IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 24, 2017, accepted June 5, 2017, date of publication June 22, 2017, date of current version July 24, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2716439

A Secure Privacy-Preserving Data Aggregation Scheme Based on Bilinear ElGamal Cryptosystem for Remote Health Monitoring Systems

ANEES ARA, Jr., (Member, IEEE), MZNAH AL-RODHAAN, YUAN TIAN, AND ABDULLAH AL-DHELAAN

Department of Computer Science, College of Computers and Information Sciences, King Saud University, Riyadh 11453, Saudi Arabia

Corresponding author: Anees Ara (aahamed@ksu.edu.sa)

This work was supported by the Deanship of Scientific Research at King Saud University, Riyadh, Saudi Arabia, through the Research Group RGP-264.

ABSTRACT Due to advancements in the development of wireless medical sensing devices and wireless communication technologies, the wireless body area network (WBAN) has become an eminent part of e-healthcare systems. WBAN uses medical sensors to continuously monitor and collect the physiological parameters of a patient's health and send them to a remote medical server through a portable digital assistance (PDA)/mobile. Due to limitations in communication, such as power, storage, and the computational capabilities of sensors, data aggregation techniques are used to reduce the communication overhead in real-time data transmission in WBAN. However, since the WBAN transmits sensitive health data, data security and data privacy are a major concern. In this paper, we propose a secure privacy-preserving data aggregation (SPPDA) scheme based on bilinear pairing for remote health monitoring systems to improve data aggregation efficiency and data privacy. Our proposed SPPDA scheme utilizes the homomorphic property of the bilinear ElGamal cryptosystem to perform privacy-preserving secure computation and combines it with the aggregate signature scheme, enabling data authenticity/integrity in the WBAN. The proposed SPPDA scheme is proved to be semantically secure under the decisional bilinear Diffie–Hellman assumption. Security analysis demonstrates that our proposed scheme preserves data confidentiality, data authenticity, and data privacy; it also resists passive eavesdropping and replay attacks. A performance evaluation based on simulation results and a comparison of computational cost with related schemes show that data aggregation and batch verification at the PDA significantly reduce communication and transmission overhead and support efficient computation at the remote server.

INDEX TERMS Wireless body area network, remote health monitoring system, secure data aggregation, bilinear pairing, bilinear ElGamal cryptosystem, homomorphic encryption, aggregate signature, batch verification.

I. INTRODUCTION

Recent advancements in cyber-physical systems (CPS), wireless sensing and communication technologies and their seamless integration in the present day world have led to the development of a wide range of applications in areas such as environmental monitoring, industrial monitoring, and real-time remote health monitoring systems. The Wireless Body Area Network (WBAN) is one such combination of tiny wearable devices referred to as medical sensors attached to a patient's body in remote health monitoring systems. The WBAN is used to monitor patient's physiological parameters such as temperature, blood pressure, and electrocardiography (ECG). Medical sensors continuously monitor and collect patient's data and send them to a remote medical server through a local processing unit (LPU) like a PDA/mobile.

The WBAN consists of small medical sensors that have scarce resources in terms of memory, energy, and storage and that communicates wirelessly with an LPU. The LPU has more resources than sensors but is still limited, as it uses the battery and communicates wirelessly with the medical server. The medical server is very powerful in terms of energy, computational power, and storage. As such, the WBAN is deployed in a hostile environment, where sensors may be

2169-3536 © 2017 IEEE. Translations and content mining are permitted for academic research only.
Personal use is also permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

incapable of providing reliable functions or can be easily compromised by malicious adversaries; thus sensitive health data may be subject to privacy issues, or data misusage may also occur [1]. According to Health Insurance Portability and Accountability (HIPAA) [2], it is mandatory to protect all sensitive medical data pertaining to a particular patient's health. Therefore, privacy preservation of sensitive health data is a legal requirement. Hence, it is very important to protect sensitive health data against eavesdropping, false injections and forgery. Unrestricted access to personal health data leads to privacy violations, while selective reporting, impersonating and masquerading leads to incorrect diagnosis and treatment of the patient who is remotely monitored.

Data aggregation is an essential technique to eliminate data redundancy and reduce energy consumption. In the data aggregation process, the sensor nodes are organized as a tree, rooted at the base station. The intermediate nodes aggregate the data from the leaf nodes and then forward the aggregated result to the base station. However, data aggregation is challengeable in some applications such as remote health monitoring systems. The sensor nodes are often deployed in hostile environments with low bandwidth and insecure communication channels. This may lead to malicious data modifications and data forgery, resulting in the violation of a user's privacy. For example, an attacker might forge a fake alarming reading and have it distributed in the network to degrade network performance. In addition, privacy is also a primary concern in remote health monitoring systems, as health data are highly relevant to the patient being monitored. For example, motion sensors can reflect certain behavior, such as walking, sleeping, and having a meal. As a result, the disclosure of such health data violates user data privacy. Therefore, how to efficiently aggregate different types of data and preserve patient privacy is a challenging task in a resource constrained WBAN.

In order to overcome the above-stated issues of security and privacy regarding medical health data during transmission and data aggregation in WBAN, we propose a bilinear pairing-based Secure Privacy-Preserving Data Aggregation (SPPDA) scheme for a remote health monitoring system. With this proposed scheme, we identify the necessary security and privacy requirements in the WBAN. In particular, we point out the necessity for an end-to-end secure data transmission from medical sensors to the remote medical server in the WBAN.

The contributions of this paper can be summarized as follows:

- We propose a Secure Privacy-Preserving Data Aggregation (SPPDA) scheme based on bilinear pairing for remote health monitoring systems. Our proposed SPPDA scheme ensures data confidentiality, data privacy and data authenticity by combining pairing based homomorphic encryption scheme and aggregate signature scheme in WBAN.
- We use data aggregation technique at the LPU in WBAN, to reduce the overall communication cost in our proposed scheme. To improve the efficiency and reduce computational complexity of the proposed scheme, computationally heavy pairing-based operations like key generations and decryption are shifted to the remote medical server, which is quite powerful in terms of energy, computational power, and storage. Hence, data aggregation efficiency and data accuracy is assured in our proposed scheme.
- We conduct a security analysis to state and prove the correctness of the proposed scheme. The proposed SPPDA scheme is proven to be semantically secure under the Decisional Bilinear Diffie-Hellman (DBDH) assumption. Security analysis also demonstrates that our proposed scheme preserves data confidentiality, data authenticity, and data privacy; it also resists passive eavesdropping and replay attacks. A performance evaluation based on simulation results and a comparison of computational cost with related schemes show that data aggregation and batch verification at the PDA significantly reduce communication and transmission overhead and support efficient computation at the remote server.

The rest of the paper is organized as follows. In Section II, related works are presented. Section III describes the system model, security requirements and the design goals of the proposed scheme. We introduce the preliminary knowledge on the cryptographic techniques used for our scheme in Section IV. In Section V, an overview of the proposed scheme and basic notation followed by the main construction of our proposed SPPDA scheme are discussed. Also, in Sections VI and VII, we present the security analysis and performance evaluation for our proposed scheme. Finally, Section VIII concludes the paper and discusses future research directions.

II. RELATED WORKS

In this section, we first explain the concept of data aggregation and the importance of security and privacy in this concern. Later, we put our emphasis on the discussion of some other literature related to our research which also achieves security, privacy-preservation and/or data integrity for WBAN.

A. DATA AGGREGATION

The data aggregation process has the benefit of achieving efficiency in bandwidth and energy in resource-constrained sensor networks. The sensors are deployed in hostile environments; hence, security and privacy are a major concern. Therefore, privacy-preserving secure data aggregation has become a hot research problem in various applications of sensor networks including remote health monitoring systems, smart grids, industrial monitoring systems and intelligent transport systems. The standard method to preserve the confidentiality of data is by encrypting it. Secure data aggregation protocols can be categorized as hop-by-hop encryption protocols and end-to-end encryption protocols [3], [4].

In hop-by-hop encryption protocols, the aggregator has to decrypt the message and then aggregate it. In end-to-end encryption protocols, the intermediate nodes aggregate the data without decrypting it. The end-to-end data aggregation scheme saves 70% of the data transmission energy [5].

Privacy homomorphism is the general method of an encryption transformation that allows direct computation on the encrypted data [4]. The first privacy homomorphism encryption transformation was done by Rivest *et al.* [6]. In WSN, this privacy homomorphism is applied for concealing in-network data processing at the intermediate aggregator node. Such a process is called concealed data aggregation (CDA) with privacy homomorphism [4]. The concealed data aggregation schemes based on symmetric homomorphism suffer from tedious key management problems compared with the schemes based on asymmetric homomorphism, which uses simple public/private keying techniques [4]. Elliptical curve cryptography in combination with bilinear pairing has emerged as a viable option for asymmetric cryptography in various applications of wireless sensor networks, WBAN being one among them. Due to the small key size, compact signatures and efficient security provided by pairing-based cryptographic techniques, these pairing-based cryptosystems are vastly studied and implemented in wireless sensor networks [7], [8]. Additionally, various secure data aggregation schemes [9] and [10] authentication and key management schemes [11] based on ECC and pairing were proposed in the literature.

B. SECURITY AND PRIVACY-PRESERVATION

Exploring simple cryptographic privacy techniques, Lu *et al.* [12], proposed an efficient and privacy preserving data aggregation (EPPA) scheme based on Paillier cryptosystem. The authors structure multidimensional data into one ciphertext by using super-increasing sequence. Similarly, Zhang *et al.* [10] proposed a priority based privacy-preserving data aggregation (PHDA) scheme for WBAN. They also used a bilinear pairing-based Paillier cryptosystem, an additively homomorphic cryptosystem, to achieve privacy in data aggregation. Same as [12], they used super-increasing sequences to combine multi-dimensional data into one ciphertext. Lin *et al.* [13], proposed a data aggregation scheme that employs the super-increasing sequence and perturbation techniques to achieve multidimensional aggregation. Chen *et al.* [14], proposed a multifunctional data aggregation (MuDA) scheme. The authors applied BGN cryptosystem for privacy preserving data aggregation. Although MuDA scheme supports statistical functions through multifunctional aggregations, it does not assure data authenticity and integrity during data aggregation.

Ren *et al.* [15], proposed sensitive data aggregation scheme based on data hiding in WBAN. They applied lossless compression techniques on the sensitive data and then combine them with other ordinary data, to reduce the transmission energy consumption and prevent disclosure of sensitive data respectively. Subsequently, Othman *et al.* [16], proposed a compressed sensing based secure data transmission protocol for WBAN. Zhu *et al.* [17], proposed a privacy-preserving data collection and query scheme for body sensor networks. They have used bilinear pairing based DNF cryptosystem for secure data collection.

Additionally, Zhou *et al.* [18] compare the techniques of secure multiparty computation, fully homomorphic encryption, and a one way trap-door function in the paradigms of privacy-preserving data aggregation and outsourced verifiable computations in a cloud assisted WBAN. More recently, Kocabas *et al.* [19] surveyed various emerging encryption schemes based on secure storage, secure sharing and secure computations for medical cyber-physical systems (MCPS). The authors compared the implementation of conventional encryption schemes such as AES and ECIES for secure storage, attribute-based encryption schemes such as CP-ABE for secure data sharing and homomorphic encryption schemes such as Paillier cryptosystem and BGV scheme for secure computations on MCPS. However, the authors suggested that none of the schemes were fit for designing the WBAN supported MCPS.

Therefore, from the above study, it can be noted that none of the above privacy preserving schemes covered data integrity assurance aspect during secure data aggregation.

C. INTEGRITY ASSURANCE

Liu *et al.* [20] proposed a bilinear pairing based Certificateless Signature Scheme (CLS) for a WBAN. They proved that the CLS scheme is unforgeable against adaptive chosen message attack under the assumption of the computational Diffie-Hellman problem. Zhou *et al.* [21] proposed a privacy-preserving key management scheme for a cloud assisted WBAN. They used a blinding technique and embedded a human body's symmetric structure into a blow's symmetric key structure to ensure the privacy of the patient's id, sensor deployment, and location privacy. Yang *et al.* [22] proposed a bilinear pairing-based privacy preserving authentication scheme with adaptive key evolution in a remote health monitoring system. They modeled the key information leakage process to set proper key renewal intervals and controlled adaptive key evolution through it [22]. To ensure data authenticity and integrity in a WBAN, Shen *et al.* [23] proposed a collision resistant aggregate signature scheme. The security model was based on [24] in combination with coalition attacks. Similarly, Wang et al proposed a bilinear pairing-based privacy-preserving remote data integrity checking and sharing (ICS) protocol for cloud assisted WBAN [25]. They proved that the ICS protocol is existentially unforgeable based on the computational Diffie-Hellman assumption and that it satisfies the security property of restrictive irretrievability and provable data integrity against malicious public cloud servers. However, these schemes do not facilitate techniques for providing confidentiality of data.

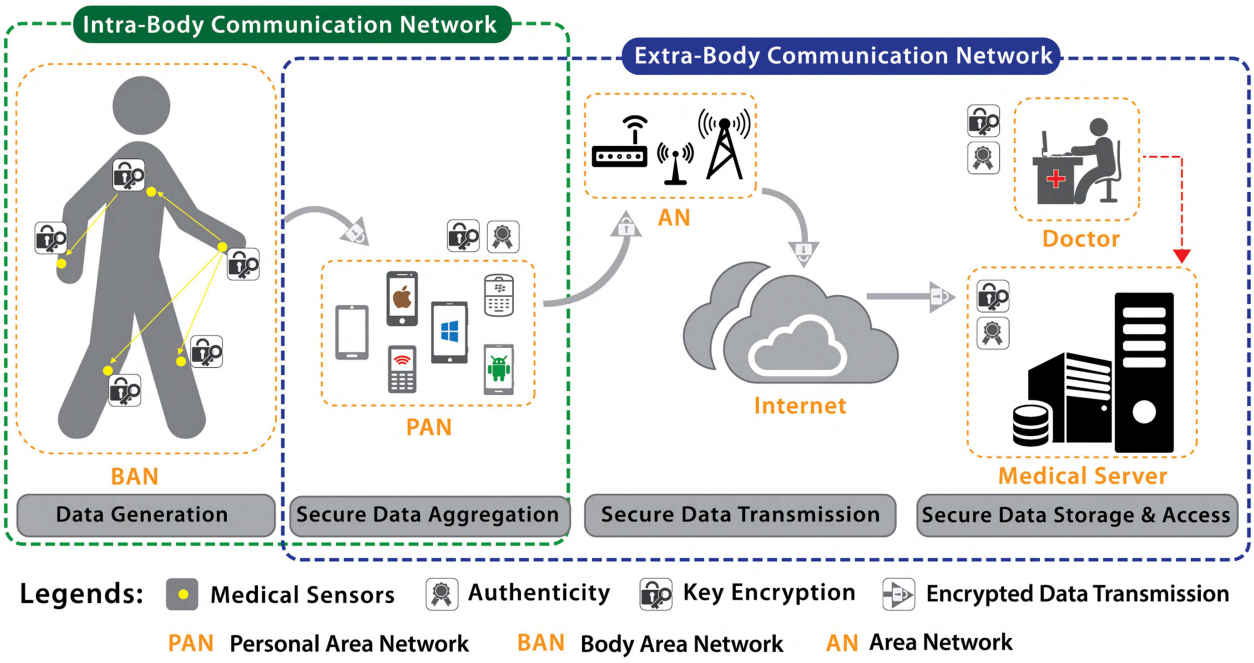

FIGURE 1. Overview of secure remote health monitoring system based on a WBAN.

D. CONFIDENTIALITY AND INTEGRITY ASSURED PRIVACY-PRESERVATION

Zhu *et al.* [26] proposed secure data aggregation scheme based on homomorphic encryption and message authentication code (MAC), to preserve confidentiality and integrity of data. Sun *et al.* [9] proposed a privacy-preserving scheme in emergency response based on a WBAN. For the privacy of the scheme, the authors use anonymous credentials based on Pederson's commitment and proof of knowledge. They make use of bilinear pairing-based signatures for the authenticity of the data. Although their work supports confidentiality, privacy and integrity but unfortunately, their scheme does not support in-network data aggregation in WBAN.

To conclude, it is observed that most of the schemes were focused only on some security requirements but not all. Hence, it is required to design a new data aggregation scheme that supports most of the security requirements such as confidentiality, data authenticity and integrity and end-to-end data privacy in remote health monitoring systems. The new scheme should be efficient and scalable in terms of computational complexity and meet the security standards. Although our proposed SPPDA scheme addresses the same issues as the above literatures to provide confidentiality and integrity assured privacy preserving data aggregation in WBAN, our research focuses on i) in our SPPDA scheme, the security is ensured both at data acquisition, data aggregation and data transmission phases; and ii) Our proposed scheme is efficient and scalable and achieves confidentiality, data authenticity, integrity and end-to-end data privacy in remote health monitoring systems.

III. PROBLEM FORMALIZATION

In this section, we formalize our research problems in WBANs, including system model, communication model, adversary model, security requirements, and design goals.

A. SYSTEM MODEL

In our system model, we consider a WBAN-based remote health monitoring system to monitor a patient's health residing at the remote location. This includes a Medical Server (which is accessed by the trusted authority TA), an aggregator (here LPU), and the sensing nodes $SN = \{s_1, s_2, ..., s_k\}$, (wearable medical sensors). In this system, we focus on collection and transmission of the patient's privacy-preserving health data to the medical server. Specifically, this process can be done in three stages such as secure data aggregation, secure data transmission and secure data storage and access as described in Fig. 1.

The stake holders of the remote health monitoring system are:

- ***Sensing Nodes (SN)***, denoted by $SN = \{s_1, s_2, ..., s_k\}$, (where '$k$' is the allowable number of sensors on a patient's body) are the wearable sensors on the patient's body; these sensors sense the patient's data, such as ECG sensor, blood pressure sensor, motion sensor, pulse oximetry sensor. The sensing nodes are responsible for reporting the sensed health data to the aggregator.
- ***Aggregator (LPU)*** is connected wirelessly to the medical sensors (SN). Its job is to collect the individual health data and compute the aggregation on them.

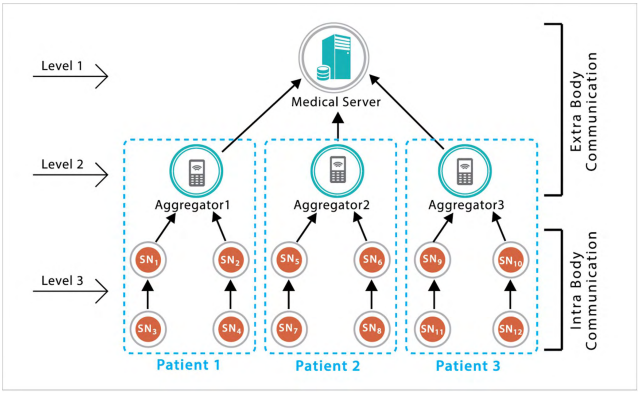

FIGURE 2. Network model.

Consequently, the aggregated data are reported to the remote medical server. The LPU will aggregate each user's health data and report the aggregated data to the remote medical server honestly, but it is also curious about the individual sensor's readings.

- ***Medical server (MS)*** represents an individual server in the remote health monitoring system. We consider a scenario where the medical server can be accessed by the trusted authorities and the concerned doctor/emergency medical team.

The network model in Fig. 2 depicts the data aggregation process in a remote health monitoring system. It follows the bottom-up approach for the transmission of medical health data from the patient to the medical server in stages of level 1, 2 and 3 respectively.

We recognize the WBAN based remote health monitoring system as a two-tier communication network (as depicted in Fig. 1):

1) The *Intra-body communication network* is responsible for secure data generation for every given epoch of time. It comprises of an aggregator connected with a set of sensing nodes given by $SN = \{s_1, s_2, \ldots, s_k\}$, as shown in Fig. 2. Each sensing node (SN) can electronically record the continuous real-time data regarding physiological measures on a patient's body. For secure data generation, the sensing nodes (SN) perform encryption and authentication on the health data of the patient. A tree-based routing protocol like Tiny Aggregation (TAG) [27] can be used in the intra-body communication network to collect the health data from various SN's and transmit it to the aggregator. For every given epoch of time, LPU performs secure data aggregation. In the process of secure data aggregation, the health data from various sensors on a patient is compressed as one and then transmitted to a remote medical server. The LPU also performs some authentication operations to guarantee the health data's authenticity and integrity.

2) *The extra-body communication network* is responsible for secure data transmission, and it secures data storage and access in remote health monitoring systems. It comprises of an aggregator (LPU) and the remote medical server (MS) (as depicted in Fig. 1). It can be noted that LPU acts as a common intersection point between both the intra-body and the extra-body communication networks. The LPU transmits the aggregated patient's health data to the remote medical server (MS), which resides in a secure location inside or outside the hospital. On receiving the physiological values as the patient's health data, the physician can get real-time situational awareness. Hence, a proper diagnosis and timely treatment can be departed to the patient.

B. COMMUNICATION MODEL

In the Intra-body communication network, the communication between each sensor node $s_i \in SN$ and the LPU is achieved through relatively inexpensive Wi-Fi technology. That is, within the Wi-Fi coverage of the LPU, each $s_i \in SN$ can directly/indirectly communicate with it. On the other hand, in an extra-body communication network, since the distance between the LPU and remote medical server (MS) is far, the communication between them is either through wired links or any other links with high bandwidth and low delay.

More precisely, we assume the following: (i) there is one MS, which is always trustworthy as it is stored in a secure location. It is responsible for generating the public and private key pairs for sensor nodes and is powered with sufficient computational and storage capability. (ii) Each sensor node communicates with exactly one LPU. The LPU is responsible for data aggregation and sends it directly to the MS. (iii) We assume that time is synchronized; (iv) we also assume that the communication channels between the LPU and medical server are secure.

C. ADVERSARY MODEL

Security plays an important role in the process of data aggregation and data transmission in remote health monitoring systems. In our security model, we consider the MS and LPU and the SN's as trustable and honest entities. However, there exists an adversary $\mathcal{A}$ residing at the LPU to eavesdrop on the medical health data. More seriously, the adversary $\mathcal{A}$ could also intrude into the database of the LPU to steal the individual patient's personal health data. In addition, the adversary $\mathcal{A}$ could also launch some active attacks such as false message injections to threaten the data integrity. This unauthorized access to sensitive data leads to privacy violations, while selective reporting, impersonating and masquerading lead to incorrect diagnosis and treatment of the patient, who is remotely monitored [1].

D. SECURITY REQUIREMENTS

Therefore, in order to prevent the adversary from learning the patient's health data and to detect the adversary's malicious actions, the following security requirements should be satisfied in a remote health monitoring system:

1) CONFIDENTIALITY AND DATA PRIVACY

To protect the patients' sensitive health data, which was collected from medical sensors, from the adversary, i.e., even if the adversary eavesdrops on the Wi-Fi communication in the LPU, it cannot identify the contents of the data packet. Also, if the adversary tries to have unauthorized access to the database on the LPU, it cannot identify the individual medical sensor's data. In this way, medical sensor's data can achieve the privacy-preserving requirement. Confidentiality also includes the prevention of aggregated data from the LPU being identified by any adversary, except the authorized MS.

2) AUTHENTICATION AND DATA INTEGRITY

To authenticate encrypted health data that has been collected and sent by a legitimate medical sensor and not altered during transmission i.e., if an adversary forges and/or modifies a report, malicious operations should be detected so that proper data aggregation is done at the LPU, and correct health data are received by the medical server.

E. DESIGN GOALS

Under the system model mentioned above and security requirements, our design goal is to develop a secure privacy-preserving data aggregation scheme for a remote health monitoring system based on a WBAN. Specifically, the following objectives should be achieved.

The aforementioned security requirements should be guaranteed in the proposed scheme. The primary security objective of our proposed scheme is to maintain the confidentiality of data been transmitted by the medical sensors to the remote server. The goal is also to retain the integrity of the data, which can be achieved by authentication of the data source. Additionally, the proposed scheme should maintain the medical data anonymity/data privacy without allowing any adversary to identify the content of the data. Finally, the freshness of data has to be maintained to know the exact current status of the patient for timely diagnosis and treatment.

IV. PRELIMINARIES

This section introduces the cryptographic primitives that are used as the building blocks in our proposed SPPDA scheme.

A. BILINEAR PAIRINGS

Let $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{G}_T$ be finite cyclic groups of prime order p, and let g_1, g_2 be the generators of $\mathbb{G}_1, \mathbb{G}_2$, respectively. The map e:$\mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ is said to be an admissible map if it satisfies the following three conditions:

1) Bi-linearity: $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab} \forall a, b \in \mathbb{Z}_p$ (where $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ is a Galois field of order)

2) Non – degeneracy: $e(g_1, g_2) \neq 1$

3) Efficiently computable

Such a mapping e is called bilinear mapping; it can be constructed by modified Weil or Tate pairings on elliptic curves [28]. Pairings are the basic operations used in the instantiation of homomorphic encryptions and data authentication involved for secure data transmission and data aggregation procedures of our scheme.

B. COMPLEXITY ASSUMPTIONS

Definition 1: Computational Diffie-Hellman assumption (CDH): Let $\mathbb{G}_1, \mathbb{G}_2$ be two multiplicative cyclic groups and g_1, g_2 be the generators, with prime order p. The CDH problem is described as follows: Given (g_2, g_2^a, g_2^b) for random $a, b \in \mathbb{Z}_p$, it is hard to compute $e(g_1, g_2)^{ab}$.

Definition 2: Bilinear Diffie-Hellman assumption (BDH): Let $\mathbb{G}_1, \mathbb{G}_2$ be two multiplicative cyclic groups and g_1, g_2 be the generators, with prime order p. The BDH problem is described as follows: Given $(g_2, g_2^a, g_2^b, g_2^c)$ for random $a, b, c \in \mathbb{Z}_p$, it is hard to compute $e(g_1, g_2)^{abc}$.

Definition 3: Decisional Bilinear Diffie-Hellman assumption (DBDH): Let $\mathbb{G}_1, \mathbb{G}_2$ be two multiplicative cyclic groups and g_1, g_2 be the generators, with prime order p. The DBDH problem is described as follows: Given $(g_2, g_2^a, g_2^b, g_2^c, X)$ for random $a, b, c \in \mathbb{Z}_p$ and $X \in \mathbb{G}_T$, it is hard to decide if $X = e(g_1, g_2)^{abc}$.

C. HOMOMORPHIC ENCRYPTION SCHEME

In our construction, we use a Bilinear ElGamal encryption scheme [29], which is a variant of the ElGamal cryptosystem [30]. The Bilinear ElGamal encryption scheme consists of four probabilistic polynomial time algorithms (Setup, Key generation, Encryption and Decryption):

1) *Setup* (1^λ): On input of security parameter λ, outputs a bilinear group $gk = (g_1, g_2, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$ where e:$\mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ is the bilinear map.

2) Keygeneration (gk): On input of $gkgk$ outputs a key pair $(E_{pk}, E_{sk}) = ((e(g_1, g_2))^u, g_1^u)$ for a random$u \in \mathbb{Z}_p$.

3) *Encryption* (m, E_{pk}): To encrypt a message $m \in \mathbb{G}_T$ under E_{pk}, select a random $r \in \mathbb{Z}_p$ and output the ciphertext as

$$C = (g_2^r, E_{pk}^r \cdot m) = [g_2^r, e(g_1, g_2)^{ur} \cdot m]$$

4) *Decryption* (E_{sk}, e): To decrypt the ciphertext $C = (C_1, C_2)$ and obtain m, compute $m = C_2/(e(g_1^u, C_1))$

Therefore to decrypt, it is enough to compute $C_2/(e(g_1^u, C_1))$, and the main idea is that we need only g_1^u to decrypt. Based on [29], we prove that this encryption scheme is semantically secure under the DBDH assumption in Theorem 1. (Refer to Section VI). The homomorphic property of the Bilinear ElGamal encryption scheme is given as

$$\begin{aligned} E(m_1, r_1) \cdot E(m_2, r_2) &= E(m_1 \cdot m_2; r_1 + r_2) \\ &= [g_2^{r_1+r_2}, e(g_1, g_2)^{u(r_1+r_2)} \cdot (m_1 \cdot m_2)] \end{aligned}$$

Here $E(m, r)$ refers to the *encryption* function as stated above, and the parameters m_1, m_2 are the message and r_1, r_2 are the random values from $\mathbb{Z}_p$. Therefore to decrypt the ciphertext and get the $m_1.m_2$, we use the function $Decryption(E_{sk}, e)$ and

compute

$$m_1 \cdot m_2 = \frac{C_2}{e(g_1^u, C_1)} = \frac{e(g_1, g_2)^{u(r_1+r_2)} \cdot m_1 \cdot m_2}{e(g_1^u, g_2^{r_1+r_2})} = \frac{e(g_1, g_2)^{u(r_1+r_2)}.m_1 \cdot m_2}{e(g_1, g_2)^{u(r_1+r_2)}}$$ by bi-linearity, we get

D. AGGREGATE SIGNATURE SCHEME

The aggregate signature scheme used in our scheme is based on the BGLS (named after the initials of the authors Boneh, Gentry, Lynn, and Shacham) [24] signature scheme. It consists of six probabilistic polynomial time algorithms (Setup, Key generation, Sign, Verify, Aggregate Sign, and Aggregate Verification):

1) *Setup* (1^λ): On input of a security parameter λ, outputs a bilinear group $gk = (g_1, g_2, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, H)$, where e:$\mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$, the bilinear map and $H : \{0, 1\}^* \rightarrow \mathbb{G}_1$ is a one-way hash function.

2) *Keygeneration* (gk): On input of gk, outputs a key pair $(S_{pk}, S_{sk}) = (g_2^x, x)$ for a random $x \in \mathbb{Z}_p$.

3) Sign (m, S_{sk}): To sign a message $m \in \mathbb{G}_T$ under the secret key $S_{sk} = x$, compute $\sigma = h^x = [H(m)]^x$.

4) *Verify* (m, σ): Given S_{pk}, a message m and a signature σ, compute $h = H(m)$ and accept if

$$e(\sigma, g_2) = e(H(m), S_{pk}) = e(h, S_{pk})$$

5) *AggregateSign* (m, σ_i): For computing aggregate signatures, each user $s_i \in SN$, input signature σ_i on each distinct message $m_i \in \{0, 1\}^*$, outputs $\sigma = \prod_{i=1}^{k} \sigma_i$ where $\sigma \in \mathbb{G}_1$.

6) *Aggregateverification* (m_i, σ): Ensure that the messages m_i are distinct. Compute $h_i = H(m_i)$ for $1 < i < k = |SN|$ and accept if $e(\sigma, g_2) = \prod_{i=1}^{k} e(h_i, S_{pk})$

The Aggregate Signature Scheme is provably secure under the CDH problem in a random oracle model as it is based on the BGLS Signature scheme [24].

V. PROPOSED SECURE PRIVACY-PRESERVING DATA (SPPDA) SCHEME

In this section, we initially discuss an overview of our proposed SPPDA scheme regarding the combination of basic preliminaries described earlier in Section IV of this paper. We also provide the formalized function definitions, which are used for various functionalities in the proposed SPPDA scheme. Finally, the construction of the proposed SPPDA scheme is discussed in four steps, namely, System Initialization, Health Data Generation, Privacy-Preserving Data Aggregation, Decryption and Verification. Further, the utilization of various formalized function definitions is explained, and correctness proof for these definitions is included.

A. OVERVIEW OF SPPDA SCHEME

In this subsection, we provide an overview of our proposed scheme and the basic notations (Refer to Table 1) that are to be used throughout the paper. Like many pairing-based cryptographic schemes, our scheme uses a special form of the bilinear map called a symmetric pairing where $\mathbb{G}_1 = \mathbb{G}_2$. In the rest of the paper, all the bilinear pairings are symmetric, and we denote $\mathbb{G}_1 = \mathbb{G}_2$ by $\mathbb{G}$.

TABLE 1. Basic notations used in SPPDA scheme.

Variables	Description
$\mathbb{G}, \mathbb{G}_T$	Cyclic multiplicative groups of prime order p
g_1, g_2	The generator of groups $\mathbb{G}$ respectively
e	It is a mapping from $\mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$
$e(g, g)$	The generator of group $\mathbb{G}_T$
H	A one-way hash function defined by $H : \{0,1\}^* \rightarrow \mathbb{G}$
SN	The set of sensor nodes on a human body
M	The set of distinct messages sent by each sensor
s_i	The ith sensor, where $s_i \in SN$
m_i	The ith message, where $m_i \in M$
k	Number of sensor nodes in set SN
E_{sk_i}	Secret key defined by public key cryptosystem
E_{pk_i}	Public key defined by public key cryptosystem
S_{sk_i}	Secret key defined by aggregate signature scheme
S_{pk_i}	Public key defined by aggregate signature scheme
CT_i	The ith ciphertext computed by s_i , given by $CT_i = (c_1, c_2)$
σ_i	The ith signature computed by s_i
gk	The bilinear group $(p, \mathbb{G}, \mathbb{G}_T, e, g_1, g_2, H)$

The proposed SPPDA scheme is constructed by considering a security parameter λ and runs a common setup (*CSetup*) function to generate the symmetric bilinear pairing group. Further, the proposed scheme calls for a common key generation (*CKey generation*) function for generating the key pairs that can be used for encryption (*Encryption*) and signature (*Sign*) generation in the next steps. The *Encryption*, *Sign*, *SigVerify*, *AggSign*, *AggVerification* functions are the symmetric variants of the functions from Bilinear ElGamal Cryptosystem and the BGLS aggregate signature scheme [Refer to Section IV.C and Section IV.D of this paper]. We build the *CipherProd* function based on the homomorphic property of the Bilinear ElGamal Cryptosystem. The *CipherProd* function is used to calculate the aggregate product of the ciphertexts obtained from the encryption function. Finally, an *AggDecryption* function is defined based on *Decryption* from Section IV.C.

The formalized function definitions of all the nine functions used in our proposed SPPDA scheme are discussed as follows:

1) CSetup (1^λ): On input of a security parameter λ, outputs a symmetric bilinear group $gk = (n, g_1, g_2, \mathbb{G}, \mathbb{G}_T, e, H)$, where e:$\mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ the bilinear map and $H : \{0, 1\}^* \rightarrow \mathbb{G}$ is a one-way hash function.

2) *CKeygeneration*(gk): On input of gk, for each sensor node $s_i \in S$ random variables $x_i, u_i \in \mathbb{Z}_p$ where

$i = 1, 2, 3 \ldots, k$, outputs key pairs for encryption and signature generation as $(E_{pk}, E_{sk}) = (e(g_1, g_2), g_1^u)$ and $(S_{pk}, S_{sk}) = (g_2^x, x)$, respectively.

3) Encryption (m_i, E_{pk_i}): To encrypt a message $m_i \in \mathbb{G}_T$ under E_{pk_i}, select a random $r_i \in \mathbb{Z}_p$ and output the cipher text as $CT_i = (C_1, C_2) = (g_2^{r_i}, E_{pk_i}^{r_i} \cdot m_i) = [g_2^{r_i}, e(g_1, g_2)^{u_i r_i} \cdot m_i]$ where computation of CT_i is based on Encryption (m, E_{pk}) as described in Section IV.C.

4) $Sign(m_i, S_{sk_i})$: Let $\mu_i = C_2$, where C_2 is the part of the i^{th} ciphertext CT_i. To sign an encrypted message μ_i, under the secret key $S_{sk_i} = x_i$, compute $\sigma_i = [H(\mu_i)||TS]^{x_i}$, where TS is the current time stamp, which can resist potential replay attacks.

5) $SigVerify(\mu_i, \sigma_i)$: Given S_{pk_i}, a message μ_i and a signature σ_i, compute $h = H(\mu_i)h = H(d_i)$ and accept if

$$e(\sigma_i, g_2) = e(H(\mu_i), S_{pk_i}) = e(h_i, S_{pk_i})$$

6) CipherProd (CT_i, k): Since the underlying encryption scheme used for obtaining the ciphertext CT_i is homomorphic in multiplication, therefore on input of CT_i, for $i = 1, 2, 3, ..., k$ outputs the aggregated cipher text by computing the product of all encrypted data as $CT = \prod_{i=1}^{k} CT_i$.

7) $AggSign(\mu_i, \sigma_i)$: For computing aggregate signatures, each sensing node $s_i \in SN$, input signature σ_i on each distinct message $\mu_i \in \{0, 1\}^*$, outputs $\sigma = \prod_{i=1}^{k} \sigma_i$, where $\sigma \in \mathbb{G}$.

8) $AggVerification(\mu_i, \sigma)$: Ensure that the messages μ_i are distinct. Compute $H(\mu_i)$ for $1 < i < k = |SN|$ and accept if $e(\sigma, g_2) = \prod_{i=1}^{k} e(h_i, S_{pk_i})$

9) $AggDecryption(E_{sk_i}, e)$: To decrypt the ciphertext, for $CT = (C_1, C_2) = \prod_{i=1}^{k} CT_i$, Compute AggDecryption $(E_{sk_i}, e) = C_2/e(g_1^U, C_1) = \prod_{i=1}^{k} m_i$, where $U = \sum_{i=1}^{k} u_i$.

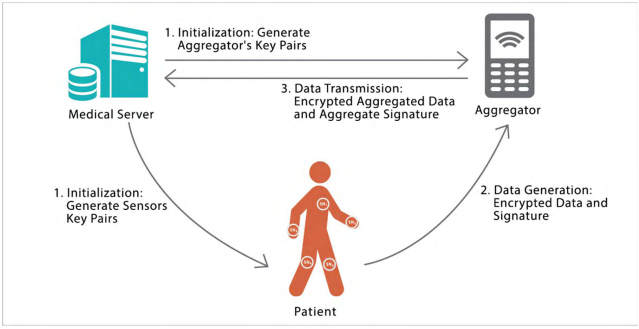

FIGURE 3. Proposed secure privacy-preserving data aggregation scheme (SPPDA).

B. PROPOSED SPPDA SCHEME

In this section, we propose the secure privacy-preserving data aggregation scheme (SPPDA) for the remote health monitoring system, which mainly consists of the following four parts (as shown in Fig. 3): System initialization, Health data generation, Privacy-preserving data aggregation, Decryption and Verification.

1) SYSTEM INITIALIZATION

During the initialization phase, the remote medical server is able to bootstrap the whole system. In particular, the medical server runs a common setup CSetup (1^λ) to acquire the initial parameters. Subsequently, the medical server utilizes the Bilinear ElGamal cryptosystem to generate the public and private key pairs through the CKeygeneration (gk) function. The detailed steps of the initial public parameter generation are as follows:

Step 1: Based on the input of security parameter λ, the common setup function given by $CSetup(1^\lambda)$ generates the tuple $gk = (p, g_1, g_2, \mathbb{G}, \mathbb{G}_T, e, H)$, where $\mathbb{G}$ and $\mathbb{G}_T$ are finite cyclic groups of prime order p; e:$\mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ is the bilinear map; g_1 and g_2 are two random generators of group $\mathbb{G}$ and H :$\{0, 1\}^* \rightarrow G_1$ is a one way hash function.

Step 2: For each sensing node $s_i \in SN$, the medical server calls the $CKeygeneration(gk)$ function and randomly selects variables $x_i, u_i \in \mathbb{Z}_p$ where $i = 1, 2, 3, .., k$. Finally, outputs a public and private key pair for encryption as $(E_{pk_i}, E_{sk_i}) = (e(g_1, g_2), g_1^{u_i})$ and a public and private key pair for signature generation as $(S_{pk_i}, S_{sk_i}) = (g_2^{x_i}, x_i)$, respectively.

The public and private key pairs (E_{pk_i}, E_{sk_i}) and (S_{pk_i}, S_{sk_i}) are used for encryption and signature generation and are computed as described in Section IV.C and Section IV.D, respectively. These parameters have to be preloaded in the medical sensor nodes and aggregator node (LPU) before implanting them on the human body.

2) HEALTH DATA GENERATION

We assume that the health data from the medical sensor nodes are reported simultaneously to the LPU after a given epoch of time. Specifically, when the LPU calls for data collection from the sensor nodes, each sensor node $s_i \in SN$ collects the datum in the form of messages $m_i \in \mathbb{G}_T$ and performs encryption and signature generation as follows:

Step 1: To encrypt a message m_i, the sensor node $s_i \in SN$ first calls the $Encryption(m_i, E_{pk_i})$ function.

Step 2: Given a public key E_{pk_i} for encryption, the sensor node $s_i \in SN$ randomly selects variable $r_i \in \mathbb{Z}_p$ and calculates the ciphertext $CT_i = (C_1, C_2)$ as:

$$\begin{aligned} CT_i = (C_1, C_2) &= (g_2^{r_i}, E_{pk_i}^{r_i} \cdot m_i) \\ &= [g_2^{r_i}, e(g_1, g_2)^{u_i r_i} \cdot m_i] \end{aligned} \quad (1)$$

where computation of CT_i is based on Encryption (m, E_{pk}) as described in Section IV.C.

Step 3: In order to achieve the end-to-end data privacy and not to reveal the message m_i at the LPU, we implement the aggregate signature scheme on μ_i instead of m_i, where $\mu_i = C_2$ is the part of the i^{th} ciphertext from (1). It is can be noted that $\mu_i = C_2$ contains message m_i in an encrypted format. Hence, if it gets revealed

at LPU for signature verification still no malicious aggregator or adversary can get the correct message. Therefore, data privacy is maintained. To sign the encrypted message μ_i, the sensor node $s_i \in SN$ first calls the $Sign(\mu_i, S_{sk_i})$ function.

Step 4: Given secret key S_{sk_i}, the sensor node $s_i \in SN$ *calculates the* signature σ_i as:

$$\sigma_i = [H(\mu_i)||TS]^{x_i} \tag{2}$$

where TS is the current time stamp.

Step 5: Finally, the sensor nodes send the encrypted health data and its signature $CT_i||TS||\sigma_i$ to the LPU.

The timestamp TS is used to resist the potential replay attack.

3) PRIVACY-PRESERVING DATA AGGREGATION

After receiving total k encrypted and signed health data $CT_i||TS||\sigma_i$ for $i = 1, 2, 3, .., k$, the LPU first checks the verification of the signature in the following steps:

Step 1: The LPU first checks the timestamp TS and calls the $SigVerify(\mu_i, \sigma_i)$ function.

Step 2: Given the public key S_{pk_i} for signing, the LPU computes hash $h = H(\mu_i)$ and verifies the validity of the signature σ_i by checking if

$$e(\sigma_i, g_2) = e(H(\mu_i), S_{pk_i}) = e(h_i, S_{pk_i}) \tag{3}$$

Step 3: Hence, LPU accepts σ_i

Step 4: For a given patient, being monitored may have multiple sensors for remote health monitoring; hence, it may take time to verify each signature. Therefore, to make the verification efficient, the LPU performs batch verification on multiple signatures together by checking if:

$$e(\sum_{i=1}^{k} \sigma_i, g_2) = \prod_{i=1}^{k} e(h_i, S_{pk_i}) \tag{4}$$

Step 5: Finally, LPU accepts $\sum_{i=1}^{k} \sigma_i$

Hence, due to the use of the batch verification process, the time-consuming pairing operations $e(.,.)$ can be reduced from $2k$ to $k + 1$ times.

After the validity check, the LPU performs privacy-preserving data aggregation by computing the product of ciphertext and generating the aggregate signature as follows:

Step 1: For $i = 1, 2, 3, ..., k$, LPU calls the $CipherProd$ (CT_i, k) function to generate aggregate ciphertext CT_i by homomorphic encryption as:

$$\begin{aligned} CT &= (C_1, C_2) = \prod_{i=1}^{k} CT_i \\ &= (g_2^{\sum_{i=1}^{k} r_i}, e(g_1, g_2)^{\sum_{i=1}^{k} u_i \sum_{i=1}^{k} r_i}. \prod_{i=1}^{k} m_i) \end{aligned} \tag{5}$$

Step 2: For $i = 1, 2, 3, ..., k$, the LPU calls the $AggSig(\mu_i, \sigma_i)$ function to generate the aggregate signature on σ_i.

Step 3: For each sensing node $s_i \in SN$, given an input signature σ_i on each distinct message $\mu_i \in \{0, 1\}^*$, compute the aggregate signature as

$$\sigma = \prod_{i=1}^{k} \sigma_i \tag{6}$$

Step 4: Finally, the LPU sends the encrypted data and aggregate signature $CT||\sigma$ to the remote medical server.

4) DECRYPTION AND VERIFICATION AT THE REMOTE SERVER

Upon receiving $CT||\sigma$, the medical server first verifies the aggregate signature and finally decrypts the message as follows:

Step 1: Before decrypting, the message medical server first calls the $AggVerification(\mu_i, \sigma)$ function for verifying the aggregate signature.

Step 2: For each distinct values of μ_i, where $1 < i < k = |SN|$, the medical server computes hash $h = H(\mu_i)$ and verifies the validity of the aggregate signature σ by checking if

$$e(\sigma, g_2) = \prod_{i=1}^{k} e(h_i, S_{pk_i}) \tag{7}$$

Step 3: Hence, the medical server accepts σ

Step 4: To decrypt the *ciphertext* CT, the medical server calls the $AggDecryption(E_{sk_i}, e)$ function

Step 5: For given *private key* $E_{sk_i} = g_1^{u_i}$ to decrypt the ciphertext CT, the LPU computes aggregate decryption as:

$$\begin{aligned} C_2/e(g_1^U, C_1) &= \prod_{i=1}^{k} m_i, \\ \text{where } U &= \sum_{i=1}^{k} u_i \end{aligned} \tag{8}$$

Therefore, the aggregated health data can be obtained by just using one parameter $g_1^{\sum_i^k u_i}$ as described in equation (8). Since $g_1^{\sum_i^k u_i}$ is not a large number and hence the computation of product of the all E_{sk_i} will be sufficient to perform the decryption.

C. COMPUTATION OF AVERAGES

1) Arithmetic Mean: Given a data set containing the elements $a_1, a_2, a_3, .., a_n$, the arithmetic mean is defined by the formula $AM = 1/n(\sum_{i=1}^{n} a_i)$,.

2) Geometric Mean: Given a data set containing the elements $a_1, a_2, a_3, .., a_n$,, the geometric mean is defined by the formula $GM = (\prod_{i=1}^{n} a_i)^{1/n}$.

Further, the geometric mean can also be expressed as the exponential of the arithmetic mean of logarithms as $(\prod_{i=1}^{n} a_i)^{1/n} = \exp(1/n(\sum_{i=1}^{n} \ln a_i))$. The inequality relationship between the geometric mean and arithmetic mean is given by $AM \geq GM$ [31].

Therefore, the trusted authorities who have access to the medical server can directly compute the statistical average

like geometric mean (GM) on the aggregated data $M = \prod_{i=1}^{k} m_i$ as $GM = (\prod_{i=1}^{k} m_i)^{1/k}$. Since data sensed by the sensors is not always drawn from the normal distribution, and there are more chances of outliers in the data [32]. Hence, in this case, based on the above discussion and the inequality $AM \geq GM$, GM are considered to be the better statistical average [33].

VI. SECURITY ANALYSIS

In this section, we analyze the correctness and security of the proposed SPPDA scheme based on the security theorems. Additionally, by following the security requirements discussed earlier, our analysis will show how the proposed SPPDA scheme achieves *confidentiality, authenticity* and *end-to-end privacy* on patient's medical health data in remote health monitoring systems.

A. SECURITY THEOREMS

Theorem 1: The proposed SPPDA scheme is semantically secure under Decisional Bilinear Diffie-Hellman assumption. More precisely, any adversary that can break the standard security of this scheme with probability $(1/2 + \varepsilon)$*can break the DBDH problem in (G, GT) with probability* $(1/2 + \varepsilon/2)$.

Proof: Suppose $\mathcal{A}$ distinguishes the ciphertexts with non-negligible probability, we simulate an adversary S that decides DBDH as follows:

1. On input $(y, y^a, y^b, y^c, e(y, y)^d)$, the simulator sets up an encryption system for the adversary A with the goal of using A to decide if $d = abc$ or not.
2. In the beginning, the simulator outputs the global parameters for the system (g, Z). Here, the simulator sets $g = y^c, Z = e(g, g) = e(y, y)^{c^2}$. Further, the simulator sends to adversary $\mathcal{A}$ the target public key $E_{pk} = e(y, y)^{c^2} = Z$ and the secret key $E_{sk} = g^t$, where t is randomly selected from $\mathbb{Z}_p$ by the simulator.
3. Eventually, $\mathcal{A}$ must output a challenge (m_0, m_1, τ), where $m_0 \neq m_1 \in M$ and τ is its internal state information. The simulator randomly selects a message and computes the ciphertext $C_s = (y^a, m_s e(y, y)^d) = (g^{a/c}, m_s e(g, g)^{d/c^2})$, sends (C_s, τ) to A, and waits for $\mathcal{A}$ to output$s' \in \{0, 1\}$.
4. If $s = s'$, then S guesses "$d = abc$"; otherwise, S guesses "$d \neq abc$".

We observe that if $d = abc$, then the simulation is perfect; that is, the ciphertext output is of the proper form $(g^{a/c}, m_b Z^{(abc)/c^2} = m_b Z^{b(a/c)})$. However, if $d \neq abc$, then m_b is information-theoretically hidden from A, since d was chosen independently of a, b, c. Thus, if A succeeds with probability $(1/2 + \varepsilon)$, then S succeeds with probability $(1/2 + \varepsilon)$ (when $d = abc$) and probability exactly $1/2$ (when $d \neq abc$), for an overall success probability of $(1/2 + \varepsilon/2)$. This contradicts the DBDH assumption when ε is non-negligible. ■

Remark: The above proof is based on the Ateniese *et al.*'s [29] proxy re-encryption scheme. The authors proved their re-encryption scheme to be semantically secure under extended DBDH assumption. Since our proposed encryption function is a variant of the ElGamal cryptosystem [30]; therefore, only DBDH assumption is enough to prove it.

Theorem 2: If all the sensing nodes (SN's) are honest, i.e. not tampered by any adversary and follow the proposed procedures, then any sensed medical health data can pass verification at the aggregator (LPU); i.e., the *SigVerify*(μ_i, σ_i) satisfies correctness.

Proof: Since (*Sign* (μ_i, S_{sk_i}), *SigVerify*(μ_i, σ_i)) is a secure signature verification algorithm [34] and all the signatures are verified at the aggregator using batch verification, $CT_i||TS||\sigma_i$ can pass the verification. Hence, according to the phases of *Sign*, *SigVerify and Batch verification,* the following formulas hold:

$$\begin{aligned} e(\sigma_i, g_2) &= e((H(\mu_i||TS))^{x_i}, g_2) \\ &= e((H(\mu_i||TS), g_2)^{x_i} \\ &= e(h_i, S_{pk_i}) \\ e(\sum_{i=1}^{k} \sigma_i, g_2) &= e(\sum_{i=1}^{k} (H(\mu_i||TS))^{x_i}, g_2) \\ &= \prod_{i=1}^{k} e((H(\mu_i||TS))^{x_i}, g_2) \\ &= \prod_{i=1}^{k} e(H(\mu_i||TS), S_{pk_i}) \\ &= \prod_{i=1}^{k} e(h_i, S_{pk_i}) \end{aligned}$$

■

Theorem 3: If the sensing nodes (SNs), aggregator (LPU) and medical server (MS) are honest and follow the proposed procedures, then any aggregated sensed medical health data can pass a data authenticity check at the medical server (MS); i.e., the *AggVerification*(μ_i, σ) satisfies correctness.

Proof: Since (*AggSig*(μ_i, σ_i),*AggVerification* (μ_i, σ_i)) is a secure aggregate signature verification algorithm [24], and all the signatures are verified before computation of aggregate signatures using batch verification $e(\sigma_i, g_2) = e(h_i, S_{pk_i})$ (Refer to Theorem 2); thus, $CT||\sigma$ can pass verification. Hence, according to the phases of *AggSig*(μ_i, σ_i) *and AggVerification* (μ_i, σ_i) *functions,* the following formulas hold:

$$\begin{aligned} e(\sigma, g_2) &= e(\prod_{i=1}^{k} \sigma_i, g_2) \\ &= \prod_{i=1}^{k} e(\sigma_i, g_2) \\ &= \prod_{i=1}^{k} e((H(\mu_i||TS))^{x_i}, g_2) \\ &= \prod_{i=1}^{k} e(H(\mu_i||TS), g_2)^{x_i} \\ &= \prod_{i=1}^{k} e(h_i, S_{pk_i}) \end{aligned}$$

■

Theorem 4: If the sensing nodes (SNs), aggregator (LPU) and medical server (MS) are honest and follow the proposed procedures, then the aggregated medical health data can be decrypted by the trusted authority at the medical server (MS); i.e., the *AggDecryption* (m_i, σ) satisfies correctness.

Proof: The (*Encryption* (m, E_{pk}), *Decryption* (E_{sk}, e)) is semantically secure under the DBDH assumption (Refer to Theorem 1). We consider, in a given epoch of time, each sensing node $s_i \in SN$ with the key pair for encryption $(E_{pk_i}, E_{sk_i}) = (e(g_1, g_2), g_1^{u_i})$, where $1 < i < k = |SN|$, generates a distinct message m_i.

In this case, we apply the homomorphic property as

$$E(m_1, r_1) \cdot E(m_2, r_2) = E(m_1 \cdot m_2; r_1 + r_2) = [g_2^{r_1+r_2}, e(g_1, g_2)^{u_1 r_1 + u_2 r_2} \cdot (m_1 \cdot m_2)]$$

where m_i stands for the message generated by the i^{th} sensing node belonging to $SN = \{s_1, s_2, ..., s_k\}$ and $g_1^{u_i}$ is the secret key for that particular i^{th} sensing node. More precisely, $'i'$ indicates the no. of sensing nodes in WBAN, but not the no. of messages stands generated by a particular sensing node.

Hence, by the homomorphic property of bilinear ElGamal Encryption Scheme as stated above, we aggregate the ciphertext using $CipherProd(CT_i, k)$ as

$$\begin{aligned} CT &= (C_1, C_2) \\ &= \prod_{i=1}^{k} CT_i \\ &= \prod_{i=1}^{k} (g_2^{r_i}, e(g_1, g_2)^{u_i r_i} . m_i) \\ &= (g_2^{\sum_{i=1}^{k} r_i}, e(g_1, g_2)^{\sum_{i=1}^{k} u_i \sum_{i=1}^{k} r_i} \cdot \prod_{i=1}^{k} m_i) \end{aligned}$$

where CT_i stands for the i^{th} ciphertext computed by i^{th} sensing node.

Therefore, to decrypt the ciphertext of the for $CT = (C_1, C_2) = \prod_{i=1}^{k} CT_i$, we use$AggDecryption$ (E_{sk_i}, e) function (described in Section V. A), and compute $AggDecryption$ $(E_{sk_i}, e) = C_2 / e(g_1^U, C_1)$

$$\Rightarrow \frac{C_2}{e(g_1^U, C_1)} = \frac{e(g_1, g_2)^{\sum_{i=1}^{k} u_i \sum_{i}^{k} r_i} \cdot \prod_{i=1}^{k} m_i}{e(g_1^{\sum_{i=1}^{k} u_i}, g_2^{\sum_{i=1}^{k} r_i})} = \prod_{i=1}^{k} m_i,$$

where $U = \sum_{i=1}^{k} u_i$. ■

B. ANALYSIS OF SECURITY REQUIREMENTS

1) THE PROPOSED SPPDA SCHEME CAN ACHIEVE CONFIDENTIAL PERSONAL MEDICAL HEALTH DATA

In the proposed scheme, the individual sensor's data are encrypted using the Bilinear ElGamal cryptosystem, which is IND-CPA (indistinguishable under the chosen ciphertext attack) secure under the DBDH assumption [29]. It is difficult for any time-bounded adversary to solve the aggregate decryption without the knowledge of the secret key, which is known only to the medical server and the sensor. On the other hand, the sensor makes use of random value $r_i \in \mathbb{Z}_p$ each time it encrypts the data, and hence, any adversary who tries to eavesdrop on the channel will not be able to compare between two ciphertexts. Hence, our scheme is also secure against passive eavesdropping.

2) THE AUTHENTICATION OF THE PERSONAL HEALTH DATA IS ACHIEVED IN THE PROPOSED SPPDA SCHEME

In the proposed SPPDA scheme, the personal health data from wearable medical sensors and the aggregated data from the LPU are signed by the BGLS aggregate signature (named after the initials of the authors Boneh, Gentry, Lynn and Shacham) [24]. Since the BGLS signature is provably secure under the CDH problem in the random oracle model, the source and aggregator's authentication can be guaranteed. Specifically, the medical health data from the sensors is signed by computing $\sigma_i = [H(\mu_i)||TS]^{x_i}$, where TS is the current time stamp to resist a potential replay attack and $S_{sk_i} = x_i$ is sensor node SN's secret key to make sure only the sensor can make the signature. After receiving the signed data item, the aggregator checks whether $e(\sigma_i, g_2) = e(H(\mu_i), S_{pk_i}) = e(h_i, S_{pk_i})$ to verify the source of the signature. Eventually, after the verification the aggregator computes $\sigma = \prod_{i=1}^{k} \sigma_i$ as the aggregate signature. Further, on receiving the aggregated data item, the medical server checks whether $e(\sigma, g_2) = \prod_{i=1}^{k} e(h_i, S_{pk_i})$ to verify the source of the signature. Therefore, any adversary's malicious behavior can be detected in the proposed scheme.

3) THE END-TO-END DATA PRIVACY IS ACHIEVED IN THE PROPOSED SPPDA SCHEME

In the proposed SPPDA scheme, the patient's data $\{m_1, m_2, ...m_k\}$, sensed by the on-body medical sensor is encrypted using the Bilinear ElGamal cryptosystem, are formed as $\{CT_1, CT_2, ...CT_k\}$. Since the Bilinear ElGamal cryptosystem is homomorphic in multiplication, the aggregator simply computes a product on cipher text for data aggregation as follows:

$$\begin{aligned} CT &= (C_1, C_2) = \prod_{i=1}^{k} CT_i \\ &= (g_2^{\sum_{i=1}^{k} r_i}, e(g_1, g_2)^{\sum_{i=1}^{k} u_i \sum_{i=1}^{k} r_i} \cdot \prod_{i=1}^{k} m_i) \end{aligned}$$

Let $\prod_{i=1}^{k} m_i = M_i$, $\sum_{i=1}^{k} u_i = U_i$, and $\sum_{i=1}^{k} r_i = R_i$; this implies $CT = (g_2^{R_i}, e(g_1, g_2)^{U_i R_i} . M_i)$ is still a valid cipher text of the Bilinear ElGamal Cryptosystem [29]. Since the Bilinear ElGamal Cryptosystem is a semantic secure by Theorem. 1, the data $\{m_1, m_2, ...m_k\}$ in M_i are also semantic secure and privacy-preserving. Therefore, the adversary who intrudes into the LPU cannot get the individual sensor readings as they are stored as the aggregate of the encrypted values, and hence, data privacy is achieved during transmission.

VII. PERFORMANCE EVALUATION

This section evaluates the performance of the proposed SPPDA scheme based on simulation results and computational complexity. In the following subsections of the simulation setup, we provide details of the simulation variables and settings about the simulation software used. We also include the detailed simulation results regarding various network scales. Further in the subsection of computational complexity,

we compute the computational cost involved and compare the proposed SPPDA scheme with its variant non-aggregate scheme and other related schemes from the literature.

4) SIMULATION SETUP

In this subsection, initially, we discuss the simulation variables and settings used for the implementation of the proposed SPPDA scheme. Later, the simulation results are discussed based on a comparison between the implementation of the proposed SPPDA scheme and its Non-Aggregate Variant scheme. We focus on the comparison of the computational cost at each processing level (i.e., Sensors, LPU and Medical Server (refer to Fig. 2)) for various network scales, in the remote health monitoring system.

5) SIMULATION VARIABLES AND SETTINGS

The proposed SPPDA scheme is implemented based on the charm framework (version 0.43) [35]. The charm framework facilitates the rapid prototyping of cryptographic schemes and protocols. In our experiment, we combine the public key encryption scheme and the aggregate signature scheme based on symmetric pairing group settings.

Namely, we have two groups $\mathbb{G}, \mathbb{G}_T$, and e is a pairing function from $\mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$. In a generic way, the assumptions and security can be translated to the symmetric settings. We use python language (version 3.4.3) to write the code. For efficient performance of the code, the routines implement the group operations using C math libraries such as PBC (version 0.5.14) [36], OpenSSL (version 1.0.0) [37] and GMP (version 6.1.0) [38]. All our simulation experiments and benchmark testing were executed using a virtual machine with 2.0 GB RAM running an Ubuntu 64bit Operating system build using Oracle VM Virtual Box manager.

Additionally, we consider that the wearable medical sensor nodes (SN's) are deployed on the patient's body according to their respective functionalities. For example, the sensor used to record the pulse of a patient is worn on the wrist of the patient. After the network is organized into an aggregation tree, we implement our proposed SPPDA scheme for various networking scales. Since the number of in-body/on-body medical sensors in remote health monitoring system has to be limited, therefore in our simulation, we considered the network size to be $1 \leq k \leq 10$, (where k is the allowable number of sensors on a patient's body).

We list out the following basic facts about the methodology used in the simulation: (i) All the operations are measured in an average running time of milliseconds. (ii) Scalar Multiplication, Exponentiation and pairing reading gives the details of the # of scalar multiplication, # of exponentiation and # of pairing operations performed at each respective group, and (iv) the Real-time and CPU-time are the benchmark flags from the charm framework, which calculates the reading in milliseconds for various network scales.

6) SIMULATION RESULTS

In our implementation, we consider three main routines: Data generation, Data Aggregation and Data decryption and verifications. These main routines further call for the subroutines for data encryption, signature generation, signature verification, cipher product, aggregate signature generation, aggregate signature verification and aggregate data decryption. Similarly, we build a Non-Aggregate scheme as a variant of the proposed SPPDA scheme by excluding the data aggregation algorithms at LPU.

TABLE 2. Computational cost of operations in SPPDA scheme.

SPPDA Scheme									
SN	SM			E			P	RT	CPU-T
	G	G_T	T	G	G_T	T			
2	2	7	9	12	9	21	10	0.11151	0.07
4	6	15	21	20	15	35	16	0.174521	0.11
6	10	23	33	28	21	49	22	0.232108	0.18
8	14	31	45	36	27	63	28	0.332535	0.23
10	18	39	57	44	33	77	34	0.324443	0.27

SN: No. Sensing Nodes, **SM:** Scalar Multiplication, **E:** Exponentiation, **P**: Pairing, **RT:** Real Time (ms), **CPU-T**: CPU Time (ms)

TABLE 3. Computational cost of operations in non-aggregate scheme.

Non-Aggregate Scheme									
SN	SM			E			P	RT	CPU-T
	G	G_T	T	G	G_T	T			
2	0	4	4	10	9	19	8	0.103457	0.06
4	0	8	8	18	17	35	14	0.116313	0.1
6	0	12	12	26	25	51	20	0.170028	0.11
8	0	16	16	34	33	67	26	0.239049	0.15
10	0	20	20	42	41	83	32	0.24686	0.18

SN: No. Sensing Nodes, **SM:** Scalar Multiplication, **E:** Exponentiation, **P**: Pairing, **RT:** Real Time, **CPU-T**: CPU Time

In this subsection, we provide a comparison of computational cost between the SPPDA and Non-Aggregate scheme by (i) changing the network scale (as k = 2, 4, 6, 8, 10) for each repetition of the experiment and (ii) keeping the network size fixed as k = 5. The simulation results, as listed in Table 2 and 3, depict the computational costs in terms of the no. of scalar multiplications, no. of exponentiations, no. of pairing operations, real-time computation and CPU time computation, involved during the runtime of our proposed SPPDA scheme and its variant Non-Aggregate scheme, respectively.

First, we analyze the computational efficiency of our proposed SPPDA scheme in comparison with its variant Non-Aggregate scheme by changing the network scale. We use Matlab to plot line graphs (refer to Fig. 4, Fig. 5, and Fig. 6) to compare the computational cost involved in operations such as exponentiations, pairing operations and scalar multiplication, respectively. From Fig. 4, it is observed that for increasing scale of sensors in the network, the proposed SPPDA scheme performs better than the Non-Aggregate scheme.

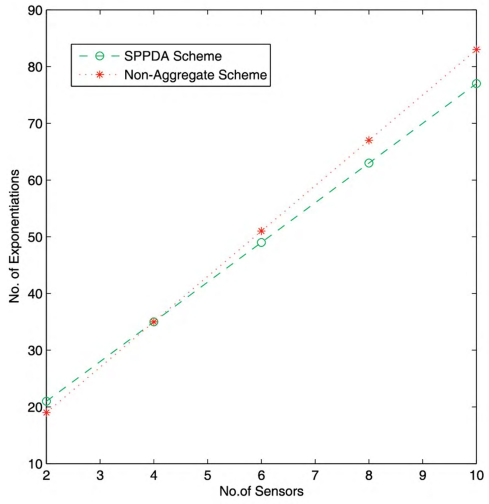

FIGURE 4. Comparison of computational costs for exponentiation operations.

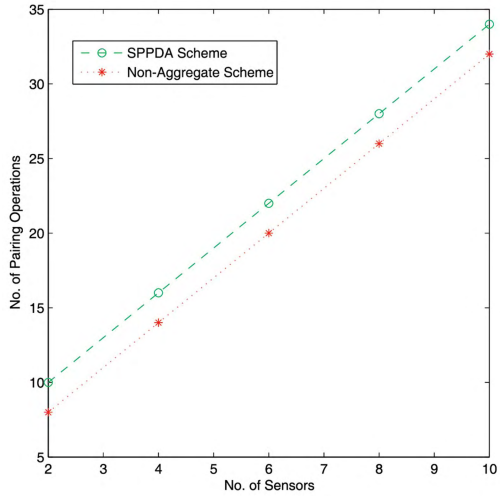

FIGURE 5. Comparison of computational cost for pairing operations.

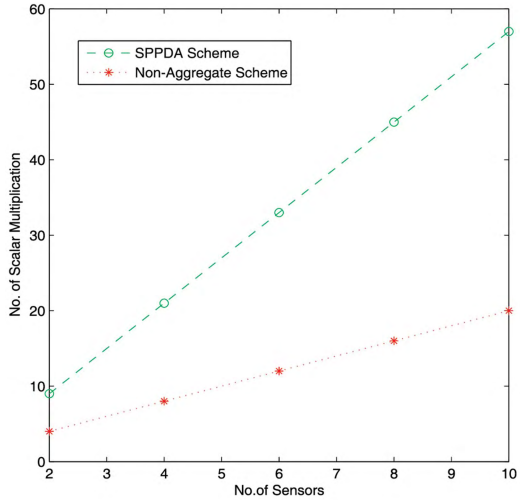

FIGURE 6. Comparison of computational costs for scalar multiplications.

Further, in Fig. 7, and Fig. 8, the comparisons between the SPPDA and Non-aggregate scheme are shown on Real Time and CPU Time flags of benchmark testing, respectively.

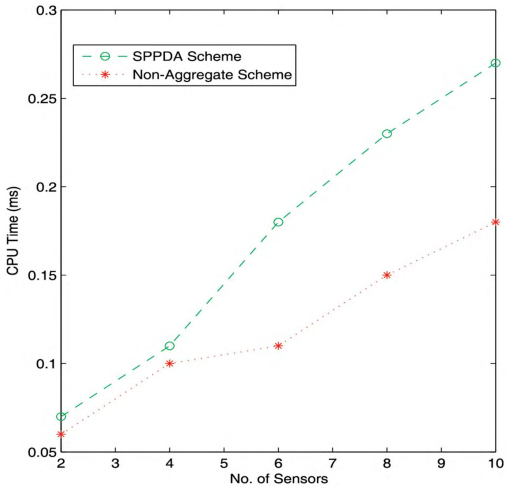

FIGURE 7. Comparison of computational costs for real time.

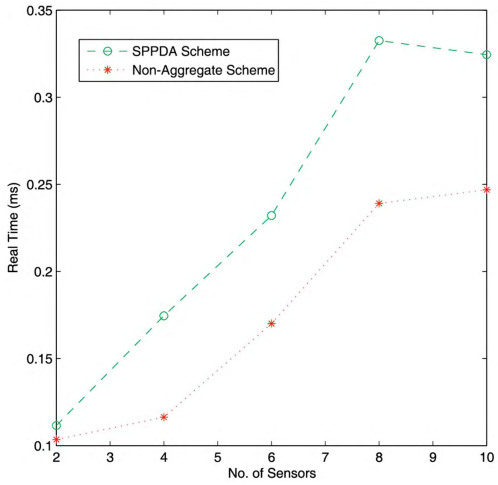

FIGURE 8. Comparison of computational costs for cpu time.

It can be observed from the graphs plotted in Fig. 4, Fig. 5, and Fig. 6 that except for scalar multiplications, the proposed SPPDA scheme performs almost similar to its Non-Aggregate variant scheme. It can be noted that scalar multiplications do not require a large amount of CPU time as that of pairing operations. We can further decrease the overall computational cost due to scalar multiplications by limiting the product of ciphertext at the aggregator to a threshold value. It can be noted that by small additional cost, a much efficient end-to-end secure privacy-preserving data aggregation scheme (SPPDA) can be constructed for the remote health monitoring system.

Secondly, we compare the computational cost between the SPPDA and Non-Aggregate scheme by keeping a fixed network size (as $k = 5$) for each repetition of the experiment. In Table 4, the computational costs regarding scalar multiplication, exponentiation and pairing operations are listed for a fixed network size at each sensor. In Table 5, the overall computational costs of the SPPDA scheme compared with the Non-Aggregate scheme regarding scalar multiplication,

TABLE 4. Computational cost of operations at each sensor.

At the Sensors					
SN	SM		E		P
	G	GT	G	GT	
1	0	1	4	3	1
2	0	1	4	3	0
3	0	1	4	3	0
4	0	1	4	3	0
5	0	1	4	3	0
Average	0	1	4	3	0.2

SN: No. Sensing Nodes, **SM:** Scalar Multiplication, **E:** Exponentiation, **P**: Pairing

TABLE 5. Computational cost of operations at each level.

L	SPPDA					Non-Aggregate Scheme				
	SM		E		P	SM		E		P
	G	GT	G	GT		G	GT	G	GT	
1	0	1	4	3	0	0	1	4	3	1
2	8	13	22	16	11	-	-	-	-	-
3	0	0	0	1	7	0	10	22	23	17

L=1(sensors), L=2 (LPU) and L=3 (Medical Server) **SN:** No. Sensing Nodes**, SM**: Scalar Multiplication**, E**: Exponentiation**, P**: Pairing

exponentiation and pairing operations is listed at Level 1: At the sensors, Level 2: At the LPU, and Level 3: At the medical server, respectively.

In Fig. 9, comparisons of the computational cost between the SPPDA scheme and its variant Non-Aggregate scheme are shown with respect to Real-Time and CPU-Time benchmark flags. It can be observed that the data aggregation process in the proposed SPPDA scheme increases the cost of computation only at the PDA. Consequently, the computational time decreases at the server. It can be noted that in the Non-Aggregate scheme, due to the absence of an aggregator, there is no computation cost involved at the PDA, whereas we observe that there is a huge computational cost required at the medical server.

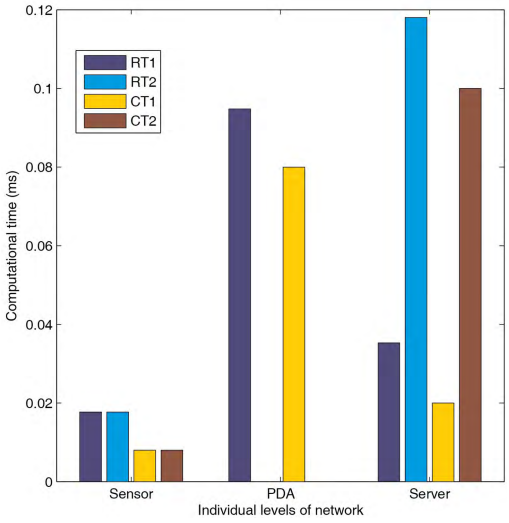

FIGURE 9. Comparison of computational costs at individual levels of network. RT1 - real time (SPPDA), RT2 - real time (non-aggregate scheme, CT1 - CPU time (SPPDA), CT2 - CPU time (non-aggregate scheme).

Therefore, from the simulation results, it can be concluded that, when efficient techniques like pre-processing are used, the additional computational cost incurred at the PDA can be further reduced. Additionally, in Table 6, we perform a comparison between some of the related data aggregation schemes in WBAN. From this comparison, it is evident that the proposed SPPDA scheme satisfies most of the security properties unlike other related data aggregation schemes in WBAN.

7) COMPUTATIONAL COMPLEXITY

The computation cost of the proposed SPPDA scheme can be calculated as three parts; (i) at the medical sensor of the patient; (ii) at the LPU of the patient; and (iii) at the medical server respectively. During health data generation at the medical sensor, each sensor generates a ciphertext CT_i, which involves a 1 point multiplication in $\mathbb{G}$, 2 exponentiation operations in $\mathbb{G}$ and 1 pairing operation for Bilinear ElGamal encryption. For signing, the sensor needs 1 hashing operation and 1 exponentiation operation. After receiving all the ciphertext and corresponding signatures, the LPU first performs batch verification, which involves $k + 1$ pairing operations.

TABLE 6. Comparison between some of the related data aggregation schemes in wban.

Security Properties	[9]	[41]	[15]	[42]	[10]	[14]	[43]	Proposed SPPDA
Confidentiality	✓	✓	✓	✓	✓	✓	✓	✓
Data Integrity	✓	✓	×	×	✓	×	×	✓
Data Authenticity	✓	✓	×	✓	✓	×	×	✓
Privacy -Preserving	✓	✓	×	×	✓	✓	✓	✓
Batch Verification	×	×	×	×	×	×	×	✓
Support statistical averages	×	×	×	×	×	✓	✓	✓

TABLE 7. Cryptographic operations execution time.

	Denotations	Time (ms)
C_m	A multiplication in $\mathbb{G}$	0.0204
C_e	An exponentiation in $\mathbb{G}$	3.7503
C_p	A pairing operation	3.9723
C_{et}	An exponentiation in $\mathbb{G}_T$	0.4844

TABLE 8. comparison of computational cost at individual sensor, Aggregator and server.

Schemes	Individual Sensor	Aggregator (LPU)	Server
EPPA	$C_m + 4C_p + 2C$	$(k+3)C_p + C_m$	$2C_p + C_e + 4C_m + C_{et}$
MDPA	C_p	-	$kC_p + C_m$
ADA	$5C_m + 2C_p$	-	$(2k+3)C_m + 2C_p + C_e$
Non-Aggregate Scheme	$3C_e + C_m + C_p$	-	$3kC_p + kC_m + kC_{et}$
Proposed SPPDA	$C_m + C_p + 3C_e$	$2kC_m + (k+1)C_p$	$2C_p + C_m + C_{et}$

It also generates an aggregated cipher text and signature, which involves $2k$ point multiplication operations. Finally, all the aggregated results are transmitted to the remote medical server, which involves 2 pairing operations for aggregate signature verification in $\mathbb{G}_T$ and it needs 1 exponentiation in $\mathbb{G}_T$, 1 point multiplication operations and 1 pairing operation in $\mathbb{G}$ for computing decryption of aggregated ciphertext.

Table 7 lists out the denotations and execution time (ms) of cryptographic operations based on average-runtime (ms), calculated using the benchmark of charm framework [39]. We denote C_e as the exponentiation operation, C_{et} as the exponentiation operation, C_m as the point multiplication operation and C_p as the pairing operation. We present the computational complexity comparison of the proposed SPPDA scheme with its non-aggregate variant scheme and other similar aggregate schemes such as EPPA (efficient and privacy-preserving aggregation) [12] MDPA (multidimensional privacy-preserving aggregation) [13] and ADA (Anonymous data aggregation)) [40] in Table 8. The null value with respect to MDPA and ADA, in Table 8 indicates that aggregation and decryption are combined and performed by the server. The null value under the non-aggregate scheme indicates the absence of the aggregator.

Furthermore, with the exact operations costs from Table 7, we depict the variation of computation costs at the aggregator and server, in terms of 'k' in Fig. 10 and Fig. 11, respectively. From Fig. 10 and Fig 11, it can be obviously shown that the proposed SPPDA scheme largely reduces the computational complexity at the aggregator and also at the server.

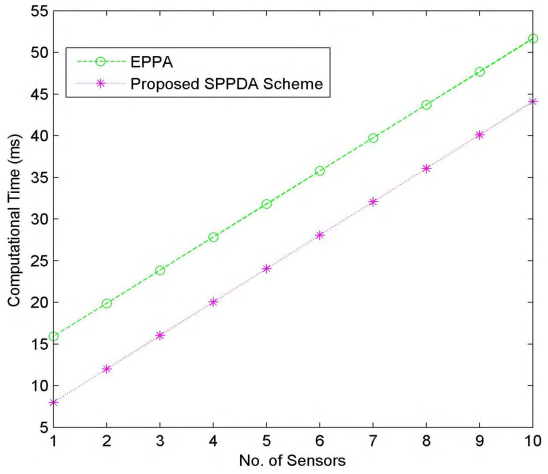

FIGURE 10. comparison of computational costs at the aggregator (PDA/LPU). SPPDA (secure privacy-preserving data Aggregation), EPPA (efficient and privacy-preserving Aggregation).

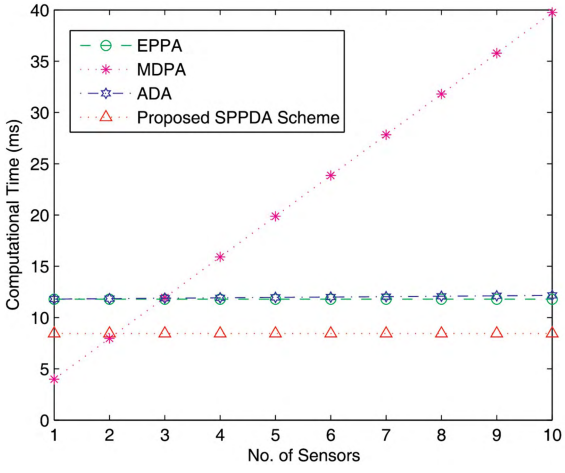

FIGURE 11. Comparison of computational costs at the server. SPPDA (secure privacy-preserving data aggregation), EPPA (efficient and privacy-preserving aggregation), MDPA (multidimensional privacy-preserving aggregation), ADA (anonymous data aggregation).

From the above analysis, the proposed SPPDA scheme is indeed efficient in terms of simulation results and computational complexity, which is suitable for privacy-preserving data aggregation in remote health monitoring systems.

VIII. CONCLUSION AND FUTURE WORK

In this paper, we have proposed a Secure Privacy-Preserving Data Aggregation (SPPDA) scheme based on bilinear pairing for remote health monitoring systems to improve aggregation efficiency and preserve data privacy. This paper formalizes the system model and security model for the remote health monitoring system. Based on the combination of a Bilinear ElGamal cryptosystem and aggregate signature, a concrete SPPDA scheme is designed. Security analysis demonstrates that our proposed scheme can preserve data confidentiality, data authenticity, and data privacy, while it also resists passive

eavesdropping and replay attacks from malicious adversaries. We have proven that the proposed SPPDA scheme is semantically secure against IND-CPA attacks in the standard model. The performance of the SPPDA scheme is tested using the charm framework [35] on the Ubuntu 64bit Operating System with 2 GB memory. The performance evaluation shows that our proposed SPPDA scheme is efficient and reduces communication complexity due to the use of data aggregation in the WBAN. The utilization of privacy homomorphism makes this scheme feasible for applicability in a cloud-assisted WBAN. In the future, we consider implementing a light weighted homomorphic aggregation scheme with more efficient Ate pairings [8] to further reduce communication and computational overhead and improve the efficiency of the proposed scheme.

REFERENCES

[1] S. Lim, T. H. Oh, Y. B. Choi, and T. Lakshman, "Security issues on wireless body area network for remote healthcare monitoring," in *Proc. IEEE Int. Conf. Sensor Netw., Ubiquitous, Trustworthy Comput.*, Jun. 2010, pp. 327–332.

[2] R. Nosowsky and T. J. Giordano, "The health insurance portability and accountability act of 1996 (HIPAA) privacy rule: Implications for clinical research," *Annu. Rev. Med.*, vol. 57, no. 1, pp. 575–590, Jan. 2006.

[3] Y. Sang, H. Shen, Y. Inoguchi, Y. Tan, and N. Xiong, "Secure data aggregation in wireless sensor networks: A survey," in *Proc. 7th Int. Conf. Parallel Distrib. Comput., Appl. Technol. (PDCAT)*, Dec. 2006, pp. 315–320.

[4] S. Peter, D. Westhoff, and C. Castelluccia, "A survey on the encryption of convergecast traffic with in-network processing," *IEEE Trans. Depend. Sec. Comput.*, vol. 7, no. 1, pp. 20–34, Jan./Mar. 2010.

[5] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: Security protocols for sensor networks," *Wireless Netw.*, vol. 8, no. 5, pp. 521–534, Sep. 2002.

[6] R. Rivest, L. Adleman, and M. L. Dertouzos, "On data banks and privacy homomorphisms," *Found. Secure Comput.*, vol. 4, no. 11, pp. 169–177, 1978.

[7] L. B. Oliveira, D. F. Aranha, E. Morais, F. Daguano, J. Lopez, and R. Dahab, "TinyTate: Computing the tate pairing in resource-constrained sensor nodes," in *Proc. 6th IEEE Int. Symp. Netw. Comput. Appl. (NCA)*, Jul. 2007, pp. 318–323.

[8] J.-L. Beuchat, J. E. González-Díaz, S. Mitsunari, E. Okamoto, F. Rodríguez-Henríquez, and T. Teruya, "High-speed software implementation of the optimal ate pairing over Barreto–Naehrig curves," in *Pairing-Based Cryptography* (Lecture Notes in Computer Science), vol. 6487. Berlin, Germany: Springer-Verlag, 2010, pp. 21–39.

[9] J. Sun, X. Zhu, and Y. Fang, "Preserving privacy in emergency response based on wireless body sensor networks," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Dec. 2010, pp. 1–6.

[10] K. Zhang, X. Liang, M. Baura, R. Lu, and X. Shen, "PHDA: A priority based health data aggregation with privacy preservation for cloud assisted WBANs," *Inf. Sci.*, vol. 284, pp. 130–141, Nov. 2014.

[11] W. Drira, E. Renault, and D. Zeghlache, "A hybrid authentication and key establishment scheme for WBAN," in *Proc. IEEE 11th Int. Conf. Trust, Secu. Privacy Comput. Commun. (TrustCom)*, Jun. 2012, pp. 78–83.

[12] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1621–1632, Sep. 2012.

[13] X. Lin, R. Lu, and X. Shen, "MDPA: Multidimensional privacy-preserving aggregation scheme for wireless sensor networks," *Commun. Mob. Comput*, vol. 10, no. 6, pp. 843–856, Jun. 2010.

[14] L. Chen, R. Lu, Z. Cao, K. AlHarbi, and X. Lin, "MuDA: Multifunctional data aggregation in privacy-preserving smart grid communications," *Peer-Peer Netw. Appl.*, vol. 8, no. 5, pp. 777–792, Sep. 2015.

[15] J. Ren, G. Wu, and L. Yao, "A sensitive data aggregation scheme for body sensor networks based on data hiding," *Pers. Ubiquitous Comput.*, vol. 17, no. 7, pp. 1317–1329, Oct. 2013.

[16] S. B. Othman, A. Trad, H. Youssef, and H. Alzaid, "Secure data aggregation with MAC authentication in wireless sensor networks," in *Proc. 12th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Jul. 2013, pp. 188–195.

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

[18] J. Zhou, Z. Cao, X. Dong, and X. Lin, "Security and privacy in cloud-assisted wireless wearable communications: Challenges, solutions, and future directions," *IEEE Wireless Commun.*, vol. 22, no. 2, pp. 136–144, Apr. 2015.

[19] O. Kocabas, T. Soyata, and M. K. Aktas, "Emerging security mechanisms for medical cyber physical systems," *IEEE/ACM Trans. Comput. Biol. Bioinformat.*, vol. 13, no. 3, pp. 401–416, May 2016.

[20] J. Liu, Z. Zhang, X. Chen, and K. S. Kwak, "Certificateless remote anonymous authentication schemes for WirelessBody area networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 332–342, Feb. 2014.

[21] J. Zhou, Z. Cao, X. Dong, N. Xiong, and A. V. Vasilakos, "4S: A secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks," *Inf. Sci.*, vol. 314, pp. 255–276, Sep. 2015.

[22] H. Yang, H. Kim, and K. Mtonga, "An efficient privacy-preserving authentication scheme with adaptive key evolution in remote health monitoring system," *Peer-to-Peer Netw. Appl.*, vol. 8, no. 6, pp. 1059–1069, Nov. 2015.

[23] L. Shen, J. Ma, X. Liu, and M. Miao, "A provably secure aggregate signature scheme for healthcare wireless sensor networks," *J. Med. Syst.*, vol. 40, no. 11, p. 244, Nov. 2016.

[24] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," in *Advances in Cryptology–EUROCRYPT*. Berlin, Germany: Springer, 2003, pp. 416–432.

[25] H. Wang, K. Ota, and J. Shen, "Remote data integrity checking and sharing in cloud-based health Internet of Things," *IEICE Trans. Inf. Syst.*, vol. E99-D, no. 8, pp. 1966–1973, 2016.

[26] L. Zhu, Z. Yang, J. Xue, and C. Guo, "An efficient confidentiality and integrity preserving aggregation protocol in wireless sensor networks," *Int. J. Distrib. Sens. Netw.*, vol. 10, no. 2, 2014. doi: https://doi.org/10.1155/2014/565480

[27] S. Madden, M. J. Franklin, J. M. Hellerstein, and W. Hong, "TAG: A tiny aggregation service for ad-hoc sensor networks," in *Proc. 5th Symp. Oper. Syst. Des. Implement.*, 2002, vol. 36, no. SI, pp. 131–146.

[28] M. Maas, "Pairing-based cryptography," M.S. thesis, Dept. Mathe. comput., Tech. Univ. Eindhoven, Eindhoven, The Netherlands, 2004.

[29] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," *ACM Trans. Inf. Syst. Secur.*, vol. 9, no. 1, pp. 1–30, 2006.

[30] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inf. Theory*, vol. 31, no. 4, pp. 469–472, Jul. 1985.

[31] J. M. Steele and J. Michael, *The Cauchy-Schwarz Master Class?: An Introduction to the Art of Mathematical Inequalities*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[32] V. Loseu, J. Wu, and R. Jafari, "Mining techniques for body sensor network data repository," in *Wearable Sensors*. Amsterdam, The Netherlands: Elsevier, 2014, pp. 383–407.

[33] A. R. Feinstein, *Principles of Medical Statistics*. Boca Raton, FL, USA: CRC Press, 2001.

[34] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," *J. Cryptol.*, vol. 17, no. 4, pp. 297–319, 2004.

[35] J. A. Akinyele *et al.*, "Charm: A framework for rapidly prototyping cryptosystems," *J. Cryptogr. Eng.*, vol. 3, no. 2, pp. 111–128, Jun. 2013.

[36] *PBC Library—Pairing-Based Cryptography—About*, accessed on Mar. 28, 2017. [Online]. Available: https://crypto.stanford.edu/pbc/

[37] *OpenSSL*, accessed on Mar. 28, 2017. [Online]. Available: https://www.openssl.org/

[38] *The GNU MP Bignum Library*, accessed on Mar. 28, 2017. [Online]. Available: https://gmplib.org/

[39] Fan Zhang. *Charm-Crypto Benchmark*, accessed on Jan. 1, 2017. [Online]. Available: http://student.seas.gwu.edu/~zfwise/crypto/report_1_4_1.pdf

[40] X. Liu, Y. Zhang, B. Wang, and H. Wang, "An anonymous data aggregation scheme for smart grid systems," *Secur. Commun. Netw.*, vol. 7, no. 3, pp. 602–610, Mar. 2014.
[41] B. Tiwari and A. Kumar, "Physiological value based privacy preservation of patient's data using elliptic curve cryptography," *Heal. Informat.-Int. J.*, vol. 2, no. 1, pp. 1–14, 2013.
[42] S. Ben Othman, A. A. Bahattab, A. Trad, and H. Youssef, "Secure data transmission protocol for medical wireless sensor networks," in *Proc. IEEE 28th Int. Conf. Adv. Inf. Netw. Appl.*, 2014, pp. 649–656.
[43] S. Han, S. Zhao, Q. Li, C.-H. Ju, and W. Zhou, "PPM-HDA: Privacy-preserving and multifunctional health data aggregation with fault tolerance," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 9, pp. 1940–1955, Sep. 2016.

ANEES ARA Jr. (M'17) received the B.Sc. degree in computer science and the M.Sc. degree in mathematics with computer science from Osmania University, Hyderabad, India, in 2005 and 2007. She is currently pursuing the Ph.D. degree in computer science with King Saud University, Riyadh, Saudi Arabia. From 2008 to 2017, she was a Research Assistant with the Department of Information Technology. Her research interest includes the network security, wireless sensor networks, cyber physical systems, Internet of Things, cloud computing, and ubiquitous computing.

MZNAH AL-RODHAAN has received the B.S. degree (Hons.) in computer applications and the M.S. degree in computer science from King Saud University in 1999 and 2003, respectively, and the Ph.D. degree in computer science from the University of Glasgow, Scotland, U.K., in 2009. She is currently the Vice Chair of the Computer Science Department, College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia. Moreover, she has served in the editorial boards for some journals, such as the *Ad Hoc Journal* (Elsevier) and has participated in several international conferences. Her current research interests include mobile ad hoc networks, wireless sensor networks, multimedia sensor networks, cognitive networks, and network security.

YUAN TIAN has received the master's and Ph.D. degrees from Kyung Hee University. She is currently an Assistant Professor with the College of Computer and Information Sciences, King Saud University, Saudi Arabia. She is a member of technical committees of several international conferences and is an Active Reviewer of many international journals. Her research interests are broadly divided into privacy and security, which are related to cloud computing, bioinformatics, multimedia, cryptograph, smart environment, and big data.

ABDULLAH AL-DHELAAN received the B.S. degree (Hons.) in statistics from King Saud University, in 1982, and the M.S. and Ph.D. degrees in computer science from Oregon State University in 1986 and 1989, respectively. He is currently the Vice Dean for Academic Affairs, Deanship of Graduate Studies, and a Professor of Computer Science, King Saud University, Riyadh, Saudi Arabia. He has guest edited several special issues for the *Telecommunication Journal* (Springer), and the *International Journal for Computers and Their Applications*. Moreover, he is currently on the editorial boards of several journals and the organizing committees for several reputable international conferences. His current research interest includes mobile ad hoc networks, sensor networks, cognitive networks, network security, image processing, and high performance computing.