Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2015, Article ID 392439, 12 pages
http://dx.doi.org/10.1155/2015/392439

Research Article

SCRHM: A Secure Continuous Remote Health Monitoring System

Qiuxiang Dong,[1,2,3] Zhi Guan,[1,2,3,4] Kunlun Gao,[5] and Zhong Chen[1,2,3]

[1]*Institute of Software, School of EECS, Peking University, Beijing 100871, China*
[2]*MoE Key Lab of High Confidence Software Technologies, PKU, Beijing 100871, China*
[3]*MoE Key Lab of Network and Software Security Assurance, PKU, Beijing 100871, China*
[4]*National Engineering Research Center of Software Engineering, PKU, Beijing 100871, China*
[5]*State Grid Smart Grid Research Institute, Beijing 102211, China*

Correspondence should be addressed to Zhi Guan; guan@pku.edu.cn

Received 8 July 2015; Revised 22 October 2015; Accepted 8 November 2015

Academic Editor: Andrei Gurtov

With the growing need for the remote caring at home and the everincreasing popularity of mobile devices, more and more applications are being developed to enable remote health monitoring. Combining cloud computing with mobile technologies has enabled the healthcare service provider to offer continuous health data collection and physicians to conveniently monitor and assess users' health while they are at home. However, users' health data contain highly confidential information, and servers in the cloud are out of users' trusted domain. Therefore, users may be reluctant to take advantage of remote health monitoring systems before they make sure their data are properly protected. In this paper, we propose a secure continuous remote health monitoring system named SCRHM with the main component, a searchable encryption scheme supporting range searches for remote health monitoring system. With this scheme, remote health monitoring service provider is able to detect outliers over encrypted health parameters. Using analysis, we prove the correctness and security of the proposed scheme on privacy protection of users' health data. Via simulation experiments, we validate the performance of the proposed scheme in terms of computation and communication overhead.

1. Introduction

Background. With the rising of life expectancy and declining birth rates, the proportion of the population above a certain age increases. This phenomenon, known as population aging, is occurring all over the world. The population report [1] indicates that the overall median age in the world rose from 23.5 in 1950 to 28.5 in 2010 and is projected to increase from 29 to 36 years between 2013 and 2050 and to 41 years in 2100. The global share of older people (aged 60 years or over) increased from 9.2% in 1990 to 11.7% in 2013 and will continue to grow as a proportion of the world population, reaching 21.1% by 2050. Globally, 40% of older persons aged 60 years or over live independently, that is, alone or with their spouse only, and this number is projected to increase in the future. These "empty-nest" seniors are vulnerable to helplessness at home when they suffer sudden health problems.

The health issues related to the aging population are complex and many health risks may lead serious sequelae and even death. One of the most serious health risks is injuries, particularly those caused by falls, which may lead to postfall syndrome, such as increased dependence, loss of autonomy, confusion, immobilization, and depression. According to [2], within the year following a hip fracture from a fall, 20% of the seniors will die. Nevertheless, if an inventive detection apparatus and compatible reporting system was used, almost 80% of the falls could be quickly determined and medical services would be provided quickly to the injured seniors. The sooner they get medical services, the better they would recover and thus the less likely they would suffer disabilities or death.

Chronic medical conditions, such as cardiovascular disease and Parkinson's disease, are another health killer to seniors. They are responsible for 60% of all deaths worldwide with almost half of chronic disease deaths occurring in people under the age of 70. According to [2], 133 million people live with chronic medical conditions. That number is projected to increase by more than 1% per year by 2030 and reaches 171 million then. It is impossible to completely cure or eliminate chronic diseases and lengthy, expensive treatments involving complex, ongoing care are often required. The global epidemic of chronic disease is an underappreciated cause of poverty and hinders the economic development of many countries (source: World Health Organization (as defined in Wikipedia, the World Health Organization (WHO) is a specialized agency of the United Nations (UN) that is concerned with international public health)). If some vital signs of chronic disease sufferers can be continuously monitored and abnormal medical conditions can be alerted once they occur so that the patients can obtain timely treatment, then some serious sequelae can be avoided. For example, according to American Heart Association [3], $16 billion can be saved per year and 42% rehospitalization could be prevented if adequate patient monitoring, instruction, and education outside hospital could be provided.

A 2012 eHealth patient survey by the public relations agency Ruder Finn found that 40% of elder patients want access to technology that can alert physicians and other caregivers if they are having a health emergency [4]. This trend demands an increased focus on preparing a continuous Remote Health Monitoring (RHM for short) system capable of caring for seniors and improving their health and independence for their late life. The recent advances in wireless sensor networks and cloud computing have made it possible to provide remote health monitoring to patients. Patients' vital signs are collected by the sensors and then forwarded to the RHM service provider. These parameters are checked by the RHM service provider to find odd conditions, deliver medication reminders, and trigger alerts. They may also be stored by the service provider for future long-term analysis or for the physicians to examine them. A fully operable prototype of PERFORM [5], which constantly measures the patient's symptoms and alerts physicians in case of any outlier based on a system of "wearable" sensors, has been tested in three European hospitals [6]. This tool is really helpful to improve the monitoring of patients with Parkinson disease and allows the physician to be constantly informed about the patient's clinical state and readjust appropriately the treatment plan. An evidence of the long-term impacts of RHM systems is that IT giant Apple and IT giant Google have participated in the battle. Not only do we have Android Wear up against the Apple Watch in the hardware and sensor stakes, but also there is now the small matter of the underlying platforms powering them: Google Fit versus Apple HealthKit [7].

Although RHM services minimize the need for physicians and caregivers and help the chronically ill and the elderly to survive an independent life, users may worry about how the providers make use of the collected data and protection that user data enjoy. In [8], four popular health monitoring services, Fitbit, JawBone, Nike+, and BASIS, were investigated. These service providers offer their service free for buyers of their hardware monitors and require users to register an online account in order to use the wearable devices. All data collected by the devices are uploaded to the provider's online service. When logging into the account, the users can obtain analysis of the data via a website or smartphone application. All of the four health monitoring services leave user data privacy to serious privacy threats. Health data of users using Fitbit and BASIS may be sold to advertisers or other companies. In which way and by whom the health data are used are out of users' control. This threatens users privacy very much, since the health data are highly sensitive, especially when they are combined with information from other sources. Even if the service providers claim not to sell users' data or collect information from other sources, the malicious inside staff or outside attackers may have the root right to the system and thus to the health data.

A trivial approach to protecting users data privacy is encryption-before-outsourcing; that is, the users encrypt their health data before uploading them onto the untrusted servers. Encryption reduces security and privacy risks by hiding all information about the plaintext data, but it brings a new problem at the same time; it removes search capabilities from the service providers, resulting in loss of functionality of finding odd conditions. Nevertheless, if the RHM services do not support real-time monitoring and emergency alert, their functional value will be greatly reduced. The elder patients who suffer sudden medical conditions cannot get help at the first moment and RHM seems to turn into simply a data recorder. To address this problem, in this paper, we propose a secure continuous RHM system (SCRHM), which is capable of finding odd health parameters over encrypted user health data uploaded continuously from users' gateway. After investigating a sample table from [9], we find that almost all the parameters are numerical values and the remaining such as "normal" or "bad" could be encoded into numerical values as well. Therefore, without loss of generality, we assume that all the health parameters are numerical, and the normal values are within given range(s). We design a searchable encryption scheme supporting numerical range searches for remote health monitoring system, in particular, encrypted health data vectors consisting of several numerical fields.

Related Works. In what follows, we introduce some related works. Firstly, we introduce secure healthcare services where encryption is utilized to protect health data privacy. Then we introduce searchable encryption used as the tool to enable secure continuous remote health monitoring.

Secure Healthcare Services. Combining healthcare with cloud computing draws more and more attentions because of the following three factors: firstly, the growing interest in transforming from paper-based health records to electronic health records (EHRs) [10]; secondly, large storage capacities and heavy burden on storing and managing EHRs [11] (the currently emerging pervasive computing technologies in healthcare [12, 13] will greatly intensify this trend); thirdly, the increasing importance of interorganizational sharing and collaborative use of health data [14]. Narayan et al. [15] propose

the use of ciphertext-policy attribute-based encryption (CP-ABE) [16] to ensure that the cloud provider cannot see or copy EHR data. Löhr et al. [17] present a security architecture for establishing privacy domains in e-health infrastructures. Li et al. [18] propose utilizing multiauthority attribute-based encryption to encrypt EHRs so that only authorized users are able to decrypt the ciphertexts. One of the most similar researches as ours is by Li et al. [19]. They establish a scalable framework for authorized private keyword search over encrypted personal health records and propose two novel solutions. Different from ours, their solutions only support keywords searches but not range searches. Thus it is not applicable in continuous remote health monitoring with numerical health parameters. The other similar work is [20]. The authors propose encrypting patients' health parameters homomorphically and outsourcing to healthcare service provider to compute statistical functions over these data and determine patients' health risks. Their scheme is capable of finding odd conditions by calculating risk values. It is a two-round protocol since the service provider cannot obtain the result but have to send it back to the patients for decryption. However, homomorphic encryption scheme is not suitable for mobile devices with power and storage constrains in most applications [21]. In continuous remote health monitoring, many encryption and decryption operations are needed, thus leading to heavy computation and communication overhead. Another deficiency of this work is that patients are not allowed to pinpoint which health parameters need monitoring but have to wear all the devices and get all necessary values, or else the collected parameters would be invalid inputs to the evaluation function.

Searchable Encryption. Searchable encryption is developed to enable searches over encrypted cloud data [22–24]. There exist several researches on searchable encryption supporting range searches over encrypted data. Boneh and Waters [25] design a predicate encryption, called Hidden Vector Encryption, which can be utilized to construct searchable encryption scheme supporting multidimensional range queries over encrypted data. Shi et al. [26] also propose an encryption scheme to handle multidimensional range queries. Both schemes are in the public-key setting, that is, multiple senders and a single search entity, and are computationally costly for real-world applications. Considering deficiencies of these two schemes, following works mainly focus on efficiency improvement. Lu [27] designs a single dimensional range search scheme (named LSED) on encrypted data in the symmetric-key setting. The author also mentions a direct extension, named LSED+, in the multidimensional setting. However the proposed scheme supporting multidimensional range searches has privacy leakage in single dimension. The recent work [28] proposed by Wang et al. also has the same privacy leakage in single dimension as LSED+. Although the scheme proposed by Wang et al. [29] is secure and more efficient, it is still too computationally costly and only supports small number of dimensions; for example, the maximal dimension size set in the simulation experiments is 6, whereas the health parameters which need monitoring may be few hundreds or more. The time costs of this scheme will be too high to use in practice. In this paper, we construct a searchable encryption scheme for remote health monitoring system.

Our Contributions. Our contributions are threefold:

(i) To enable secure monitoring of users' health conditions, we propose a secure continuous remote health monitoring system, SCRHM. With SCRHM, users encrypt their monitored health parameters and upload the encrypted data to the remote health monitoring service provider without worrying about private information leakage.

(ii) We design a searchable encryption scheme for the RHM system, so that the RHM service provider can perform numerical range searches over the encrypted data without knowing users' private health data.

(iii) Using analysis, we prove the correctness and security of the proposed searchable encryption scheme and validate the performance of this scheme via simulation experiments.

Paper Organization. The rest of the paper is organized as follows. Section 2 describes the problem and the main component of SCRHM system, that is, a searchable encryption scheme supporting range searches for remote health monitoring system. Section 3 provides correctness and security analysis and evaluates the performance of the proposed scheme. Finally, Section 4 concludes the paper.

2. Problem Statement and Solution

2.1. Problem Statement. In this section, we introduce the system model, system workflow, and adversarial model as well as our design goals. In the part of *System Model* and *System Workflow*, we describe how sensitive health data are collected and processed in SCRHM. The remote health monitoring service provider and malicious users may collude to pry into the uploaded sensitive data. Their malicious activities and interested sensitive information are presented in the part of *Adversarial Model*. To prevent data leakage, as discussed in Section 1, sensitive health data should be encrypted before outsourcing. Traditional encryption schemes such as 3DES (Triple Data Encryption Standard) (http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf) or AES (Advanced Encryption Standard) (http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf) and existing searchable encryption schemes ([22–24], to name a few) are not suitable for secure continuous remote health monitoring. To address this problem, we propose a new searchable encryption scheme supporting range searches in the remote health monitoring system. By incorporating this searchable encryption scheme into the system, SCRHM should achieve the design goals described in *Design Goals*. In particular, to protect sensitive health data, SCRHM should prevent service provider and malicious users from getting known of the solutions to the questions shown in *Adversarial Model*.

System Model. The system architecture of SCRHM is depicted as in Figure 1. Note that the authors of [9] propose a novel

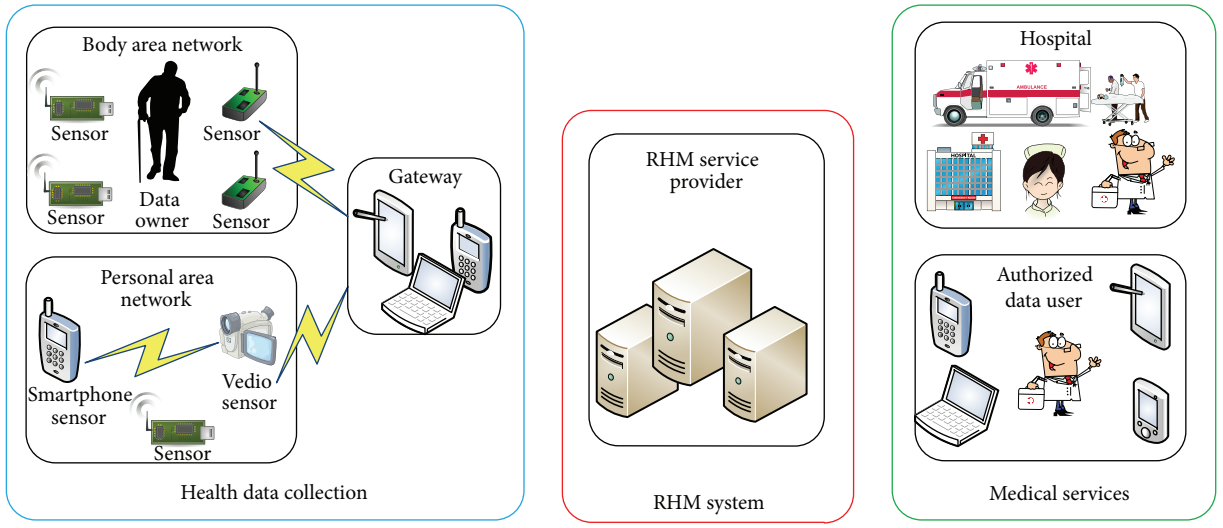

Figure 1: Architecture of the secure continuous RHM system.

remote health monitoring system with a similar three-tier architecture as ours; however they do not take secure data processing into consideration. In what follows, we show the functionality of each component in our system.

(i) *Health Data Collection.* The body area network subsystem consists of body sensors, which are placed in, on, or around a user's body for continuous monitoring of the user's physiological conditions such as heart rate, SpO2, and body temperature. The personal area network subsystem is optional and is composed of ambient sensors. These sensors are deployed in the surrounding of a user, so that the environmental conditions of the user's body such as air temperature, humidity, and brightness can be monitored. Multihop wireless links interconnect the body sensors and the ambient sensors. The gateway, which can be a mobile phone or personal digital assistant, collects the sensory data transmitted from the sensors. In our system, the gateway not only is responsible for collecting sensory data but also generates trapdoors and encrypts the collected health data. All these sensors and the gateway, connected by the multihop wireless links, constitute the health data collection module of the SCRHM system.

(ii) *Communication and Networking.* The advanced wireless communication technologies, for example, 3G/4G/GSM/GPRS/WiFi, link the gateway to the Internet. In this way, various types of sensory data collected by the health data collection module can be sent to the remote health monitoring service provider.

(iii) *Remote Health Monitoring Service Provider (RHMSP).* The RHM service provider is responsible for recording and analyzing user health data, which are in the encrypted form in our system. Once health deterioration of a user is detected by the RHM server, it may alert the caregiver or the physician. If a user is identified to be in an emergency, the RHM service provider may trigger an immediate procedure (e.g., informing the emergency contact and/or hospital, or dispatching ambulance directly) to save the user's life.

(iv) *Medical Service Provider.* The medical service provider is responsible for providing timely medical assistance when a user is in a health emergency and also performs routine checks of users' physical conditions to recommend long-time medical treatment.

System Workflow. In what follows, we describe the workflow of the SCRHM system as depicted in Figure 2.

(1) In the system setup phase, each user generates user specific secret key and sends the key to authorized medical service providers. Besides uploading searchable health data ciphertexts, in step (2) the users also upload ciphertexts encrypted under a symmetric encryption scheme. To enable medical service providers to look inside the health data records, users also send the symmetric key to the authorized medical service providers.

(2) Each user creates trapdoor, encrypts the health parameters, and then uploads the trapdoor, encrypted indexes, and encrypted records to RHM service provider. Trapdoor generation is implemented only once when the user registers the RHM service. The indexes are encrypted with our searchable encryption scheme and the records are encrypted with symmetric key encryption scheme, for example, AES or 3DES.

(3) RHMSP stores the uploaded health data records and analyzes whether they are abnormal by implementing the *Search* algorithm of our searchable encryption scheme over the encrypted data. According to the search results, RHMSP notifies the medical service

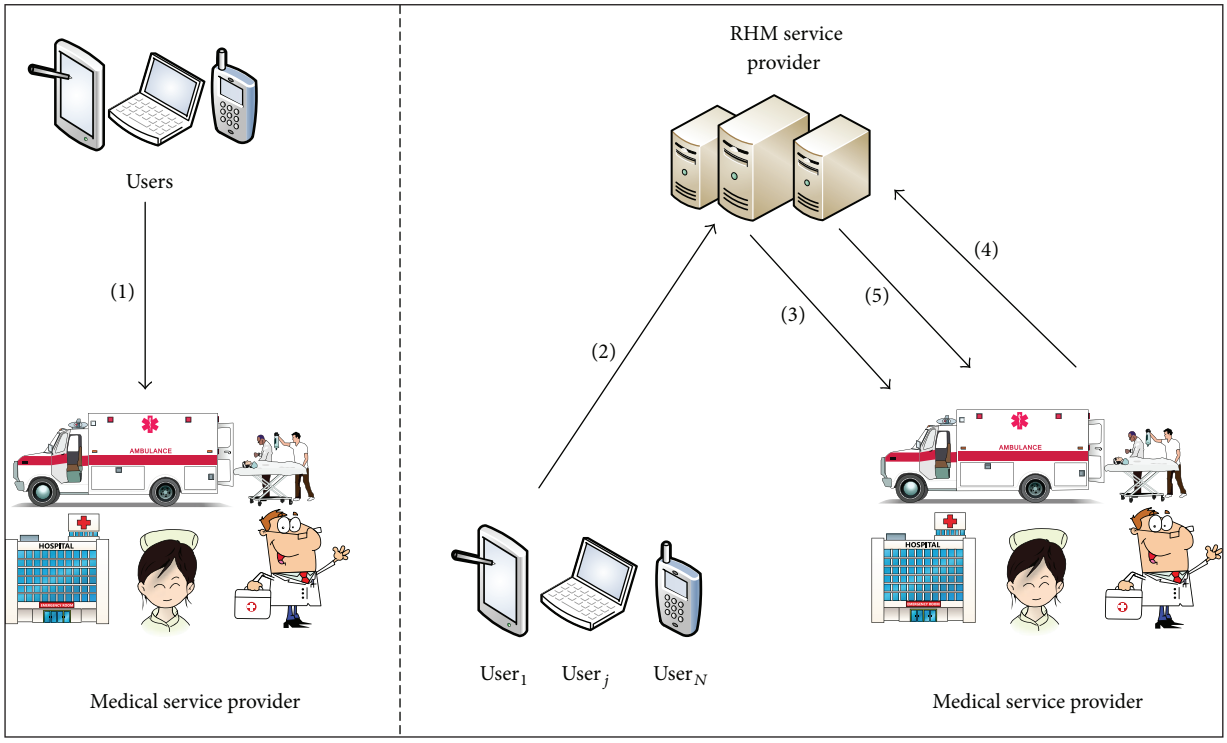

Figure 2: Workflow of the secure continuous RHM system.

providers, including calling ambulance, notifying caregivers, and physicians.

(4) The medical service providers may also want to search interested health records. They generate the corresponding trapdoors and send them to the RHM service provider.

(5) RHMSP runs the *Search2* algorithm of our searchable encryption scheme. The encrypted records satisfying search requirements corresponding to the trapdoors are sent to the medical service providers, who decrypt the ciphertexts with the secret key obtained from the users.

Note that, in this paper, we focus on how to enable the remote health monitoring system to search outliers or data records designated by the medical service provider over encrypted user health data. Access control of the health data records, which is a perpendicular problem of ours in this paper, could be implemented by applying other mechanisms, such as attribute based encryption. We refer interested readers to [15, 16, 18, 30–32] for further information.

Adversarial Model. In our system, authorized medical service providers are fully trusted. The RHM service provider is considered as semihonest; that is, it will honestly follow the designated protocol but curiously infer additional private information based on the data available to it. Specifically, the RHM service provider may be interested in the following questions. *What is the value of the monitored parameter? Which health parameter of a user is abnormal? And is it below the lower bound or above the upper bound? Do user1 and user2 suffer from the same abnormal health parameters?* The above-mentioned information about a user can be sold by the RHM service provider to advertisement companies for profits or other commercial purposes. Some of the RHM service users may be malicious and they may collude with RHMSP to get private information about other users. Therefore our system aims to protect honest users from being attacked by the RHM service provider and malicious users.

Design Goals. Our system should satisfy the following requirements:

(i) *Functionality.* Firstly, RHMSP should be capable of searching over the encrypted health data so that any outliers can be detected at the first moment. Secondly, authorized medical service providers could generate trapdoors to search health data satisfying designated requirements.

(ii) *Security.* To protect private information about honest users' health conditions, our system should prevent RHMSP from getting the solutions to the questions mentioned in the adversarial model. In particular, the following security requirements should be met. (1) Confidentiality: the RHM service provider can access the encrypted indexes and the trapdoors. Therefore, we should guarantee that RHMSP will not learn private information from them. Firstly, the encrypted indexes should not leak any information

about the users' health parameters. This aims to protect confidentiality of users' monitored parameters. Secondly, the trapdoor generation algorithm should guarantee that any information about the health parameter encrypted in the trapdoor will not be leaked. If this information is known by the RHM service provider, it can get private information about the encrypted parameters through running the search algorithm. (2) Single parameter privacy: the service provider should be prevented from getting known of the mapping between the trapdoors (uploaded by the users) and the parameters and whether the abnormal parameters are higher or lower than the normal values. (3) Trapdoor uniqueness: trapdoors generated with one user's secret key should not be used to search the other users' encrypted indexes. This security requirement prevents the RHMSP from getting known whether two users suffer from the same abnormal health parameters or guessing the exact parameter values through a divide-and-conquer or brute-force approach with the help of malicious users.

(iii) *Efficiency.* SCRHM is required to achieve both computation and communication efficiency. Specifically, trapdoor generation, data encryption, and search over the encrypted data should be efficient and the size of the trapdoors and the encrypted indexes should be suitable for applications in practice.

2.2. Preliminaries. The encryption scheme we adopt to construct searchable index and trapdoor is extended from the *Asymmetric Scalar-Product Preserving Encryption* (ASPE) scheme, which is proposed in [33] for efficient secure nearest neighbor search on the cloud. It is also utilized by the authors of [34] to enable searches over encrypted data.

Suppose that P_1 and P_2 are two data points and Q is a query point in an Euclidean space. If P_1, P_2, and Q are encrypted by ASPE, then a third party will not learn the values of the points and the query. But it can still determine whether P_1 is closer to Q than P_2. The secret key consists of a $(d+1)$-bit binary vector as S and two $(d+1)\times(d+1)$ invertible matrices as $\{M_1, M_2\}$, where d is the number of dimensions for each data point P. First, every data vector P and query vector Q are extended to a $(d+1)$-dimension vector as $\overline{P}$ and $\widehat{Q}$, where the $(d+1)$-dimension is set to $-0.5\|P\|^2$ and 1, respectively. Besides, the query vector $\widehat{Q}$ is scaled by a random number $r > 0$ as (rQ, r). Then $\overline{P}$ is split into two random vectors as $\{P_a, P_b\}$, and $\widehat{Q}$ is also split into two random vectors as $\{Q_a, Q_b\}$ with S as a splitting indicator. That is, if the jth bit of S is 0, then $P_a[j]$ and $P_b[j]$ are the same as $\overline{P}[j]$, while Q_a and Q_b are set to two random numbers so that their sum is equal to $\widehat{Q}[j]$; if the jth bit of S is 1, the splitting process is similar except that $\overline{P}$ and $\widehat{Q}$ are switched. The split data vector pair $\{P_a, P_b\}$ is encrypted as $[(M_1^T P_a)^T, (M_2^T P_b)^T]^T$, and the split query vector pair $\{Q_a, Q_b\}$ is encrypted as $[(M_1^{-1} Q_a)^T, (M_2^{-1} Q_b)^T]^T$.

In the query step, the product of $[P_a^T, P_b^T]^T$ and $[Q_a^T, Q_b^T]^T$, that is, $-0.5r(\|P\|^2 - 2P \cdot Q)$, is serving as the indicator of Euclidean distance between P and Q. Wong et al. [33] show that the security of ASPE is roughly equal to a symmetric encryption scheme with d-bit key. In the following we briefly discuss the correctness of the protocol. The full proof of correctness and security of the ASPE scheme can be found in [33]:

Fact 1

$$\overline{P} \odot \widehat{Q} = P_a \odot Q_a + P_b \odot Q_b. \tag{1}$$

Fact 2

$$\left(\overline{P}_1 - \overline{P}_2\right) \odot \widehat{Q} = 0.5r\left(d^2\left(P_2, Q\right) - d^2\left(P_1, Q\right)\right), \tag{2}$$

where $\odot$ denotes inner product of two vectors and function d measures the Euclidean distance between two points. Based on the two facts above, we have

$$\begin{aligned}
&\left(\left[\left(M_1^T P_{1a}\right)^T, \left(M_2^T P_{1b}\right)^T\right]^T\right. \\
&\quad \left. - \left[\left(M_1^T P_{2a}\right)^T, \left(M_2^T P_{2b}\right)^T\right]^T\right) \\
&\quad \odot \left[\left(M_1^{-1} Q_a\right)^T, \left(M_2^{-1} Q_b\right)^T\right]^T \\
&= \left(\left[\left(M_1^T P_{1a}\right)^T, \left(M_2^T P_{1b}\right)^T\right]^T\right. \\
&\quad \left. - \left[\left(M_1^T P_{2a}\right)^T, \left(M_2^T P_{2b}\right)^T\right]^T\right)^T \\
&\quad \cdot \left[\left(M_1^{-1} Q_a\right)^T, \left(M_2^{-1} Q_b\right)^T\right]^T = \left(\left[P_{1a}^T, P_{1b}^T\right]^T\right. \\
&\quad \left. - \left[P_{2a}^T, P_{2b}^T\right]^T\right) \odot \left[Q_a^T, Q_b^T\right]^T = \left(\overline{P}_1 - \overline{P}_2\right) \odot \widehat{Q} \\
&\quad = 0.5r\left(d^2\left(P_2, Q\right) - d^2\left(P_1, Q\right)\right).
\end{aligned} \tag{3}$$

Therefore, $0.5r(d^2(P_2, Q) - d^2(P_1, Q)) > 0 \Leftrightarrow d^2(P_2, Q) > d^2(P_1, Q)$. Without learning the values of the points and the query, we can determine whether P_1 is closer to Q than P_2.

The notations we use in the remaining of this paper are listed as follows:

(i) κ—it is an integer and denotes the security parameter.

(ii) $v[i]$—it denotes the ith element of a vector v.

(iii) $v_1 + v_2$—v_1 and v_2 are vectors; the jth element of $v_1 + v_2$ is $v_1[j] + v_2[j]$.

(iv) $\mathcal{U}$—it denotes the service user collection; a set of N users $\mathcal{U} = \{U_1, U_2, \ldots, U_N\}$.

(v) $\mathcal{L}$, $\mathcal{H}$—the lower bound set is denoted as $\mathcal{L} = \{L_1, L_2, \ldots, L_m\}$ and the upper bound set is denoted as $\mathcal{H} = \{H_1, H_2, \ldots, H_m\}$.

(vi) $\mathcal{I}$—the encrypted index set is stored on the RHM server. Element $I_j \in \mathcal{I}$ is the encrypted index corresponding to user U_j's health data.

(vii) M^T and M^{-1}—M^T is the transpose matrix of matrix M and M^{-1} is the inverse matrix of matrix M.

2.3. The Proposed Searchable Encryption Scheme. By extending the kNN computation scheme, we propose a searchable encryption scheme for continuous health monitoring system consisting of the following algorithms.

(i) Setup(κ, m). If the health data dimension m is smaller than κ, extra dummy fields can be added; therefore, in what follows, without loss of generality, we assume $m \geq \kappa$.

The gateway of user U_j generates a secret key

$$\mathrm{SK} = \left(S_j, M_j, M_j'\right), \tag{4}$$

where S_j is an $m+1$-dimensional binary vector and M_j, M_j' are both $(m+1) \times (m+1)$ invertible matrices. SK is sent to the authorized medical service providers trusted by user U_j.

(ii) GenIndex(S_j, M_j, M_j', P_j). After collecting sensory data, the gateway creates an m-dimensional health data vector P_j. Then the health data vector P_j is encrypted by the gateway with the ASPE scheme in the following way.

Extend P_j to $\overline{P_j} = r(P_j{}^T, 1)^T$, where r is a positive random number. Generate (P_{ja}, P_{jb}) such that

(i) if $S_j[i] = 1$, set $P_{ja}[i] = P_{jb}[i] = \overline{P_j}[i]$;

(ii) if $S_j[i] = 0$, set $P_{ja}[i] = \sigma_i$ and $P_{jb}[i] = \overline{P_j}[i] - \sigma_i$, where σ_i is a random number.

The encrypted index for P_j is $I_j = [(M_j{}^{-1}P_{ja})^T, (M_j'^{-1}P_{jb})^T]^T$.

(iii) GenTrapdoor$(S_j, M_j, M_j', \mathscr{L}, \mathscr{H})$. When registering the RMH service, the user generates trapdoors for the RHM server so that the server can search over the encrypted health data in the future. The gateway creates two m-dimensional vectors for each value in $\mathscr{L}$ and $\mathscr{H}$. In particular, for $\alpha = L_\lambda \in \mathscr{L}$, the vectors are constructed according to (5), and for $\alpha = H_\lambda \in \mathscr{H}$, the vectors are created according to (6). One has

$$\begin{aligned} Q_{j\lambda 1} &= (\gamma_1, \gamma_2, \ldots, \gamma_{\lambda-1}, \alpha - s, \gamma_{\lambda+1}, \ldots, \gamma_m), \\ Q_{j\lambda 2} &= (\gamma_1, \gamma_2, \ldots, \gamma_{\lambda-1}, \alpha + s, \gamma_{\lambda+1}, \ldots, \gamma_m), \end{aligned} \tag{5}$$

$$\begin{aligned} Q_{j\lambda 1} &= (\gamma_1, \gamma_2, \ldots, \gamma_{\lambda-1}, \alpha + s, \gamma_{\lambda+1}, \ldots, \gamma_m), \\ Q_{j\lambda 2} &= (\gamma_1, \gamma_2, \ldots, \gamma_{\lambda-1}, \alpha - s, \gamma_{\lambda+1}, \ldots, \gamma_m), \end{aligned} \tag{6}$$

where s and γ_i $(i = 1, 2, \ldots, \lambda-1, \lambda+1, \ldots, m)$ are randomly chosen private positive numbers. Then $Q_{j\lambda 1}$ and $Q_{j\lambda 2}$ are encrypted by an encryption function E, which proceeds as follows.

Let Q be an m-dimensional vector. Extend Q to $\widehat{Q} = (Q^T, -0.5\|Q\|^2)^T$. Create (Q_a, Q_b) such that

(i) if $S_j[i] = 0$, set $Q_a[i] = Q_b[i] = \widehat{Q}[i]$;

(ii) if $S_j[i] = 1$, set $Q_a[i] = \rho_i$, and $Q_b[i] = \widehat{Q}[i] - \rho_i$, where ρ_i is a random number.

The encryption of Q is $E(Q) = [(M_j^T Q_a)^T, (M_j'^T Q_b)^T]^T$. The trapdoor for the λth parameter is

$$TQ_{j\lambda}^{\mathscr{L}} = \left(TQ_{j\lambda}[1] = E\left(Q_{j\lambda 1}\right), TQ_{j\lambda}[2] = E\left(Q_{j\lambda 2}\right)\right), \tag{7}$$

where $Q_{j\lambda 1}$ and $Q_{j\lambda 2}$ are set as in (5);

$$TQ_{j\lambda}^{\mathscr{H}} = \left(TQ_{j\lambda}[1] = E\left(Q_{j\lambda 1}\right), TQ_{j\lambda}[2] = E\left(Q_{j\lambda 2}\right)\right), \tag{8}$$

where $Q_{j\lambda 1}$ and $Q_{j\lambda 2}$ are set as in (6).

The gateway randomly permutes the $2m$ trapdoors and sends the trapdoors to the RHM service provider

$$\begin{aligned} TQ_j &= \left\{TQ_{j1}, TQ_{j2}, \ldots, TQ_{jm}, TQ_{j(m+1)}, \ldots, TQ_{j(2m)}\right\} \\ &= \left\{TQ_{j\lambda}^{\mathscr{L}}, TQ_{j\lambda}^{\mathscr{H}} \mid \lambda = 1, 2, \ldots, m\right\}. \end{aligned} \tag{9}$$

(iv) GenTrapdoor2$(S, \mathscr{M}, \mathscr{M}', \alpha, op)$. The medical service provider may want to search interested health data, for example, health data records with the λth parameter greater or smaller than α. First generate the following two vectors:

(i) when op is "$\leq$", that is, search records with the λth parameter greater than α,

$$\begin{aligned} Q_1 &= (\gamma_1, \gamma_2, \ldots, \gamma_{\lambda-1}, \alpha - s, \gamma_{\lambda+1}, \ldots, \gamma_m), \\ Q_2 &= (\gamma_1, \gamma_2, \ldots, \gamma_{\lambda-1}, \alpha + s, \gamma_{\lambda+1}, \ldots, \gamma_m), \end{aligned} \tag{10}$$

(ii) when op is "$\geq$", that is, search records with the λth parameter smaller than α,

$$\begin{aligned} Q_1 &= (\gamma_1, \gamma_2, \ldots, \gamma_{\lambda-1}, \alpha + s, \gamma_{\lambda+1}, \ldots, \gamma_m), \\ Q_2 &= (\gamma_1, \gamma_2, \ldots, \gamma_{\lambda-1}, \alpha - s, \gamma_{\lambda+1}, \ldots, \gamma_m), \end{aligned} \tag{11}$$

where s and γ_i $(i = 1, 2, \ldots, \lambda-1, \lambda+1, \ldots, m)$ are randomly chosen private positive numbers. Set token TQ as $TQ = (TQ[1], TQ[2])$, with $TQ[1] = E(Q_1)$ and $TQ[2] = E(Q_2)$, where $E(\cdot)$ is the encryption function, the same as in the algorithm *GenTrapdoor* but with the secret key of a specific user U_j, denoted by $(S, \mathscr{M}, \mathscr{M}')$, as the encryption key.

(v) Search(TQ_j, I_j). For user U_j, the remote health monitoring service provider calculates $(TQ_{ji}[1] - TQ_{ji}[2]) \cdot I_j$. The server gets the comparison results according to the following equations:

$$\left(TQ_{ji}[1] - TQ_{ji}[2]\right) \odot I_j \leq 0 \quad (1 \leq i \leq 2m). \tag{12}$$

For $\alpha = L_\lambda \in \mathscr{L}$, $(TQ_{ji}[1] - TQ_{ji}[2]) \odot I_j \leq 0$ means that the λth parameter is greater than or equal to α, while for $\alpha = H_\lambda \in \mathscr{H}$, this equation indicates that the λth parameter is smaller than or equal to α. If for any $i \in \{1, 2, \ldots, 2m\}$, this equation does not hold, that is, some health parameter is out of the range of $[L_\lambda, H_\lambda]$, then the RHM service provider would notify the medical service provider. When uploading the trapdoors the users may attach emergency tags on some vital health parameters, so that when RHMSP detects these parameters abnormal, direct help from the health center can be provided to the patients.

(vi) Search2$(TQ, \mathscr{I}, j)$. This search algorithm is run when RHMSP receives search requests from the medical service

provider. Note that the medical service provider can only search over the encrypted health data, whose owner permits it to search over the encrypted data; that is, it sends the user specific secret key to it. The RHM service provider sends the records satisfying the search request to the medical service provider according to the following equation:

$$(TQ[1] - TQ[2]) \odot I_J \leq 0, \quad I_J \in \mathcal{F}. \tag{13}$$

3. System Evaluation

In Section 2.3, we construct a searchable encryption scheme for continuous health monitoring system. In the following, we first prove that it achieves the functionality goal and the security goal. On the one hand, the service provider is able to find odd conditions over the encrypted data. In particular, on the other hand, the searchable encryption scheme ensures that curious service provider or malicious users would not get known of private information about honest users' sensitive health data, thus protecting user privacy. Then, through simulation experiments, we evaluate system performance in terms of computation and communication overhead.

3.1. Correctness Analysis. In the following, we briefly discuss the correctness of the proposed searchable encryption scheme on the basis of the correctness proof of the ASPE scheme shown in Section 2.2. We prove the correctness of GenTrapdoor2(·) and Search2(·), and it is easy to prove the correctness of the other trapdoor generation and search algorithm designed for supporting detection of outliers over the encrypted health data in the same way.

In vector Q_1 and Q_2, except for the values on the λth position, all the others are the same. Therefore, when the operation is "$\leq$" we have

$$\begin{aligned}
&(TQ[1] - TQ[2]) \odot I_J \\
&= \left(\left[Q_{1a}^T, Q_{1b}^T\right]^T - \left[Q_{2a}^T, Q_{2b}^T\right]^T\right) \odot \left[P_{ja}^T, P_{jb}^T\right]^T \\
&= \left(\widehat{Q_1} - \widehat{Q_2}\right) \odot \overline{P_J} \\
&= 0.5r\left(d^2\left(Q_2, P_J\right) - d^2\left(Q_1, P_J\right)\right) \\
&= 2rs\left(\alpha - P_J[\lambda]\right).
\end{aligned} \tag{14}$$

When the operation is "$\geq$" we have

$$\begin{aligned}
&(TQ[1] - TQ[2]) \odot I_J \\
&= \left(\left[Q_{1a}^T, Q_{1b}^T\right]^T - \left[Q_{2a}^T, Q_{2b}^T\right]^T\right) \odot \left[P_{ja}^T, P_{jb}^T\right]^T \\
&= \left(\widehat{Q_1} - \widehat{Q_2}\right) \odot \overline{P_J} \\
&= 0.5r\left(d^2\left(Q_2, P_J\right) - d^2\left(Q_1, P_J\right)\right) \\
&= 2rs\left(P_J[\lambda] - \alpha\right).
\end{aligned} \tag{15}$$

Furthermore, r and s are positive numbers; therefore it is easy to verify that

$$\begin{aligned}
&2rs\left(\alpha - P_J[\lambda]\right) \leq 0, \quad \text{iff } \alpha \leq P_J[\lambda], \\
&2rs\left(P_J[\lambda] - \alpha\right) \leq 0, \quad \text{iff } \alpha \geq P_J[\lambda].
\end{aligned} \tag{16}$$

Therefore, SCRHM, which aims to perform range searches over the encrypted health data, can accomplish the claimed functionality correctly.

3.2. Security Analysis. In what follows, we prove that our system satisfies the three proposed security requirements, that is, confidentiality, single parameter privacy, and trapdoor uniqueness.

Confidentiality. The privacy protection of searchable indexes and trapdoors is based on the security of the ASPE scheme. On the security of this scheme, Wong et al. claim that it can guard against any attacks based on the knowledge of a number of (plaintext, ciphertext) pairs, and their argument is as follows [33]. If the boolean vector S is known to the adversary, then he/she would be able to use the known (plaintext, ciphertext) pairs to construct linear equations about M_1 and M_2 and then solve the equations to obtain M_1 and M_2. However, since S is secret, it would be hard for the adversary to derive the correct linear equations to use, since the formulation of the equations depends on S. A brute-force approach would require the adversary to examine all possible bit vector S, which leads to $2^{|S|}$ linear equation systems that cannot be solved in reasonable time when $|S|$ is large. That is, the RHM service providers are unable to obtain the matrices M_J and M_J' of a honest user U_J. Therefore, the encrypted index $[(M_J{}^{-1}P_{ja})^T, (M_J'^{-1}P_{jb})^T]^T$ will not leak private information of data vector P_J. The trapdoors will keep the confidentiality of the corresponding λth searched health parameter as well.

However Yao et al. [35] propose a chosen plaintext attack that can recover the data point not by solving the aforementioned linear equations. Their attack is as follows [35]. Assume that the server obtains d query points and their corresponding ciphertexts (by asking the oracle in the chosen plaintext attack model). For each Q of those query points, the server would have two encrypted points Q_a and Q_b generated by the query point encryption function. The ASPE scheme ensures that dot product between Q and any data point P can be calculated based on the following equation: $P \cdot Q = P_a \cdot Q_a + P_b \cdot Q_b$. Notice that the above equation contains only d variables unknown to the adversary, that is, the d fields of the data point P. Since the adversary has the (plaintext, ciphertext) pair of d query points, he can construct d linear equations to derive all the fields of P. Therefore, the ASPE scheme is prone to chosen plaintext attack and this attack still works if data point is encrypted by the query point encryption function, and the query point is encrypted with the data point encryption function, which is the case in our scheme.

Fortunately, this attack will not affect the security of our proposed scheme. The most important part in the above mentioned attack is that the adversary knows the plaintext,

whereas, in our scheme, even if the adversary is allowed to access the trapdoor generation oracle, he is unable to obtain the plaintext. For example, the adversary's query is denoted by Q, according to the trapdoor generation algorithm in our scheme; the adversary will get the ciphertexts $E(Q_1)$ and $E(Q_2)$ (or $E(Q_{j\lambda 1})$ and $E(Q_{j\lambda 2})$), where Q_1 and Q_2 (or $Q_{j\lambda 1}$ and $Q_{j\lambda 2}$) are two random vectors which are only known by the honest user U_j and fully trusted authorized medical service providers but unknown to neither the RHM service provider nor malicious users. Therefore, the adversary cannot implement the chosen plaintext attack in our scheme. The adversary is only able to obtain the private information within the encrypted indexes and trapdoors by implementing brute force search, whereas brute force search is computationally infeasible when the number of dimensions is greater than 80 [33].

Single Parameter Privacy. Trapdoor generation is a randomized algorithm. For each value $\alpha \in \mathscr{L} \cup \mathscr{H}$, two random vectors Q_1 (or $Q_{j\lambda 1}$) and Q_2 (or $Q_{j\lambda 2}$) are generated and both of them are randomly split into two vectors which are then multiplied by two secret matrices M_j and M'_j. That is, the trapdoors are indistinguishable from random vectors. After the user randomly permutes the $2m$ trapdoors before uploading them to RHSMP, it is impossible to establish a mapping between the parameters and the trapdoors since all the $2m$ trapdoors are random and indistinguishable from each other. For lower bound and upper bound, the trapdoor generation phase is different, so that in the search phase, the criteria of whether the values are abnormal or not are the same, that is, whether $(TQ[1] - TQ[2]) \odot I_j \leq 0$ holds or not. As a result, even if RHMSP finds that a certain health data record is an outlier, it will not get known of which parameter is abnormal and whether it is greater than the upper bound or smaller than the lower bound, thus protecting single parameter privacy proposed in our security requirements.

Trapdoor Uniqueness. From the above confidentiality analysis, we know that even if the RHM service provider colludes with malicious users, the private information in the indexes and trapdoors cannot be recovered; however we omit some other possible approaches. That is, if the trapdoors generated by the honest users or medical service provider can be used to search the encrypted indexes by the malicious users or vise verse, then the malicious users can recover the values in a divide-and-conquer or brute-force way. For example, if the trapdoors generated by a malicious user A can be used to search a honest user B's encrypted indexes, then A generates trapdoors for all possible values of a specific health parameter with the algorithm *GenTrapdoor2* and runs the search algorithm *Search2* over the encrypted indexes; if the equation $(TQ[1] - TQ[2]) \odot I_j = 0$ holds for a certain trapdoor, then A can get known that the encrypted health parameter equals to the value α encrypted by this trapdoor. The malicious users can recover the value encrypted in the honest users' or medical service providers' trapdoors in a similar way by generating encrypted indexes for all possible values and running the *Search2* algorithm with these encrypted indexes and the trapdoors as inputs. Therefore it is of great importance that the trapdoor is unique; that is, the trapdoor generated by user A can only be used to search the encrypted indexes generated by him/herself but not other users. Fortunately, our scheme satisfies this property since when using different user specific secret key to generate the encrypted indexes and trapdoors, Fact 1 and Fact 2 in Section 2.2 do not hold. When trapdoor generated by malicious user A is used for searching over honest user B's encrypted indexes, $([(M_A^T Q_{1a})^T, (M_A'^T Q_{1b})^T]^T - [(M_A^T Q_{2a})^T, (M_A'^T Q_{2b})^T]^T) \odot [(M_B^{-1} P_a)^T, (M_B^{-1} P_b)^T]^T$ (M_A, M'_A are user A's secret key and M_B, M'_B are user B's secret key) will be a random value, which does not leak any information about the honest user B's encrypted indexes. In a similar way, we can prove that A cannot get private information of B's trapdoors. Therefore, trapdoor uniqueness required in our design goals is satisfied in our scheme.

From analysis above, we can conclude that our scheme is secure in terms of the three security requirements proposed in Section 2.1.

3.3. Performance Evaluation. In this section, we run simulation experiments to evaluate the performance of the proposed scheme in terms of computation and communication overhead. All the data vectors used in our experiments below are generated randomly.

Computation Overhead. The computations are performed on a 1.4 GHz MAC OS X Yosemite system. All the data reported below are averaged over 100 randomized runs. Time costs of the algorithms are evaluated with varied size of parameters and users. We set the number of parameters to be four different values: 80, 120, 160, and 200. On the one hand, the size is set to be greater than 80 for guaranteeing the security property of the ASPE scheme; on the other hand, 200 parameters are enough for remote health monitoring systems in practice. As for user numbers, we choose 10000, 50000, 100000, 150000, and 200000 to evaluate system performance. Algorithms running on the remote health monitoring server can be parallelized; therefore computation efficiency can be further improved.

Time for Generating Index and Trapdoors. In what follows, we consider the time cost for each RHM service user to generate indexes and trapdoors. To generate an index, firstly an m-dimensional data vector is created by the gateway. Each dimension of the vector represents a monitored parameter. This vector is encrypted by the ASPE encryption scheme; that is, it is split into two random vectors with a secret binary vector S as the splitting indicator and encrypted by two $(m + 1) \times (m + 1)$ invertible matrices. To create trapdoors for $2m$ bounds, firstly two m-dimensional random vectors are generated and then each vector is encrypted by the ASPE encryption scheme. We study whether the size of health data parameters will affect the time costs for generating an index or trapdoors. As shown in Figure 3, index for one health data record can be generated within 0.5 ms. Figure 4 indicates that the trapdoors for all parameters can be created in less than 0.35 s (note that trapdoors are created once for all), which is efficient for practical applications. The computation cost of

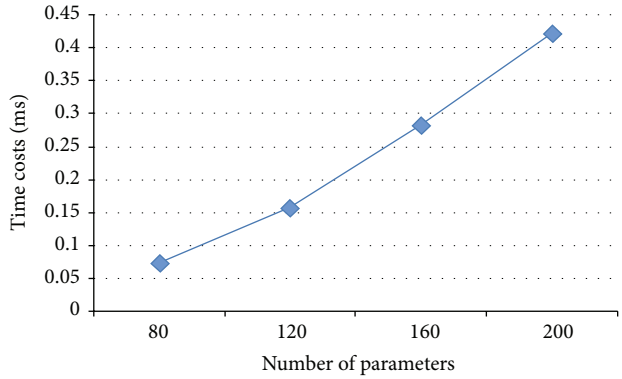

Figure 3: Encrypted index generation.

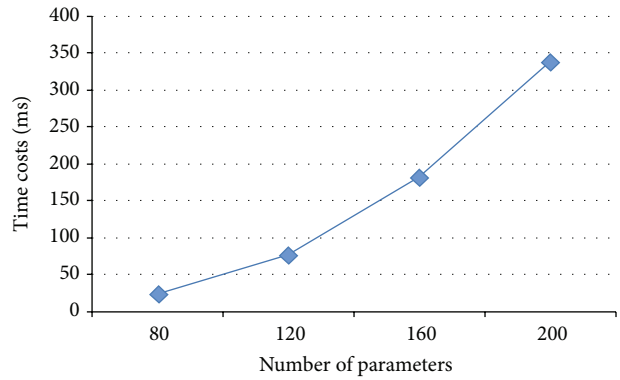

Figure 4: Trapdoor generation.

algorithm *GenTrapdoor2* is almost the same as *GenIndex*; we omit the experimental results here.

Time for Searches. In each time interval, an encrypted health data is uploaded to the remote health monitoring service provider, who runs the search algorithm *Search*. We show the time cost in Figure 5. For each health data record, outliers detection can be accomplished very efficiently; for example, only about 5 μs is consumed when the parameter size is 200. When a medical service provider wants to search interested health data records, the search time is related with the size of the specific user's health data records. From Figure 6, when we set the health data record size to 200000, the time consumed is only about 450 ms, which is efficient for practical applications.

Communication Overhead. We mainly focus on the communication overhead of the index and trapdoor generation phase, since these phases may be executed on a mobile devices, which requires low communication costs. From Figures 7 and 8, when the size of the health parameters is set as $m = 200$, the size of the index is 1.6 KB and the size of the trapdoors is about 700 KB, which is a feasible storage requirement on most mobile devices. In addition, the trapdoor generation is run only once; therefore, our scheme achieves communication efficiency and is applicable on mobile devices.

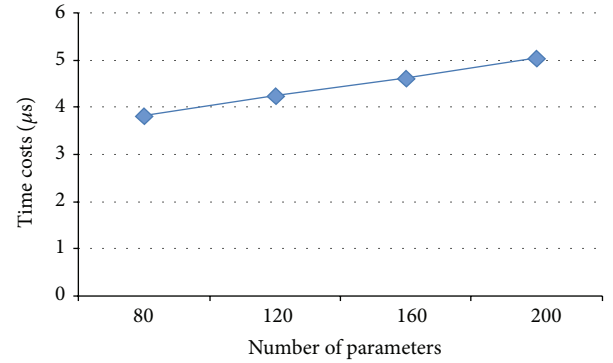

Figure 5: Outlier detection computation overhead.

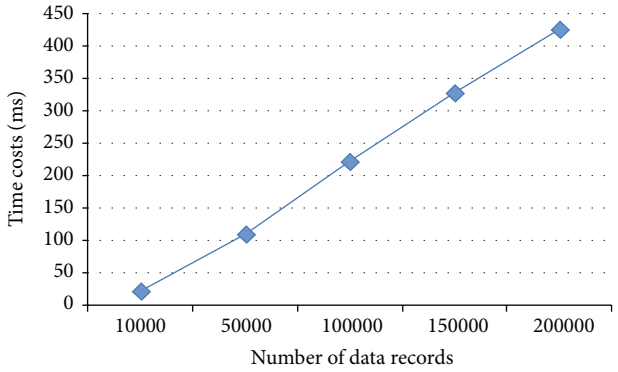

Figure 6: Search2 computation overhead.

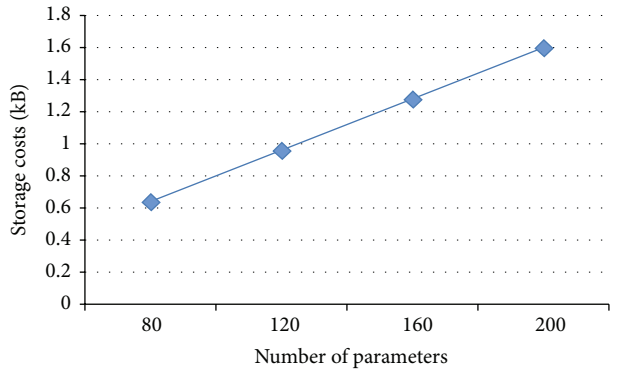

Figure 7: Size of index.

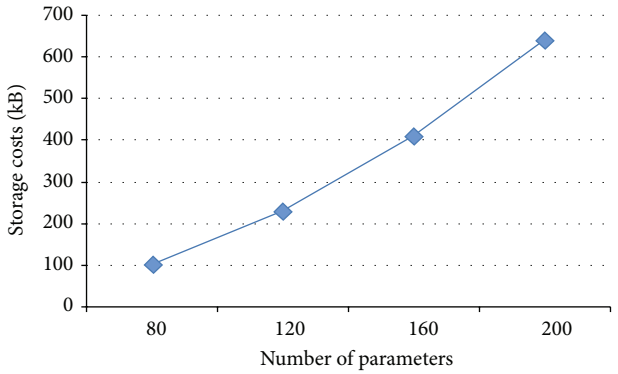

Figure 8: Size of trapdoor.

4. Conclusion

In this paper, considering the increasing need for remote health monitoring and confidential property of the health data, we introduce a secure continuous remote health monitoring system, named SCRHM. To enable remote health monitoring service provider to find odd conditions while preserving users' data privacy, a searchable encryption scheme, which supports range searches for the remote health monitoring system, is proposed. We perform the correctness and security analysis of the proposed scheme and prove that our proposed scheme supports range searches over encrypted data correctly and achieves the security goals to protect user privacy. Through extensive simulation experiments, we validate the performance of our system. In particular, high performance in terms of computation and communication overhead can be achieved. In the future, we would like to extend our system to support more complex computation over encrypted health data, so that remote health monitoring service provider would be able to perform more versatile analyses and provide more plentiful services for users.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This work is partially supported by the National Natural Science Foundation of China under Grants nos. 61170263 and 60911140102.

References

[1] Population Division, *World Population Prospects: The 2012 Revision Population Database*, Population Division, 2012.

[2] G. Anderson, "Chronic conditions: making the case for ongoing care," 2004, http://www.partnershipforsolutions.org/DMS/files/chronicbook2004.pdf.

[3] A. Tesanovic, G. Manev, M. Pechenizkiy, and E. Vasilyeva, "eHealth personalization in the next generation RPM systems," in *Proceedings of the 22nd IEEE International Symposium on Computer-Based Medical Systems (CBMS '09)*, pp. 1–8, IEEE, Albuquerque, NM, USA, August 2009.

[4] J. Morrissey, "Remote patient monitoring: How mobile devices will curb chronic conditions," 2014, http://medicaleconomics.modernmedicine.com/medical-economics/content/tags/chronic-care/remote-patient-monitoring-how-mobile-devices-will-curb-c?page=full.

[5] A. T. Tzallas, M. G. Tsipouras, G. Rigas et al., "Perform: a system for monitoring, assessment and management of patients with Parkinson's disease," *Sensors*, vol. 14, no. 11, pp. 21329–21357, 2014.

[6] F. Guerrini, "Spanish researchers design wearable remote monitoring system for patients with parkinson's disease," 2015, http://www.forbes.com/sites/federicoguerrini/2015/02/03/spanish-researchers-design-wearable-remote-monitoring-system-for-patients-with-parkinson-disease/.

[7] D. Nield, "Google fit v apple health they just want you for your body: apple and google are going head-to-head again," October 2015, http://www.wareable.com/sport/google-fit-vs-apple-health.

[8] G. Paul and J. Irvine, "Privacy implications of wearable health devices," in *Proceedings of the 7th International Conference on Security of Information and Networks (SIN '14)*, p. 117, ACM, Glasgow, UK, 2014.

[9] X. Liang, M. Barua, L. Chen et al., "Enabling pervasive healthcare through continuous remote health monitoring," *IEEE Wireless Communications*, vol. 19, no. 6, pp. 10–18, 2012.

[10] T. Schabetsberger, E. Ammenwerth, S. Andreatta et al., "From a paper-based transmission of discharge summaries to electronic communication in health care regions," *International Journal of Medical Informatics*, vol. 75, no. 3, pp. 209–215, 2006.

[11] Osirix dicom viewer, dicom sample image sets, http://www.osirix-viewer.com/datasets/.

[12] G. Acampora, D. J. Cook, P. Rashidi, and A. V. Vasilakos, "A survey on ambient intelligence in healthcare," *Proceedings of the IEEE*, vol. 101, no. 12, pp. 2470–2494, 2013.

[13] A. Pantelopoulos and N. G. Bourbakis, "A survey on wearable sensor-based systems for health monitoring and prognosis," *IEEE Transactions on Systems, Man and Cybernetics, Part C: Applications and Reviews*, vol. 40, no. 1, pp. 1–12, 2010.

[14] B. Fabian, T. Ermakova, and P. Junghanns, "Collaborative and secure sharing of healthcare data in multi-clouds," *Information Systems*, vol. 48, pp. 132–150, 2015.

[15] S. Narayan, M. Gagné, and R. Safavi-Naini, "Privacy preserving EHR system using attribute-based infrastructure," in *Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop*, pp. 47–52, ACM, Chicago, Ill, USA, October 2010.

[16] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proceedings of the IEEE Symposium on Security and Privacy (SP '07)*, pp. 321–334, IEEE, Berkeley, Calif, USA, May 2007.

[17] H. Löhr, A.-R. Sadeghi, and M. Winandy, "Securing the e-health cloud," in *Proceedings of the 1st ACM International Health Informatics Symposium*, pp. 220–229, ACM, November 2010.

[18] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 1, pp. 131–143, 2013.

[19] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized private keyword search over encrypted data in cloud computing," in *Proceedings of the 31st International Conference on Distributed Computing Systems (ICDCS '11)*, pp. 383–392, IEEE, Minneapolis, Minn, USA, July 2011.

[20] M. Naehrig, K. Lauter, and V. Vaikuntanathan, "Can homomorphic encryption be practical?" in *Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop (CCSW '11)*, pp. 113–124, Chicago, Ill, USA, October 2011.

[21] R. A. Popa, *Building practical systems that compute on encrypted data [Ph.D. thesis]*, Massachusetts Institute of Technology, Cambridge, Mass, USA, 2014.

[22] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *Proceedings of the IEEE Symposium on Security and Privacy (S&P '00)*, pp. 44–55, IEEE, Berkeley, Calif, USA, May 2000.

[23] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06)*, pp. 79–88, ACM, Alexandria, Va, USA, October 2006.

[24] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in *Advances in Cryptology—EUROCRYPT 2004*, vol. 3027 of *Lecture Notes in Computer Science*, pp. 506–522, Springer, Berlin, Germany, 2004.

[25] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in *Theory of Cryptography*, pp. 535–554, Springer, 2007.

[26] E. Shi, J. Bethencourt, T.-H. H. Chan, D. Song, and A. Perrig, "Multi-dimensional range query over encrypted data," in *Proceedings of the IEEE Symposium on Security and Privacy (SP '07)*, pp. 350–364, IEEE, Berkeley, Calif, USA, May 2007.

[27] Y. Lu, "Privacy-preserving logarithmic-time search on encrypted data in cloud," in *Proceedings of the 19th Network & Distributed System Security Symposium (NDSS '12)*, San Diego, Calif, USA, February 2012.

[28] P. Wang and C. V. Ravishankar, "Secure and efficient range queries on outsourced databases using Rp-trees," in *Proceedings of the 29th International Conference on Data Engineering (ICDE '13)*, pp. 314–325, IEEE, Brisbane, Australia, April 2013.

[29] B. Wang, Y. Hou, M. Li, H. Wang, and H. Li, "Maple: scalable multi-dimensional range search over encrypted cloud data with tree-based index," in *Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security (ASIA CCS '14)*, pp. 111–122, ACM, Kyoto, Japan, June 2014.

[30] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *Proceedings of the IEEE Conference on Computer Communications (INFOCOM '10)*, pp. 1–9, San Diego, Calif, USA, March 2010.

[31] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM Conference on Computer and Communications Security*, pp. 89–98, ACM, November 2006.

[32] J. Sun, X. Zhu, C. Zhang, and Y. Fang, "HCPP: cryptography based secure EHR system for patient privacy and emergency healthcare," in *Proceedings of the 31st International Conference on Distributed Computing Systems (ICDCS '11)*, pp. 373–382, IEEE, Minneapolis, Minn, USA, July 2011.

[33] W. K. Wong, D. W.-l. Cheung, B. Kao, and N. Mamoulis, "Secure kNN computation on encrypted databases," in *Proceedings of the ACM International Conference on Management of Data (SIGMOD '09)*, pp. 139–152, Providence, RI, USA, July 2009.

[34] Z. Shen, J. Shu, and W. Xue, "Preferred keyword search over encrypted data in cloud computing," in *Proceedings of the IEEE/ACM 21st International Symposium on Quality of Service (IWQoS '13)*, pp. 207–212, Montreal, Canada, June 2013.

[35] B. Yao, F. Li, and X. Xiao, "Secure nearest neighbor revisited," in *Proceedings of the IEEE 29th International Conference on Data Engineering (ICDE '13)*, pp. 733–744, IEEE, Brisbane, Australia, April 2013.