Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 5594159, 18 pages
https://doi.org/10.1155/2021/5594159

Research Article

EPPDA: An Efficient and Privacy-Preserving Data Aggregation Scheme with Authentication and Authorization for IoT-Based Healthcare Applications

Faris A. Almalki[1] **and Ben Othman Soufiene**[2]

[1]*Department of Computer Engineering, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia*
[2]*PRINCE Laboratory Research, ISITcom, Hammam Sousse, University of Sousse, Tunisia*

Correspondence should be addressed to Ben Othman Soufiene; ben_oth_soufiene@yahoo.fr

Received 18 January 2021; Revised 17 February 2021; Accepted 21 February 2021; Published 9 March 2021

Academic Editor: Chien-Ming Chen

Nowadays, IoT technology is used in various application domains, including the healthcare, where sensors and IoT enabled medical devices exchange data without human interaction to securely transmit collected sensitive healthcare data towards healthcare professionals to be reviewed and take proper actions if needed. The IoT devices are usually resource-constrained in terms of energy consumption, storage capacity, computational capability, and communication range. In healthcare applications, many miniaturized devices are exploited for healthcare data collection and transmission. Thus, there is a need for secure data aggregation while preserving the data integrity and privacy of the patient. For that, the security, privacy, and aggregation of health data are very important aspects to be considered. This paper proposes a novel secure data aggregation scheme called "An Efficient and Privacy-Preserving Data Aggregation Scheme with authentication for IoT-Based Healthcare applications" (EPPDA). EPPDA is based to verification and authorization phase to verify the legitimacy of the nodes that need to join the process of aggregation. EPPDA, also, uses additive homomorphic encryption to protect data privacy and combines it with homomorphic MAC to check the data integrity. The major advantage of homomorphic encryption is allowing complex mathematical operations to be performed on encrypted data without knowing the contents of the original plain data. The proposed system is developed using MySignals HW V2 platform. Security analysis and experimental results show that our proposed scheme guarantees data privacy, messages authenticity, and integrity, with lightweight communication overhead and computation.

1. Introduction

The IoT is a paradigm that is rapidly gaining ground in the modern wireless telecommunications scenarios. The basic idea behind this concept is that the ubiquitous presence around us of a variety of things or objects—such as RFID, sensors, actuators, cell phones, which able to interact with each other to achieve common goals through unique addressing schemes [1]. The IoT can promote the development of applications in many different fields (e.g., smart buildings, automation, industrial automation, medical aids, mobile healthcare, intelligent energy management, and traffic management) [2]. These applications can be used to generate big data to provide new services to citizens, businesses, and public administrations to make smart decisions [3]. More in-depth understanding of IoT with its applications, challenges, and open research issues is discussed in [1–7]. Many benefits are provided by IoT technologies to the healthcare field, and the resulting applications can be grouped mainly in the tracking of objects and people (staff and patients); identification and authentication of persons; automatic data collection and detection [8]. Figure 1 shows the typical structure of the healthcare surveillance system using IoT. The sensors are deployed in the human body to monitor parameters

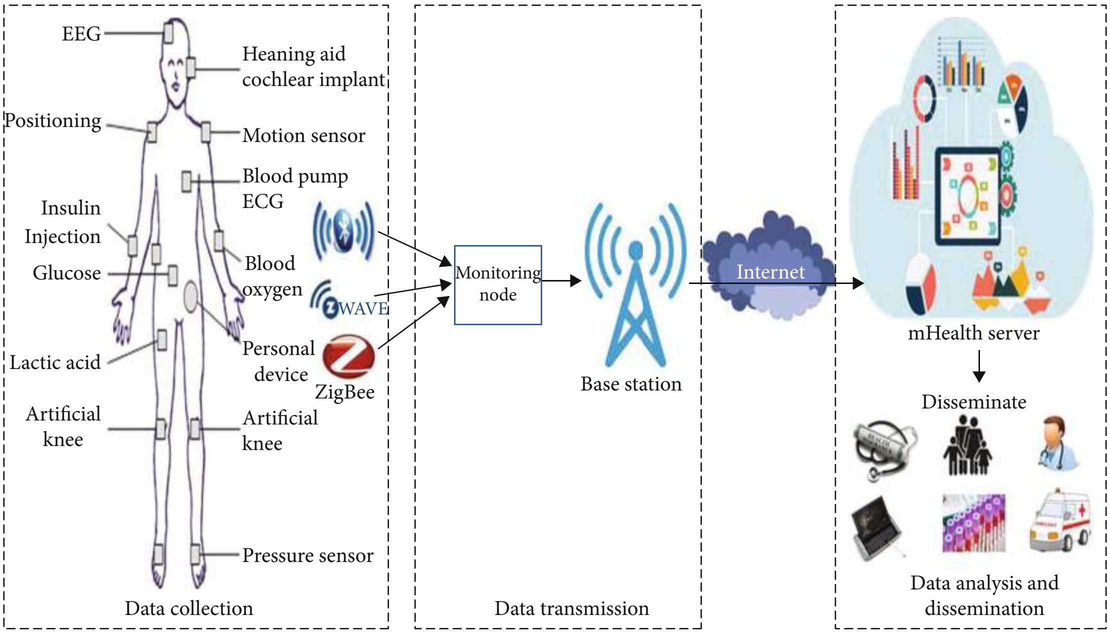


Figure 1: IoT-based healthcare monitoring architecture.

like temperature, heart rate, and blood pressure. The values read from the sensors are transmitted to the server where physicians can access this data. Therefore, healthcare remote monitoring solutions could potentially reduce medical costs across the country [9].

IoT-based healthcare systems are extremely vulnerable to be attacked for several reasons. First, system components are mostly unattended, and thus, it is easy to attack them physically. Second, most communications are wireless, which makes eavesdropping more vulnerable than wired scenarios [10]. Finally, most IoT components are characterized by low capacities in terms of energy and computing resources; therefore, these cannot implement complex schemes supporting security. According to Health Insurance Portability and Accountability (HIPAA) [11], it is mandatory to protect all sensitive medical data relating to a patient's health. Data aggregation is a process of collecting data and aggregating it from the sensor node, which can be considered as one of the essential procedures for not only removing redundant data but also saving energy [12, 13]. However, data aggregation scheme faces many security challenges, which should be carefully addressed [10–20]. Sensor nodes are often deployed in hostile environments with low bandwidth and unsecured communication channels [21]. This can lead to malicious modification of data and tampering with data, resulting in the violation of a user's privacy [22, 23].

To solve the problems mentioned above, this paper proposes a novel secure data aggregation scheme based on homomorphic primitives, called Secure and Privacy Preserving Data Aggregation (EPPDA) designed to reduce the requirements of existing security protocols. EPPDA is based on the verification and authorization phase to verify the legitimacy of the nodes want to join the process of aggregation. In our proposed work, we distinguish different types of health data with different characteristics, including Emergency Data, Vital Health Data and Regular Health Data. The emergency data considers as the highest priority data, where it should be successfully delivered to the Medical Server as soon as required. The vital health data are the requested data by doctors for continuous monitors a patient's condition. The regular data are not for emergency data and do not presents urgent delivery requirements. The Medical Server receives periodical updates.

To the best of our knowledge, the literature shows that detection of attacks can only be performed after reception of aggregate. Thus, this detection is inefficient and too late; besides, it may result in significant loss in terms of computation and communication costs as well as the privacy of patients' information. Therefore, this proposal uses a signature scheme based on Chebyshev polynomials. By this process, sensor devices, aggregator, and medical server are mutually authenticated before the actual health data transmission. The confidentiality of data is mandatory in data aggregation within healthcare-based IoT. It ensures that the data cannot be accessed by unauthorized person while they flow in the network. The homomorphic encryption algorithm which can protect end-to-end data confidentiality will be applied in this protocol. The proposed EPPDA uses additive homomorphic encryption to protect data privacy and combines it with homomorphic MAC to check the data integrity. Security analysis and performance evaluation based on experimental results of the proposed work is presented.

The remainder of this paper is organized as follows: The related works are investigated in Section 2. Network model and design goals are presented in Section 3. In Section 4, we described in detail the solution, followed by the security analysis and performance evaluation in Sections 5 and 6, respectively. Finally, Section 7 concluded this paper.

2. Related Work

Security is one of the important factors that must be considered when developing IoT-based healthcare systems [5, 6]. This section describes the popular research projects on secure data aggregation of IoT-based healthcare applications. Then, we used this review to highlight the research gaps and report own research motivations. Table 1 shows all techniques that been discussed above and summarized it in.

Authors in [15] present a health data aggregation scheme, namely, a priority-based health data aggregation with privacy preservation for cloud assisted WBANs (PHDA). It is used to improve the efficiency of aggregation between different types of health data. Based on different data priorities, adjustable transfer strategies that can be selected to transmit user's health data to cloud servers at reasonable communication costs. In addition, PHDA can resist tampering attacks and achieve a desirable delivery rate with reasonable communication costs and reduced delivery time for data in different priorities. But at the same time, it reduces the communication overload. Indeed, their system was not tolerant of failure in the event of failure of users or cloud servers, nor is it resistant to different types of attacks.

In [16], an efficient and privacy-friendly data aggregation known as Fault Tolerance Multifunctional Health and Privacy Preserving Data Aggregation for Cloud Assisted WBANs (PPM-HAD) is introduced. The PPM-HAD is aimed at addressing the need for a fault-tolerant cloud framework to manage sensitive user health data in a large-scale network. The aggregation of temporal and spatial statistical data on health is taken into account. In other words, the PPM-HDA mechanism preserves not only differential confidentiality for additive aggregations, such as summation and variance aggregations, but also nonadditive aggregations, such as min/max, median, percentile, and histogram. The additive aggregation feature uses the Boneh-Goh Nissim Encryption System, which is a public key encryption scheme used to protect user privacy. The PPM-HDA scheme ensures that the remaining uncompromising cloud servers can decrypt the aggregated data, which is collected by the healthcare sensors. The prefix membership check scheme is used to reduce computational overhead by changing the question of whether a data item belongs to a range of data or not to a few check questions whether a numeric value is equal or not.

Another approach proposed by Othman et al. in [17] was named Lightweight Secure Data Aggregation Scheme in Healthcare using IoT (LSDA). This new scheme is characterized by the use of homomorphic encryption. In addition, each aggregator should check all the packets received from its member nodes, which can filter out the false packets in the network, and thus, the nodes can save power in the transmission phase. The LSDA scheme has three phases: encryption, authentication and aggregation, and decryption and verification. By using this LSDA, many advantages can be obtained, such as reduced power consumption as well as improved bandwidth utilization and data privacy. Indeed, the limit of the approach is that it does not consider different types of health data.

In [18], Othman et al. present an end-to-end secure data aggregation scheme, namely, Robust and Efficient Secure Data Aggregation Scheme in Healthcare Using IoT (RESDA). The main objective of the proposed scheme is the security of the data aggregation to be achieved without introducing significant overheads on the sensors limited by the battery. The proposed approach uses homomorphic privacy encryption. The proposed RESDA program meets several security requirements, including confidentiality, authenticity, and integrity. The results of the performance appraisal demonstrated the feasibility and advantages of the proposed system as well as the performance gains. Indeed, the limit of the approach is that it does not take into account different types of health data.

Liu et al. [19] proposed a new contribution, namely, a Reliable and Energy-Efficient Communication System based on trust for remote monitoring of patients in body-zone wireless networks (ERCS). Is a trust-based communication scheme to ensure the reliability and confidentiality of the WBAN. To ensure reliability, a cooperative communication approach is used, while for the preservation of confidentiality, a cryptographic mechanism is used. The cooperative strategy was adopted to create trust between the biosensors in order to make the network more reliable. Additionally, the trust was generated at the remote medical server by applying the trust certificate. The performance evaluation has shown that the proposed system outperforms previously offered advanced systems in terms of confidence, energy efficiency, and reliability.

Researchers in [20] proposed a novel contribution, namely, an efficient and provable secure Certificate-Based Combined Signature, Encryption and Signcryption Scheme for Internet of Things in Mobile Health System (CBCSES). The novelty of this scheme lies in the fact that it offers the functions of digital signature and encryption simultaneously and individually. To show the effectiveness of the proposed scheme, detailed security analyzes, i.e., indistinguishable under chosen adaptive ciphertext attacks and tamper-proof under selected adaptive message attacks, and comparisons with relevant existing schemes are performed. The results obtained confirm the superiority of the scheme in terms of computation and communication costs with enhanced security.

3. System Model and Design Objectives

In this section, we formalize the system model, the adversary model, and the design goals of the EPPDA scheme.

3.1. Network Model. The proposed architecture is shown in Figure 2, where it can be utilized in a hospital and by even a located remotely patient. The architecture model of our proposed scheme comprises three architectural components, namely, a Medical Sensors Nodes, an Aggregator, and a Medical Server.

(i) Medical Sensor Nodes: The patients are equipped through wearable devices that were forming a Wireless Medical Sensors (MSs). These sensors are on

Table 1: Summary of techniques.

Technique and reference	Focus area(s) of the paper	Strengths	Weakness
PHDA [15]	(i) Priority-based health data aggregation. (ii) Paillier cryptographic technique	(i) Low energy consumption (ii) Ensure data privacy and integrity	(i) Asymmetric cryptosystem is computationally expensive
PPM-HAD [16]	(i) Privacy-preserving and multifunctional health data aggregation	(i) High fault tolerant (ii) Ensure data privacy and integrity	(i) Not verified in a real-life environment (ii) High traffic load
LSDA [17]	(i) Secure data aggregation in healthcare using IoT (ii) Homomorphic encryption and MAC. (iii) Packet checking at aggregator	(i) Evaluation results using an experimental network of medical sensors (ii) Robust communication (iii) Efficient communication between doctors and patients	(i) ECEG is power hungry cryptography (ii) Low fault tolerant (iii) Can be vulnerable to impersonation attack
RESDA [18]	(i) Secure data aggregation in healthcare using IoT (ii) Homomorphic encryption and MAC (iii) No packet checking at aggregator	(i) Evaluation results using an experimental network of medical sensors (ii) Providing strong privacy guarantees	(i) ECEG is power hungry cryptography (ii) Easy target for high-end attacks
ERCS [19]	(i) Trust-based communication scheme to ensure reliability and privacy of WBAN (ii) Cooperative communication approach	(i) Increases service delivery ratio, reliability, and trust with reduced average delay (ii) Guaranteeing the confidentiality of sensitive medical data	(i) High traffic load (ii) Not verified in a real-life environment (iii) Energy consumption
CBCSES [20]	(i) Efficient and provable secure scheme for IoT in Mobile health system (ii) Certificate-based combined signature, encryption and signcryption	(i) Securing the patients' sensitive data (ii) Providing efficient performance in terms of energy consumption, frequency and cost.	(i) Not verified in a real-life environment (ii) Communication cost is high. (iii) Not considering heterogeneity of sensors
Proposed EPPDA	(i) Secure and energy-efficient data aggregation in healthcare using IoT with malicious node detection. (ii) Homomorphic encryption and MAC (iii) Packet checking at aggregator (iv) Priority-based health data aggregation	(i) Evaluation results using an experimental network of medical sensors (ii) Ensure data privacy and integrity (iii) Efficient communication between doctors and patients (iv) Malicious node detection (v) Considering heterogeneity of sensors	(i) Can have high storage overhead to store large number of keys

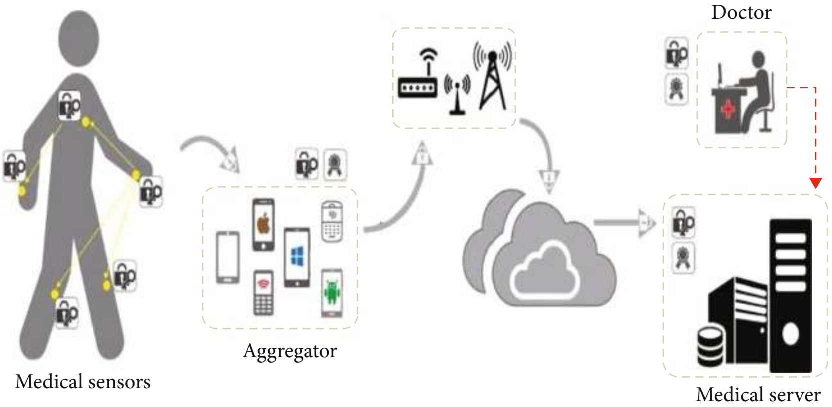


Figure 2: The proposed architecture for IoT-based healthcare.

human body to monitor body functions and the surrounding environment. Each sensor node is integrated with biosensors which are body temperature, electromyography, electrocardiography, blood pressure, pulsi-oximeter, and electroencephalography. The Medical Sensors are responsible for reporting the sensed health data to the Aggregator.

(ii) Aggregator: Is a special sensor node with a superior certain ability to calculation and communication range. Aggregation nodes, as the name suggests, will aggregate the data using aggregation functions. The Aggregator collects the individual health data and check the legitimacy of the Medical Sensors wishing to communicate with it to prevent the adversary nodes from joining the network, then compute the aggregation on them. The patient's mobile device is used as the Aggregator. The Aggregator works as a router between the Medical Sensor nodes and the Medical Server.

(iii) Medical Server: The Medical Server includes healthcare providers (e.g., doctors, physicians, nurses, and researchers). It possesses almost infinite storage capability and the computation of the resources. The Medical Server has the computation abilities to execute the calculations over the stored data including disease learning and prediction. We consider a scenario where the medical server can be accessed by the trusted authorities and the concerned doctor/emergency medical team. On receiving the patient's health data, the doctor can get real-time situational awareness.

3.2. Adversary Model of the EPPDA Scheme. An algorithm is considered to provide security of data aggregation to provide confidentiality, integrity, and authenticity as the basic requirements that can be targeted by attackers.

(i) Category A: Attacks against Confidentiality. Attackers always attempt to access keys by launching one of the following attacks such as known plaintext attack, chosen ciphertext attack, and chosen plaintext attack. Once the attacker gains control over the key, the aggregated data can be decrypted.

(ii) Category B: Attack on Integrity. Attackers successfully compromises one or more aggregator or sensor nodes, which may lead to either drop some data or change aggregated result with the intention of propagating false aggregate to the Medical Server (e.g., replay attack).

(iii) Category C: Attack on Authenticity. There are two types of attacks that can form threat against authenticity: (i) attacker pretends to be Medical Server and injects query into the network; (ii) attacker pretends to be a genuine sensor node or aggregator and injects false data into the network.

3.3. Design Objectives of the EPPDA Scheme. The following design goals are to be achieved.

(i) High Efficiency: The proposed aggregation scheme should be efficient, where the computational costs at IoT devices should be as less as possible, while the communication overheads should also be minimal in order to conserve energy and prolong the networks lifetime.

(ii) Security: The proposed aggregation scheme should resist against the false data injection attack from external attackers, where the proposed system must filter false data locally at the Aggregator. In the IoT-Based Healthcare Applications, the security services are obligatory desired to prevent the unauthorized nodes to access to the sensitive data, which leads to data confidentiality. Further, data integrity and authentication are considered to prevent attacks that target the integrity of sensitive data and to detect impersonation.

(iii) Robustness: A security mechanism must guarantee the availability of packet even with the presence of some compromised or defective nodes.

4. Proposed EPPDA Solution

In this section, we present the EPPDA protocol for secure data aggregation in healthcare-based IoT, which mainly consists of the following five parts: (1) setup and key generation phase; (2) encryption-sign data; (3) verification and authorization phase; (4) data aggregation phase with priority; and (5) decryption and verification phase. The flowchart for the proposed solution process is shown in Figure 3.

4.1. Setup and Key Generation Phase. For each patient, putting an admitted-on sensor-based monitoring can rely on the recommendation of the doctor. According to the patient's health data needs, the medical personnel places the medical sensors on the patient's body. Each patient must be registered into the Medical Server prior attaching any sensors. When the hardware configuration ends, the Medical Server sends a demand key information from each sensor. Then, after receiving the request by the Aggregator, the Medical Sensor nodes process the request and send the key parameter as a broadcast message toward the Aggregator.

For each Medical Sensor, the ID and the private key are generated and sent to the Aggregator, which can be denoted as $\mathrm{ID}_{\mathrm{MS}}$ and $\mathrm{MS}_{\mathrm{Pvkey}}$, respectively. The private key of the sensor node is created using the Diffie-Hellman key exchange [24]. While the Aggregator receives the sensor node ID and the private key and stores it. On the other hand, the Aggregator generates the $\mathrm{ID}_{\mathrm{Agg}}$ and $\mathrm{Agg}_{\mathrm{Pvkey}}$, before transferring the generated info to the Medical Server. Then, the Medical Server receives the ID and private key of Aggregator and stores it. Table 2 shows symbol description of the proposed EPPDA solution, whereas Figure 4 presents the key exchange model of the setup and key generation phase of the proposed

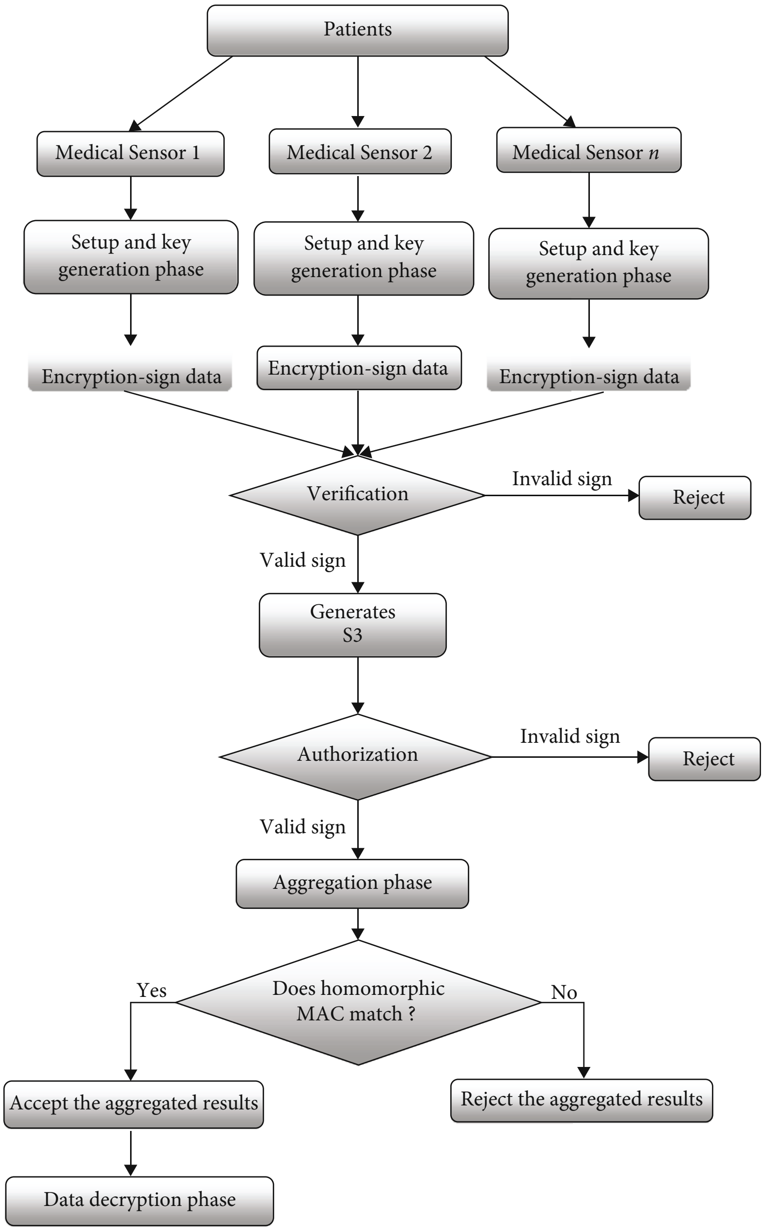


Figure 3: Concrete sequence flow diagram of the EPPDA.

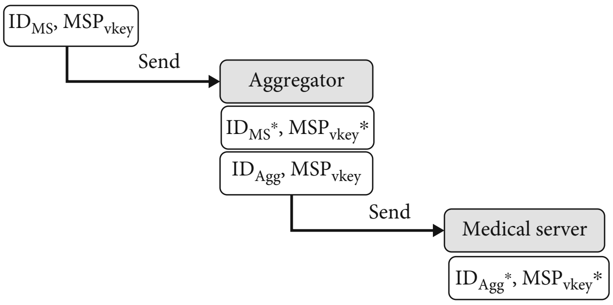
EPPDA. The pseudocode of the setup and key generation phase can be seen in Algorithm 1.

4.2. Encryption and Signing Phase. The health data comes from various devices, which in turn leads to large volume of data records [15]. In general, we differentiate different types of health data with different characteristics, including emergency situation, vital health data, and regular health data. The Medical Sensors sensing the physiological parameters (e.g., blood pressure, glucose level), where for each parameter, the normal range is recorded in a table. For most emergency situations, some alerts will be generated if a patient is in danger. For example, the blood pressure readings suddenly exceed 180/120 mmHg, which may be signs of organ damage that requires immediate medical attention. Hence, an alert message should be sent to a doctor immediately. The emergency situations are the highest priority data; thus, it should be successfully delivered to the Medical Server as soon as need be. The vital health data are the requested data by doctors for continuous monitors of a patient's condition. There are many diseases that can be diagnosed and controlled through regular monitoring of these medical data, where regular data are not for emergency situation and do not need urgent delivery requirements. The Medical Server receives periodical updates, in order to validate the data. If a patient's data falls within the reference interval, no emergency alert will be sent to doctors. However, in case of any abnormalities of the data, the Medical Server sends a notification to doctors for actions to be taken.

The confidentiality of data is mandatory in data aggregation in healthcare-based IoT. It ensures that the data cannot be accessed by unauthorized person while they flow in the

Table 2: Symbol description of the proposed EPPDA solution.

Symbol	Description
$\mathrm{ID}_{\mathrm{MS}}$	Medical sensor ID
m_i	Health data
$\mathrm{ID}_{\mathrm{Agg}}$	Aggregator ID
$\mathrm{MS}_{\mathrm{Pvkey}}$	Private key of medical sensor
$\mathrm{Agg}_{\mathrm{Pvkey}}$	Private key of aggregator
*	Stored
S_1, S_2	Messages exchange
RN_1, $\mathrm{RN}_{\ 2}$	Random numbers
$\mathrm{PK}_{\mathrm{MS}}$	Public key of medical server
$\mathrm{SK}_{\mathrm{MS}}$	Secret key shared between the medical sensor and medical server.



$\mathrm{ID}_{\mathrm{MS}}$, $\mathrm{MSP}_{\mathrm{vkey}}$
Send
Aggregator
$\mathrm{ID}_{\mathrm{MS}}$*, $\mathrm{MSP}_{\mathrm{vkey}}$*
$\mathrm{ID}_{\mathrm{Agg}}$, $\mathrm{MSP}_{\mathrm{vkey}}$
Send
Medical server
$\mathrm{ID}_{\mathrm{Agg}}$*, $\mathrm{MSP}_{\mathrm{vkey}}$*

Figure 4: Setup and key generation phase of the proposed solution.

```
Generate sensor ID: $\mathbf{ID_{MS}}$
Generate private key of Medical Sensor: $\mathbf{MS_{Pvkey}}$
Send the $\mathbf{ID_{MS}}$ and $\mathbf{MS_{Pvkey}}$ to Aggregator
Generate ID of Aggregator: $\mathbf{ID_{Agg}}$
Generate private key of Aggregator: $\mathbf{Agg_{Pvkey}}$
Send the $\mathbf{ID_{Agg}}$ and $\mathbf{Agg_{Pvkey}}$ to Medical Server
```

Algorithm 1: Setup and key generation phase.

network. The homomorphic encryption algorithm which can protect end-to-end data confidentiality will be applied in this protocol. The major advantage of homomorphic encryption is allowing complex mathematical operations to be performed on encrypted data without knowing the contents of the original plain data [25]. As calculations are performed on encrypted texts, the data privacy and confidentiality are protected [26]. Therefore, we can ensure that the content exchanged between Medical Sensors and Medical Server is protected against any modification by malicious or unauthorized users. Moreover, to allow the Medical Server determining the evil data, we use a homomorphic Message Authentication Code (MAC) scheme, to provide data integrity. MAC ensures that received message is from the authenticated source and it is not tempered by any third-party during transmission [26]. The proposed solution can guarantee data freshness in time and value. In each exchange of encrypted data between of the proposed network devices, we send a nonce N, which is an implicit sequence number that is used only once for data freshness. Algorithm 2 describes the algorithm that executed by the Medical Sensor for encryption and signing the collected data.

In the literature, attack detection can only be performed after receiving aggregate, which is considered as an inefficient detection, due to lateness of detection, significant loss in terms of computation and communication costs, and privacy information of patients [27, 28]. Hence, this proposed solution uses a scheme that allows early detection of any attack, which aims to verify the legitimacy communication between of the proposed network devices. In this regard, the proposed solution also presents a verification and authorization phase using a signature scheme based on Chebyshev polynomials [29–31]. The first verification is between Medical Sensors and Aggregator, and for this, a signature is created by the Medical Sensor. In the first order, the Medical Sensor creates two different messages as, S_1 and S_2 and the Chebyshev polynomial factor. The message S_1 is generated by encrypting the private key of the Medical Sensor, then get modulated with the random number RN_1. Message S_1 is expressed as

$$S_1 = E\left(\mathrm{MS}_{\mathrm{Pvkey}}\right) \bmod \mathrm{RN}_1. \tag{1}$$

Message S_2 is computed as follows. The sensor node $\mathrm{ID}_{\mathrm{MS}}$ is concatenated with the Chebyshev polynomial, which is concatenated with the message S_1. The hashing function is applied to the concatenated factor to generate the message S_2.

$$S_2 = h(\mathrm{ID}_{\mathrm{MS}}//M//S_1), \tag{2}$$

where M denotes Chebyshev polynomial and h denotes the hashing function. The Chebyshev polynomial factor M generated at the Medical Sensor is expressed as

$$M = 8b^4 - 8b^2 + 1. \tag{3}$$

The EX-OR operation is applied with the private key of the Medical Sensor and the hashing function of the node $\mathrm{ID}_{\mathrm{MS}}$ to generate the factor b, where the term b is computed as

$$b = \mathrm{MS}_{\mathrm{Pvkey}} \oplus h(\mathrm{ID}_{\mathrm{MS}}). \tag{4}$$

Finally, the signature α is generated using the messages S_1 and S_2, respectively. Therefore, the signature generated at the Medical Sensor is denoted as

$$\alpha = (S_1, S_2). \tag{5}$$

The signature α generated by the Medical Sensors is forwarded and stored in the Aggregator to perform the verification phase. The messages that is stored in the Aggregator is denoted as S_1^* and S_2^*, respectively. Figure 5 shows the different stages of the encryption and signing phase in the proposed EPPDA. The pseudocode of the generated signature α stage can be seen in Algorithm 3.

```
Input: $\mathrm{PK_{MS}}$, $\mathrm{SK_{MS}}$, $m_i$, Nonce
Output :$C_i$, $\mathrm{MAC_i}$
    (1) Map $m_i$ into point of the elliptic curve $Pi$
      (i) If Emergency Situation, the Medical Sensor calculate and send to the Aggregator:
        (a) Compute: $C_i^{\mathrm{ES}} = ((P_i + \mathrm{SKMS} * \mathrm{PK_{MS}})\|\mathrm{ID_{MS}}\|N_i\|\mathrm{Time}\|\mathrm{Location})$
        (b) Compute: $\mathrm{MAC}_i^{\mathrm{ES}} = \mathrm{HMAC}\,(C_i^{\mathrm{ES}}, \mathrm{SKMS})$
      (ii) If Vital Health data, the Medical Sensor calculate and send to the Aggregator:
        (a) Compute: $C_i^{\mathrm{VD}} = ((P_i + \mathrm{SKMS} * \mathrm{PK_{MS}})\|\mathrm{ID_{MS}}\|N_i\|\mathrm{Time})$
        (b) Compute: $\mathrm{MAC}_i^{\mathrm{VD}} = \mathrm{HMAC}\,(C_i^{\mathrm{VD}}, \mathrm{SKMS})$
      (iii) If Regular Health data, the Medical Sensor calculate and send to the Aggregator:
        (a) Compute : $C_i^{\mathrm{RD}} = ((P_i + \mathrm{SKMS} * \mathrm{PK_{MS}})\|\mathrm{ID_{MS}}\|N_i\|\mathrm{Time})$
        (b) Compute : $\mathrm{MAC}_i^{\mathrm{RD}} = \mathrm{HMAC}\,(C_i^{\mathrm{RD}}, \mathrm{SKMS})$
    (2) Send $(C_i^{\mathrm{ES}}, \mathrm{MAC}_i^{\mathrm{ES}})$, $(C_i^{\mathrm{VD}}, \mathrm{MAC}_i^{\mathrm{VD}})$, and $(C_i^{\mathrm{RD}}, \mathrm{MAC}_i^{\mathrm{RD}})$ to Aggregator
```

Algorithm 2: Encrypt and Signing the collected data.

4.3. Verification and Authorization Phase. Authentication is a process of verifying the legitimacy of the nodes wanting to join the process of aggregation. This local authentication phase is aimed at verifying the legitimacy of the Medical Sensors wishing to communicate with the Aggregator. The Medical Sensor and Aggregator establish interaction for local verification to prevent the adversary nodes from joining the network. The Aggregator calculates S_1^* and S_2^*, and check the legality of the Medical Sensors; if it passes the verification, the Aggregator authenticates the legality of the Medical Sensors, and receives the related health data successfully. Conversely, if the Medical Sensors is malicious and unauthorized, the Aggregator rejects the Medical Sensors from joining his network. The Aggregator receives the signature generated by the Medical Sensors and stores it to perform the verification process. The messages S_1 and S_2 that are stored in the Aggregator are specified as

$$\begin{aligned} S_1^* &= E\left(\mathrm{MS}^*_{\mathrm{Pvkey}} \bmod \mathrm{RN}_1\right), \\ S_2^* &= h(\mathrm{ID}^*_{\mathrm{MS}}//M^*//S_1^*). \end{aligned} \tag{6}$$

The Chebyshev polynomial will be sent to the Aggregator and get stored for further processing. Thus, the Chebyshev polynomial that is received by the Aggregator is specified as

$$M^* = 8b^4 - 8b^2 + 1. \tag{7}$$

Here, the term m is expressed as

$$b = \mathrm{MS}^*_{\mathrm{Pvkey}} \oplus h(\mathrm{ID}^*_{\mathrm{MS}}). \tag{8}$$

If the signature received by the Aggregator and the signature generated by the Medical Sensor are equal, $S_1 = S_1^*$ and $S_2 = S_2^*$, then the signatures are well verified. After the verification of the legitimacy of the Medical Sensors is completed, the Aggregator sends a demand to the Medical Server to request the Aggregation authorization. So, the Aggregator generates the message S_3, which can be specified as

$$S_3 = h\left(ID_{\mathrm{Agg}}//\mathrm{RN}_2\right) \oplus \mathrm{Agg}_{\mathrm{Pvkey}}. \tag{9}$$

The message S_3 generated at Aggregator is sent to the Medical Server and stored as S_3^*. The message S_3^* is expressed as

$$S_3^* = h\left(\mathrm{ID}^*_{\mathrm{Agg}}//\mathrm{RN}_2^*\right) \oplus \mathrm{Agg}_{\mathrm{Pvkey}}. \tag{10}$$

Once the Medical Server receives S_3, the S_3^* gets verified with the message S_3. If $S_3 = S_3^*$ then, the Medical Server generates an Aggregation Authorization messages S_{AA} for Aggregator. Conversely, if the Aggregator is malicious and unauthorized, the Medical Server rejects the Aggregator from joining his network. By this process, the sensor devices, gateway device, and medical server are mutually authenticated before the actual heath data transmission. Next, the Medical Server sends the message S_{AA} to Aggregator. Then, the Aggregation phase is activated. Figure 6 shows the system model of the verification phase, while the pseudocode of the verification phase can be seen in Algorithm 4.

4.4. Data Aggregation Phase with Priority. After receiving the Aggregation an authorization message from the Medical Server, the Aggregator runs the Data Aggregation phase. In the proposed EPPDA solution, the data aggregation phase is based on priority of data. In our proposed solution, the ciphertexts for each data priorities cannot be combined. Whereas only the ciphertext from the same data priority can be combined. The pseudocode of the Data Aggregation phase can be seen in Algorithm 5.

4.5. Decryption and Verification Phase. In this phase, after receiving all data packets (e.g., aggregated data), the medical server invokes the decryption and verification processes. The medical server decrypts the aggregated ciphertext and checks the end-to-end integrity. If the verification holds, the aggregated data will be accepted, otherwise rejected. Then, the data can be accessed by different entities, including hospital,

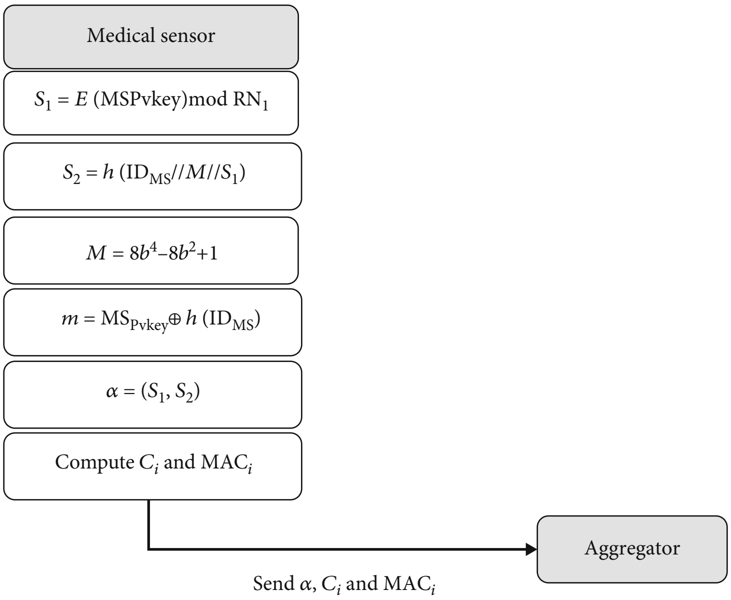

Medical sensor
$S_1 = E$ (MSPvkey)mod RN_1
$S_2 = h\ (\mathrm{ID}_{\mathrm{MS}}//M//S_1)$
$M = 8b^4 - 8b^2 + 1$
$m = \mathrm{MS}_{\mathrm{Pvkey}} \oplus h\ (\mathrm{ID}_{\mathrm{MS}})$
$\alpha = (S_1, S_2)$
Compute C_i and MAC_i
Aggregator
Send α, C_i and MAC_i

Figure 5: Encryption and signing stages of the proposed solution.

```
Created the $S_1$ and $S_2$
$S_1 = E(\mathrm{MS}_{\mathrm{Pvkey}})$ mod $\mathrm{RN}_1$
$S_2 = h(\mathrm{ID}_{\mathrm{MS}}//M//S_1)$
Generate the signature $\alpha = (S_1, S_2)$
The Medical Sensors Send $\alpha$ to Aggregator
```

Algorithm 3: Generate the signature α.

doctors, insurance companies. The pseudocode of the Data Decryption and Verification phase can be seen in Algorithm 6.

5. Security Analysis

This section discusses the security strength of our proposed EPPDA scheme, which is aimed at achieving confidentiality, authenticity, and end-to-end privacy on patient's medical health data.

(i) End-to-End Data Confidentiality: To protect the data patient's privacy, the data should be transmitted securely. The data confidentiality is the most important factor to be considered when designing the healthcare security architecture using the IoT. In the proposed EPPDA scheme, the collected sensor's data are encrypted using the homomorphic encryption algorithm. Thus, the Aggregator or attacker has no access to the data even if the Aggregator is compromised physically or virtually since the major advantage of homomorphic encryption is allowing operations to be performed on encrypted data without knowing the contents of the original data. In the following, we analyse how our scheme is secured against attacks launched by an adversary of category A.

(a) Eavesdrop Attack: In our scheme, the sensing data are encrypted under the public key of the Medical Server during the transmission process. After receiving packets from its member nodes, an Aggregator does not decrypt messages but only aggregates them. Only the Medical Server can decrypt messages to obtain the sensing data. Even though an adversary eavesdrops on a transmitted packet, he has no way to decrypt the ciphertext without the private key of the base station. Hence, the privacy is maintained end-to-end.

To conclude, our proposed scheme provides a good level of confidentiality for patient's health data (e.g., protects users' privacy of data patient's). The security proofs of the homomorphic encryption are provided in [25, 26].

(ii) End-to-End Data Integrity: To guarantee the integrity of the health data, our scheme allows the Medical Server to check whether the aggregation is done correctly since the data can be perceived at any time. We claim that the proposed scheme provides data integrity and originality. As previously described and to maintain data integrity, each Medical Sensor computes the HMAC for its encrypted measurement and sends the result to the Aggregator. The Aggregator calculates the aggregates on encrypted data without knowing the contents of the original data. The security proof of HMAC is provided in [26]. Hence, an adversary will be unable to generate a valid HMAC unless he/she knows the secret key that is shared between the Medical Sensors and the Medical Server. Even if the attacker successfully modifies the

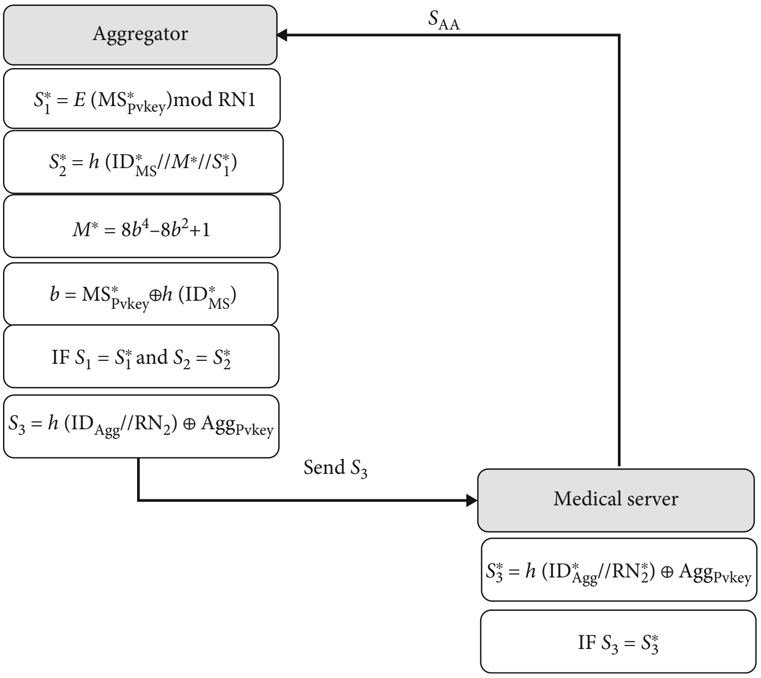

Aggregator
$S_1^* = E\,(\mathrm{MS}^*_{\mathrm{Pvkey}})\mathrm{mod\ RN1}$
$S_2^* = h\,(\mathrm{ID}^*_{\mathrm{MS}}//M^*//S_1^*)$
$M^* = 8b^4–8b^2+1$
$b = \mathrm{MS}^*_{\mathrm{Pvkey}} \oplus h\,(\mathrm{ID}^*_{\mathrm{MS}})$
IF $S_1 = S_1^*$ and $S_2 = S_2^*$
$S_3 = h\,(\mathrm{ID}_{\mathrm{Agg}}//\mathrm{RN}_2) \oplus \mathrm{Agg}_{\mathrm{Pvkey}}$
Send S_3
S_{AA}
Medical server
$S_3^* = h\,(\mathrm{ID}^*_{\mathrm{Agg}}//\mathrm{RN}_2^*) \oplus \mathrm{Agg}_{\mathrm{Pvkey}}$
IF $S_3 = S_3^*$

Figure 6: Verification phase of the proposed solution.

```
Message $S_1$ and $S_1$ are stored in the Aggregator
The Aggregator calculate:
$S_1^* = E(\mathrm{MS}^*_{\mathrm{Pvkey}})\ \mathrm{mod}\ \mathrm{RN}_1$
$S_2^* = h(\mathrm{ID}^*_{\mathrm{MS}}//M^*//S_1^*)$
If $S_1 = S_1^*$ and $S_2 = S_2^*$, signature is verified
The Aggregator generates the message $S_3$
$S_3 = h(\mathrm{ID}_{\mathrm{Agg}}//\mathrm{RN}_2) \oplus \mathrm{Agg}_{\mathrm{Pvkey}}$
The Aggregator send $S_3$ to Medical Server and stored
The Medical Server calculate:
$S_3^* = h(\mathrm{ID}^*_{\mathrm{Agg}}//\mathrm{RN}_2^*) \oplus \mathrm{Agg}_{\mathrm{Pvkey}}$
If $S_3 = S_3^*$
The Medical Server generate the Aggregation Authorization message $S_{\mathrm{AA}}$
The Medical Server send $S_{\mathrm{AA}}$ to Aggregator
```

Algorithm 4: Verification and Authorization phase.

```
Input: $(C_i^{\mathrm{ES}}, \mathrm{MAC}_i^{\mathrm{ES}})$, $(C_i^{\mathrm{VD}}, \mathrm{MAC}_i^{\mathrm{VD}})$, and $(C_i^{\mathrm{RD}}, \mathrm{MAC}_i^{\mathrm{RD}})$
    If Emergency Situation, the Aggregator calcute and send to the Medical Server:
        For $L$ ciphertexts $(C_1^{\mathrm{ES}} \ldots C_i^{\mathrm{ES}})$: Compute $C_{\mathrm{Agg}}^{\mathrm{ES}} = \sum_{i=1\cdots.L}^{j} C_i^{\mathrm{ES}}$
        For $L$ MACs $(\mathrm{MAC}_1^{\mathrm{ES}} \ldots \mathrm{MAC}_i^{\mathrm{ES}})$: Compute $\mathrm{MAC}_{\mathrm{Agg}}^{\mathrm{ES}} = \oplus\,\mathrm{MAC}_i^{\mathrm{ES}}$
    If Vital Health data, the Aggregator calculate and send to the Medical Server:
        For $L$ ciphertexts $(C_1^{\mathrm{VD}} \ldots C_i^{\mathrm{VD}})$: Compute $C_{\mathrm{Agg}}^{\mathrm{VD}} = \sum_{i=1\cdots.L}^{j} C_i^{\mathrm{VD}}$
        For $L$ MACs $(\mathrm{MAC}_1^{\mathrm{VD}} \ldots \mathrm{MAC}_i^{\mathrm{VD}})$: Compute $\mathrm{MAC}_{\mathrm{Agg}}^{\mathrm{VD}} = \oplus\,\mathrm{MAC}_i^{\mathrm{VD}}$
    If Regular Health data, the Aggregator calculate and send to the Medical Server:
        For $L$ ciphertexts $(C_1^{\mathrm{RD}} \ldots C_i^{\mathrm{RD}})$: Compute $C_{\mathrm{Agg}}^{\mathrm{RD}} = \sum_{i=1\cdots.L}^{j} C_i^{\mathrm{RD}}$
        For $L$ MACs $(\mathrm{MAC}_1^{\mathrm{RD}} \ldots \mathrm{MAC}_i^{\mathrm{RD}})$: Compute $\mathrm{MAC}_{\mathrm{Agg}}^{\mathrm{RD}} = \oplus\,\mathrm{MAC}_i^{\mathrm{RD}}$
Output: $(C_{\mathrm{Agg}}^{\mathrm{ES}}, \mathrm{MAC}_{\mathrm{Agg}}^{\mathrm{ES}})$, $(C_{\mathrm{Agg}}^{\mathrm{VD}}, \mathrm{MAC}_{\mathrm{Agg}}^{\mathrm{VD}})$, and $(C_{\mathrm{Agg}}^{\mathrm{RD}}, \mathrm{MAC}_{\mathrm{Agg}}^{\mathrm{RD}})$
```

Algorithm 5: Data Aggregation phase with Priority.

```
**Input:**$(C^{\mathrm{ES}}_{\mathrm{Agg}}, \mathrm{MAC}^{\mathrm{ES}}_{\mathrm{Agg}}), (C^{\mathrm{VD}}_{\mathrm{Agg}}, \mathrm{MAC}^{\mathrm{VD}}_{\mathrm{Agg}})$, and $(C^{\mathrm{RD}}_{\mathrm{Agg}}, \mathrm{MAC}^{\mathrm{RD}}_{\mathrm{Agg}})$
**Output :**$\boldsymbol{m_i}$
For each pair $((C^{\mathrm{ES\ or\ VD\ or\ RD}}_{\mathrm{Agg}}\ {}_{g}, (\mathrm{MAC}^{\mathrm{ES\ or\ VD\ or\ RD}}_{\mathrm{Agg}}\ {}_{g})$ do
Compute $\mathrm{MAC}'_{\mathrm{agg}}$ of $C_{\mathrm{agg}}$ using SKMS
If $\mathrm{MAC}'_{\mathrm{agg}} = C_{\mathrm{agg}}$ then
Decrypt $C_{\mathrm{agg}}$
else
Reject $(C_{\mathrm{agg}}, \mathrm{MAC}_{\mathrm{agg}})$
```

Algorithm 6: Decryption and Verification Phase.

information or launches replay attacks, the Medical Server can verify the correctness of the received data. In the following, we analyse how our scheme is secured against attacks launched by an adversary of category B.

(a) Malleability: An adversary can alter a ciphertext by injecting false data, but it will not be detected due to the homomorphic property. In our scheme, we use a homomorphic MAC scheme to verify the integrity of the data. If the encrypted data is tampered, the integrity verification will fail; thus, the Medical Server will refuse the received packet.

(b) Replay Attack: An adversary can impersonate any node through replaying old packets recorded from past communications; therefore, we add current timestamps to messages being signed to resist replay attacks. Thus, the Medical Server can ensure data freshness by checking the validity of the timestamps.

(c) Injection Attack: With public key cryptography, any adversary can generate a reasonable ciphertext and inject it into the network to deceive the Medical Server. In our scheme, each sender computes a MAC using the symmetric key shared with the Medical Server, so the receiver will reject these injected packets in the verification of MAC step if an adversary injects its false data.

To conclude, our proposed scheme provides a good level of integrity for patient's health data.

(iii) Identity Anonymity and Authenticity: To verify the legitimacy communication between the network component devices, we propose an authentication phase in each layers of proposed network model. We analyse how our scheme is secured against attacks launched by an adversary of category C. In the proposed scheme, the authentication of the communicating parties depends on the verification of proposed signature. In the authentication phase, the hash Chebyshev polynomials are jointly applied to achieve mutual authentication. The initial authentication is between the Medical Sensors and the Aggregator, where the Aggregator authenticates the Medical Sensors using the shared signatures. If the signature stored by the Aggregator and the signature generated by the Medical Sensor are equal, $S_1 = S_1^*$ and $S_2 = S_2^*$, then the signatures are well verified. In case of a successful authentication, the Aggregator receives the related health data successfully. Conversely, if the Medical Sensor is in successful authentication, the Aggregator rejects the health data and not accept the Medical Sensors wants to join its network. On the other hand, the second authentication is between the Aggregator and the Medical Server. The Medical Server verifies the legitimacy of the Aggregator. The Aggregator is authenticated when the S_3^* value stored in the Medical Server matches with the received S_3. If $S_3 = S_3^*$, then the successful authentication. Conversely, if the Aggregator is malicious and unauthorized, the Medical Server rejects the Aggregator from joining its network. However, our identity authenticity mechanism can identify the identity fraud behaviour. We can see that the proposed scheme realizes the mutual authentication of between the communication parties. By this process, the sensor devices, the gateway device, and medical server are mutually authenticated before the actual heath data transmission.

(iv) Unauthorized Aggregation: In the proposed scheme and to protect from unauthorized aggregation, the Medical Sensor and Aggregator establish interaction for local verification to prevent the adversary nodes from joining the network and in order to prevent any unauthorized third parties from performing illicit alterations. The Aggregator calculates S_1^* and S_2^*, and check the legality of the Medical Sensors. If it passes the verification, the Aggregator authenticates the legality of the Medical Sensors, and receives the related health data successfully. Conversely, if the Medical Sensor is malicious and unauthorized, the Aggregator rejects the Medical Sensors from joining its network.

(v) Data Freshness: To ensure the data freshness of the message originator, the number of the nonce and the time of sensing data are added to each data transmissions. An attacker who attempts to send valid packets already transmitted, called replay attack, cannot disrupt the network, because even if it is

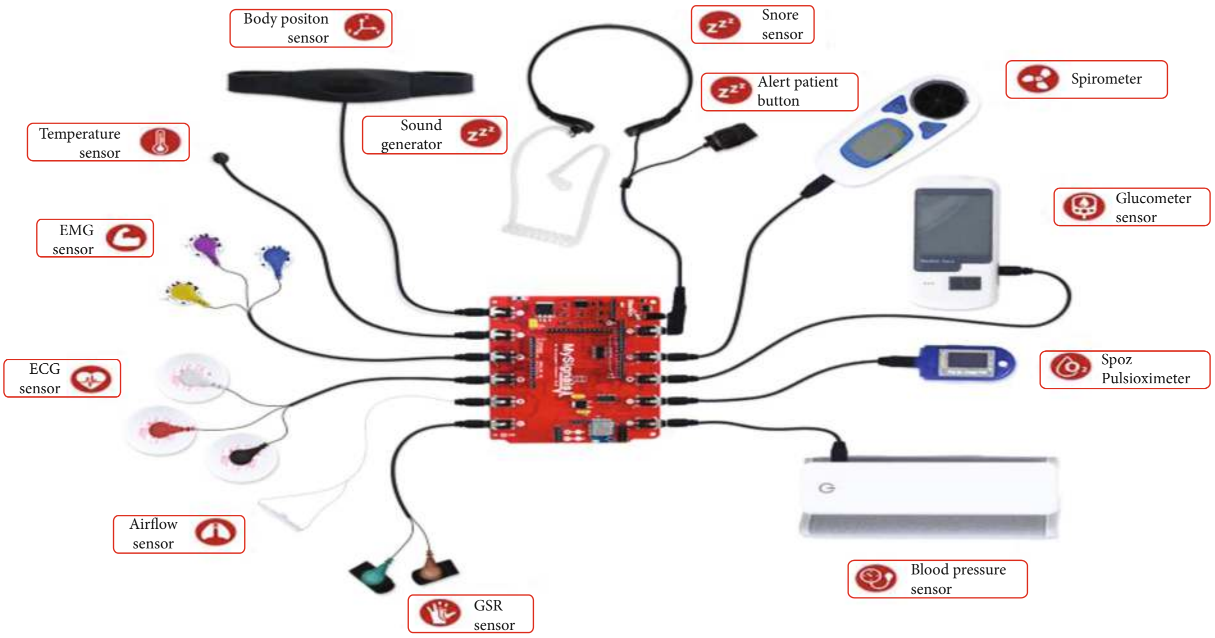


Figure 7: MySignals HW V2 platform [33].

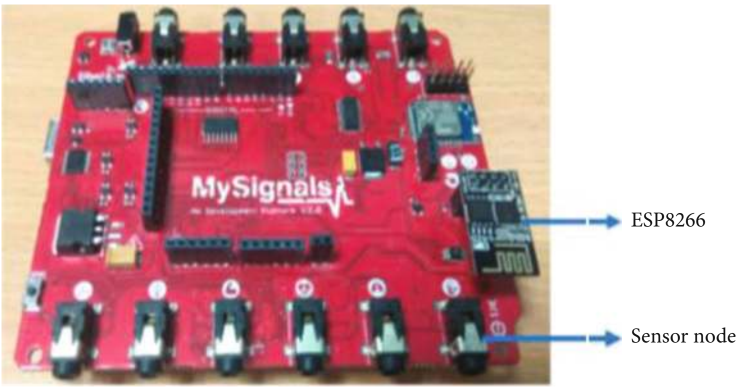


Figure 8: MySignals with sensor nodes and WiFi module.

valid, it is not fresh, and the use of nonce prevents that attack, so the scheme ensures the data freshness.

6. Performance Analyses and Experimental Results

The EPPDA scheme is evaluated by providing an overview of the hardware platform, before presenting the performance results of our proposed EPPDA scheme.

6.1. Hardware Components. The vital sign sensing unit of this system is the MySignals HW V2 platform, which is a development platform for medical devices and health applications, as Figure 7 displays [32]. It monitors patients' health by deploying different medical sensors on patients' body to get vital data of patients for subsequent analysis that is done by physicians [33]. The MySignals HW V2 platform is one of the most comprehensive versions on the market, as it supports more than 20 biomedical sensors to measure biometric parameters such as ECG signals, blood pressure, blood oxygen, pulse, respiratory rate, and body temperature. The MySignals HW V2 platform relies on the Atmega 328 (Arduino UNO) microcontroller to manage various sensors and allows tablets and smartphones to communicate with it [34].

In contrast to the medical sensor, the Aggregator should be a device that has access to unlimited power and resources. The tablet acts as the Aggregator role and communicates with the MySignals HW V2 platform via WiFi to collect the vital signs. Figure 8 shows the MySignals platform with various sensor ports. This platform can be also integrated with a WiFi serial transceiver module ESP8266, where all the data gathered by MySignals is encrypted and sent to the Aggregator through WiFi. Therefore, the Medical server is developed with the purpose of receiving, storing, and distributing the medical data from patients. In healthcare application, the medical information usually needs to be distributed among medical doctors and display, archival, and analysis devices. In the proposed solution, the Medical server is a laptop.

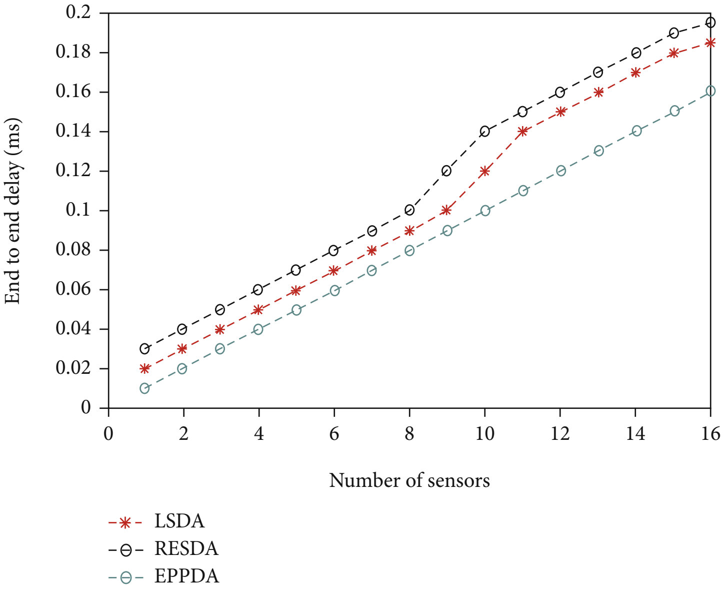


Figure 9: The end-to-end delay for LSDA, RESDA, and EPPDA.

These laptops have relatively powerful processing, memory, and transmission capacity; thus, there is no power constraint, which in turn lead to long battery life. Further, it can be displayed in an easy-to-read format for fast assessment and action. The Medical Server is composed of presentation tier, web tier, and database tier. The medical information of the patient that is stored the Medical Server will be accessible by specific people who have the authorization to access such as patient himself, doctor, and patient's family member. The aggregated data between the system components can be encrypted by our proposed EPPDA scheme to protect it from any malicious acts of the hackers [35].

6.2. Experiment and Performance Evaluation. This section analyses the efficiency of the proposed EPPDA scheme by evaluating the end-to-end delay, computation overhead, communication overhead, and energy consumption, following by presenting the comparative analysis of our proposed system with the existing systems LSDA [17] and RESDA [18].

6.2.1. End-to-End Delay. The end-to-end delay considers as the total time consumed between the data packet sending by the Medical Sensors and the time when the packet arrives at the Medical Server, and can be mathematically expressed as

$$\text{Av.End to End Delay} = \frac{\left(\text{Start time}\left(_{ij}\right)\text{-End time}\left(_{ij}\right)\right)}{N}, \quad (11)$$

where ij is the time when sending/receiving of packet j at node i starts/stops and N is the total number of nodes. Figure 9 demonstrates the results of end-to-end delay for our proposed scheme with a comparison with other solutions in the literature. We notice that the EPPDA protocol had an enough end-to-end delay in comparison of other solutions. The experimental results revealed that the end-to-end delay of the proposed EPPDA show decreases with 17%, 28%, and 34% under varying time intervals in compassion to LSDA and RESDA, respectively. Thus, the end-to-end delay of proposed EPPDA is the best compared to the existing protocols especially when the Medical Sensors count increases. It consists of two reasons for the reduction of end-to-end delay in EPPDA:

(i) In the proposed solution, the Medical Sensors wants join the process of aggregation are verified, if the Medical Sensors is in-successful authentication, the Aggregator rejects their data in order to prevent the adversary nodes inject the false traffic; thus, avoid energy consumption unnecessary due to transmitting them.

(ii) In the medical server of the proposed solution, the packet of each Medical Sensor is verified individually. In this way, if the verification fails to pass for one packet, only this packet is discarded. Unlike other schemes, once the verification fails, all packets, including valid packets will be abandoned, which means all data need to be retransmitted.

6.2.2. Computational Cost. The computation cost of the proposed EPPDA scheme can be calculated as three levels: (i) at the Medical Sensors; (ii) at the Aggregator; and (iii) at the medical server, respectively. In the Medical Sensor, we calculate the computational cost of data encryption, generation of MAC, and generation of signature used for the verifying the legitimacy of the Medical Sensor at the Aggregator. The same, at the Aggregator, we calculate the computation cost of verifying the legitimacy of the Medical Sensors, the generation of aggregate ciphertext, generation of aggregate MAC, and generation of signature used of the verifying the

TABLE 3: Computation complexity of the proposed EPPDA scheme.

Entity name	Involving operations	Computation complexity
Medical sensors	(1) Crypt his health data (2) Generate the MAC (3) Generates the signature of verification the medical sensor at the aggregator	2SM + 2PA + 2H
Aggregator	(1) Verify the legitimacy of the medical sensors (2) Generates an aggregated cipher text C_{agg} (3) Generates an aggregated MAC_{agg} (4) Generates the signature of verification the aggregator at the medical server	$((n * 2\mathrm{SM}) + 2\mathrm{H})$
Medical server	(1) Verify the legitimacy of the aggregator (2) Aggregated data integrity verification (3) Data decryption	5

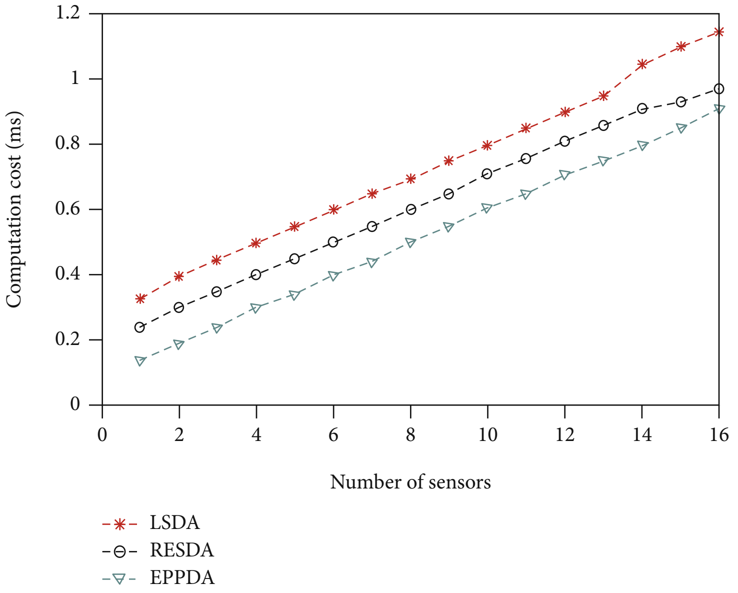


FIGURE 10: The computational cost for LSDA, RESDA, and EPPDA.

legitimacy of the Aggregator and medical server. At the medical server, we calculate computational cost of verifying the legitimacy of the Aggregator and verification of aggregate MAC.

In the computational overhead, we designate symbol SM as the cost of one Scalar Multiplication, PA is the cost of one Point Addition, E is the cost of one modular Exponentiation, and H is the cost of one Hash operation.

In our proposed scheme, when the medical sensor crypt his health data, he needs one Scalar Multiplication and two modular Exponentiation. Consequently, the computation involves (1SM+2PA) operations. Also, for generating the MAC, the sensor needs 1 hashing operation and 1 exponentiation operation. Subsequently, the computation involves (1SM+1H) operations. Moreover, each sensor generates the signature of verification which requires 1 hashing operation. The computational overhead of each medical sensor is (2SM+2PA+2H) in total for every health data.

After receiving all the ciphertext and corresponding signatures, the Aggregator first verify the legitimacy of the Medical Sensors, which involves 1 hashing operation. After the verification of the legitimacy of each Medical Sensor, the Aggregator generates an aggregated cipher text C_{agg}, which involves Scalar Multiplication. Moreover, it generates an aggregated MAC_{agg}, which involves Scalar Multiplication. Moreover, the Aggregator generates the signature of verification which requires 1 hashing operation for authentication between the Aggregator and the Medical Server. The computational overhead at Aggregator is $((n * 2\mathrm{SM}) + 2\mathrm{H})$.

At the medical server, the computational cost of verifying the legitimacy of the Aggregator involves 1 hashing operation. Moreover, when the medical server receives the aggregated results, it needs 1 hashing operation for verifying the aggregate MAC, and it needs one Scalar Multiplication and two modular Exponentiation for computing decryption of aggregated ciphertext. The computational overhead at Aggregator is (SM +2H). The computation complexities of the major entities in the system are shown in Table 3.

In Figure 10, we present the computational cost of the proposed EPPDA scheme with a comparison to other

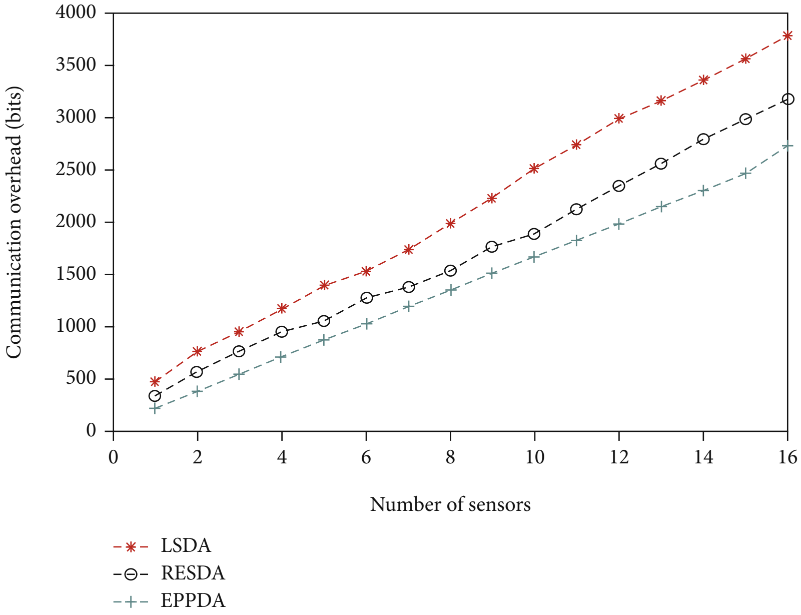


Figure 11: The communication overhead for LSDA, RESDA, and EPPDA.

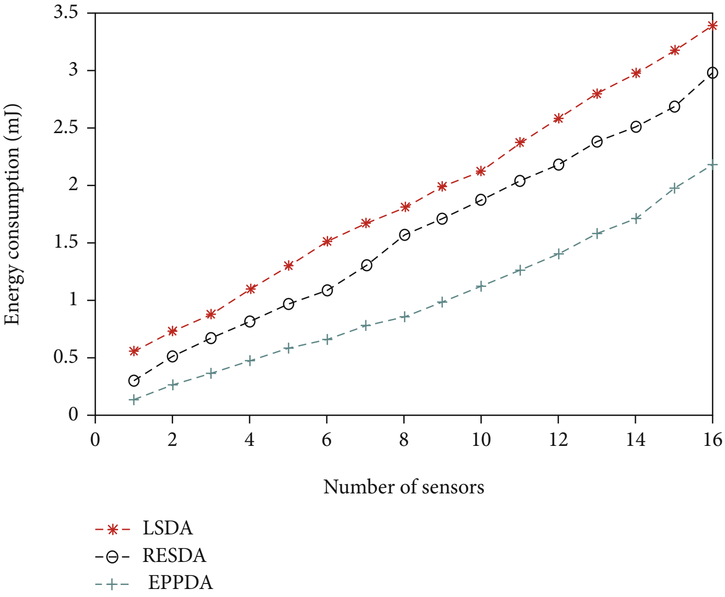


Figure 12: The total energy consumption for LSDA, RESDA, and EPPDA.

solutions. It can be observed that our proposed scheme achieves a significant reduction in the total computation cost compared with LSDA and RESDA. To illustrate more, when the number of Medical Sensors is 10, the total computation cost of our proposed scheme is 0.6 ms, which means 20% and 35% less than LSDA and RESDA, respectively.

6.2.3. Communication Overhead. The communication overhead in the proposed EPPDA scheme is divided into two levels, namely, the communication overhead between the Medical Sensors and the Aggregator. While the second level is the communication overhead between the Aggregator and the Medical Server. The communication overhead is measured as the total data transmitted in the networks.

In the Medical Sensors-to-Aggregator communication, each Medical Sensor sign their health data and transmit the data to the Aggregator. According to [18], a ciphertext generated by the OU algorithm is 160 bits. Moreover, we consider a 4-byte homomorphic MAC for calculation in accordance to [33], while the signature of verification is also 4 bytes. Therefore, in our scheme, the size of one packet transmitted to Aggregator from each Medical Sensor is 224 bits. In the Aggregator-to-Medical Server communication, the length of ciphertext C_j is 160 bits, the communication overhead of

Table 4: Comparison between EPPDA and other solutions in the IoT-based healthcare.

Solutions	Security features					Efficiency		
	Confidentiality	Integrity	Authentication	Freshness	Scalability	Computational cost	Communication cost	Communication overhead
PHDA [15]	Yes	No	Yes	Yes	No	Very high	High	Large
PPM-HAD [16]	Yes	Yes	No	No	No	High	High	Very high
LSDA [17]	No	Yes	Yes	No	No	Very high	Very high	Fair
RESDA [18]	Yes	Yes	Yes	Yes	No	Medium	Medium	Fair
ERCS [19]	Yes	Yes	No	No	⊗	Very	Medium	Medium
CBCSES [20]	Yes	No	Yes	Yes	No	Low	Very high	Large
EPPDA	Yes	Yes	Yes	Yes	Yes	Small	Very low	Very small

C_{agg} is equals $160 * n$, when their n sensors are evolved into the process. In our scheme, we consider a 4-byte MAC, 4 bytes MACagg, 4 bytes for the signature of verification. Therefore, the size of one transmitted packet in our scheme is $(160 * n) + 32 + 32$ bits. In Figure 11, we present the communication overhead of the proposed EPPDA scheme with a comparison to other solutions.

6.2.4. Energy Consumption. Energy consumption is the central issue in application based on IoT. The Computational and communication cost are two aspects that have a direct impact on energy consumption, which subsequently leading to shorten the life of sensor nodes. Thus, the energy consumption is calculated for cryptographic operations as follows:

$$E(\mathrm{mJ}) = U(V) \times I(\mathrm{mA}) \times t(\mathrm{ms}), \tag{12}$$

where U represents the supply voltage, I represent the current draw of the hardware, and t represents the time. According to the datasheet available in [28], with MySignals HW V2 platform, the voltage is 3 V, and the wireless transceiver draws a current of 20 mA for receiving and 17.7 mA for radio transmissions. The current draw for CPU is about 1.8 mA, and in low power mode, the current draw is 0.0545 mA. The wireless communication currents (20 mA for listening and 17.7 mA for radio transmission) are much more important than the CPU current (1.8 mA); that is why communications are more expensive in terms of energy consumption than the computational primitives. In MySignals HW V2 platform, the timer produces 32,768 ticks per second. The Communication Cost is computed with the following equation, where T_x and T_r are, respectively, the Transmission time and the Receiving time.

$$\mathrm{CommCost(mJ)} = \frac{[(T_x \times 17.7\mathrm{mA}) + (T_r \times 20\mathrm{mA})]}{32768} \times 3\mathrm{V}. \tag{13}$$

The Computational Energy Cost of sensor nodes is a key constituent of the overall operational energy costs in IoT. The Computational Cost is computed according to the following equation where T_{cpu} is the time elapsed in CPU operations:

$$\mathrm{ComptCost(mJ)} = \frac{T_{\mathrm{cpu}}}{32768} \times 1.8\mathrm{mA} \times 3\mathrm{V}. \tag{14}$$

The total power consumption by the sensor node for EPPDA scheme is estimated with the following equation:

$$\mathrm{TotalEnergy(mJ)} = \mathrm{EnergyComm} + \mathrm{EnergyCompt}. \tag{15}$$

Figure 12 shows the energy consumption by EPPDA is lower than that of two other schemes. The reason is that the ECIPAP and SDA-HP schemes generate too many unnecessary messages for providing integrity and privacy in data aggregation. This gain can be explained by the fact that far fewer computational loads are engaged in our algorithm, because of the use of homomorphic encryption and the Medical Sensors wanting to join the process of aggregation are verified, thus, avoid energy consumption unnecessary due to transmitting them.

6.3. Comparison of Secure Data Aggregation Protocols. This section compares the proposed protocol with existing secure data aggregation protocols. The comparison is based on the security requirements and the performance evaluation. From Table 4, it is evident that the proposed EPPDA scheme satisfies most of the security properties unlike other related data aggregation schemes in IoT-based healthcare applications. In addition, through performance evaluation, we have also demonstrated the proposed EPPDA satisfies the communication and computation overheads requirements.

7. Conclusions

The recent developments in the area of IoT shows a great promise for providing solutions for healthcare. Yet, protecting data privacy and integrity during data aggregation at the same time is a common challenge in IoT-based healthcare systems. This paper presents a novel secure aggregation scheme that provide provably secure message integrity with different trade-off between computation cost, communication payload, and security assumptions. The proposed EPPDA is based on the verification and authorization phase to verifying the legitimacy of the nodes wanting to join the process of aggregation. The proposed scheme, also, uses on an additive homomorphic encryption algorithm that allows aggregation on encrypted data that combined with homomorphic MAC. The security analysis and performance evaluation show that our scheme is able to resist against various attacks such as compromise node attacks and unauthorized aggregation. A comparison of the communication overhead with respect to the existing protocols exhibits the viability efficiency of the proposed protocol on resource-constrained devices. Further research can be considered to study the possibility of applying this algorithm in different types of medical sensors and then assess whether or not there are better outcome results can be obtained.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors are grateful to the Deanship of Scientific Research at Taif University, Kingdom of Saudi Arabia for funding this project through Taif University Researchers Supporting Project Number (TURSP-2020/265).

References

[1] S. Selvaraj and S. Sundaravaradhan, "Challenges and opportunities in IoT healthcare systems: a systematic review," *SN Applied Sciences*, vol. 2, no. 1, p. 139, 2020.

[2] L. M. Dang, M. Piran, D. Han, K. Min, and H. Moon, "A survey on internet of things and cloud computing for healthcare," *Electronics*, vol. 8, no. 7, p. 768, 2019.

[3] K. T. Kadhim, A. M. Alsahlany, S. M. Wadi, and H. T. Kadhum, "An overview of patient's health status monitoring system based on internet of things (IoT)," *Wireless Personal Communications*, vol. 114, no. 3, pp. 2235–2262, 2020.

[4] Y. Zhan and B. Wang, "Cryptanalysis of a certificateless aggregate signature scheme for healthcare wireless sensor network," *Security and Communication Networks*, vol. 2019, Article ID 6059834, p. 5, 2019.

[5] Y. Pu, J. Luo, C. Hu et al., "Two secure privacy-preserving data aggregation schemes for IoT," *Wireless Communications and Mobile Computing*, vol. 2019, Article ID 3985232, 11 pages, 2019.

[6] A. Ara, M. Al-Rodhaan, Y. Tian, and A. Al-Dhelaan, "A secure privacy-preserving data aggregation scheme based on bilinear ElGamal cryptosystem for remote health monitoring systems," *IEEE Access*, vol. 5, pp. 12601–12617, 2017.

[7] Y. Zhang, J. Zhao, D. Zheng et al., "Privacy-preserving data aggregation against false data injection attacks in fog computing," *Sensors*, vol. 18, no. 8, article 2659, 2018.

[8] S. B. Othman, A. A. Bahattab, A. Trad, and H. Youssef, "Confidentiality and integrity for data aggregation in WSN using homomorphic encryption," *Wireless Personal Communications*, vol. 80, no. 2, pp. 867–889, 2015.

[9] C. Guo, P. Tian, and K.-K. R. Choo, "Enabling privacy-assured fog-based data aggregation in E-healthcare systems," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 3, pp. 1948–1957, 2021.

[10] J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, "PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 8, 2017.

[11] M. Azees, P. Vijayakumar, and L. J. Deboarh, "EAAP: efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 9, pp. 2467–2476, 2017.

[12] J. Cui, L. Wei, H. Zhong, J. Zhang, Y. Xu, and L. Liu, "Edge computing in VANETs-an efficient and privacy-preserving cooperative downloading scheme," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 6, pp. 1191–1204, 2020.

[13] Y. Choi, Y. Lee, J. Moon, and D. Won, "Security enhanced multi-factor biometric authentication scheme using bio-hash function," *PLoS One*, vol. 12, no. 5, article e0176250, 2017.

[14] C. T. Li, C. C. Lee, C. Y. Weng, and S. J. Chen, "A secure dynamic identity and chaotic maps based user authentication and key agreement scheme for e-healthcare systems," *Journal of Medical Systems*, vol. 40, no. 11, 2016.

[15] K. Zhang, X. Liang, M. Baura, and R. Lu, "PHDA: a priority based health data aggregation with privacy preservation for cloud assisted WBANs," *Information Sciences*, vol. 284, pp. 130–141, 2014.

[16] S. Han, S. Zhao, Q. Li, C. Ju, and W. Zhou, "PPM-HDA: privacy-preserving and multifunctional health data aggregation with fault tolerance," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 9, pp. 1940–1955, 2016.

[17] S. B. Othman, A. A. Bahattab, A. Trad, and H. Youssef, "LSDA: lightweight secure data aggregation scheme in healthcare using IoT," in *10th International Conference on Information Systems and Technologies*, Lecce, Italy, December 2019.

[18] B. O. Soufiene, A. A. Bahattab, A. Trad, and H. Youssef, "RESDA: robust and efficient secure data aggregation scheme in healthcare using the IoT," in *2019 International Conference on Internet of Things, Embedded Systems and Communications(IINTEC)*, pp. 209–213, Tunis, Tunisia, December 2019.

[19] G. Mehmood, M. Z. Khan, A. Waheed, M. Zareei, and E. M. Mohamed, "A trust-based energy-efficient and reliable communication scheme (trust-based ERCS) for remote patient monitoring in wireless body area networks," *IEEE Access*, vol. 8, pp. 131397–131413, 2020.

[20] I. Ullah, N. U. Amin, M. A. Khan, H. Khattak, and S. Kumari, "An efficient and provable secure certificate-based combined signature, encryption and signcryption scheme for internet of things (IoT) in mobile health (M-health) system," *Journal of Medical Systems*, vol. 45, no. 1, p. 4, 2021.

[21] Y. Li, Q. Cheng, X. Liu, and X. Li, "A secure anonymous identity-based scheme in new authentication architecture for mobile edge computing," *IEEE Systems Journal*, vol. 14, pp. 1–12, 2020.

[22] M. R. Nassoro, "SUAA: a secure user authentication scheme with anonymity for the single & multi-server environments," *Information Sciences*, vol. 477, pp. 369–385, 2019.

[23] Z. Ma, Y. Yang, X. Liu et al., "EmIr-Auth: eye movement and iris-based portable remote authentication for smart grid," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 10, pp. 6597–6606, 2020.

[24] U. M. Maurer and S. Wolf, "The Diffie–Hellman protocol," *Designs, Codes and Cryptography*, vol. 19, no. 2/3, pp. 147–171, 2000.

[25] Y. Harbi, Z. Aliouat, A. Refoufi, and S. Harous, "Efficient end-to-end security scheme for privacy-preserving in IoT," in *2019 International Conference on Networking and Advanced Systems (ICNAS)*, pp. 1–6, Annaba, Algeria, 2019.

[26] C. A. Lara-Nino, A. Diaz-Perez, and M. Morales-Sandoval, "Lightweight elliptic curve cryptography accelerator for internet of things applications," *Ad Hoc Networks*, vol. 103, article 102159, 2020.

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

[28] Y. Tian, Y. Li, X. Liu, R. H. Deng, and B. Sengupta, "Pri-BioAuth: privacy-preserving biometric-based remote user authentication," in *2018 IEEE Conference on Dependable and Secure Computing (DSC)*, pp. 1–8, Kaohsiung, Taiwan, December 2018.

[29] C. Quan, J. Jung, H. Lee, D. Kang, and D. Won, "Cryptanalysis of a chaotic chebyshev polynomials based remote user authentication scheme," in *2018 International Conference on Information Networking (ICOIN*, pp. 438–441, Chiang Mai, Thailand, January 2018.

[30] X. Guo, Q. Guo, Y. Li et al., "User authentication protocol based on Chebyshev polynomial for wireless sensor networks," in *2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, pp. 1588–1592, Chongqing, China, October 2018.

[31] E. O. Adeyefa, L. S. Akinola, and O. D. Agbolade, "A new cryptographic scheme using the Chebyshev polynomials," in *2020 International Conference in Mathematics, Computer Engineering and Computer Science (ICMCECS)*, pp. 1–3, Ayobo, Nigeria, March 2020.

[32] M. T. Almalchy, V. Ciobanu, and S. M. Algayar, "Solutions for healthcare monitoring systems architectures," in *2018 IEEE 16th International Conference on Embedded and Ubiquitous Computing (EUC)*, pp. 123–128, Bucharest, Romania, October 2018.

[33] H. Ben Hassen, W. Dghais, and B. Hamdi, "An E-health system for monitoring elderly health based on internet of things and fog computing," *Health Information Science and Systems*, vol. 7, no. 1, p. 24, 2019.

[34] D. Sadhukhan, S. Ray, G. P. Biswas, M. K. Khan, and M. Dasgupta, "A lightweight remote user authentication scheme for IoT communication using elliptic curve cryptography," *The Journal of Supercomputing*, vol. 77, no. 2, pp. 1114–1151, 2021.

[35] N. Bandyopadhyay, P. Gaurav, M. Kundu, B. Misra, and B. Hoare, "IoT-based health and farm monitoring system via LoRa-based wireless sensor network," in *2020 4th International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech)*, pp. 1–7, Kolkata, India, October 2020.