performance of the PPC scheme. The results show that the proposed PPC scheme is efficient in both computational cost and communication overhead. The security analysis also demonstrates that our proposed PPC scheme can preserve the privacy of the users' personal information and the confidentiality of the healthcare center's disease models.

The remainder of this paper is organized as follows. In Section II, we formalize our system model, security requirement and identify design goal. In Section III, we introduce some preliminaries for our scheme. And in Section IV, we present our PPC scheme, followed by its security analysis and performance evaluation in Section V and Section VI respectively. We also discuss the related works in Section VII. Finally, we draw our conclusions in Section VIII.

II. MODELS AND DESIGN GOAL

In this section, we formalize the system model, security requirement in this paper, and identify our design goal.

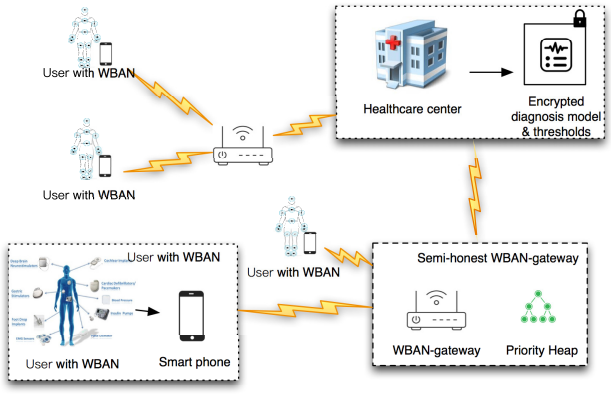

FIGURE 2. System model of medical packet classification and relay in remote eHealthcare system under consideration.

A. SYSTEM MODEL

Privacy-preserving remote eHealthcare system has been studied in both cloud-based outsourced setting and two-party communication setting between user and healthcare center. In our work, we focus on the communication between the users and the healthcare center through relay WBAN-gateways. The WBAN-gateways receive medical packets from different users, and relay these packets on account of the criticalities of the medical packets and their waiting time. As shown in Fig. 2, the system mainly

contains three entities: healthcare center, WBAN-users, and WBAN-gateways.

- *Healthcare center*: The healthcare center is a medical organization, which is professional in offering healthcare service, and has abundant diagnosis models for different diseases. The healthcare center offers custom medical service for different users. In other words, it provides individual diagnosis service for different diseases for different users according to the users' equipped sensors. Moreover, it sets different criticality thresholds for different users with the same disease because of their different physical conditions. However, the disease models and the thresholds are the intellectual properties of the healthcare center. The healthcare center is not willing to disclose the valuable intellectual properties to the users and the WANB-gateways. Thus, it encrypts all the data, and sends the encrypted disease models and the thresholds to the authenticated users.
- *WBAN-users*: The users equipped with a list of body sensors and smartphones register from the healthcare center, send their sensor list and personal information to the healthcare center and retrieve the encrypted disease models and thresholds. The sensors periodically collect a user's physiological information, and send these raw data to the user's smartphone for preprocessing and encryption. Then, the user sends the encrypted medical packets to a WBAN-gateway. The WBAN-gateway will relay the packets to the healthcare center.
- *WBAN-gateways*: The WBAN-gateways are responsible for relaying users' medical packets to the healthcare center. The users' packets are randomly aggregated at the WBAN-gateways. These medical packets' transmission to remote healthcare center relying on a priority-based classification scheme managed by the WBAN-gateways. To simplify the description of our proposed scheme, we consider only one WBAN-gateway in our proposed scheme.

B. SECURITY REQUIREMENT

In our system, the WBAN-gateway is considered as semi-honest, which means the WBAN-gateway would strictly execute the protocol to guarantee the correctness of the medical packets relay task, but it has financial incentives to recover the healthcare center's valuable disease model, the users' privacy information. Moreover, the WBAN-gateway may be compromised by hackers. Therefore, to guarantee the privacy of users' physiological data and the confidentiality of the healthcare center's disease model, the following security requirements should be satisfied:

- *Privacy*. In our remote eHealthcare system, each user collects his/her physiological information and personal information, and sends these information to the healthcare for remote healthcare monitoring. These sensitive personal data should be prevented from leaking to the WBAN-gateway. Specifically, the WBAN-gateway can not recover the users' physiological data by observing the encrypted medical packets, which means our system is secure under ciphertext-only attack. What's more, if an attacker knows the plaintext of some encrypted medical packets, the attacker can not reveal a user's physiological data corresponding to other encrypted medical packets. In other words, it is secure under known-plaintext attack.
- *Confidentiality*. The disease models and the thresholds for each user are the intellectual properties of the healthcare center. Same as above, the WBAN-gateway can not recover the disease models and the thresholds by observing the encrypted data. In our system, the encrypted disease models and thresholds would be sent to the authenticated users. The authenticated users are allowed to make use of the encrypted data to conduct the preprocessing for the privacy-preserving priority classification, but can not recover the disease models and the thresholds. Moreover, even when an attacker knows some plaintext of one encrypted disease model, it is unable for the attacker to reveal other disease models, thresholds and the users' personal data, which is secure under known-plaintext attack.
- *Authentication*. Only the users, who have registered in the healthcare center and gained the encrypted parameters, can conduct the remote healthcare monitoring service. The DDoS attack is not considered in our paper. We focus on how to achieve the privacy-preserving priority classification task.

Note that, other attacks such as differential privacy attack, access-pattern attack and DDoS attack could be possible in eHealthcare system. However, since this work focus on the privacy-preserving medical packets classification, those attacks will not be discussed, and would be exploited in our future work.

C. DESIGN GOAL

Based on the system model mentioned above, our design goal is to develop an efficient and privacy-preserving priority classification in remote eHealthcare system. Specially, the following three objectives should be achieved:

- *Efficiency*. Considering the real-time requirements of the emergency healthcare remote monitoring system and the diversity of the users, the proposed scheme should be efficient in computation and communication. In our system, some medical packets come from users with very critical situation. Thus, the privacy-preserving priority calculation for the packets should be efficient.
- *Security*. The aforementioned security requirements should be satisfied. The healthcare center's disease models and thresholds should not be recovered by the users and WBAN-gateway. On the other hand, the users' physiological data and personal information should be prevented from the WBAN-gateway.
- *Accuracy*. Because of the criticality of the eHealthcare system, the accuracy of the priority classification scheme in the remote eHealthcare system should

be guaranteed. In some privacy-preserving schemes, the accuracy is compromised. However, in this system related to users' emergency healthcare monitoring, the privacy-preserving priority classification scheme should achieve high accuracy.

III. PRELIMINARIES

In this section, we outline the bilinear pairing with composite order, the BGN homomorphic cryptosystem and the max heap, which will serve as the basis of our PPC scheme.

A. BILINEAR PAIRING WITH COMPOSITE ORDER

Let p, q be two large distinct prime numbers of the same κ-bit length, and set $N = pq$. $\mathbb{G}$ and $\mathbb{G}_T$ are two cyclic groups of the same composite order N. $\mathbb{G}$ and $\mathbb{G}_T$ are called bilinear map with composite order if there is a computable mapping $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ with following properties:

- Bilinearity. $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$ for any $a, b \in \mathbb{Z}_N$ and $g_1, g_2 \in \mathbb{G}$.
- Non-degeneracy. $e(g, g) \neq 1$.
- Computability. $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ can be computed efficiently.

The definitions of composite bilinear generator and the subgroup decision problem are shown as below:

Definition 1. $\mathcal{G}en$ is a probabilistic algorithm that takes a security parameter κ as input and output a 5-tuple $(g, N, \mathbb{G}, \mathbb{G}_T, e)$, where $N = pq$, p and q are two κ-bit length prime numbers.

Definition 2. Subgroup decision problem is shown as: Let g be a generator of $\mathbb{G}$, then $g_1 = g^p \in \mathbb{G}$ can generate the subgroup $\mathbb{G}_p = \{g_1^0, g_1^1, \ldots, g_1^{p-1}\}$ of order p, and $g_2 = g^q \in \mathbb{G}$ can generate the subgroup $\mathbb{G}_q = \{g_2^0, g_2^1, \ldots, g_2^{p-1}\}$ of order q. Given a tuple $(e, \mathbb{G}, \mathbb{G}_T, N, h)$, where h is drawn randomly from either $\mathbb{G}$ or the subgroup $\mathbb{G}_p$, decide whether $h \in \mathbb{G}_p$. The hard subgroup decision problem ensures the security of the BGN homomorphic cryptosystem below.

B. BGN HOMOMORPHIC CRYPTOSYSTEM

The BGN cryptosystem was proposed by Dan *et al.* [13], which is the first "somewhat homomorphic" cryptosystem with a constant-size ciphertext. The key idea in the BGN cryptosystem is based on the subgroup decision assumption, which supports polynomially many additions and just one multiplication. Concretely, it mainly contains three functions: key generation, encryption and decryption:

- $\mathcal{G}en(\kappa)$: Given a secret parameter κ, choose two κ-bit prime number p, q and set $N = pq$. Let g be a generator of $\mathbb{G}$ with order N. Find a computable mapping $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$. Set $h = g^q$, which is a generator of the subgroup $\mathbb{G}$ with order p. Output the public key $pk = (N, \mathbb{G}, \mathbb{G}_T, e, g, h)$ and private key $sk = p$.
- $Enc(pk, m)$: Given a message m from a small space, we choose a random value $r \in \mathbb{Z}_N$. Output the ciphertext $C = Enc(pk, m) = g^m h^r \in \mathbb{G}$.
- $Dec(sk, C)$: Given a ciphertext $C \in \mathbb{G}$ and the secret key $sk = p$, perform the calculation $C^p = (g^m h^r)^p = (g^p)^m$. As mentioned above, the message m is from small spaces, it suffices to solve the discrete log of $(g^p)^m$ with base g^p.

The BGN cryptosystem enjoys the following properties:

- Addition in $\mathbb{G}$: Given two ciphertext $Enc(m_1)$, $Enc(m_2) \in \mathbb{G}$, we have $Enc(m_1) \cdot Enc(m_2) = Enc(m_1 + m_2)$.
- Addition in $\mathbb{G}_T$: Given two ciphertext $Enc_T(m_1)$, $Enc_T(m_2) \in \mathbb{G}_T$, we have $Enc_T(m_1) \cdot Enc_T(m_2) = Enc_T(m_1 + m_2)$.
- Multiplication from $\mathbb{G}$ to $\mathbb{G}_T$: Given two ciphertext $Enc(m_1), Enc(m_2) \in \mathbb{G}$, we have $e(Enc(m_1), Enc(m_2)) = Enc_T(m_1 \cdot m_2) \in \mathbb{G}_T$.

C. MAX HEAP

A max-heap is a complete binary tree, in which the value in each internal node is greater than or equal to the values in the children of that node. The max-heap is widely used in top-k ranking algorithm. As shown in the Fig. 3, mapping the elements of a max-heap into an array is trivial: If a node is stored at index k, then its left child is stored at index $2k + 1$ and its right child at index $2k + 2$, and its parent is at index $(k - 1)/2$, if exist.

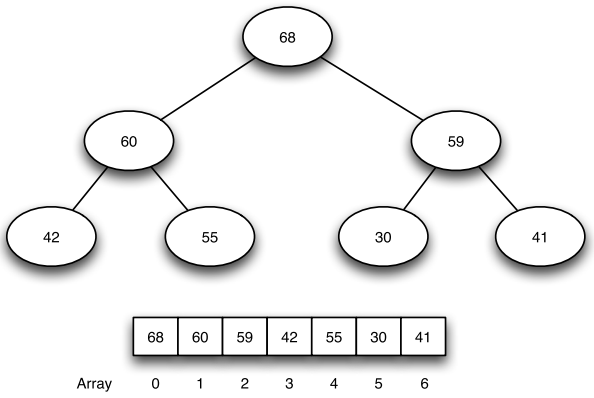

FIGURE 3. A sample of max heap.

Because a max-heap is a complete binary tree, it can be efficiently represented using a simple array. Moreover, given an array of N values, a heap containing those values can be built by simply sifting each internal node down to its proper location.

The cost of inserting a node into a max-heap with N nodes: the same as the max-heap buildup, the inserting algorithm is involved in sifting nodes from the leaf to the root. The number of steps required for sifting values down will be maximized if the heap is full, which means $N = 2^d - 1$, and the heap height is d. The cost of inserting a node is $O(d)$, or $O(\lg N)$.

IV. PROPOSED PPC SCHEME

In this section, we propose a non-interactive privacy-preserving PPC scheme, which mainly consists of system setup, user registration, user data collection, WBAN-gateway packet classification and relay.

A. OVERVIEW

The proposed PPC scheme allows the WBAN-gateway to manage users' medical packets based on their emergency levels in a privacy-preserving way.

In PPC, each user is equipped with a wearable WBAN, which is comprised of a number of wearable sensor nodes wirelessly capturing and collaboratively processing physiological signals. These raw data are transmitted to the user's smartphone for standardization, encryption before being relayed to the WBAN-gateway. Some raw data are decimal numbers. To simplify the implementation of the encryption technique, the decimal data need to be increased by a factor of 1000 times and rounded up. We let $\mathbb{X} = \{x_1 \dots x_n\}$ be the standardized physiological data in the PPC scheme. Considering the decimal data like the AC conductance for skin conductance [14], for instance, the original $0.65\,\mu S$ needs to be increased to $x = 650$. The standardization keeps the physiological data positive. Moreover, it ensures the inner product of the user's physiological data and the disease model offered by the healthcare center positive, which is an important property for our privacy-preserving emergency relay scheme. On the other hand, the healthcare center owns the disease model $(a_1, a_2, \dots, a_k)$ and thresholds $(t_1, t_2, \dots, t_l)$. The disease risk score S for the user, can be computed by $S = \sum_{i=1}^{k} a_i \cdot x_i$ [15]–[17]. We can calculate a user's disease risk by comparing the disease risk score and the thresholds $(t_1, t_2, \dots, t_l)$. For a more comprehensive description of the disease risk score, the reader can refer to [15]–[17].

Before describing the PPC scheme, we define the priority classification on patients' health data in remote eHealthcare system without considering the users' privacy and healthcare center's disease model confidentiality. The system consists of three stages:

- Each authenticated user retrieves the disease model $(a_1, a_2, \dots, a_k)$ and thresholds $(t_1, t_2, \dots, t_l)$ from the healthcare center according to the user's sensor list.
- The user's sensors collect the physiological data and send these data to the user's smartphone. Then the user conducts the calculation $sum = \sum_{i=1}^{k} a_i \cdot x_i$. The user sends a medical packet containing the physiological data $(x_1, x_2, \dots, x_k)$, user information *userinfo*, the calculation result *sum* and the thresholds $(t_1, t_2, \dots, t_l)$ to a WBAN-gateway. Remark, that the user can calculate the priority for the packet by himself/herself. But to clearly describe the same data flow over encrypted data in the PPC scheme, we let the WBAN-gateway calculate the priority of the medical packet.
- Shown as the samples in Fig. 4, receiving the medical packet from the user, the WBAN-gateway picks two consecutive thresholds t_i, t_j, where $t_i < sum < t_j$, and assigns the priority j to this medical packet. If *sum* is larger than the largest threshold $sum > t_l$, the WBAN-gateway assigns the priority $l + 1$ to the packet. Finally, the WBAN-gateway relays all the aggregated packets to the healthcare center according to their priorities.

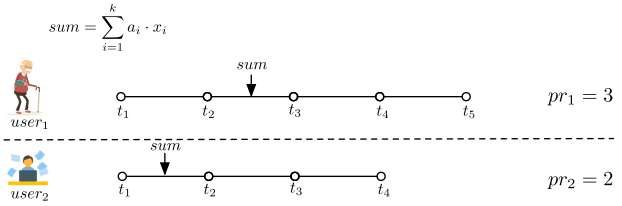

FIGURE 4. Two samples of the priority calculation with *sum* and the thresholds $(t_1, t_2, \dots, t_l)$.

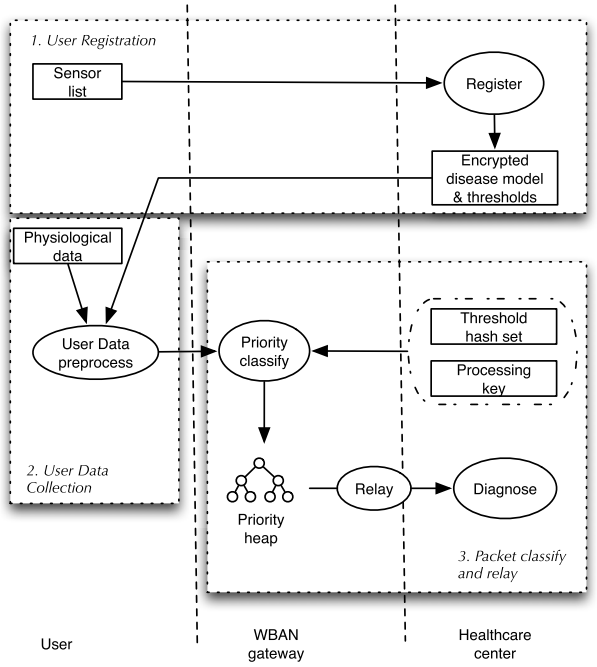

FIGURE 5. Data flow of the PPC scheme.

The proposed PPC scheme is comprised of user registration, data collection and WBAN-gateway packet priority classification and relay. Fig. 5 depicts the data flow. The sensor-collected data are processed in the smartphone as mentioned above periodically. Then, these data are encrypted, and processed with encrypted disease model offered by the healthcare center. The calculated result will be transmitted to the WBAN-gateway. Receiving these encrypted medical packets from different users, the WBAN-gateway conducts privacy-preserving priority calculations for all these medical packets, and inserts these medical packets into a priority-based relay heap. Thus, the medical packets with high priority will be relayed to the healthcare center first. Specifically, the WBAN-gateway conducts the privacy-preserving priority calculation based on the encrypted data in a non-interactive way, which as we know, is very novelty. For the reader's convenience, we summarize the important notations to be used in Table 1.

B. SYSTEM SETUP

The healthcare center is the trust entity in our model and sets up the system, which takes a security parameter κ, and runs the bilinear generation algorithm $\mathcal{G}en(\kappa)$. The output of the generation algorithm are the public

TABLE 1. Notations frequently used in PPC.

Notation	Description
κ	security parameter
$\mathcal{G}en(\kappa)$	bilinear generation algorithm
$\mathbb{G}, \mathbb{G}_T$	two group of composite order $N = pq$
p, q	two κ-bit prime numbers
g	a generator of group $\mathbb{G}$
e	a computable mapping $\mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$
p	private key
$\alpha, \beta, \gamma \in \mathbb{Z}_N$	three secret random values
$Enc(\cdot)$	an hybrid ECIES [18] encryption algorithm
$K_G = g^{\alpha p}$	a processing key owned by the healthcare center
$H(\cdot)$	a hash function set by the healthcare center
$H_i, i \in \{1, 2, ..., t_m\}$	a hash set created by the healthcare center
t_m	the maximum threshold for all the diseases owned by the healthcare center
$\mathbb{X} = \{x_1 \ldots x_k\}$	standardized physiological data
$\overrightarrow{X}_u$	user's physiological data vector
$\overrightarrow{A} = (a_1, a_2, ..., a_k)$	a disease model for one user
$(t_1, t_2, ..., t_l)$	l thresholds for a user for one disease
$A_i = [a_i], i = 1, 2, ..., k$	encrypted disease model coefficients
$T_j = [t_j], j = 1, 2, ..., l$	encrypted thresholds

parameters $(N, g, \mathbb{G}, \mathbb{G}_T, e)$, where $\mathbb{G}, \mathbb{G}_T$ are two group of composite order $N = pq$, p, q are two κ-bit prime numbers, g is a generator of group $\mathbb{G}$, e is a computable mapping $\mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$. Then, the healthcare center sets the BGN public key $pk = (N, g, \mathbb{G}, \mathbb{G}_T, e, h)$, where $h = g^q$, and the private key $sk = p$. Moreover, the healthcare center chooses three secret random values $\alpha, \beta, \gamma \in \mathbb{Z}_N$. Further, an hybrid ECIES [18] encryption algorithm $Enc(\cdot)$ is chosen by the healthcare center. To encrypt the long user's physiological data vector and user information, we choose the hybrid ECIES encryption [18] rather than a simple public encryption algorithm. Finally, the healthcare center publishes the public parameters $pk = (N, g, \mathbb{G}, \mathbb{G}_T, e, h)$ and the ECIES $Enc(\cdot)$, keeps the private parameters $(p, \alpha, \beta, \gamma)$ secret.

In order to let the WBAN-gateway conduct the privacy-preserving priority calculation over encrypted data, the healthcare center assigns the processing key $K_G = g^{\alpha p}$ to the WBAN-gateway. Further, the healthcare center defines a hash function $H(\cdot)$ and a set of hash values as follows:

$$H_i = H(e(g, g)^{\alpha\beta p(\gamma+i)}),\ i \in \{1, 2, \ldots, t_m\}$$

where t_m is the maximum threshold for all the diseases owned by the healthcare center. In other words, for each disease dis_i, according to the disease levels, it has different thresholds $t_{i1}, t_{i2}, \ldots, t_{ik}$, and $t_m = max(t_{ik})$. For example, if the healthcare center has threshold $t_{11} = 50$ for disease dis_1, $t_{21} = 60$ for disease dis_2 and $t_{31} = 70$, $t_{32} = 65$ for disease dis_3, then the maximum threshold $t_m = t_{31} = 70$.

For a user u, we assume some properties:

- The inner product of the user's physiological data vector $\overrightarrow{X}_u$ and the healthcare center's disease model $\overrightarrow{A}_u$ is positive: $\overrightarrow{X}_u \cdot \overrightarrow{A}_u > 0$;
- When the user is in normal state for a disease level with the related threshold t_u, the inner product result is less than t_u: $\overrightarrow{X}_u \cdot \overrightarrow{A}_u < t_u$; On the other hand, if the user is in abnormal status for threshold t_u, $\overrightarrow{X}_u \cdot \overrightarrow{A}_u \geq t_u$;

The healthcare center also sends the hash set $\{H_1, H_2, \ldots, H_{t_m}\}$ and the hash function $H(\cdot)$ to the WBAN-gateway.

After the system setup, the WBAN-gateway gets the processing key $K_G = g^{\alpha p}$, the hash set $\{H_1, H_2, \ldots, H_{t_m}\}$ and the hash function $H(\cdot)$.

Algorithm 1 User_Register()

\\ Input: $(S_1, S_2, \ldots, S_k)$, user's sensor list
\\ Input: *userinfo*, user's information like name, age, etc.
\\ Output: $A_i,\ i = 1, 2, \ldots, k$, encrypted disease model coefficients
\\ Output: $T_j,\ j = 1, 2, \ldots, l$, encrypted thresholds
\\ $Enc(\cdot)$, an hybrid ECIES [18] encryption algorithm
User does:
$Enc_{sensors} = Enc(S_1|S_2|...|S_k|userinfo)$
send the $Enc_{sensors}$ to the healthcare center
——————>
Healthcare center does:
decrypts the $Enc_{sensors}$, gets the $(S_1, S_2, \ldots, S_k)$ and *userinfo*
finds out disease *dis*, disease model $a_i, i = 1, 2, ..., k$ and related thresholds $t_j, j = 1, 2, \ldots, l$ according to the $(S_1, S_2, \ldots, S_k)$ and *userinfo*
for $i = 1$ to k **do**
    $A_i = [a_i] = g^{\beta a_i} h^{r_i}$
end for
for $j = 1$ to l **do**
    $T_j = [t_j] = g^{\beta(t_j+\gamma)} h^{r_j}$
end for
sends the $A_i,\ i = 1, 2, \ldots, k$ and $T_j,\ j = 1, 2, \ldots, l$ to the user

C. USER REGISTRATION

Firstly, a user registers in the healthcare center for this emergency monitoring service. Shown as the Algorithm. 1, according to the user's sensor list, the healthcare center finds the related disease the user needs to monitor. Accordingly, the healthcare center fetches the related disease model $\overrightarrow{A} = (a_1, a_2, ..., a_k)$ and the l thresholds $(t_1, t_2, ..., t_l)$. Note that, a user's number of thresholds l can be different from that of other users' thresholds. The healthcare center encrypts the disease model and thresholds as follows:

$$A_i = [a_i] = g^{\beta a_i} h^{r_i},\ i = 1, 2, \ldots, k$$
$$T_j = [t_j] = g^{\beta(t_j+\gamma)} h^{r_j},\ j = 1, 2, \ldots, l$$

where $r_i, r_j \in \mathbb{Z}_N$ are random values secretly chosen by the healthcare center. These encrypted disease model $A_i,\ i = 1, 2, \ldots, k$ and thresholds $T_j,\ j = 1, 2, \ldots, l$ are sent to the authorized user.

D. USER DATA COLLECTION

The authorized user equipped with sensors collects the physiological data periodically. In each round, after standardization, the user gets the physiological data vector

Algorithm 2 User_Data_Collect()

\\ Input: $\overrightarrow{X} = (x_1, x_2, ..., x_k)$, physiological data vector
\\ Input: $A_i, i = 1, 2, \ldots, k$, encrypted disease model coefficients
\\ Input: $T_j, j = 1, 2, \ldots, l$, encrypted thresholds
\\ Output: $C||C'_1||C'_2||...||C'_l$, encrypted packet
user does:
$prod = \prod_{i=1}^{k} A_i^{-x_i}$
for $j = 1$ to l **do**
    $C'_j = T_j \cdot prod \cdot h^{r_j}$
end for
$C = Enc(x_1||x_2||...||x_k||userinfo)$
sends the $C||C'_1||C'_2||...||C'_l$ to the WBAN-gateway

$\overrightarrow{X} = (x_1, x_2, ..., x_k)$. Shown as the Algorithm. 2, with the encrypted disease model, the user performs the computation for all the thresholds:

$$\begin{aligned} C'_j &= \frac{T_j}{\prod_{i=1}^{k} A_i^{x_i}} \cdot h^{r_j}, \ j = 1, 2, \ldots, l \\ &= g^{\beta(\gamma + t_j - \sum_{i=1}^{k} a_i \cdot x_i)} \cdot h^{r_j}, \ j = 1, 2, \ldots, l \end{aligned}$$

where each $r_j \in \mathbb{Z}_N$ is a random value. The user also makes use of the ECIES encryption algorithm $Enc(\cdot)$ to encrypt the physiological data vector and the user's information *userinfo* such as name, age, etc.

$$C = Enc(x_1||x_2||...||x_k||userinfo)$$

Finally, the user sends the data $C||C'_1||C'_2||...||C'_l$ to the WBAN-gateway.

E. WBAN-GATEWAY PACKET CLASSIFICATION AND RELAY

The WBAN-gateway receives the encrypted medical packets from different users. Shown as the Algorithm. 3, for each medical packet, the WBAN-gateway calculates the priority, and inserts it into a priority-based relay heap.

In the priority-based packet classification algorithm, the WBAN-gateway takes the $C'_1, C'_2, \ldots, C'_l$ and the processing key K_G as the inputs, performs the priority calculations as follow:

$$\begin{aligned} D_j &= e(C'_j, K_G) \\ &= e(g^{\beta(\gamma + t_j - \sum_{i=1}^{k} a_i \cdot x_i)} \cdot h^{r_j}, g^{\alpha p}) \\ &= e(g, g)^{\alpha\beta p(\gamma + t_j - \sum_{i=1}^{k} a_i x_i)} \end{aligned}$$

where $j = 1, 2, \ldots, l$. The WBAN-gateway assigns the priority of the medical packet based on which hash value $H(D_j), = 1, 2, \ldots, l$ is in the hashset $\{H_1, H_2, \ldots, H_{t_m}\}$. Then the medical packet is inserted into the priority-based relay heap, the root packet of which is the highest priority packet. However, it is unreasonable for the low priority packets to be preempted by the high priority packets all the way. So a timer frequently increases the priority by one for all the packets in the priority-based relay heap.

Algorithm 3 Packet_Classify_Relay()

\\ Input: $C'_1, C'_2, \ldots, C'_l$, encrypted data got from a user
\\ Result: assigns priority pr_u to the packet, and insert it into the relay heap
\\ C: $C = Enc(x_1||x_2||...||x_k||userinfo)$, encrypted physiological data and user info
\\ K_G, a processing key
WBAN-gateway does:
for $j = 1$ to l **do**
    $D_j = e(C'_j, K_G)$
end for

$pr_u = -1$
for $j = 1$ to l **do**
    if $H(D_j) \in \{H_1, H_2, \ldots, H_{t_m}\}$ **then**
        $pr_u = j$
        break
    else if $H(D_j) \notin \{H_1, H_2, \ldots, H_{t_m}\}$ **then**
        go on
    end if
end for
if $pr_u = -1$ **then**
    $pr_u = l + 1$
end if
$C.priority = pr_u$
$RelayHeap.insert(C)$

$Relaypacket = RelayHeap.removeMax()$
relay the *Replaypacket* to healthcare center
for $i = 1$ to $RelayHeap.size()$ **do**
    $packet = RelayHeap.packet(i)$
    $packet.priority++$
end for

F. CORRECTNESS PROOF

First, we prove that for a healthy user u, the WBAN-gateway assigns the $pr_u = 1$ priority to this user's packet, if $0 < \overrightarrow{A} \cdot \overrightarrow{X} < t_1$. Recall that all the physiological data $x_i \in \mathbb{X}$ are positive, and the healthcare center's disease model coefficients $a_i, i = 1, 2, \ldots, k$ are positive. It's easy to find out $\overrightarrow{A} \cdot \overrightarrow{X} = \sum_{i=1}^{k} a_i \cdot x_i > 0$. On the other hand, For the threshold t_1, the WBAN-gateway conducts the calculation:

$$\begin{aligned} D_1 &= e(C'_1, K_G) \\ &= e(g^{\beta(\gamma + t_1 - \sum_{i=1}^{k} a_i \cdot x_i)} \cdot h^{r_j}, g^{\alpha p}) \\ &= e(g, g)^{\alpha\beta p(\gamma + t_1 - \sum_{i=1}^{k} a_i x_i)} \end{aligned}$$

Because $t_1 > \sum_{i=1}^{k} a_{ui} x_{ui}$, it ensures $t_1 > t_1 - \sum_{i=1}^{k} a_i x_i > 0$. We define a function $PH(x) = H(e(g, g)^{\alpha\beta p(\gamma + x)})$. It is easy to find out $PH(t_1 - \sum_{i=1}^{k} a_i x_i)$ is in the set $\{PH(1), PH(2), \ldots, PH(t_1)\}$. Therefore, $H(D_1)$ is in the hashset $\{H_1, H_2, \ldots, H_{t_1}\}$, which is the subset of $\{H_1, H_2, \ldots, H_{t_m}\}$. So the priority of this user's packet is $pr_u = 1$.

Second, we prove that for a user u with $t_{bottom} < \sum_{i=1}^{k} a_i x_i < t_{up}$, the WBAN-gateway assigns the *up* to this

user's packet $pr_u = up$. Same as above, if $\sum_{i=1}^{k} a_i x_i < t_{up}$, $H(D_{up})$ is in the hashset $\{H_1, H_2, ..., H_{t_{up}}\}$, which is the subset of $\{H_1, H_2, ..., H_{t_m}\}$. For the $t_{bottom} < \sum_{i=1}^{k} a_i x_i$, we have the calculation:

$$\begin{aligned} D_{bottom} &= e(g,g)^{\alpha\beta p(\gamma + t_{bottom} - \sum_{i=1}^{k} a_i x_i)} \\ \Rightarrow \because\ & t_{bottom} < \sum_{i=1}^{k} a_i x_i,\ t_{bottom} - \sum_{i=1}^{k} a_i x_i < 0 \\ & PH(t_{bottom} - \sum_{i=1}^{k} a_i x_i) = PH(value < 0) \\ \Rightarrow \because\ & PH(value < 0) \notin \{PH(1), PH(2), \ldots, PH(t_m)\} \\ & PH(t_{bottom} - \sum_{i=1}^{k} a_i x_i) \notin \{PH(1), PH(2), \ldots, PH(t_m)\} \\ & H(D_{bottom}) \notin \{H_1, H_2, ...H_{t_m}\} \end{aligned}$$

Thus, in the line 15-16 of the Algorithm 3, the algorithm will go on until meeting $H(D_{up})$. Then, the WBAN-gateway assigns the priority up to the user's packet, which means $pr_u = up$.

Third, we prove that the medical packets aggregated in the WBAN-gateway will be relayed to the healthcare center according to their priorities. As mentioned above, each medical packet C containing the encrypted user physiological data $x_1, x_2, \ldots, x_k$ and user information $userinfo$ is inserted into the relay heap. This heap is a max heap based on the packets' priorities. The WBAN-gateway removes and relays the max element (root element), which is the packet with the highest priority. Then the heap is sifted to be a full tree again. Moreover, a timer frequently updates the priorities of all the packets in the heap to prevent too long starving time for low priority packets.

V. SECURITY ANALYSIS

In this section, we analyze the security properties of the proposed priority classification scheme. Specifically, following the security requirements discussed earlier, our analysis will focus on how the proposed scheme can achieve the users' data privacy and healthcare center's disease model confidentiality.

In our system model, the users' data privacy involves protecting the sensitive physiological data in the relay packets and the procedure of priority classification. On the other hand, the healthcare center's disease model confidentiality includes protecting the disease model coefficients and the thresholds for different authenticated users. The security of the remote monitoring eHealthcare system depends on the underlying standard encryption, and our PPC scheme. The standard encryption is responsible for preventing the WBAN-gateway from learning the users' personal information. And our PPC scheme is responsible for protecting the users' data and the healthcare center's disease model while achieving the priority classification for all the packets from different users. The ECIES encryption that consists of the symmetric encryption and the public key encryption is secure under the cipher-only, known-sample and known-plaintext attacks. Thus, we focus on the analysis of the user's data privacy and the healthcare center's disease model confidentiality with our PPC scheme.

Security of the user's data encryption and the disease model encryption. First, in our PPC scheme, the coefficients of the disease model $a_i, i = 1, 2, \ldots, k$ are encrypted as $A_i = [a_i] = g^{\beta a_i} h^{r_i},\ i = 1, 2, \ldots, k$, and the thresholds $t_j, j = 1, 2, \ldots, l$ for the user are encrypted as $T_j = [t_j] = g^{\beta(t_j+\gamma)} h^{r_j},\ j = 1, 2, \ldots, l$. Because the BGN encryption is secure, without knowing the private parameters $\{\alpha, \beta, \gamma\}$ and $sk = p$, it is hard for the WBAN-gateway to recover $a_i, i = 1, 2, \ldots, k$ and $t_j, j = 1, 2, \ldots, l$. Moreover, the user's physiological data $x_i, i = 1, 2, \ldots, k$ are encrypted in the $C'_j = g^{\beta(\gamma + t_j - \sum_{i=1}^{k} a_i \cdot x_i)} \cdot h^{r_j},\ j = 1, 2, \ldots, l$, from which, it is impossible for WBAN-gateway to recover the $x_i, i = 1, 2, \ldots, k$ directly. As mentioned above, the user's physiological data $x_i, i = 1, 2, \ldots, k$ that are encrypted inside $C = Enc(x_1||x_2||...||x_k||userinfo)$ are also secure due to the security of the ECIES encryption.

Security of the user's data and healthcare center's disease model in the priority classification scheme. As discussed above, it is hard to reveal the user's data and the healthcare center's disease model from the encrypted data. Alternatively, the attacker may attempt to recover the priority of the user's medical packet or the inner product $\overrightarrow{A} \cdot \overrightarrow{X}$ first, then reveal the vector containing the disease model and the user's physiological data. Now we show the countermeasures against this kind of attacks.

The attacker may attempt to recover the inner product of the priority calculation over $D_j, j = 1, 2, \ldots, l$. However, each D_j is calculated by the WBAN-gateway with C'_j and K_G as:

$$D_j = e(g,g)^{\alpha\beta p(\gamma + t_j - \sum_{i=1}^{k} a_i x_i)}$$

Because both $e(g,g)^{\alpha\beta p}$ and γ are unknown, it is unable for the attacker to solve $t_j - \sum_{i=1}^{k} a_i x_i$, according to the discrete logarithm problem. Therefore, the attacker could not recover the $a_i, i = 1, 2, \ldots, k, x_i, i = 1, 2, \ldots, k, t_j, j = 1, 2, \ldots, l$.

Knowing the priority-based packet relay heap, the attacker may also attempt to recover the user's data and the healthcare center's disease model from the heap. The WBAN-gateway assigns the priority of the packets based on the hash function $H(D_j)$ and the hashset $\{H_1, H_2, ..., H_m\}$. The hash function is non-invertible. The membership operation on whether a $H(D_j)$ is a member of the hashset $\{H_1, H_2, ..., H_m\}$ only reveals the priority of the packet, which is not a privacy for our system model. The timer updates the priority of the packets in the priority-based relay heap. All the operation over the heap relies on the packet's calculated priority, which reveals no user's physiological data and the healthcare center's disease model.

VI. PERFORMANCE EVALUATION

In this section, we evaluate the performance of the proposed PPC scheme in terms of computational cost and communication overhead.

A. IMPLEMENTATION AND EXPERIMENTAL SETTINGS

We have implemented the PPC scheme in java. We test PPC's performance in a testbed of a mac osx laptop and one android phone. We deploy the programs of the healthcare center and WBAN-gateway in the mac osx laptop. The android phone plays the role of the mobile user. For comparison, we also implement a paillier-based privacy-preserving priority classification scheme. Thus, an ECS server plays the role of the decryption helper in the paillier-based scheme. The hardware and software of these machines are shown in Table 2.

TABLE 2. Experimental setting.

Role	Machine	Hardware & Software
Health center	Mac laptop	CPU:2.9 GHz Intel Core i5, memory: 8GB
WBAN-gateway	Mac laptop	CPU:2.9 GHz Intel Core i5, memory: 8GB
User	MEIZU phone	CPU: Exynos 7872 3 GB ram; Android 6.0.1
Decryption helper(paillier)	Alibaba ECS	Instance: ecs.xn4.small, CentOS 7.2 64-bit and java

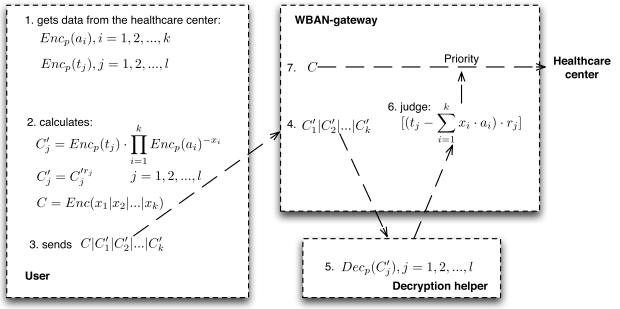

FIGURE 6. Paillier-based priority classification scheme.

B. PAILLIAR-BASED PRIVACY-PRESERVING PRIORITY CLASSIFICATION SCHEME

To clearly evaluate the performance of the proposed PPC scheme, we propose a pailliar-based privacy-preserving priority classification scheme for comparison. Shown as Fig. 6, in the pailliar-based priority classification scheme, the WBAN-gateway fulfills the priority classification task for the aggregated medical packets with the help of a decryption helper, who owns the private key $sk_{paillier}$ and the decryption algorithm $Dec(\cdot, sk_{paillier})$ of the paillier-based encryption system. The $Enc_p(\cdot)$ and $Dec_p(\cdot)$ are the encryption algorithm and the decryption algorithm of the pailliar encryption system. Specifically, in the step 2, the random number r_j is a small number, which would not make the bit length of $[(t_j - \sum_{i=1}^{k} x_i \cdot a_i) \cdot r_j]$ change too much. Moreover, in the step 6, the WBAN-gateway judges the priority of the packet according to the bit length of $[(t_j - \sum_{i=1}^{k} x_i \cdot a_i) \cdot r_j]$, which means: 1) if the bit length of $[(t_j - \sum_{i=1}^{k} x_i \cdot a_i) \cdot r_j]$ is close to the bit length of n, t_j is less than $\sum_{i=1}^{k} x_i \cdot a_i$; 2) otherwise, t_j is larger than $\sum_{i=1}^{k} x_i \cdot a_i$.

C. HEALTHCARE CENTER'S COMPUTATIONAL COST

First, in the proposed PPC scheme, the healthcare center is the trust authority who initializes the system including: setup the BGN encryption, setup ECIES encryption and setup the hashset $\{H_1, H_2, ..., H_{t_m}\}$. The system initialization is conducted only once, so we focus on the healthcare center's computational cost in the user registration algorithm.

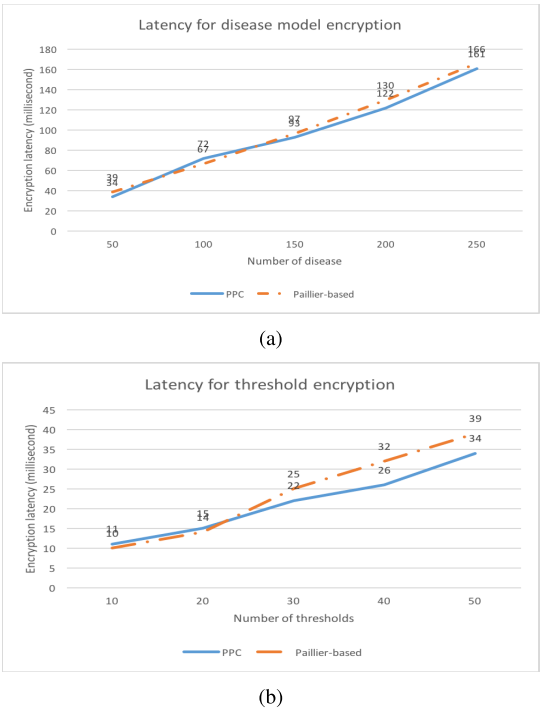

FIGURE 7. Computational cost of healthcare center for PPC. (a) Disease model encryption. (a) Threshold encryption.

In the user registration, the healthcare center fetches a disease model, related thresholds and encrypted these data. Thus, we test the time for the healthcare center to encrypt the disease model with the coefficient number of 50, 100, 150, 200, 250, and the threshold number of 10, 20, 30, 40, 50. Shown as Fig. 7a and Fig. 7b, the encryption latency increases slowly with the number of the disease model coefficients and the thresholds. For the max number of 250 disease model coefficients and 50 thresholds, the healthcare center spends 161 milliseconds and 34 milliseconds to encrypt these data. The user registration is conducted only once for a user, so the computational cost is acceptable for both the user and the healthcare center.

We also shows the latency for disease model encryption and threshold encryption for paillier-based priority classification scheme in Fig. 7. The figure shows the computational costs of healthcare center for PPC scheme and paillier-based scheme are almost same.

D. COMPUTATIONAL COST AT USER SIDE

Assume that a user gets an encrypted disease model with k coefficients and l thresholds from the healthcare center,

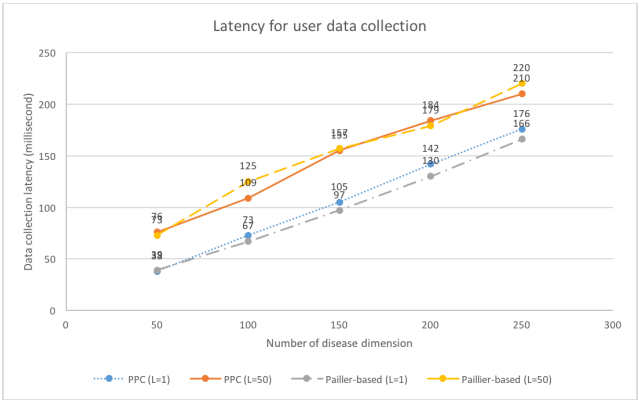

FIGURE 8. Latency for user data collection.

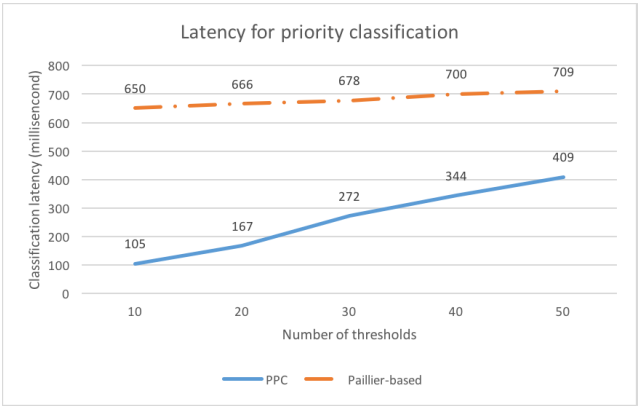

FIGURE 9. Latency for priority classification.

the user spends most of the time for the computations for $C'_j, j = 1, 2, \ldots, l$. For each $C'_j = \frac{T_j}{\prod_{i=1}^{k} A_i^{x_i}} \cdot h^{r_j}$, it is involved of $k+1$ exponentiations, $k-1$ additions, one division, one multiplication. The algorithm can be optimized to speed up by computing the time-consuming $\prod_{i=1}^{k} A_i^{x_i}$ before the calculations of $C'_j, j = 1, 2, ..., l$. As we have tested, the latency for the calculations of $C'_j, j = 1, 2, ..., 50$ increases lightly more than that for one $C'_j, j = 1$. Thus, we measure the latency of user data collection for $C'_j, j = 1, 50$, which means the data collection latency for one threshold and 50 thresholds, and the results are shown as Fig. 8. As expected, the latency increases much slower when increasing the disease dimension. Moreover, we test the latency for the paillier-based priority classification scheme. Shown as Fig. 8, the user data collection latency of the paillier-based scheme is almost same as the PPC scheme.

E. COMPUTATIONAL COST AT WBAN-GATEWAY SIDE

In the packet priority classification and relay algorithm, the WBAN-gateway conducts l mapping operations for the $D_j = e(C'_j, K_G), j = 1, 2, \ldots, l$. After calculating the priority of the packet, the WBAN-gateway inserts the packet into the relay heap, relays the packet with the highest priority from the relay heap, and updates the priorities of the packets in the relay heap. Therefore, the latency for the WBAN-gateway consists of two parts: 1) time for packet priority classification; 2) time for inserting the packet into the relay heap and updating the relay heap. The latency for the second part is $O(d)$, in which d is the height of the relay heap. We have evaluated that this algorithm is very efficient and costs not too much time. So we focus on the first part latency. Shown as Fig. 9, the priority classification latency increases slowly with the number of the thresholds offered by the packet. Even for the 50 thresholds, which is large in real scenarios, the priority classification latency is 409 milliseconds. The results demonstrate the priority classification algorithm is very efficient in computational cost.

In Fig. 9, we also demonstrate the packet priority classification latency in the paillier-based scheme, which is involved of: 1) The decryption helper decrypts the $C'_j, j = 1, 2, \ldots, l$; 2) The WBAN-gateway judges the priority according to $[t_j - \sum_{i=1}^{k} x_i \cdot a_i]$; 3) The WBAN-gateway inserts the packet into the heap and relays the packet with highest priority to the healthcare center. As we have tested, the algorithms for the part 2 and part 3 do not cost too much. Thus, we focus on the latency for the part 1, which includes the communication latency for the data transmission between the WBAN-gateway and the decryption helper. We test the communication latency for the data transmission, which is around 636 milliseconds. We demonstrate the total latency for the paillier-based scheme in Fig. 9, which shows the priority classification latency for the paillier-based scheme is much larger than the PPC scheme because of the large communication latency.

F. COMMUNICATION COST

Our PPC scheme is a non-interactive scheme, which ensures the scheme is very efficient in communication cost. We focus on 1) the communication cost between the healthcare center and user in user registration algorithm; 2) the communication cost between the authenticated user and the WBAN-gateway in user data collection algorithm.

In the user registration, the healthcare center sends the encrypted disease model $A_i, i = 1, 2, ..., k$ and the encrypted thresholds $T_j, j = 1, 2, ..., l$ to the authenticated user. As the BGN encryption is 1024 bits length in our setting, the communication cost for the healthcare center to the user is $(k + l) * 1024$ bits. This communication only occurs once for one user, so it is acceptable for a user.

In the user data collection algorithm, the user sends the encrypted $C'_j, j = 1, 2, ..., l$ and the C to the WBAN-gateway. In our setting, the relationship of the length of plain text and cipher text in the ECIES encryption is $CipherTextLen = (PlainTextLen/BLOCKSIZE + 1) * BLOCKSIZE$. We set the block size to 16. Therefore, the communication cost between authenticated user and the WBAN-gateway in user data collection algorithm is about $1024 * l + (userInfoLen + 16)$ bits, where the $userInfoLen$ is the length of the user's original physiological data. Specifically, the communication cost for the packet relay from the WBAN-gateway to the healthcare

center is $userInfoLen + 16$ bits, because only the encrypted C needs to be relayed to the healthcare center.

VII. RELATED WORKS

As the increasing security and privacy requirements of the eHealthcare system, a large number of privacy-preserving related works have been proposed in recent years. In this section, we introduce the related research works devoted to privacy-preserving methods around eHealthcare system.

There are many techniques involved in achieving the privacy-preserving eHealthcare system, such as pseudonymization, data encryption, access control, private-preserving data outsourcing. We focus on three kinds of privacy-preserving techniques used for privacy-preserving eHealthcare system: 1) pseudonymization; 2) access control; 3) data encryption. Most of the schemes proposed in recent years are hybrid solutions making use of these techniques. We have also proposed some privacy-preserving works on eHealthcare system [15], [19], [20]. Next, we review the works applying these techniques to achieve privacy-preserving eHealthcare system.

A. PSEUDONYMIZATION BASED SCHEMES FOR eHEALTHCARE SYSTEM

The pesudonymization is the earliest technique used for privacy-preserving eHealthcare system. Many protocols around the pesudonymization [21]–[25] have been studied in recent years. The key idea is to remove all the information that can identify the users. The real identity is replaced by the pseudonym before data sharing or data publishing. The attacker can not link the pseudonym to the patients. Proposals [26], [27] categorize the patients' data into two sets: user-relevant data and personal, pseudonymized data. These schemes not only deny any link between the pseudonym and the real users, but also securely store tabled entities of these identities. However, the pseudonymization solved the privacy concern in the early stage of the eHealthcare system, when the cloud computing based architecture is not pervasive. Recently, when data information are aggregated from different data sources, the pesudonymization itself is a weak protection technique for user's privacy.

B. ACCESS CONTROL BASED SCHEMES FOR eHEALTHCARE SYSTEM

The access control policies are proper techniques used for privacy-preserving. Most of time, hybrid access control policies are adopted to propose a privacy-preserving access control mechanisms [28]–[33]. It is common to use the combination of the access control and the pseudonymization in one privacy-preserving scheme, which stores the users' data in an anonymized manner, and shared the anonymized data according to the access control policies. A patient monitoring scheme [34] was proposed to give patients control over who can access their protected health information (PHI). The patients assigns various categories of access to their PHI after signing the contact with the healthcare center regarding use of their PHI. A cloud-centered privacy-aware role based access control (CPRBAC) mechanism [35] was proposed to improve the traditional RBAC. It is involved of not only the context-based access control, information sharing among different could servers, and authorization delegation from the traditional RBAC, but also four new conditions: purpose, obligations, conditions, organizations to define complex access control policies.

C. DATA ENCRYPTION BASED SCHEMES FOR eHEALTHCARE SYSTEM

Data encryptions are widely used in the privacy-preserving eHealthcare schemes. Some pseudonymization schemes encrypt the real identities of the user record as the pseudonyms. Encryption are also widely used in the access control, such as identity-based encryption in the identity-based access control (RBAC) scheme [36]. Moreover, a number of privacy-preserving eHealthcare system are proposed on encrypted patient data [37]–[44]. Most of these schemes are build upon homomorphic encryptions, which include partial homomorphic encryption (PHE) [45], [46] that allows addition of encrypted data, fully homomorphic encryption (FHE) [12], [47] that allows both addition and multiplication on encrypted data. Recently, many papers [5], [6] have studied the privacy-preserving health monitoring scheme with wearable devices and cloud service provider on encrypted medical data. Some other works [7], [8] improve patients' location privacy in mobile medical queries.

VIII. CONCLUSIONS

In this paper, we have proposed an efficient privacy-preserving priority classification (PPC) scheme on patient healthcare data in remote eHealthcare system. The proposed PPC scheme achieves the priority classification and packets relay tasks, while preserving the privacy of the users and the confidentiality of the healthcare center's disease models. Because it is a non-interactive procedure, the communication cost is low. We have also implemented an android app and two java programs to demonstrate that our PPC scheme is efficient in computational cost and communication overhead.

REFERENCES

[1] C. A. Otto, E. Jovanov, and A. Milenkovic, "A WBAN-based system for health monitoring at home," in *Proc. 3rd IEEE/EMBS Int. Summer School Med. Devices Biosensors*, Sep. 2006, pp. 20–23.

[2] O. Omeni, A. C. W. Wong, A. J. Burdett, and C. Toumazou, "Energy efficient medium access protocol for wireless medical body area sensor networks," *IEEE Trans. Biomed. Circuits Syst.*, vol. 2, no. 4, pp. 251–259, Dec. 2008.

[3] A. Argyriou, A. C. Breva, and M. Aoun, "Optimizing data forwarding from body area networks in the presence of body shadowing with dual wireless technology nodes," *IEEE Trans. Mobile Comput.*, vol. 14, no. 3, pp. 632–645, Mar. 2015.

[4] S. Rezvani and S. A. Ghorashi, "Context aware and channel-based resource allocation for wireless body area networks," *IET Wireless Sensor Syst.*, vol. 3, no. 1, pp. 16–25, Mar. 2013.

[5] N. Mcdonald, D. Atkinson, Y. Khmelevsky, and S. McMillan, "Sport wearable biometric data encrypted emulation and storage in cloud," in *Proc. IEEE Can. Conf. Elect. Comput. Eng. (CCECE)*, May 2016, pp. 1–4.

[6] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," *IEEE Wireless Commun.*, vol. 17, no. 1, pp. 51–58, Feb. 2010.
[7] Z. Chen, H. Hu, and J. Yu, "Privacy-preserving large-scale location monitoring using bluetooth low energy," in *Proc. 11th Int. Conf. Mobile Ad-Hoc Sensor Netw. (MSN)*, Dec. 2015, pp. 69–78.
[8] C.-Y. Chou, E.-J. Chang, H.-T. Li, and A.-Y. Wu, "Low-complexity privacy-preserving compressive analysis using subspace-based dictionary for ECG telemonitoring system," *IEEE Trans. Biomed. Circuits Syst.*, vol. 12, no. 4, pp. 801–811, Aug. 2018.
[9] C. Dwork and M. Naor, "On the difficulties of disclosure prevention in statistical databases or the case for differential privacy," *J. Privacy Confidentiality*, vol. 2, no. 1, 2008.
[10] M. Fredrikson, E. Lantz, S. Jha, S. Lin, D. Page, and T. Ristenpart, "Privacy in pharmacogenetics: An end-to-end case study of personalized warfarin dosing," in *Proc. USENIX Secur. Symp.*, Aug. 2014, pp. 17–32.
[11] B. Dan and M. Zhandry, "Multiparty key exchange, efficient traitor tracing, and more from indistinguishability obfuscation," in *Proc. Cryptol. Conf.*, 2014, pp. 480–499.
[12] M. van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, *Fully Homomorphic Encryption Over the Integers*. Berlin, Germany: Springer, 2010.
[13] D. Boneh, E.-J. Goh, and K. Nissim, "Evaluating 2-DNF formulas on ciphertexts," in *Proc. Theory Cryptogr. Conf.*, 2005, pp. 325–341.
[14] D. Harrison, S. Boyce, P. Loughnan, P. Dargaville, H. Storm, and L. Johnston, "Skin conductance as a measure of pain and stress in hospitalised infants," *Early Hum. Develop.*, vol. 82, no. 9, pp. 603–608, 2006.
[15] G. Wang, R. Lu, and C. Huang, "PGuide: An efficient and privacy-preserving smartphone-based pre-clinical guidance scheme," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2015, pp. 1–6.
[16] P. K. Anooj, "Clinical decision support system: Risk level prediction of heart disease using weighted fuzzy rules," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 24, no. 1, pp. 27–40, 2012.
[17] J. B. Guerard, Jr., "Regression analysis and forecasting models," in *Introduction to Financial Forecasting in Investment Analysis*. 2007, pp. 277–301.
[18] A. Ara, M. Al-Rodhaan, Y. Tian, and A. Al-Dhelaan, "A secure privacy-preserving data aggregation scheme based on bilinear ElGamal cryptosystem for remote health monitoring systems," *IEEE Access*, vol. 5, pp. 12601–12617, 2017.
[19] G. Wang, R. Lu, and C. Huang, "PSLP: Privacy-preserving single-layer perceptron learning for e-Healthcare," in *Proc. 10th Int. Conf. Inf., Commun. Signal Process. (ICICS)*, Dec. 2015, pp. 1–5.
[20] G. Wang, R. Lu, and Y. L. Guan, "Enabling efficient and privacy-preserving health query over outsourced cloud," *IEEE Access*, vol. 6, pp. 70831–70842, 2018.
[21] J. Wang, Y. Zhao, S. Jiang, and J. Le, "Providing privacy preserving in cloud computing," in *Proc. 3rd Int. Conf. Hum. Syst. Interact.*, May 2010, pp. 472–475.
[22] H. Aamot, C. D. Kohl, D. Richter, and P. Knaup-Gregori, "Pseudonymization of patient identifiers for translational research," *BMC Med. Inform. Decis. Making*, vol. 13, no. 1, p. 75, 2013.
[23] T. Neubauer and J. Heurix, "A methodology for the pseudonymization of medical data," *Int. J. Med. Inform.*, vol. 80, no. 3, pp. 190–204, 2011.
[24] T. Neubauer and A. Ekelhart, "An evaluation of technologies for the pseudonymization of medical data," in *Proc. ACM Symp. Appl. Comput. (SAC)*, 2009, pp. 857–858.
[25] J. Heurix and T. Neubauer, *Privacy-Preserving Storage and Access of Medical Data Through Pseudonymization and Encryption*. Berlin, Germany: Springer, 2011.
[26] B. Riedl, T. Neubauer, G. Goluch, O. Boehm, G. Reinauer, and A. Krumboeck, "A secure architecture for the pseudonymization of medical data," in *Proc. 2nd Int. Conf. Availability, Rel. Secur. (ARES)*, Apr. 2007, pp. 318–324.
[27] M. Hansen, P. Berlich, J. Camenisch, S. Clauß, A. Pfitzmann, and M. Waidner, "Privacy-enhancing identity management," *Inf. Secur. Tech. Rep.*, vol. 9, no. 1, pp. 35–44, Jan./Mar. 2004.
[28] D. Choi, D. Kim, and S. Park, "A framework for context sensitive risk-based access control in medical information systems," *Comput. Math. Methods Med.*, vol. 2015, p. 265132, 2015.
[29] S. Z. R. Rizvi, P. W. L. Fong, J. Crampton, and J. Sellwood, "Relationship-based access control for an open-source medical records system," in *Proc. 20th ACM Symp. Access Control Models Technol.*, Jun. 2015, pp. 113–124.
[30] E. Kamateri, E. Kalampokis, E. Tambouris, and K. Tarabanis, "The linked medical data access control framework," *J. Biomed. Inform.*, vol. 50, pp. 213–225, Aug. 2014.
[31] L. Seitz, J.-M. Pierson, and L. Brunie, "Semantic access control for medical applications in grid environments," in *Parallel Processing* (Lecture Notes in Computer Science), vol. 2790. 2017, pp. 374–383.
[32] P. Vimalachandran, H. Wang, and Y. Zhang, "Securing electronic medical record and electronic health record systems through an improved access control," in *Health Information Science* (Lecture Notes in Computer Science), vol. 9085. 2015, pp. 17–30.
[33] H. A. Maw, H. Xiao, B. Christianson, and J. A. Malcolm, "An evaluation of break-the-glass access control model for medical data in wireless sensor networks," in *Proc. IEEE 16th Int. Conf. E-Health Netw., Appl. Services (Healthcom)*, Oct. 2014, pp. 130–135.
[34] J. Sun, Y. Fang, and X. Zhu, *Privacy and Emergency Response in E-Healthcare Leveraging Wireless Body Sensor Networks*. Piscataway, NJ, USA: IEEE Press, 2010.
[35] L. Chen and D. B. Hoang, "Novel data protection model in healthcare cloud," in *Proc. IEEE Int. Conf. High Perform. Comput. Commun.*, Sep. 2011, pp. 550–555.
[36] H. A. J. Narayanan and M. H. Göneş, "Ensuring access control in cloud provisioned healthcare systems," in *Proc. IEEE Consum. Commun. Netw. Conf.*, Jan. 2011, pp. 247–251.
[37] M. Kim and K. Lauter, "Private genome analysis through homomorphic encryption," *BMC Med. Inform. Decis. Making*, vol. 15, p. S3, Dec. 2015.
[38] J. Shi, J. Lai, Y. Li, R. H. Deng, and J. Weng, "Authorized keyword search on encrypted data," in *Proc. Eur. Symp. Res. Comput. Secur.*, 2014, pp. 419–435.
[39] J. W. Bos, K. Lauter, and M. Naehrig, "Private predictive analysis on encrypted medical data," *J. Biomed. Inform.*, vol. 50, pp. 234–243, Aug. 2014.
[40] Y. Liu, X. Qu, and G. Xin, "A ROI-based reversible data hiding scheme in encrypted medical images," *J. Vis. Commun. Image Represent.*, vol. 39, pp. 51–57, Aug. 2016.
[41] S. Wang, J. Li, C. Zhang, J. Liang, and Z. Wang, "A robust algorithm of encrypted medical volume data retrieval based on 3D DWT and 3D DFT," in *Proc. IEEE 15th Int. Conf. Softw. Eng. Res., Manage. Appl.*, Jun. 2017, pp. 143–149.
[42] M. Huang, W. Xie, and P. Zhang, "Efficient fuzzy keyword search over encrypted medical and health data in hybrid cloud," *J. Med. Imag. Health Inform.*, vol. 7, no. 4, pp. 867–874, 2017.
[43] N. Kittawi and A. Al-Haj, "Reversible data hiding in encrypted images," in *Proc. 8th Int. Conf. Inf. Technol.*, May 2017, pp. 808–813.
[44] Y. Elmehdwi, B. K. Samanthula, and W. Jiang, "Secure k-nearest neighbor query over encrypted data in outsourced environments," in *Proc. IEEE 30th Int. Conf. Data Eng.*, Mar./Apr. 2014, pp. 664–675.
[45] J. Groth, "A verifiable secret shuffe of homomorphic encryptions," in *Proc. Int. Workshop Public Key Cryptogr.*, 2003, pp. 145–160.
[46] D. Boneh and D. M. Freeman, "Homomorphic signatures for polynomial functions," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, 2011, pp. 149–168.
[47] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proc. Annu. ACM Symp. Theory Comput.*, 2009, vol. 9, no. 4, pp. 169–178.

Authors' photographs and biographies not available at the time of publication.