Received 18 July 2023, accepted 30 August 2023, date of publication 6 September 2023, date of current version 12 September 2023.

*Digital Object Identifier 10.1109/ACCESS.2023.3312549*

RESEARCH ARTICLE

# A Privacy-Preserving Remote Heart Rate Abnormality Monitoring System

**JIANHONG ZHANG AND HAOWEI YANG**
School of Electrical and Computer Engineering, North China University of Technology, Beijing 100144, China

Corresponding author: Haowei Yang (yanghw1228@163.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 62172005, in part by the Natural Science Foundation of Beijing under Grant 4212019 and Grant M22002, and in part by the Open Research Fund of the Key Laboratory of Cryptography of Zhejiang Province under Grant ZCL21014.

**ABSTRACT** Heart rate arrhythmia is an important manifestation of common clinical cardiovascular diseases, posing a serious threat to human life and health. Due to its suddenness, insidiousness and rapid changes, it often causes patients to miss the best treatment time. Therefore, real-time monitoring of heart rate changes is particularly important to monitor and prevent the onset of such diseases. Nonetheless, heart rate information in telemedicine systems is often presented in plaintext, rendering it vulnerable to interception or tampering, and posing a substantial threat to users' privacy. To address this issue, we propose a privacy-preserving remote heart rate abnormality monitoring system, which utilizes a privacy comparison protocol. By implementing a two-server model, the privacy comparison protocol ensures privacy not only during the comparison process but also in the resulting outcomes. During the monitoring process, the monitor is only able to obtain the final number of abnormalities of the patient's heart rate and cannot obtain information about the patient's original heart rate. This allows for a more rational and effective use of medical experts, so that patients can enjoy a high level and quality of service from medical experts without having to leave home. Finally, a detailed security analysis demonstrates that our scheme can effectively protect the privacy and security of patient medical data and hospital health indicators. And our experimental results show that our scheme is computationally efficient and the scheme is effective and feasible.

**INDEX TERMS** Homomorphic encryption, privacy-preserving, abnormal heart rate monitoring, telemedicine system.

## I. INTRODUCTION

The emergence and outbreak of the COVID-19 epidemic have highlighted the importance of telemedicine in modern healthcare. The infectious nature of the virus and the limited medical resources make face-to-face consultation between patients and doctors impossible, resulting in many underlying diseases not receiving timely treatment. Telemedicine provides a breakthrough solution to time and space limitations, reduces the risk of cross-infection between doctors and patients during epidemics, enables critical patients to receive rapid diagnosis and treatment, and offers a new way of treatment for patients with underlying diseases. In telemedicine, doctors often monitor the health status of patients based on their physiological indicators, with heart rate being a critical physiological indicator that reflects a person's health status. Normally, a person's heart rate will be in a heart rate range. Abnormal heart rate can lead to various potential health problems, including cardiovascular disease, stroke, heart failure, and more, with cardiovascular disease being the most severe. The World Health Organization reports that the mortality rate of cardiovascular disease remains high and is increasingly affecting younger individuals, posing a significant threat to human life and health, while also imposing a substantial economic burden on society and families. The insidious, sudden, and rapidly changing nature of the cardiovascular disease makes it challenging for patients to receive timely treatment, emphasizing the critical need for real-time heart rate monitoring for both working individuals and the elderly.

The associate editor coordinating the review of this manuscript and approving it for publication was Zijian Zhang.

Wearable devices play a critical role in achieving real-time monitoring for telemedicine. With the help of wearable devices, telemedicine systems can achieve real-time monitoring of patient's heart rate, detecting abnormal heart rates in time for early diagnosis or taking preventive measures in advance. However, smart wearable devices typically have limited storage space and computing power, which can restrict their functionality and performance. As a result, some schemes have proposed uploading patient data to a cloud server to reduce power consumption and increase efficiency. However, using cloud servers as an untrusted entity for processing patient's heart rate information can pose significant security risks to patient data privacy. For instance, Huang et al. [1] employed body sensors and convolutional neural networks to identify human activities for the elderly and rehabilitation monitoring. However, this scheme lacks the protection of patients' private information, which can easily lead to the leakage of patients' private information. Some existing schemes propose privacy protection for medical data. Liang et al. [2] proposed a privacy-preserving query for implementing multiple sources of electronic health records in public clouds in a healthcare system, using symmetric encryption for encrypting electronic health records, but a single cloud server is not as protective of the results compared to a dual server. In the remote monitoring system, malicious entities may infer the patient 's personal information, such as age, occupation, etc., by observing the value of the patient's specific abnormal data, which will leak the patient's privacy. There are existing schemes that may only achieve privacy for input data but not for output results. For example, Pettai and Laud [3] propose a scheme that uses secure multi-party computation and differential privacy together to protect the privacy of input data by adding noise but cannot protect the privacy of output results. After the computation results are published, participants may analyze the distributions and statistical properties of the noise to infer the inputs of other participants, thus revealing the privacy information of other participants. Similarly, Zhou et al. [4] proposed a secure multi-party computation scheme based on secret sharing, but this scheme also cannot protect the privacy of the output results. After the computation results are published, participants may use some of the computation results to infer the inputs of other participants. Privacy leaks in every part of the monitoring process can cause many problems. In healthcare, patient information is sensitive, and China's ''Personal Information Protection Law of the People's Republic of China'', officially implemented on November 1, 2021, emphasizes the need to protect the legitimate rights and interests of personal information subjects. Therefore, privacy protection in telemedicine demands immediate attention and effective solutions.

Generally speaking, the healthy heart rate range is different for each category because of differences in patient's gender, age, and so on. Abnormal heart rate can induce various diseases, so real-time monitoring of heart rate is particularly important. In this paper, we aim to determine whether a patient's heart rate value is normal by comparing it with patient's own healthy heart rate range uploaded by the hospital. However, heart rate data usually presented in plaintext, which can lead to privacy leakage [5], [6], [7], [8]. Specifically, a malicious entity would infer a patient's personal information, such as occupation, gender, etc., from the patient's own healthy heart rate range and abnormal heart rate data. Encryption can provide a better solution to address this issue. Various methods are available for heart rate data encryption [9], [10], [11], [12], [13], [14], [15], [16], including symmetric key-based encryption algorithms (e.g., AES), asymmetric key-based encryption algorithms (e.g., RSA), elliptic curve cipher-based encryption algorithms (e.g., ECC), and others. All of these algorithms can be used to encrypt heart rate data and protect personal privacy. However, the main drawback of these methods compared to homomorphic encryption is that they do not support computation in the ciphertext state, which means that encrypted heart rate data must first be decrypted before computation, potentially leading to security issues. Additionally, these encryption methods may have problems with key management and distribution, such as securely generating and distributing keys and protecting them from disclosure. Homomorphic encryption, allows computations to be performed in the ciphertext state, enabling more complex data processing and computation while maintaining data privacy.

In response to the above questions, we propose a dual cloud server model collaborative computing method and apply it to the remote heart rate abnormality monitoring system. The main contributions of this paper are as follows:

- To achieve privacy security at every step of the entire monitoring process, we propose a privacy comparison protocol (PC) based on dual servers, which offers more protection of results than a single server. In this protocol, we can calculate the number of abnormal heart rates and use this data to monitor the patient's physical health during this time period. Since the results are calculated collaboratively by the two servers, neither server can calculate the results alone without collusion between two servers, which enhances the security of the patient's heart rate information.
- We propose a privacy-preserving remote heart rate abnormality monitoring system, which focuses on the daily monitoring and analysis of the patient's physical condition, and plays an auxiliary warning role, and the doctor can propose corresponding protective opinions based on the monitoring results. The scheme achieves monitoring of the patient's heart rate while protecting the privacy of the patient's heart rate data, the patient's own healthy heart rate range and results. The final result of the scheme will only reflect whether the patient's heart rate data is normal or not, it will not show what the specific value is. Therefore, only the number of abnormal data can be known, and there is no way to know the specific value of the abnormal data.

- Through detailed security analysis, we demonstrate that our scheme can effectively protect the privacy and security of patient heart rate data and patient's own health indicators uploaded by the hospital. And we analyze the performance of our scheme, and the results show that our scheme is effective and feasible.

The remainder of this paper is organized as follows. In Section II, we introduce the system and security models along with design goals. Then, we briefly review some relevant preliminaries in Section III. After that, in Section IV, we describe our proposed scheme, followed by its security analysis in Section V. Next, The performance evaluation is given in Section VI. Finally, this paper is concluded in Section VIII with a review of related works in Section VII.

## II. MODELS AND DESIGN GOALS

In this section, we introduce our system model, security model, and design goal.

### A. SYSTEM MODEL

In our system, to ensure privacy and security at every step of the entire monitoring process, we introduce two cloud servers to calculate and process the data uploaded by patients and hospitals. The model has three entities: Patient ($P$), Cloud Server($CS_1$,$CS_2$), and Hospital($H$), as shown in Figure 1.

#### 1) PATIENT(P)

In our model, patients collect their own heart rate information through smart wearable devices and encrypt it before uploading to $CS_1$. The collected heart rate information is considered private information of patients, and therefore, their heart rate information can only be accessed by the patients themselves. Patients are authorized users of their heart rate information and unauthorized users of other patients' heart rate information. They can manage the heart rate data uploaded to the cloud server, but they cannot access the heart rate data of other patients.

#### 2) CLOUD SERVERS ($CS_1$,$CS_2$)

Cloud servers have powerful storage capabilities and computing power, it's a good choice to outsource the heart rate data to them and compute the heart rate data in them. So we deployed two powerful cloud servers, $CS_1$ and $CS_2$, to jointly monitor abnormal heart rate data of patients. Notably, they're privately owned. Specifically, $CS_1$ stores encrypted heart rate data and patient's own healthy heart rate range, and with the collaboration of $CS_2$, calculates and returns the patient's heart rate status to the hospital during the time period.

#### 3) HOSPITAL (H)

Hospitals are data providers for patient's own healthy heart rate range, and authorized hospitals can monitor patients' heart rate information in real-time and provide timely medical assistance to patients.

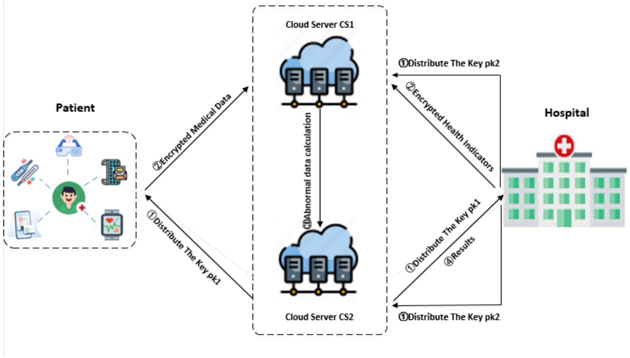

FIGURE 1. System Model.

### B. SECURITY MODEL

In our safety model, both the hospital and the patient are considered honest-but-curious. Specifically, they will perform the designed protocol truthfully, but the hospital may try to obtain the patient's heart rate data and the patient may be curious about other patients' heart rate data. Besides, since medical data and initiated query requests usually involve sensitive personal information, they need to be kept secret from the cloud server $CS_1$, $CS_2$. Therefore, we assume that the cloud servers are honest-but-curious, i.e., they will honestly follow the underlying scheme but may be curious about sensitive information including medical data, patient's own healthy heart rate range, and health status information. Also, we assume that cloud servers do not collude with each other. This assumption is reasonable due to the loss of reputation from collusion, the user's personal property will suffer significant losses, and the reputation of the outsourcer in the society will be reduced, affecting the further development of the outsourcer. And this assumption is widely accepted in secure two-sided computing models. Notably, since we focus on secure computing techniques, other active attacks, such as injection attacks, are beyond the scope of this paper and will be discussed in our future work.

### C. DESIGN GOALS

The scheme proposed in this paper should achieve the following design goals.

- *Privacy protection:* During the whole process of remote monitoring, we need to ensure the security issues at every step, and the heart rate data and patient's own healthy heart rate range should be kept secret from the cloud servers. In addition, we must protect the privacy of the access pattern, which means that the cloud servers don't know the patient's heart rate information returned to the hospital.
- *Efficiency:* Achieving the above privacy goals will incur additional communication overhead, and our goal is to achieve privacy-preserving conditions while we also aim to minimize the computational costs for patients, cloud servers, and hospitals.

- *Accuracy:* The accuracy of the monitoring results should be guaranteed. In order to provide a high-quality remote heart rate abnormality monitoring service, the designed privacy-preserving strategy cannot sacrifice the accuracy of the monitoring results. Therefore, the proposed framework should also achieve a high level of accuracy.
- *Resist Replay Attacks:* The proposed scheme should be able to resist replay attacks by malicious people.

## III. PRELIMINARY

### A. OVERVIEW OF HOMOMORPHIC ENCRYPTION

Cryptographic algorithm is one of the key technologies for securing data. Homomorphic Encryption (HE) means that the original data is encrypted by homomorphic encryption and then the ciphertext obtained is subjected to a specific operation, and then the plaintext obtained after the calculation result is then decrypted by homomorphic decryption is equivalent to the data result obtained by the same calculation directly on the original plaintext data, which is a good choice to solve the privacy problem.

The homomorphic cryptographic structure can correspond to a pair of mappings in the abstract algebra. Let the encryption algorithm be $Enc()$ and the decryption algorithm be $Dec()$. The finite set of plaintexts is $D = \{m_1, m_2, \ldots, m_n\}$, corresponding ciphertext is a finite set $C = \{c_1, c_2, \ldots, c_n\}$. $\odot$ and $\oplus$ represent valid calculations. If satisfied:

$$c_1 \odot c_2 = Enc(m_1) \odot Enc(m_2) = Enc(m_1 \oplus m_2) \tag{1}$$

Then it is considered to have homomorphism.

### B. PAILLIER HOMOMORPHIC ENCRYPTION ALGORITHM

Paillier encryption is an additive homomorphic encryption system, which is widely used in privacy protection applications. It has three parts: key generation $KeyGen(k)$, encryption $E(pk, m)$ and decryption $D(sk, c)$.

- Key generation:
  1) Randomly choose two large prime numbers $p$ and $q$, ensuring that $p$ and $q$ are as close or equal in length as possible (high security).
  2) Calculate $n = pq$ and $\lambda = lcm(p-1, q-1)$, where $lcm$ denotes the least common multiple.
  3) Randomly select $g$ and $g$ needs to satisfy the equation

  $$gcd\,(L(g^{\lambda} \bmod n^2), n)^{-1} = 1 \tag{2}$$

  where $g \in Z^*_{n^2}$, $L(x) = \frac{x-1}{n}$, $Z$ is an integer and the subscript indicates how many elements there are in the set of integers.
  4) The public key is $(n, g)$.
  5) The private key is $(\lambda, \mu)$,where

  $$\mu = (L(g^{\lambda} \bmod n^2))^{-1} \bmod n \tag{3}$$

- Encryption: For any plaintext message $m$, a random number $r$ is arbitrarily chosen and the ciphertext $c$ is calculated $c = E(m) = g^m \cdot r^n \bmod n^2$ where $m \in Z_n$, $r \in Z^*_n$.
- Decryption: For the ciphertext $c$, the plaintext $m$ is computed as follows:

$$\begin{aligned} m = D(c) &= \frac{L(c^{\lambda} \bmod n^2)}{L(g^{\lambda} \bmod n^2)} \bmod n \\ &= L(c^{\lambda} \bmod n^2) \cdot \mu \bmod n \end{aligned} \tag{4}$$

### C. PROPERTIES OF PAILLIER ENCRYPTION

- Properties of additive homomorphism

  For any plaintext $m_1, m_2 \in Z_n$ and any random number $r_1, r_2 \in Z^*_n$, the corresponding ciphertext satisfies:

$$\begin{aligned} c_3 &= c_1 \cdot\ c_2 \\ &= E(m_1, r_1) \cdot E(m_2, r_2) \\ &= g^{m_1 + m_2} \cdot (r_1 \cdot r_2)^n \bmod n^2 \end{aligned} \tag{5}$$

  where $c_1 = E(m_1, r_1)$, $c_2 = E(m_2, r_2)$

  after decryption, we get:

$$\begin{aligned} m_3 &= D(\ c_3) \\ &= D(\ c_1 \cdot\ c_2) \\ &= D(E(m_1, r_1) \cdot E(m_2, r_2) \bmod n^2) \\ &= m_1 + m_2 \bmod n^2 \end{aligned} \tag{6}$$

  that is, we get: $c_3 = c_1 \cdot c_2 = E(m_1 + m_2)$.
- Properties of scalar multiplication

  For any plaintext $m_4 \in Z_n$ and any random number $r_3 \in Z^*_n$, $a \in Z_p$, the corresponding ciphertext satisfies: $c_4 = g^{m_4} \cdot r_3^n \bmod n^2$ is the ciphertext of $m_4$, then

$$\begin{aligned} {c_4}^a &= (g^{m_4} \cdot r_3^n)^a \bmod n^2 \\ &= g^{am_4} \cdot (r_3^a)^n \bmod n^2 \end{aligned} \tag{7}$$

  ${c_4}^a$ is obviously $a$ valid ciphertext of $a\,m_4$.

### D. SECURE MULTIPARTY COMPUTATION (SMC)

SMC was first proposed by The origin of Secure Multiparty Computation (SMC) can be traced back to the 1980s when it was first proposed by Andrew Yao. SMC refers to some joint function that refers to a set of parties with private inputs who wish to compute their inputs. There are techniques, such as garbled circuits and secret sharing, that can be used for SMC. In this paper, we propose an algorithm that assumes a two-party setup, but with the traditional SMC setup. That is, we have $CS_1$ with the encrypted input and $CS_2$ with the private key sk. Our goal is to let $CS_2$ obtain the encrypted result of a function without revealing to $CS_1$ or $CS_2$ the value of the original input to $CS_1$ or $CS_2$.

## IV. OUR PROPOSED SCHEME

In this section, because two cloud servers provide higher privacy protection for computation results than a single server and to achieve privacy protection throughout the monitoring process, we introduce two cloud servers as the

**TABLE 1.** Summary of notations.

| Notation | Definition |
|---|---|
| $CS_1, CS_2$ | Cloud Server I, Cloud Server II |
| $P$ | Patient |
| $H$ | Hospital |
| $E$ | Homomorphic encryption of $CS_2$ |
| $E^{'}$ | Homomorphic encryption of hospital |
| $(pk_1, sk_1)$ | The key pair of $CS_2$ |
| $(pk_2, sk_2)$ | The key pair of hospital |
| $d_i$ | Patient's heart rate information |
| $[t_1, t_2]$ | Patient's own healthy heart rate range uploaded by hospital |
| $h$ | Heart rate values unreachable by humans, e.g. 200 |
| $p_i$ | $CS_1$ generated random number |
| $\theta_i$ | Difference between patient data and health indicators multiplied by $p_i$ |
| $z_i^x$ | Generated by $CS_1$, determined by $p_i$ |
| $z_i^y$ | Generated by $CS_2$, determined by $\theta_i$ |
| $z_i$ | Judgment result of a single data from patient |
| $Z$ | Total number of patient medical data abnormalities |

main framework and design a privacy comparison protocol based on it.

Our encryption all uses the paillier encryption algorithm. We assume that $CS_2$ generates the key pair $(pk_1, sk_1)$, where $pk_1$ is the public key and $sk_1$ is the private key. The hospital generates the key pair $(pk_2, sk_2)$, where $pk_2$ is the public key and $sk_2$ is the private key. Table 1 shows the notations used in this paper and their meanings.

### A. PRIVACY COMPARISON (PC) PROTOCOL

We convert the determination of whether a heart rate value is normal to a comparison between the heart rate value and the value of the upper and lower bounds of the patient's own healthy heart rate range. The comparison process and the proof of its correctness are as follows:

$CS_1$ has $E(A)$ and $E(B)$, the PC protocol determines whether $B < A$ and uses $z_i$ to indicate the comparison result without leaking $A$, $B$, $z_i$ to any party. If $B < A$, $z_i = 1$, indicates that number of heartbeats of the patient is abnormal at this time; otherwise $z_i = 0$, where $z_i = z_i^x \oplus z_i^y$ and $\oplus$ represents the XOR operation. Consequently, the calling method of its algorithm is $PC(A, B)$, the PC protocol works as follows:

*Step-1:* $CS_1$ takes random number $p_i \in \{1, -1\}$, and perform a difference operation on the encrypted values coming from the patient and the hospital to get

$$E(\theta_i) = [E(B) \cdot E(A)^{-1}]^{p_i} = E[p_i \cdot (B - A)]. \tag{8}$$

And if $p_i = -1$, $z_i^x = 0$, on the contrary, $z_i^x = 1$.

*Step-2:* $CS_1$ encrypts $z_i^x$ with $pk_2$ from the hospital to get $E^{'}(z_i^x)$, $CS_1$ sends $E(\theta_i)$ and $E^{'}(z_i^x)$ to $CS_2$, $CS_2$ uses $sk_1$ to decrypt $E(\theta_i)$ to recover $\theta_i$ and judge the size of $\theta_i$. If $\theta_i \leq 0$, $z_i^y = 0$, otherwise, $z_i^y = 1$.

*Step-3:* $CS_2$ encrypts $z_i^y$ with $pk_2$ from the hospital to get $E^{'}(z_i^y)$, because $CS_2$ has $E^{'}(z_i^x)$, it can calculate:

$$E^{'}(z_i) = E^{'}(z_i^x \oplus z_i^y) = \begin{cases} E^{'}(z_i^x), & z_i^y = 0 \\ E^{'}(1 - z_i^x), & z_i^y = 1 \end{cases} \tag{9}$$

Correctness.When $p_i = 1$, if $\theta_i \leq 0$, we have $B{-}A < 0$. In this case, $z_i = z_i^x \oplus z_i^y = 1 \oplus 0 = 1$. That is, number of heartbeats of the patient is abnormal at this moment, and $B{-}A < 0$ is also exactly in line with this situation. If $\theta_i > 0$, $z_i = z_i^x \oplus z_i^y = 1 \oplus 1 = 0$, it means $B{-}A > 0$. Number of heartbeats of the patient is normal at this moment. In the same way, we can verify that the privacy comparison protocol is correct when $p_i = -1$.

**Algorithm 1** Privacy Comparison Protocol (PC)

```
Input: $E(A)$, $E(B)$, $pk_1$, $pk_2$, $sk_1$
Output: $E^{'}(z_i)$
$CS_1$ chooses a random number $p_i \in \{1, -1\}$
$CS_1$ calculates $E(\theta_i)$ by the following
    equation:$E(\theta_i) = [E(B) \cdot E(A)^{-1}]^{p_i} = E[p_i \cdot (B{-}A)]$
if ($p_i = -1$) then
    $z_i^x = 0$
else
    $z_i^x = 1$
end if
$CS_1$ encrypts $z_i^x$ with $pk_2$ from the hospital to
    get $E^{'}(z_i^x)$
$CS_1$ sends $E(\theta_i)$ and $E^{'}(z_i^x)$ to $CS_2$
$CS_2$ uses $sk_1$ to decrypt $E(\theta_i)$ to recover $\theta_i$ and
    determine the size of $\theta_i$
if $\theta_i \leq 0$ then
    $z_i^y = 0$
else
    $z_i^y = 1$
end if
$CS_2$ encrypts $z_i^y$ with $pk_2$ from the hospital to
    get $E^{'}(z_i^y)$
$CS_2$ calculates the $E^{'}(z_i)$,
    $E^{'}(z_i) = E^{'}(z_i^x \oplus z_i^y) = \begin{cases} E^{'}(z_i^x), z_i^y = 0 \\ E^{'}(1 - z_i^x), z_i^y = 1 \end{cases}$
```

### B. PAILLIER HOMOMORPHIC ENCRYPTION ALGORITHM OPTIMIZATION

1) Parameter $g$ optimization

In the original Paillier scheme, the value of $g$ only needs to satisfy $g \in Z_{n^2}^*$. In their paper, Ivan and Mads give an optimization scheme using $g = n + 1$ and show that the same security as the original Paillier algorithm can be maintained with the use of this scheme. The performance improvement of the key generation and encryption process is achieved after using $g = n + 1$. After taking $g = n + 1$ in the encryption phase, the part of the encryption process that is computed can be simplified as follows:

For $g^m = (n+1)^m$, by the Binomial Theorem, since:

$$\begin{aligned} g^m &= (n+1)^m \\ &= \binom{m}{0} n^m + \binom{m}{1} n^{m-1} + \\ &= \ldots + \binom{m}{m-2} n^2 + mn + 1 \bmod n^2 \end{aligned} \tag{10}$$

The first $m-1$ terms are all multiples of $n^2$ and are eliminated under modulo $n^2$. Therefore, the modal exponential operation is simplified to 1 modal multiplication, which speeds up the encryption process, the formula is as follows:

$$(n+1)^m = mn + 1 \bmod n^2 \tag{11}$$

The optimized key generation algorithm and encryption algorithm are represented as follows:

- *Key generation:* Bring $g = n+1$ into the generating formula of $\mu$, we get the formula as follows:

$$\begin{aligned}\mu &= (L(g^{\lambda} \bmod n^2))^{-1} \bmod n\\ &= L\left((n+1)^{\lambda} \bmod n^2\right)^{-1} \bmod n\\ &= L\left((1+\lambda n) \bmod n^2\right)^{-1} \bmod n\\ &= \lambda^{-1} \bmod n\end{aligned} \tag{12}$$

  The generation of $\mu$ can be done directly by taking the modulo inverse element of $\lambda$ for $n$.
- *Encryption:* Bringing $g = n+1$ into the encryption formula, we can get

$$\begin{aligned}c &= g^m \cdot r^n \bmod n^2\\ &= (n+1)^m \cdot r^n \bmod n^2\\ &= (nm+1) \cdot r^n \bmod n^2\end{aligned} \tag{13}$$

  The encryption process turns the operation of computing the m-th power of $g$ into a simple multiplication operation: $c = (nm+1) \cdot r^n \bmod n^2$.

### C. DESCRIPTION OF OUR PROPOSED SCHEME

We will now describe in detail our scheme for achieving heart rate monitoring of patients. It consists of four phases:

(1) System initialization (2) Data encryption upload (3) Abnormal data calculation (4) Return query response to the hospital

1) System initialization
   *$CS_2$ Initialization:*$CS_2$ chooses two large prime numbers $p$ and $q$, then $CS_2$ calculates $n = pq$, $g = n+1$, $\lambda = lcm(p-1, q-1)$, and defines the function as $L(x) = \frac{x-1}{n}$. Then, $CS_2$ calculates $\mu$ based on formula $\mu = (L(g^{\lambda} \bmod n^2))^{-1} \bmod n$. $CS_2$ will get the public key $pk_1 = (n, g)$ and the private key $sk_1 = (\lambda, \mu)$. $CS_2$ publishes the public key and keeps the private key.

   *Hospital Initialization:*Hospital chooses two large prime numbers $p'$ and $q'$. Hospital calculates $n' = p'q'$, $g' = n'+1$, $\lambda' = lcm(p'-1, q'-1)$, and defines the function as $L'(x) = \frac{x-1}{n'}$. Then, hospital calculates $\mu'$ based on formula $\mu' = (L'(g'^{\lambda'} \bmod n'^2))^{-1} \bmod n'$. Hospital will get the public key $pk_2 = (n', g')$ and the private key $sk_2 = (\lambda', \mu')$. Hospital publishes the public key and keeps the private key.
2) Encrypted data upload
   The hospital generates patient's own healthy heart rate range $[t_1, t_2]$ and the hospital encrypts it with the public key $pk_1$ distributed by $CS_2$ to generate $E(t_1)$ and $E(t_2)$. The patient uploads the data collected by the device $d = \{d_1, d_2, d_3 \ldots, d_l\}$, $i \in [1, l]$, (note: $d$ in the form of a numeric value), the patient encrypts the values in $d$ one by one using $pk_1$ distributed by $CS_2$ to generate $E(d_i)$, at the same time the patient generates a timestamp $T_1$ and then uploads them together to $CS_1$.
3) Abnormal data calculation
   First, before the $CS_1$ processes the ciphertext from the patient, the $CS_1$ needs to determine whether the ciphertext is a valid message at the current time. Therefore, the server generates a current time $T_2$ and does a difference calculation with the patient's timestamp with the following formula:

$$|T_1 - T_2| < \tau \tag{14}$$

   where $\tau$ is the threshold value. If Equation (14) is not satisfied, the patient data is proven not to be a valid ciphertext and it is discarded, otherwise, the patient information is proven to be a valid message and the server executes Algorithm 2. Note: Algorithm 1 is a larger-than-algorithm, so the first parameter should be larger than the second parameter when it is called.

**Algorithm 2** Cloud Server Computation (CSC)

```
Input: $E(t_1), E(t_2), E(h), E(d_i)\{i = 1, 2, \ldots, l\}$, $pk_1, pk_2, sk_1$
Output: $E'(Z)$
Initialize $E'(Z) = E'(0)$.
for $i = 1, 2, \ldots, l$ do
    Execute $PC(E(d_i), E(t_2))$
    $E'(z_i) = PC(E(d_i), E(t_2))$
    $E'(Z) = E'(Z) \cdot E'(z_i)$
end for
for $i = 1, 2, \ldots, l$ do
    Execute $PC(E(h - d_i), E(h - t_1))$
    $E'(z_i) = PC(E(h - d_i), E(h - t_1))$
    $E'(Z) = E'(Z) \cdot E'(z_i)$
end for
```

4) Return query response to the hospital
   $CS_2$ sends $E'(Z)$ to the hospital, which decrypts it with $sk_2$ to get $Z$, that is, we can get the number of abnormal heart rate data of patients in a period of time.

## V. SECURITY ANALYSIS

In this section, we will discuss the privacy protection of our scheme. According to our design goals, our scheme should protect the privacy of heart rate data, patient's own healthy heart rate range, specific values of abnormal heart rate, results, and be able to resist replay attacks on the database by malicious entities.

*Theorem 1: The proposed scheme ensures the privacy of every aspect of the entire monitoring process, patient's heart* *rate data, the patient's own healthy heart rate range, the intermediate parameters, and the results.*

*Proof:* The privacy of the entire monitoring process is maintained through the use of Paillier encryption. The patient's heart rate data, represented as $d = \{d_1, d_2, d_3 \ldots, d_l\}$, $i \in [1, l]$, is encrypted using the Paillier encryption algorithm before being uploaded to $CS_1$, ensuring that only the patient has access to the original data. Similarly, the patient's own healthy heart rate range is also encrypted using Paillier encryption to maintain its privacy. In this way, it is ensured that malicious entities are unable to infer patient information through their own healthy heart rate ranges, such as gender, age, etc. During the monitoring process, intermediate parameters are generated and transmitted between $CS_1$ and $CS_2$. To ensure their privacy, these parameters are also encrypted using Paillier encryption. The results calculated by $CS_2$ are encrypted using the hospital's key and uploaded to the hospital. This guarantees that the final result is only known to the hospital. And for hospital, hospital only know the total number of abnormal heart rates of patients, and do not know the specific abnormal heart rate data, which protects the privacy of patient's information. The Paillier homomorphic encryption algorithm is based on two mathematical problems, namely the Discrete Logarithm Problem (*DLP*) and the Modular Inversion Problem [17], [18], [19]. These problems provide a high degree of privacy, ensuring that the monitoring process is reliable and trustworthy.

*Theorem 2: The PC protocol should achieve privacy of intermediate parameters throughout the monitoring process, ensuring that no single server can calculate the results individually.*

*Proof:* We propose a privacy comparison protocol, which is a collaborative calculation method by two cloud servers, and the calculation of the whole remote monitoring process is done by $CS_1$ and $CS_2$ collaboratively, so that neither party can calculate the result alone. And the dual server protects the privacy and security of every step of the monitoring process compared to the single server. For $CS_1$, since it does not have the key of $CS_2$, it ensures the security of $t_2$ and $d_i$. For $CS_2$, $CS_2$ obtains $\theta_i$, because $\theta_i$ is perturbed by $p_i$, it has no way to know the relationship between the size of $t_2$ and $d_i$. And because $CS_2$ does not have the key of the hospital, the security of $E^{'}(z_i^x)$ is ensured, $CS_2$ has no way to know the final result after decryption. So our privacy comparison protocol ensures the privacy of the protocol input and the protocol result.

*Theorem 3: The scheme can resists database replay attacks by introducing timestamps.*

*Proof:* We solve this problem by introducing a timestamp method. When the patient uploads the encrypted data and also uploads a timestamp $T_1$, the cloud server can calculate the difference between the timestamp $T_1$ sent by the patient and the current time of the server $T_2$ before processing it, and if the difference is within the threshold value we set, the data sent by the patient is proved to be valid, and the cloud server will only perform the next operation on the ciphertext sent by the patient. This will be able to effectively resist replay attacks by malicious people.

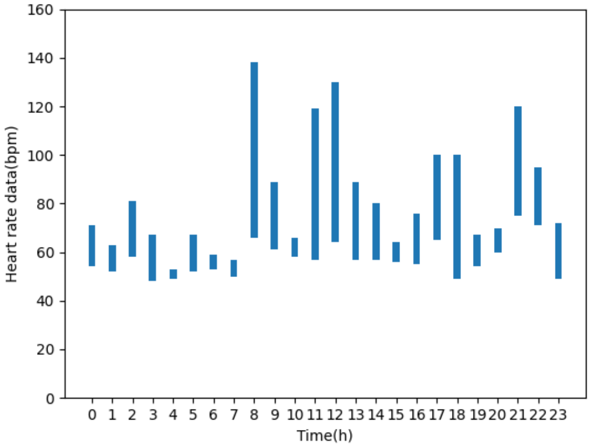

**FIGURE 2.** Heart rate data during the day.

## VI. PERFORMANCE EVALUATION

In this section, we confirm the effectiveness of the scheme through detailed experimental results, and the communication overhead required for the implementation of the scheme is small.

### A. EXPERIMENTAL SETTING

The scheme was implemented in Python3.6 and evaluated on a machine with 8GB memory. Parameters required for this experiment are as follows: private key size k, patient heart rate data n=100,150,200,250,300. Our experimental data is the result of many tests, we take the patient's heartbeat value once every 1 minute on average, the specific experimental analysis is as follows:

### B. ABNORMAL HEART RATE MONITORING

Figure.2 shows the collected heart rate data of the patient within 24h, which is encrypted and uploaded. Through the experiment, we can get the number of abnormal heart rate data of the patient within 24h plotted as Figure.3. From Figure.3 we can analyze that the number of abnormal heartbeats of the patient before waking up in the morning and before sleeping at night is significantly increased. Therefore, the patient should pay more attention to the health protection of these two time periods. Our scheme can protect the original heart rate data of the patient at the same time, the doctor can get the accurate health information about the patient through monitoring to make a more effective treatment plan.

### C. COMPARISON EXPERIMENT

To show the effectiveness of our scheme, we compare our scheme with CEP [20].

- *Encryption time.* In order to illustrate the effectiveness of our scheme, we compare our scheme with CEP, and

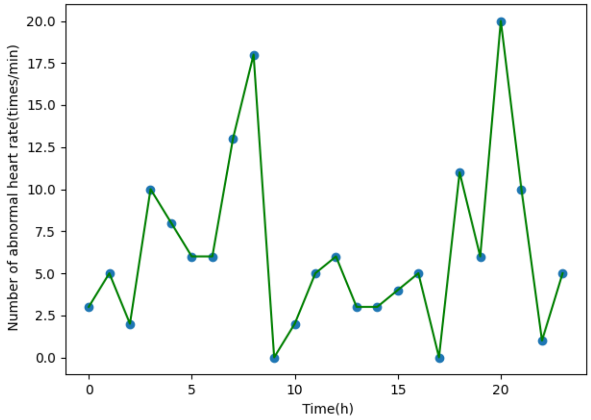

**FIGURE 3.** Number of abnormal heart rate during the day.

it can be seen from Fig. 4 that our scheme outperforms CEP in terms of efficiency of encryption.The schemes are both privacy-protecting the data through homomorphic encryption.The CEP scheme introduces BGN homomorphic encryption for the privacy and security of the data. The BGN encryption, although relatively secure, takes longer time to encrypt the data because of the need for its noise adjustment and requires polynomial operation. Moreover, its scheme transforms the data into a matrix structure, there is a lot of encryption processing of vectors, and needs time-consuming pairing operations. In contrast, we use paillier encryption to encrypt the data directly, which also ensures data privacy, with a relatively small amount of computation and without need pairing operations. In the case of processing small exponent, the advantages of our scheme are more obvious. Our heart rate data usually belongs to the small exponent, so the paillier encryption used in this scheme belongs to the process of the small exponent, we get the encryption time for the small exponent is 0.009s on average through many times of testing, which is much smaller than the average encryption time of the paillier encryption for the large exponent in the usual situation, i.e., 0.09s. Therefore, the process of the small exponent will not produce a significant time overhead and is more effective. Meanwhile, this scheme adopts a parameter-optimized encryption scheme, i.e., $g = n + 1$, which can improve the encryption efficiency even more while maintaining the same security as the original paillier encryption.

- *The computational time.* Figure.5 shows the comparison between our scheme and CEP in terms of computation time, and experiments show that our scheme is more effective than CEP in terms of computation time. The CEP scheme uses BGN homomorphic encryption for data privacy security, which is based on operations on polynomial rings, and spends a large amount of time on polynomial operations and NTT transformations. Moreover, the scheme transforms the data into a matrix structure, there exists a large number of encryption and decryption processes on vectors, and needs time-consuming pairing operations. In our scheme, the data is processed directly, which reduces the time-consuming pairing operation. Moreover, the paillier homomorphic encryption is used to protect the privacy of the data, which is relatively small in terms of computation while also ensuring the privacy and security of the data processing process. What's more, our scheme adopts a dual-server model, and the final results are computed with the assistance of two cloud servers, $CS_1$ and $CS_2$. Therefore, in the whole monitoring process, no single entity can calculate the final result alone, which is more secure compared to the single server used in the CEP scheme.

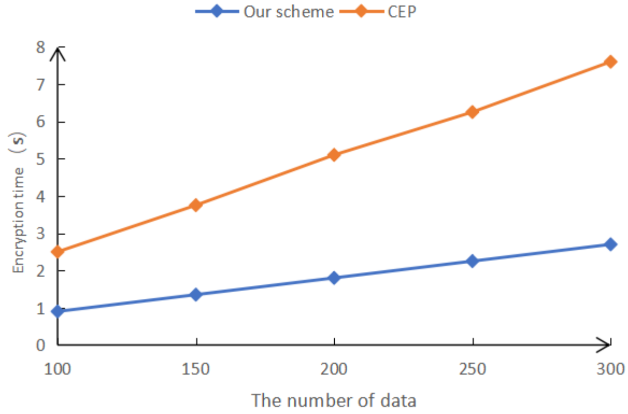

**FIGURE 4.** Encryption time.

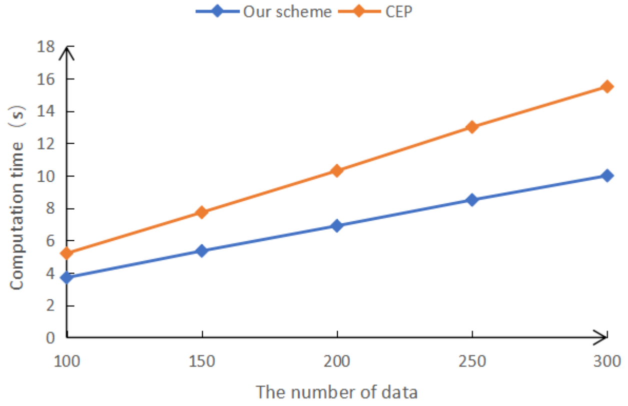

**FIGURE 5.** Computational time.

## VII. RELATED WORK

In this paper, we address the issue of privacy protection in the context of conducting effective health status monitoring. In the following, we review related work on privacy protection in healthcare systems.

Health condition monitoring is one of the most important applications of artificial intelligence technology. One of the most important is the monitoring of heart rate, the number of heartbeats per minute we call heart rate or pulse. It is one of the indicators to monitor health, and if the heart rate is not in the normal range, it can induce many diseases. Therefore, many methods of remote monitoring of heart rate have been proposed. For example, Rasheed et al. [21] proposed a wearable autonomous heart rate sensor that can be used for multi-point monitoring to monitor the patient's heart rate in real time. But it has the problem of privacy protection of the patient's heart rate information. To solve this problem, Lu et al. [22] proposed a SPOC framework scheme, which ensured efficient user-centric privacy access control by introducing a user-centric privacy control in the framework. By using IoT sensors and machine learning, medical centers can monitor patients' health status remotely and respond to emergencies in a timely manner. In order to solve the problem of privacy protection in this process, Li et al. [23] studied the data privacy protection algorithm for wireless sensor networks. Panda et al. [24] proposed a scheme for a blockchain emergency monitoring system, which is implemented through blockchain. This scheme uses the blockchain approach, so it has the problem of real-time, and the cost of maintaining the blockchain is relatively large, which brings a large overhead. Yang et al. [25] ensured efficient monitoring of human body conditions, such as heart rate information, by introducing differential privacy in human health monitoring, which effectively ensured the privacy protection of health data and also ensured that the privacy of human data was not maliciously leaked. However, user's data are stored in the database, which may be curious about the user's information. And smart wearable devices usually have small storage capacity and computing power, which may limit the functionality and performance of the devices. With the development of science, architectures for building telemedicine are becoming more sophisticated, Sokolova and Buldakova [26] proposed a detailed network architecture for telemedicine systems used to monitor a person's condition. And with the development of cloud computing and fog computing, more and more privacy protection schemes have been proposed [20], [27], [28], [29], [30]. At the same time, more telemedicine system schemes have been proposed. Hochreiter and Schmidhuber [31] constructed a network architecture in conjunction with a long neural network, and Kalyan et al. [32] proposed a non-invasive on-line heart rate monitoring system. In the detailed telemedicine framework, most schemes use a single-server approach [33], [34], but compared to the dual cloud server, they are less secure. Wang et al. [35] proposes a dual cloud server scheme, but it uses symmetric homomorphic encryption to encrypt data, and its security is relatively weaker than homomorphic encryption.

## VIII. CONCLUSION

In this paper, we propose a privacy-preserving scheme for remote heart rate abnormality monitoring system. This scheme protects the privacy of the patient's heart rate data, the patient's own healthy heart rate range, and the final monitoring results by using Paillier homomorphic encryption. The final result of the scheme will only reflect whether the patient's heart rate data is normal or not, it will not show what the specific value is. With this approach, a doctor can learn the number of final abnormal heart rates without knowing the patient's original heart rate data, and provide the patient with appropriate protective advice. Moreover, malicious entities cannot infer the patient's personal information, such as occupation and gender, from the patient's heart rate range and the value of the specific abnormal heart rate, thus protecting the privacy of the patient's personal information even more. In order to better improve the security of this scheme, i.e., to ensure the privacy and security of each step in the whole monitoring process, we propose a model of dual cloud server-assisted computing. And we propose a privacy comparison protocol (PC) based on this model. In this protocol, we convert the determination of whether the heart rate value is within the patient's own healthy heart rate range into a comparison between the heart rate value and the upper and lower bounds values of patient's own healthy heart rate range. And since the results are calculated by the two servers collaboratively, neither of the two servers can calculate the results individually without colluding with each other, this is more protective of results than a single server. The experimental results show that the proposed scheme is effective, and in addition, we analyze the security of our scheme, and the results show that it can achieve the security design goals.

## REFERENCES

[1] J. Huang, S. Lin, N. Wang, G. Dai, Y. Xie, and J. Zhou, "TSE-CNN: A two-stage end-to-end CNN for human activity recognition," *IEEE J. Biomed. Health Informat.*, vol. 24, no. 1, pp. 292–299, Jan. 2020, doi: 10.1109/JBHI.2019.2909688.

[2] J. Liang, Z. Qin, S. Xiao, J. Zhang, H. Yin, and K. Li, "Privacy-preserving range query over multi-source electronic health records in public clouds," *J. Parallel Distrib. Comput.*, vol. 135, pp. 127–139, Jan. 2020.

[3] M. Pettai and P. Laud, "Combining differential privacy and secure multiparty computation," in *Proc. 31st Annu. Comput. Secur. Appl. Conf.*, Dec. 2015, pp. 17–19, doi: 10.1145/2818000.2818027.

[4] Y. Zhou, Y. Tian, F. Liu, J. Liu, and Y. Zhu, "Privacy preserving distributed data mining based on secure multi-party computation," in *Proc. IEEE 11th Int. Conf. Adv. Infocomm Technol. (ICAIT)*, Oct. 2019, pp. 173–178, doi: 10.1109/ICAIT.2019.8935900.

[5] M. Tebaa, S. E. Hajji, and A. E. Ghazi, "Homomorphic encryption applied to the cloud computing security," in *Proc. World Congr. Eng.*, vol. 1, no. 1. London, U.K., 2012, pp. 4–6.

[6] S. J. Mohammed and D. B. Taha, "Performance evaluation of RSA, ElGamal, and Paillier partial homomorphic encryption algorithms," in *Proc. Int. Conf. Comput. Sci. Softw. Eng. (CSASE)*, Mar. 2022, pp. 89–94, doi: 10.1109/CSASE51777.2022.9759825.

[7] Z. H. Mahmood and M. K. Ibrahem, "New fully homomorphic encryption scheme based on multistage partial homomorphic encryption applied in cloud computing," in *Proc. 1st Annu. Int. Conf. Inf. Sci. (AiCIS)*, Nov. 2018, pp. 182–186, doi: 10.1109/AiCIS.2018.00043.

[8] N. Dawar and N. Kehtarnavaz, "A convolutional neural network-based sensor fusion system for monitoring transition movements in healthcare applications," in *Proc. IEEE 14th Int. Conf. Control Autom. (ICCA)*, Jun. 2018, pp. 482–485, doi: 10.1109/ICCA.2018.8444326.

[9] J. Liu, J. Yang, L. Xiong, and J. Pei, "Secure skyline queries on cloud platform," in *Proc. IEEE 33rd Int. Conf. Data Eng. (ICDE)*, Apr. 2017, pp. 633–644, doi: 10.1109/ICDE.2017.117.

[10] S. Zhang, S. Ray, R. Lu, Y. Zheng, Y. Guan, and J. Shao, ''Towards efficient and privacy-preserving user-defined skyline query over single cloud,'' *IEEE Trans. Depend. Secure Comput.*, vol. 20, no. 2, pp. 1319–1334, Mar. 2023, doi: 10.1109/TDSC.2022.3153790.

[11] S. Zhang, S. Ray, R. Lu, and Y. Guan, ''PPsky: Privacy-preserving skyline queries with secret sharing in eHealthcare,'' in *Proc. GLOBECOM IEEE Global Commun. Conf.*, Dec. 2022, pp. 5469–5474, doi: 10.1109/GLOBECOM48099.2022.10000905.

[12] S. Paliwal, C. V. Lakshmi, and C. Patvardhan, ''Real time heart rate detection and heart rate variability calculation,'' in *Proc. IEEE Region 10 Humanitarian Technol. Conf. (R-HTC)*, Dec. 2016, pp. 1–4, doi: 10.1109/R10-HTC.2016.7906818.

[13] H.-Y. Kwon and M.-K. Lee, ''Comments on 'PassBio: Privacy-preserving user-centric biometric authentication,''' *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 2816–2817, 2022, doi: 10.1109/TIFS.2022.3195380.

[14] Y. Liu, Y. Yang, Z. Ma, X. Liu, Z. Wang, and S. Ma, ''PE-HEALTH: Enabling fully encrypted CNN for health monitor with optimized communication,'' in *Proc. IEEE/ACM 28th Int. Symp. Quality Service (IWQoS)*, Jun. 2020, pp. 1–10, doi: 10.1109/IWQoS49365.2020.9212822.

[15] J. Hua, H. Zhu, F. Wang, X. Liu, R. Lu, H. Li, and Y. Zhang, ''CINEMA: Efficient and privacy-preserving online medical primary diagnosis with skyline query,'' *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1450–1461, Apr. 2019, doi: 10.1109/JIOT.2018.2834156.

[16] A. Alnemari, R. K. Raj, C. J. Romanowski, and S. Mishra, ''Interactive range queries for healthcare data under differential privacy,'' in *Proc. IEEE 9th Int. Conf. Healthcare Informat. (ICHI)*, Aug. 2021, pp. 228–237, doi: 10.1109/ICHI52183.2021.00044.

[17] M. Nassar, A. Erradi, and Q. M. Malluhi, ''Paillier's encryption: Implementation and cloud applications,'' in *Proc. Int. Conf. Appl. Res. Comput. Sci. Eng.*, 2015, pp. 1–5, doi: 10.1109/ARCSE.2015.7338149.

[18] M. Zheng, Y. Cui, and L. Chen, ''Security analysis of a Paillier-based threshold proxy signature scheme,'' in *Proc. 12th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Jul. 2013, pp. 683–687, doi: 10.1109/TrustCom.2013.83.

[19] X. Liang, R. Lu, L. Chen, X. Lin, and X. Shen, ''PEC: A privacy-preserving emergency call scheme for mobile healthcare social networks,'' *J. Commun. Netw.*, vol. 13, no. 2, pp. 102–112, Apr. 2011, doi: 10.1109/JCN.2011.6157409.

[20] R. Lu, ''A new communication-efficient privacy-preserving range query scheme in fog-enhanced IoT,'' *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2497–2505, Apr. 2019, doi: 10.1109/JIOT.2018.2871204.

[21] A. Rasheed, E. Iranmanesh, W. Li, H. Ou, A. S. Andrenko, and K. Wang, ''A wearable autonomous heart rate sensor based on piezoelectric-charge-gated thin-film transistor for continuous multi-point monitoring,'' in *Proc. 39th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBC)*, Jul. 2017, pp. 3281–3284, doi: 10.1109/EMBC.2017.8037557.

[22] R. Lu, X. Lin, and X. Shen, ''SPOC: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency,'' *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 3, pp. 614–624, Mar. 2013, doi: 10.1109/TPDS.2012.146.

[23] P. Li, C. Xu, H. Xu, L. Dong, and R. Wang, ''Research on data privacy protection algorithm with homomorphism mechanism based on redundant slice technology in wireless sensor networks,'' *China Commun.*, vol. 16, no. 5, pp. 158–170, May 2019, doi: 10.23919/j.cc.2019.05.012.

[24] S. Panda, A. Mukherjee, R. Halder, and S. Mondal, ''Blockchain-enabled emergency detection and response in mobile healthcare system,'' in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2022, pp. 1–5, doi: 10.1109/ICBC54727.2022.9805544.

[25] M. Yang, J. Guo, and L. Bai, ''A data privacy-preserving method for students' physical health monitoring by using smart wearable devices,'' in *Proc. IEEE Int. Conf Depend., Autonomic Secure Comput., Int. Conf. Pervasive Intell. Comput., Int. Conf Cloud Big Data Comput., Int. Conf Cyber Sci. Technol. Congr. (DASC/PiCom/CBDCom/CyberSciTech)*, Aug. 2020, pp. 29–34, doi: 10.1109/DASC-PICom-CBDCom-CyberSciTech49142.2020.00021.

[26] A. V. Sokolova and T. I. Buldakova, ''Network architecture of telemedicine system for monitoring the Person's condition,'' in *Proc. 3rd Int. Conf. Control Syst., Math. Modeling, Autom. Energy Efficiency (SUMMA)*, Nov. 2021, pp. 361–365, doi: 10.1109/SUMMA53307.2021.9632199.

[27] T. Li, Y. Liu, N. N. Xiong, A. Liu, Z. Cai, and H. Song, ''Privacy-preserving protocol for sink node location in telemedicine networks,'' *IEEE Access*, vol. 6, pp. 42886–42903, 2018, doi: 10.1109/ACCESS.2018.2858274.

[28] G. A. Macriga, S. R. L. Siddarth, and P. Sivadinesh, ''Monitoring real time data and secure retrieval for telemedicine systems,'' in *Proc. Int. Conf. Smart Syst. Inventive Technol. (ICSSIT)*, Nov. 2019, pp. 552–556, doi: 10.1109/ICSSIT46314.2019.8987813.

[29] S. S. Sahoo and S. Mohanty, ''Cloud-assisted privacy preserving authentication scheme for telecare medical information systems,'' in *Proc. IEEE Int. Conf. Adv. Netw. Telecommun. Syst. (ANTS)*, Dec. 2018, pp. 1–6, doi: 10.1109/ANTS.2018.8710128.

[30] M. Bian, G. He, G. Feng, X. Zhang, and Y. Ren, ''Verifiable privacy-preserving heart rate estimation based on LSTM,'' *IEEE Internet Things J.*, early access, Jun. 29, 2023, doi: 10.1109/JIOT.2023.3290651.

[31] S. Hochreiter and J. Schmidhuber, ''Long short-term memory,'' *Neural Comput.*, vol. 9, no. 8, pp. 1735–1780, Nov. 1997.

[32] K. Kalyan, V. K. Chugh, and C. S. Anoop, ''Non-invasive heart rate monitoring system using giant magneto resistance sensor,'' in *Proc. 38th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBC)*, Aug. 2016, pp. 4873–4876, doi: 10.1109/EMBC.2016.7591819.

[33] D. Zhu, H. Zhu, C. Huang, R. Lu, D. Feng, and X. Shen, ''Efficient and accurate cloud-assisted medical pre-diagnosis with privacy preservation,'' *IEEE Trans. Depend. Secure Comput.*, early access, Apr. 3, 2023, doi: 10.1109/TDSC.2023.3263974.

[34] M. Zalloum and H. Alamleh, ''Privacy preserving architecture for healthcare information systems,'' in *Proc. IEEE Int. Conf. Commun., Netw. Satell. (Comnetsat)*, Dec. 2020, pp. 429–432, doi: 10.1109/Comnetsat50391.2020.9328985.

[35] W. Wang, Y. Jin, and B. Cao, ''An efficient and privacy-preserving range query over encrypted cloud data,'' in *Proc. 19th Annu. Int. Conf. Privacy, Secur. Trust (PST)*, Aug. 2022, pp. 1–10, doi: 10.1109/PST55820.2022.9851989.

**JIANHONG ZHANG** received the Ph.D. degree from Xidian University, in 2004. He is currently a Professor with the School of Information Sciences and Technology, North China University of Technology. His research interests include big data privacy, cloud security, and the IoT security.

**HAOWEI YANG** received the B.S. degree in information and control from the Qingdao University of Technology, in 2021. She is currently pursuing the master's degree with the School of Information Sciences and Technology, North China University of Technology. Her current research interests include data security and cryptography.