Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

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

Faris. A. Almalki
Taif University

Ben othman Soufiene (ben_oth_soufiene@yahoo.fr)
ISIMed: Universite de Gabes Institut Superieur d'Informatique de Medenine

Research Article

Keywords: Internet of Things, Healthcare, Data Aggregation, Security, Homomorphic Encryption

Posted Date: March 23rd, 2021

DOI: https://doi.org/10.21203/rs.3.rs-172603/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

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

Faris. A. Almalki[1], Ben othman Soufiene[2*]
[1]Department of Computer Engineering, College of Computers and Information Technology, Taif University, Taif, Kingdome of Saudi Arabia.
[2]PRINCE Laboratory Research, ISITcom, Hammam Sousse, University of Sousse, Tunisia.
[*]Corresponding author: ben_oth_soufiene@yahoo.fr

Abstract

Internet of Things (IoT) connects various kinds of intelligent objects and devices using the internet to collect and exchange data. Nowadays, The IoT is used in diverse application domains, including the healthcare. In the healthcare domain, the IoT devices can collects patient data, and its forwards the data to the healthcare professionals can view it. The IoT devices are usually resource-constrained in terms of energy consumption, storage capacity, computational capability, and communication range, data aggregation techniques are used to reduce the communication overhead. However, in healthcare system using IoT, the heterogeneity of technologies, the large number of devices and systems, and the different types of users and roles create important challenges in terms of security. For that, the security and privacy aggregation of health data are very important aspects. In this paper, we propose a novel secure data aggregation scheme based on homomorphic primitives in IoT based healthcare systems, called "An Efficient and Privacy-Preserving Data Aggregation Scheme with authentication for IoT-Based Healthcare applications" (EPPDA). EPPDA is based the Verification and Authorization phase to verifying the legitimacy of the nodes wants to join the process of aggregation. EPPDA uses additive homomorphic encryption to protect data privacy and combines it with homomorphic MAC to check the data integrity. The security analysis and experimental results show that our proposed scheme guarantees data privacy, messages authenticity, and integrity, with lightweight communication overhead and computation.

Keywords: Internet of Things; Healthcare; Data Aggregation; Security; Homomorphic Encryption.

1. Introduction

The Internet of Things (IoT) is a new paradigm that is rapidly gaining ground in the modern wireless telecommunications scenario. 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, etc, this through unique addressing schemes, are able to interact with each other and cooperate with their neighbors to achieve common goals [1]. The IoT will promote the development of applications in many different fields, such as home automation, industrial automation, medical aids, mobile health, assistance to the elderly, intelligent energy management and networks. intelligent, automotive, traffic management, and many others [2]. These applications will use the potentially enormous amount and variety of data generated by these objects to provide new services to citizens, businesses and public administrations [3]. The interested reader is referred to [1-7] for a more in-depth understanding of IoT.

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 like temperature, heart rate, blood pressure, etc. 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 attack 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 extremely easy [10]. Finally, most IoT components are characterized by low capacities in terms of energy and computing resources and therefore 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. This is one of the essential processes for removing redundant data and saving energy [12]. The main purpose of data aggregation is to collect and aggregate data. In addition, it can be extended the life of the network [13]. The data aggregation scheme also faces many security challenges [10-20]. Sensor nodes are often deployed in hostile environments with low bandwidth and unsecured communication channels. This can lead to malicious modification of data and tampering with data, resulting in the violation of a user's privacy [14].

To solve the problems mentioned above, in this paper, we propose 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 the Verification and Authorization phase to verifying the legitimacy of the nodes wants to join the process of aggregation. EPPDA uses additive homomorphic encryption to protect data privacy and combines it with homomorphic MAC to check the data integrity. The security analysis and the performance evaluation based on experimental results and a comparison of computational cost with related schemes show the proposed solution reduce communication and computation overhead.

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.

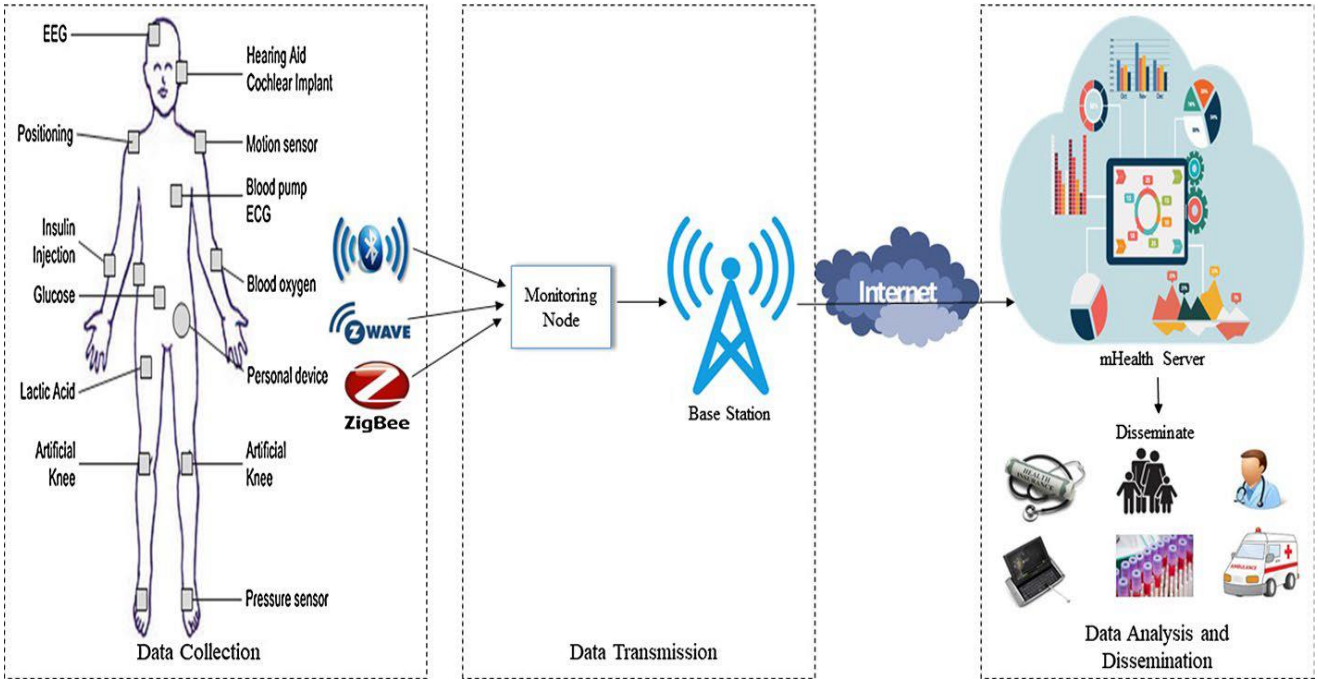

Figure.1. IoT-based healthcare monitoring architecture [3].

2. Related work

Security is one of the important factors that must be considered when developing IoT-based healthcare systems [14]. 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.

In [15], Zhang et al. present a health data aggregation scheme named: 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], et al. Introduce an efficient and privacy-friendly data aggregation known as Fault Tolerance Multifunctional Health and Privacy Preserving Data Aggregation for Cloud Assisted WBANs (PPM-HAD). This aims to address 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 non-additive 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 Ben othman et al. [17] 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 take into account different types of health data.

In [18], Ben othman et al. presents an end-to-end secure data aggregation scheme named: 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.

Yi Liu et al. [19] proposed a new contribution named: 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 bio-sensors 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.

Insaf Ullah et al. [20] proposed a novel contribution named: 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.

The techniques are discussed above and summarized in table 1.

Table 1: Summary of techniques.

Literature	Focus area(s) of the paper	Strengths	Weakness
PHDA [15]	▪ Priority based health data aggregation. ▪ Paillier cryptograph	▪ Low energy consumption ▪ Ensure data privacy and integrity.	▪ Asymmetric Cryptosystem which is computationally expensive.
PPM-HAD [16]	▪ Privacy-Preserving and Multifunctional Health Data Aggregation.	▪ High fault tolerant ▪ Ensure data privacy and integrity.	▪ No verifying it in a real-life environment. ▪ High traffic load
LSDA [17]	▪ Secure Data Aggregation in Healthcare using IoT. ▪ Homomorphic encryption and MAC. ▪ Packet checking at Aggregator	▪ Evaluation results using an experimental network of medical sensors. ▪ Robust communication. ▪ Efficient communication between doctors and patients.	▪ ECEG is power hungry cryptography. ▪ Low fault tolerant. ▪ Can be vulnerable to impersonation attack.
RESDA [18]	▪ Secure Data Aggregation in Healthcare using IoT. ▪ Homomorphic encryption and MAC. ▪ Not Packet checking at Aggregator	▪ Evaluation results using an experimental network of medical sensors. ▪ Providing strong privacy guarantees.	▪ ECEG is power hungry cryptography. ▪ Easy target for high-end attacks
ERCS [19]	▪ Trust-based communication scheme to ensure the reliability and privacy of WBAN ▪ Cooperative communication approach.	▪ Increases service delivery ratio, reliability, and trust with reduced average delay. ▪ Guaranteeing the confidentiality of sensitive medical data.	▪ High traffic load ▪ No verifying it in a real-life environment. ▪ Energy consumption.
CBCSES [20]	▪ Efficient and provable secure Scheme for Internet of Things in Mobile Health System ▪ Certificate-based combined signature, encryption and signcryption.	▪ Securing the patients' sensitive data ▪ Providing efficient performance in terms of energy consumption, frequency and cost.	▪ No verifying it in a real-life environment. ▪ The communication cost is high. ▪ Not Considering the heterogeneity of sensors
Proposed EPPDA	▪ Secure and Energy-Efficient Data Aggregation in Healthcare using IoT. ▪ With malicious node detection. ▪ Homomorphic encryption and MAC. ▪ Packet checking at Aggregator ▪ Priority based health data aggregation.	▪ Evaluation results using an experimental network of medical sensors. ▪ Ensure data privacy and integrity. ▪ Efficient communication between doctors and patients. ▪ Malicious node detection ▪ Considering the heterogeneity of sensors	▪ Can have high storage overhead to store a large number of keys.

3. System Model and design Objectives

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

3.1 Network Model

The architecture considered in the proposed work is shown in Figure 2. The proposed model can be utilized in a hospital and by even a located remotely patient. The architecture model of our proposed scheme comprises three architectural components: Medical Sensors Nodes, an Aggregator, and 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 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 Sensors 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.

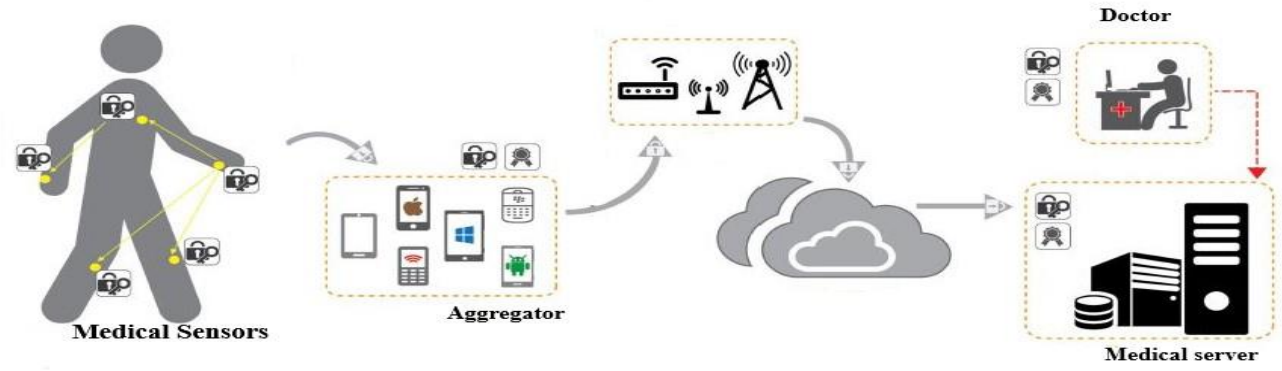

Figure. 2. The proposed architecture for IoT-based healthcare

3.2 Design goal of the EPPDA Scheme

The following design goals are to be achieved.

- **High efficiency:** The proposed aggregation scheme should be efficient, that is, the computational costs at IoT devices should be as less as possible, and the communication overheads should also be minimal.
- **Security:** The proposed aggregation scheme should be can resist against the false data injection attack from external attackers, that is, the proposed system must filter false data locally at the Aggregator.

4. Proposed EPPDA Solution

The proposed protocol provides efficient secure data aggregation with an mutual authentication. In this section, we present the EPPDA protocol for secure data aggregation in healthcare Based IoT, which mainly consists of the following four parts: (1) Setup and key generation phase; (2) Encryption-Sign data; (3) Verification and Authorization phase, and (4) Data Aggregation phase. The flowchart for the proposed solution process is shown in Figure 3.

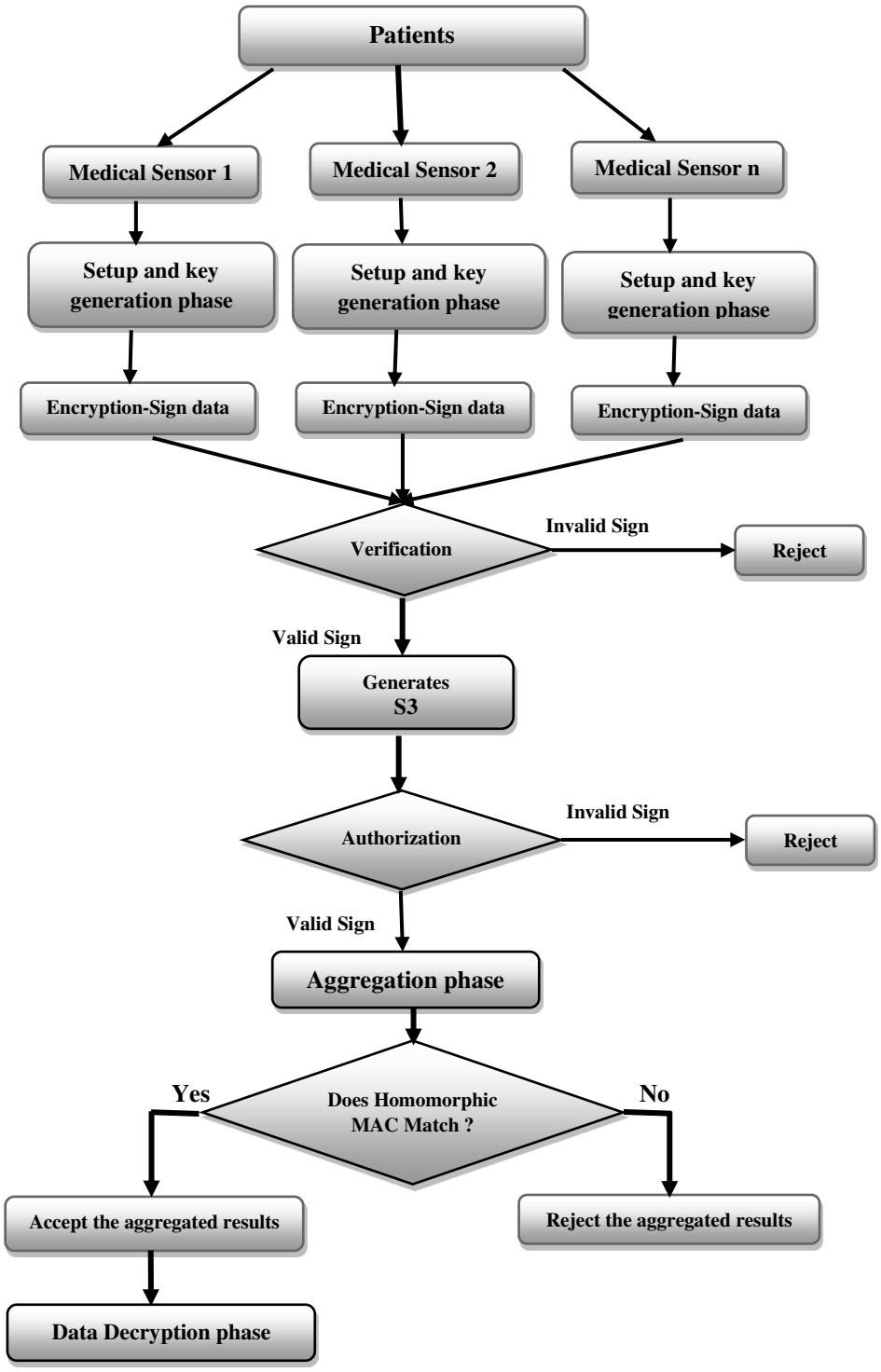

Figure. 3. Concrete sequence flow diagram of the EPPDA.

4.1. Setup and key generation phase

For each patient, the putting an admitted on sensor-based monitoring is based on the recommendation of the doctor. The according to the patient's health data needs, the medical personnel places the medical sensors on the patient's body. First, each patient must be registered into the Medical Server prior to attaching to him or her any body sensor network. When the hardware configuration is end, the Medical Server send a demand the Keys information from each sensors. After receiving the request by the Aggregator, the Medical Sensor Nodes processes the request and send the Keys paramatr as a broadcast message toward the Aggregator.

For each Medical Sensor, the ID and the private key is generated and sended to the Aggregator. The ID and the private key is specified as ID_{MS} and MS_{Pvkey}. The private key of the sensor node is created using the Diffie-Hellman key exchange [21]. The Aggregator receive the sensor node ID and the private key and stores it.

Moreover, the Aggregator generates the ID_{Agg} and Agg_{Pvkey}. The Aggregator transfers the generated ID and private key to the Medical Server. The Medical Server receives the ID and private key of Aggregator and and stores it.
The symbol of the various symbol are shown in Table 2. Figure 4 represent the Keys exchange model of the setup and key generation phase in the proposed EPPDA. The pseudocode of the Setup and key generation phase can be seen in Algorithm 1.

Symbol	Description
ID_{MS}	Medical Sensor ID
m_i	Health data
ID_{Agg}	Aggregator ID
MS_{Pvkey}	Private key of Medical Sensor
Agg_{Pvkey}	Private key of Aggregator
*	Stored
S_1, S_2	Messages Exchange
RN_1, RN_2	Random Numbers
PK_{MS}	Public key of Medical Server
SK_{MS}	Secret key shared between the Medical Sensor and Medical Server.

Table 2: Symbol description of the proposed EPPDA Solution

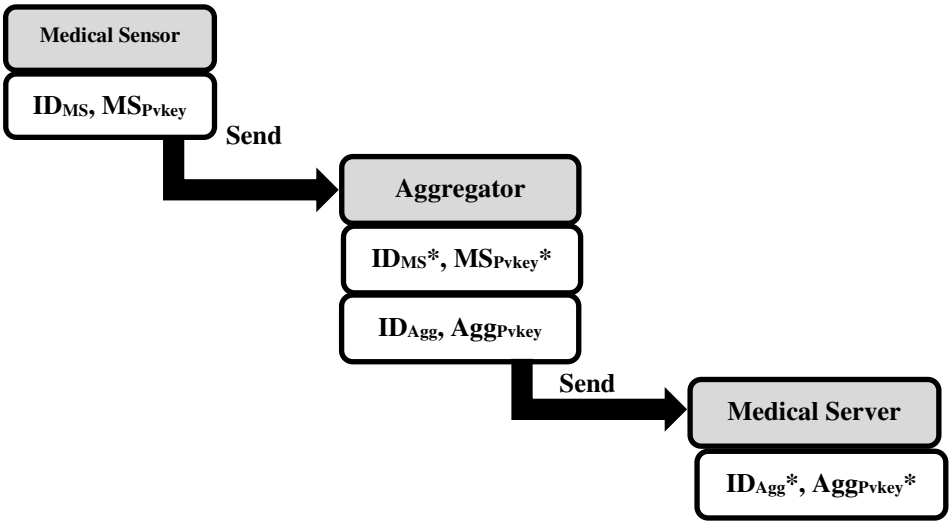

Figure. 4. Setup and key generation phase of the proposed Solution

Algorithm 1 : Setup and key generation phase
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

4.2. Encryption and Signing Phase

The health data comes from a variety of devices, resulting in a large number of data records [15]. In general, we distinguish 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 like blood pressure, glucose level,etc.. For each parameter, the normal range is recorded in a table. For most emergency situations, some alerts are be generated if a patient is in danger. For example, if the blood pressure readings suddenly exceed 180/120mmHg, it may be signs of organ damage and it requires immediate medical attention. Hence, an alert message should be sent to a doctor immediately. The emergency situations are the highest priority data and 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. There are many diseases that can be diagnosed and controlled through regular monitoring of these medical data.

The regular data are not for emergency situation and do not present urgent delivery requirements. The Medical Server receives periodical updates. At each update, the Medical Server validates the data. If the patient's data falls within the reference interval, no sending an emergency alert for the doctor. In case of any abnormalities of the data, the Medical Server send a notification for the doctor.

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 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 allows complex mathematical operations to be performed on encrypted data without know the contents of the original plain data [22]. As calculations are performed on encrypted texts, the data privacy and confidentiality are protected [23].

So that we can ensures the content exchanged between the Medical Sensors and Medical Server is protectedagainst any modification by malicious or unauthorized users, and moreover to allow the Medical Server to determine the evil data, we uses the homomorphic Message Authentication Code (MAC) scheme, in order 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 [23].

The proposed solution can guarantee data freshness in time and value. Each echange of the encryption data between of the proposed network devices, we send a nonce N. The nonce is an implicit sequence number that is used only once for data freshness.

In the Algorithm 2, we describe the algorithm executed by the Medical Sensor for encryption and Signing the collected data.

Algorithm 2: Encrypt & Signing the collected data

Input : PK_{MS}, SK_{MS}, m_i, Nonce

Output : C_i, MAC_i

1. Map m_i into point of the elliptic curve Pi
   - If Emergency Situation, the Medical Sensor calcute and send to the Aggregator:
     - ✓ Compute : $C_i^{ES} = ((P_i + SK_{MS} * PK_{MS}) \| ID_{MS} \| N_i \| Time \| Location)$
     - ✓ Compute : $MAC_i^{ES} = HMAC\ (C_i^{ES}, SK_{MS})$
   - If Vital Health data, the Medical Sensor calcute and send to the Aggregator:
     - ✓ Compute : $C_i^{VD} = ((P_i + SK_{MS} * PK_{MS}) \| ID_{MS} \| N_i \| Time)$
     - ✓ Compute : $MAC_i^{VD} = HMAC\ (C_i^{VD}, SK_{MS})$
   - If Regular Health data, the Medical Sensor calcute and send to the Aggregator:
     - ✓ Compute : $C_i^{RD} = ((P_i + SK_{MS} * PK_{MS}) \| ID_{MS} \| N_i \| Time)$
     - ✓ Compute : $MAC_i^{RD} = HMAC\ (C_i^{RD}, SK_{MS})$
2. Send C_i and MAC_i to Aggregator

In the previous most work, the detection of the attacks can only be performed after reception of aggregate, this detection is inefficient and too late, it can a significant loss in terms of computation and communication costs and well privacy information patient's. In this proposed solution, we uses a scheme that allows early detection of the attack. The proposed solution aims to verify the legitimacy communication between of the proposed network devices.

In this regard, and as an effective solution to the above mentioned issue, we propose an Verification and Authorization phase, and for that we are using a signature scheme based on Chebyshev polynomials [24-26]. The first verification is between Medical Sensors and the Aggregator. For that, a signature is created by the Medical Sensor.

In the first ordre, 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 and is modulated with the random number RN_1. The message S_1 is expressed as,

$$S_1 = E(MS_{Pvkey}) \bmod RN_1 \quad (1)$$

Moreover, the message S2 is computed as following. The sensor node ID_{MS} is concatenated with the chebyshev polynomial, which is then concatenated with the message S_1. Finally, the hashing function is applied to the concatenated factor to generate the message S_2.

$$S_2 = h(ID_{MS} // M // S_1) \quad (2)$$

Where, M is the Chebyshev polynomial, and h is the hashing function. The chebyshev polynomial factor M generated at the Medical Sensor is expressed as,

$$M = 8m^4 - 8m^2 + 1 \quad (3)$$

The EX-OR operation is applied with the private key of the Medical Sensor and the hashing function of the node ID_{MS} to generate the factor m. Where, the term ***m*** is computed as,

$$m = MS_{Pvkey} \oplus h(ID_{MS})$$

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,

$$\alpha = (S_1, S_2) \quad (4)$$

The signature α generated by the Medical Sensors is forward and stores it 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 generate the signature α stage can be seen in Algorithm 3.

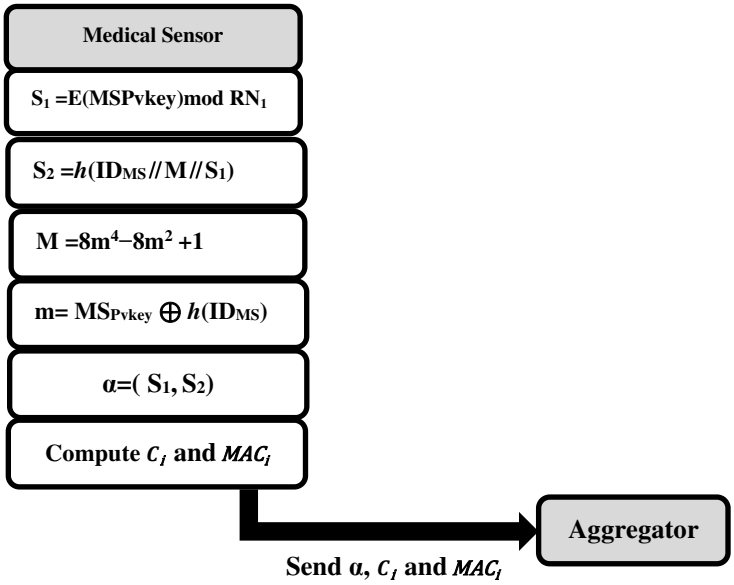

Figure. 5. Encryption and Signing stages of the proposed Solution

Algorithm 3 : Generate the signature α
Created the S_1 and S_2
$S_1 = E(MS_{Pvkey}) \bmod RN_1$
$S_2 = h(ID_{MS} // M // S_1)$
Generate the signature $\alpha = (S_1, S_2)$
Send α to Aggregator

4.3. Verification and Authorization phase

Authentication is the process of verifying the legitimacy of the nodes wants join the process of aggregation. This local authentication phase aims to verify 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 will reject 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 message S_1 and S_2 that are stored in the Aggregator is specified as,

$$S_1^* = E(MS_{Pvkey}^*) \bmod RN_1 \quad (5)$$

$$S_2^* = h(ID_{MS}^* // M^* // S_1^*) \quad (6)$$

The chebyshev polynomial is send to the Aggregator and is stored for further processing. The chebyshev polynomial that is received by the Aggregator is specified as,

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

Here, the term m is expressed as,

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

If the signature received by the Aggregator and the signature generated by the Medical Sensor are equals, $S_1 = S_1^*$ and $S_2 = S_2^*$, then the signatures are well verified.

After the Verification of the legitimacy of the Medical Sensors, the Aggregator send an demand to the Medical Server to demand the Aggregation authorization.

The Aggregator generates the message S_3. The message S_3 generated at the Aggregator is speified as,

$$S_3 = h(ID_{Agg} // RN_2) \oplus Agg_{Pvkey} \tag{9}$$

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

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

Once the Medical Server receives of the S3, it verifies the message S_3^* with the message S_3. If $S_3 = S_3^*$ then, the Medical Server generates an Aggregation authorization messages A_1 for Aggregator. Conversely, if the Aggregator is malicious and unauthorized, the Medical Server will reject the Aggregator from joining his network.

By this process, the sensors devices,the gateway device, medical server, are mutually authenticated before the actual heath data transmission. Next, the Medical Server sends the message A_1 to Aggregator. After reception of Aggregation authorization message A_1, the Aggregation phase is activate. Figure 6 shows the system model of the verification phase.

The pseudocode of the Verification phase can be seen in Algorithm 4.

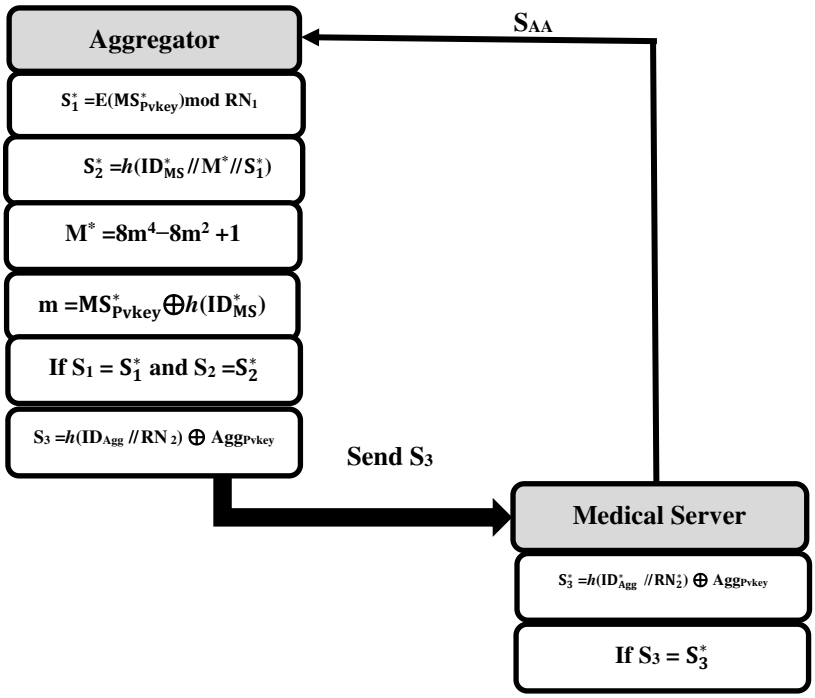

Figure. 6. Verification Phase of the proposed Solution

Algorithm 4 : Verification and Authorization phase
Message S_1 and S_1 are stored in the Aggregator
$S_1^* = E(MS_{Pvkey}^*) \bmod RN_1$
$S_2^* = h(ID_{MS}^* // M^* // S_1^*)$
If $S_1 = S_1^*$ and $S_2 = S_2^*$, signature is verified
Generates the message S_3
$S_3 = h(ID_{Agg} // RN_2) \oplus Agg_{Pvkey}$
Send S_3 to Medical Server and stored
$S_3^* = h(ID_{Agg}^* // RN_2^*) \oplus Agg_{Pvkey}$
If $S_3 = S_3^*$
Generate the Aggregation authorization messages A_1 and A_2
Send A_1 Aggregator

4.4. Data Aggregation phase with priority

After receiving the the Aggregation authorization message from the Medical Server, the Aggregator run the Data Aggregation phase. In the EPPDA solution, the data aggregation phase is based- priority of data. In our proposed solution, the ciphertexts for each data priorities cannot be combined together. only the ciphertext from the same data priority can be combined together. In the rest of this section, we describe the different forwarding strategies for the data with different priorities. The pseudocode of the Data Aggregation phase can be seen in Algorithm 5.

Algorithm 5 : Data Aggregation phase
Input : C_i, MAC_i ❖ If Emergency Situation, the Aggregator calcute and send to the Medical Server: ✓ For L ciphertexts ($C_{1j} \ldots C_{Lj}$): Compute $\boldsymbol{C_{Agg}^{ES}} = \sum_{i=1\ldots L}^{j} C_{ij}$ ✓ For L MACs ($MAC_{1j} \ldots MAC_{Lj}$): Compute $MAC_{agg} = \oplus MAC_{ij}$ ❖ If Vital Health data, the Aggregator calcute and send to the Medical Server: ✓ For L ciphertexts ($C_{1j} \ldots C_{Lj}$): Compute $\boldsymbol{C_{Agg}^{VD}} = \sum_{i=1\ldots L}^{j} C_{ij}$ ✓ For L MACs ($MAC_{1j} \ldots MAC_{Lj}$): Compute $MAC_{agg} = \oplus MAC_{ij}$ ❖ If Regular Health data, the Aggregator calcute and send to the Medical Server: ✓ For L ciphertexts ($C_{1j} \ldots C_{Lj}$): Compute $\boldsymbol{C_{Agg}^{RD}} = \sum_{i=1\ldots L}^{j} C_{ij}$ ✓ For L MACs ($MAC_{1j} \ldots MAC_{Lj}$): Compute $MAC_{agg} = \oplus MAC_{ij}$ **Output :** C_{agg}, MAC_{agg}

4.5. Decryption and Verification phase:

In this step, after receiving all data packets i.e. the aggregated data, the medical server invokes the decryption and verification processes. The medical server first 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, doctors, insurance companies. The pseudocode of the Data Decryption and Verification phase can be seen in Algorithm 6.

Algorithm 6: End-to-end verification
Input : C_{agg}, MAC_{agg}
For each pair (C_{agg}, MAC_{agg}) do
Compute MAC'_{agg} of C_{agg} using SK_{MS}
If $MAC'_{agg} = C_{agg}$ then
Decrypt C_{agg}
else
Reject (C_{agg}, MAC_{agg})
Output : m_i

5. Security analysis

In this section, we discuss the security strength of our proposed EPPDA scheme. The proposed EPPDA scheme achieves confidentiality, authenticity and end-to-end privacy on patient's medical health data.

- **Data Confidentiality:** To protect the data patient's privacy, the data should be transmitted securely. The data confidentiality is the most important factors 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 allows operations to be performed on encrypted data without know the contents of the original data. Hence, the privacy is maintained end-to-end. Therefore, our proposed scheme provides good confidentiality for patient's health data, i.e., it protects the users' privacy data patient's. The security proof of the homomorphic encryption is provided in [22, 23].
- **Integrity:** In order 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 Sensors computes the HMAC for its encrypted measurement and sends the result to the Aggregator. The Aggregator calcute the aggregat on encrypted data without know the contents of the original data. The security proof of HMAC is provided in [23]. 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 information or launches replay attacks, the Medical Server can verify the correctness of the received data. As a result, our developed scheme guarantees the integrity and validity of the patient's private data.

- **Identity anonymity and authenticity:** In order to verify the legitimacy communication between the network components devices, we propose an authentication phase in each layers of proposed network model. 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. 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 equals, $S_1 = S_1^*$ 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 Sensors is in-successful authentication, the Aggregator will reject the health data and not accept the Medical Sensors wants to join his network. On the other side, 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 will reject the Aggregator from joining his network. However, our identity authenticity mechanism can identify the identity fraud behavior. We can see that the proposed scheme realizes the mutual authentication of between the communication parties. By this process, the sensors devices,the gateway device, medical server, are mutually authenticated before the actual heath data transmission.
- **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 Sensors is malicious and unauthorized, the Aggregator will reject the Medical Sensors from joining his network.
- **Data Freshness:** In order 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 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

In this section, we evaluate the EPPDA scheme described in the previous section in terms of performance. First, we provide an overview of the Hardware Platform. Then, we present the performance results of our proposed EPPDA scheme.

6.1 Hardware Components

The vital signs sensing unit of this system is the MySignals HW V2 platform, which is a development platform for medical devices and ehealth applications, figure 7 shows the platform. It monitors patients' health by deploying different medical sensors on patients' body to get sensitive data of patients for subsequent analysis by physicians [27]. The MySignals HW V2 platform is the most complete 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 also allows tablets and smartphones to communicate with it. Figure 6 represents the MySignals HW V2 platform [28].

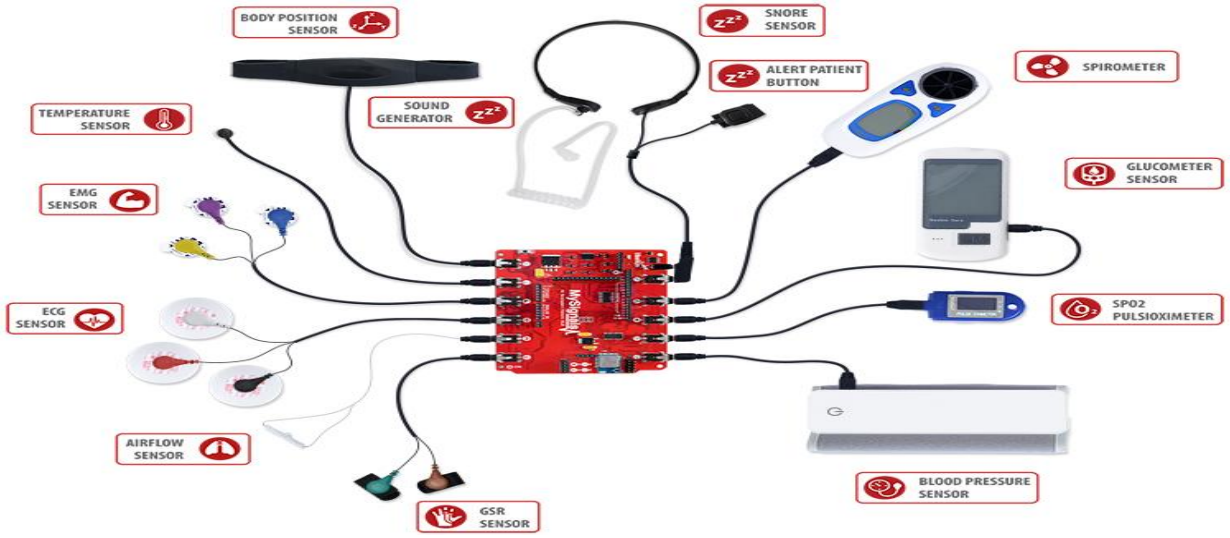

Fig. 7. MySignals HW V2 platform [27].

In contrast to the medical sensor, the Aggregator should be a device that has access to unlimited power and resources. The tablet plays the Aggregator role and communicates with the MySignals HW V2 platform via WiFi to collected the vital signs. Figure 7 is the MySignals platform with various sensor ports. This platform is also integrated with a WiFi serial transceiver module ESP8266 in figure 8. 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 laptops PC. These PCs have relatively powerful processing, memory, transmission capacity, and have long battery life, so that there is no power constraint. Also, 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, patient's family member, etc. The aggreted data between the system components will encrypted by our proposed EPPDA scheme to protect it from any malicious acts of the hackers.

Figure 8. MySignals with Sensor Nodes and WiFi Module.

6.2 Experiment and Performance Evaluation

We analyze the efficiency of the proposed EPPDA scheme in this section by evaluating the End-to-End delay, Computation overhead, Communication overhead, and Energy consumption. We also present the comparative analysis of our proposed system with the existing systems LSDA [17] and RESDA [18].

A. End-to-End Delay

The End-to-End Delay is the total time consumed between the data packet sending by the Medical Sensors and the time when the packet arrives at the Medical Server.

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

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 displays 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 EPPDA decreases the end-to-end delay by 17%, 28%, and 34% under varying time intervals as that of RESDA and LSDA, respectively.

The end-to-end delay of proposed EPPDA is the best compared to the existing protocols especially when the Medical Sensors count increases. It exists are two reasons for the reduction of end-to-end delay in EPPDA:

- 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 will reject their data in order to prevent the adversary nodes inject the false traffic, thus, avoid energy consumption unnecessary due to transmitting them.
- Also, in our scheme, in the medical server, 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.

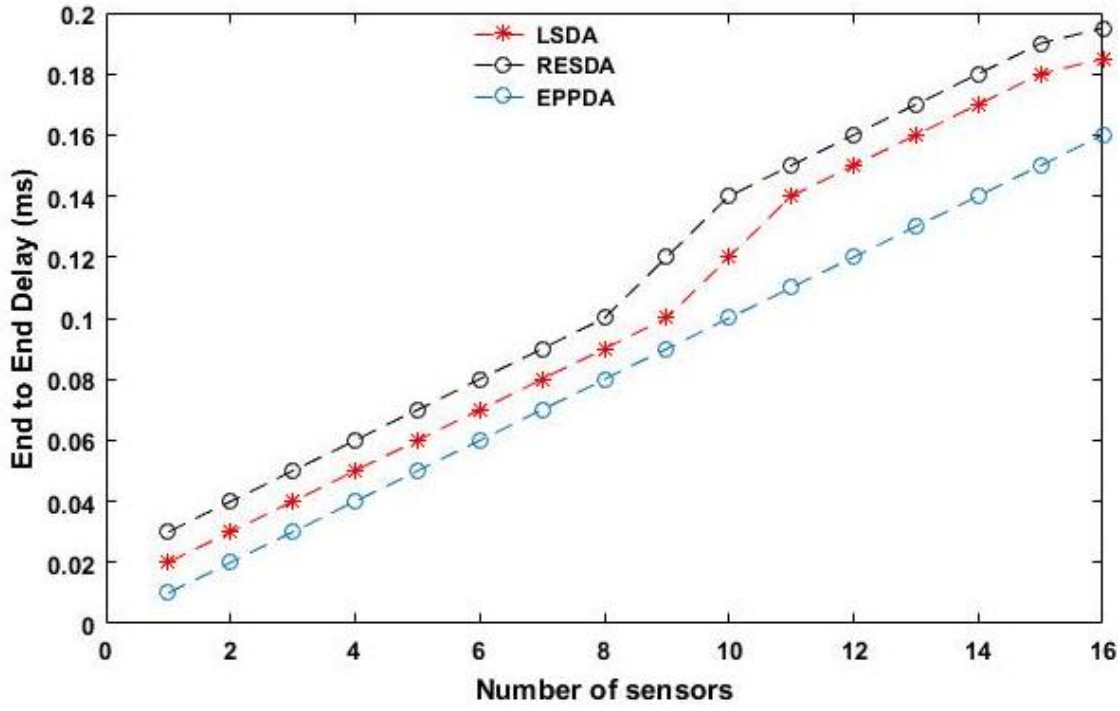

Fig. 9. The End-to-End Delay

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

In the computational overhead, we designate symbol SM is 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 is need one Scalar Multiplication and two modular Exponentiation. So, the computation involves (1SM+2PA) operations. Also, for generate the MAC, the sensor needs 1 hashing operation and 1 exponentiation operation. So, 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*2SM) +2H).

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 as show in Table 3.

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*2SM) +2H).
Medical Server	**1)** Verify the legitimacy of the Aggregator **2)** Aggregated data integrity verification **3)** Data decryption	SM +2H

Table 3: Computation complexity of the proposed SPPDA scheme

In Figure 10, we present the computational cost of the proposed EPPDA scheme with a comparison with other solutions. We can observe that our proposed scheme achieves a significant reduction in the total computation cost compared with LSDA and RESDA. For example, when the number of Medical Sensors is 10, the total computation cost of our proposed scheme is 0.6ms, which reduces by 11% and 20% that of RESDA and LSDA, respectively.

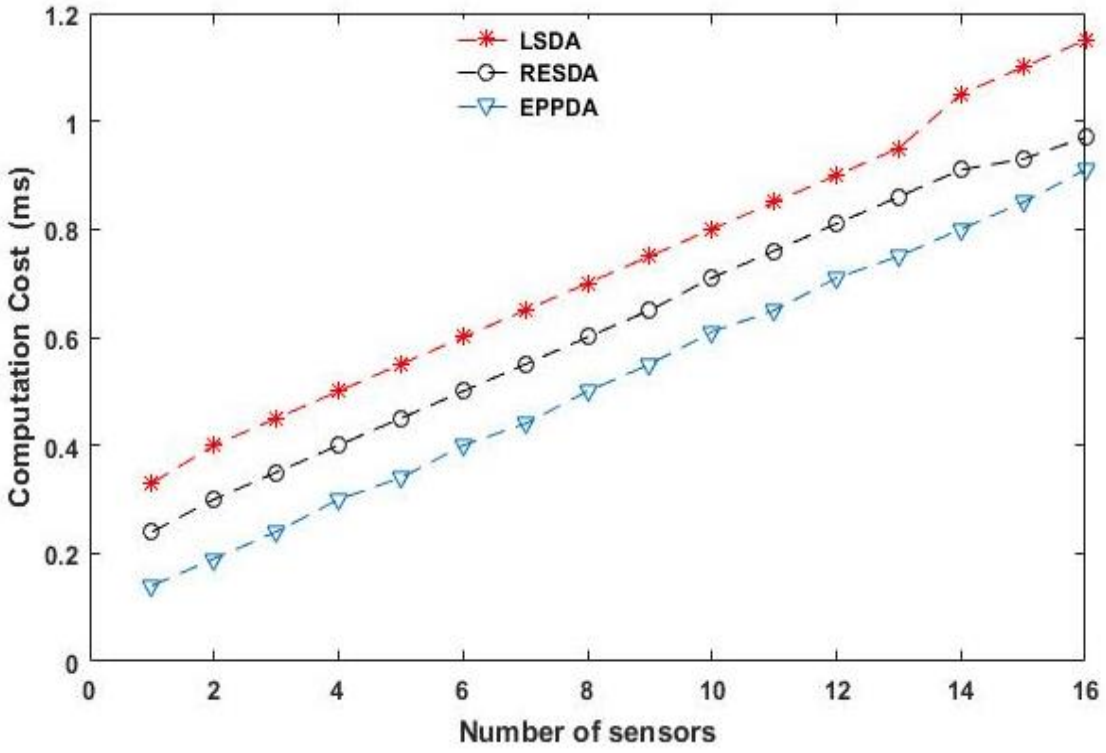

Figure. 10. Computational cost

C. Communication Overhead

The communication overhead in the proposed EPPDA scheme is divided into two levels: The communication overhead between the Medical Sensors and the Aggregator, and the other part is the communication overhead between the Aggregator and the Medical Server. The communication overhead is measured as the total data transmitted in the networks. The number of messages increases proportional to the number of sensor nodes.

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 with [27]. 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 Cagg is equals $160 * n$, when their n are sensors are evolved into the process. In our scheme, we consider a 4-byte MAC. The MACagg is also 4 bytes. The signature of verification is also 4 bytes. 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 with other solutions. We can observe that our proposed scheme achieves a significant reduction in the total communication overhead compared with LSDA and RESDA. For example, when the number of Medical Sensors is 10, the total communication overhead of our proposed scheme is 1664bits, which reduces by 10% and 15% that of RESDA and LSDA, respectively.

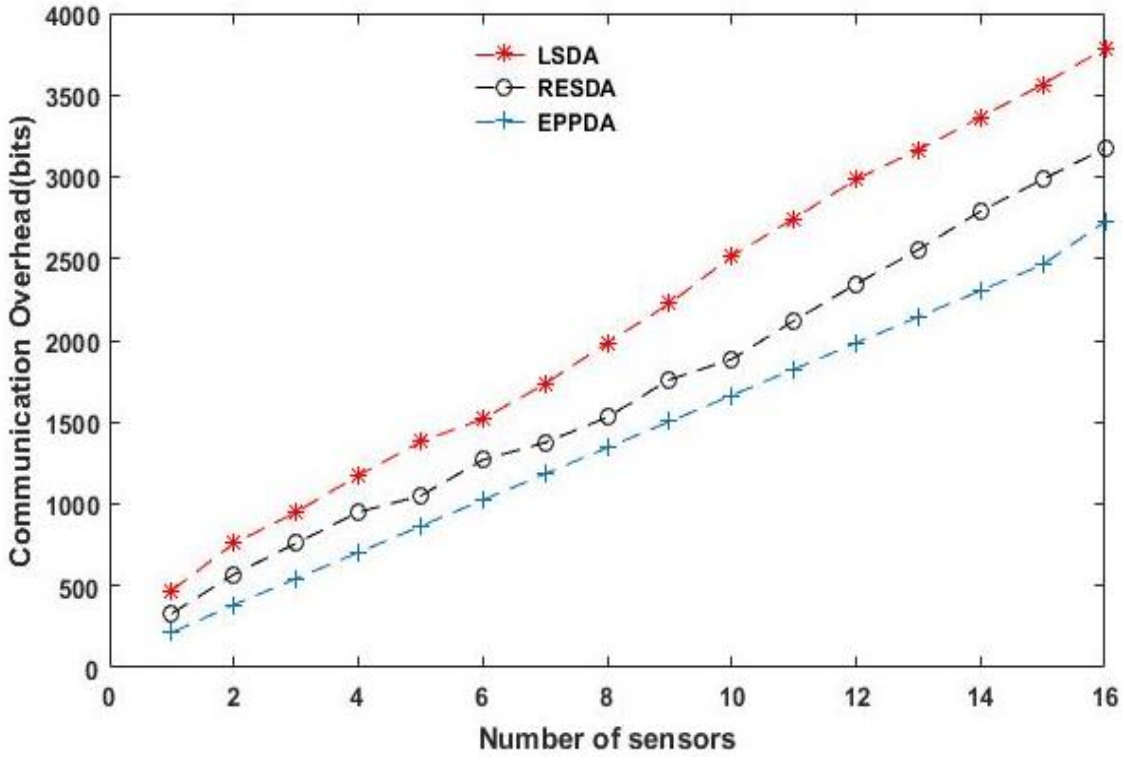

Figure. 11. Communication Overhead

D. 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 and therefore the life of the sensor nodes.

We calculate the energy consumption for cryptographic operations as follows: E (mJ) = U (V) × I (mA) × t (ms) where U represents the supply voltage, I is the current draw of the hardware, and t is the time. According to the datasheet available in [32], with MySignals HW V2 platform, the voltage is 3V and the wireless transceiver draws a current of 20mA for receiving and 17.7mA 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 (1.8mA); 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.

$$\text{CommCost(mJ)} = \frac{[(T_x \times 17.7\text{mA}) + (T_r \times 20\text{mA})]}{32768} \times 3\text{V} \tag{12}$$

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:

$$\text{ComptCost(mJ)} = \frac{T_{\text{cpu}}}{32768} \times 1.8\text{mA} \times 3\text{V} \tag{13}$$

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

$$\text{TotalEnergy(mJ)} = \text{EnergyComm} + \text{EnergyCompt} \quad (14)$$

Figure 12 shows that the energy consumption by EPPDA is lower than that of two other schemes. The reason is that the RESDA and LSDA 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 wants to join the process of aggregation are verified, thus, avoid energy consumption unnecessary due to transmitting them.

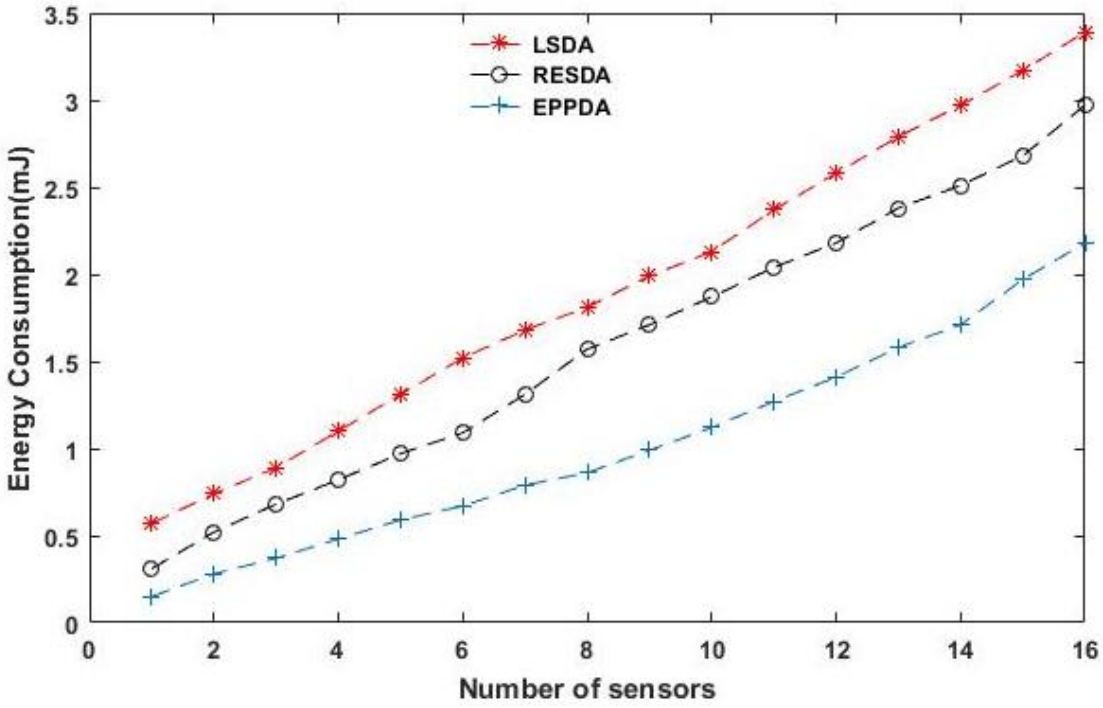

Figure. 12. The total energy consumption.

7. Comparison of Secure Data Aggregation Protocols

In this section, we compare the proposed protocol with existing secure data aggregation protocols. The comparison is based on the security requirements and the performance evaluation. From the table 4, it is evident that the proposed EPPDA scheme satisfies most of the security properties unlike other related data aggregation schemes in Internet of Things-Based Healthcare applications. In addition, through performance evaluation, we have also demonstrated the proposed EPPDA satisfies the communication and computation overheads requirements.

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
Proposed EPPDA	Yes	Yes	Yes	Yes	Yes	Small	Very low	Very Small

8. Conclusions and Future Work

The recent developments in the area of Internet of Things (IoT) show a great promise for providing solutions for healthcare. Protecting data privacy and integrity during data aggregation at the same time is challenging in IoT Based Healthcare Systems. This paper presents a novel secure aggregation scheme that provide provably secure message integrity with different trade-offs between computation cost, communication payload, and security assumptions. EPPDA is based the Verification and Authorization phase to verifying the legitimacy of the nodes wants to join the process of aggregation. The proposed scheme uses on an additive homomorphic encryption algorithm that allows aggregation on encrypted data, combined with homomorphic MAC. The security analysis and performance evaluation shows 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 will be to can study and improve the performance of this proposed scheme by applying this algorithm in different types of medical sensors.

References

[1] Selvaraj, S., Sundara varadhan, S., Challenges and opportunities in IoT healthcare systems: a systematic review. SN Applied Sciences, Volume 2, pp. 139, 2020.

[2] Farahani B., Firouzi F., Chakrabarty K. (2020), Healthcare IoT. In : Book : Intelligent Internet of Things, Springer, Cham, 2020.

[3] Khatoon N., Roy S., Pranav P., A Survey on Applications of Internet of Things in Healthcare. In : Book : Internet of Things and Big Data Applications. Intelligent Systems Reference Library, vol 180. Springer, 2020.

[4] Ansari, Seema,et al., Internet of Things-Based Healthcare Applications, In : Book : IoT Architectures, Models, and Platforms for Smart City Applications, IGI Global, pp. 1-28, 2020.

[5] Jaiswal K., Anand V., A Survey on IoT-Based Healthcare System : Potential Applications, Issues, and Challenges. In : Book : Advances in Biomedical Engineering and Technology. Lecture Notes in Bioengineering. Springer, pp 459-471, Singapore, 2021.

[6] Kadhim, K.T., Alsahlany, A. M., Wadi, S.M. et al. An Overview of Patient's Health Status Monitoring System Based on Internet of Things (IoT). Wireless Personal Communications, vol. 114, 2235–2262, October 2020.

[7] Mohapatra, Manas Ranjan; Sheetlani, Jitendra; Patra, Rasmi Ranjan., Privacy-Preserving data aggregation in internet of things (iot): an overview, International Journal of Advanced Research in Computer Science; Vol. 11, N° 5, pp: 17-19, Sep 2020.

[8] Suganthi, S.D., Anitha, R., Sureshkumar, V. et al. End to end light weight mutual authentication scheme in IoT-based healthcare environment. Journal of Reliable Intelligent Environments, vol 6, pp. 3–13, 2020.

[9] S. G. Mavinkattimath, R. Khanai and D. A. Torse, "A Survey on Secured Wireless Body Sensor Networks,"International Conference on Communication and Signal Processing (ICCSP), Chennai, India, pp. 0872-0875, 2019.

[10] 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," in IEEE Access, vol. 5, pp. 12601-12617, 2017.

[11] S. Anitha, P. Jayanthi, V. Chandrasekaran, An intelligent based healthcare security monitoring schemes for detection of node replication attack in wireless sensor networks, Measurement, Volume 167, 2021.

[12] Xuefeng Fang, Qingqing Gan, Xiaoming Wang, "Secure and Efficient Data Aggregation Scheme with Fine-Grained Access Control and Verifiability for CWBANs," Journal of Internet Technology, vol. 20, no. 3, pp. 771-780, May. 2019.

[13] W. Tang, J. Ren, K. Deng and Y. Zhang, Secure Data Aggregation of Lightweight E-Healthcare IoT Devices With Fair Incentives, IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8714-8726, Oct. 2019.

[14] C. Guo, P. Tian and K. -K. R. Choo, Enabling Privacy-Assured Fog-Based Data Aggregation in E-Healthcare Systems, in IEEE Transactions on Industrial Informatics, vol. 17, no. 3, pp. 1948-1957, March 2021.

[15] Kuan Zhang, Xiaohui Liang, Mrinmoy Baura, Rongxing Lu, Xuemin Shen, PHDA : A priority based health data aggregation with privacy preservation for cloud assisted WBANs, Information Sciences, Volume 284, Pages 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, in IEEE Transactions on Information Forensics and Security, vol. 11, no. 9, pp. 1940-1955, Sept. 2016,

[17] Othman SB, Bahattab AA, Trad A, Youssef H, LSDA : Lightweight Secure Data Aggregation Scheme in Healthcare using IoT, 8th International Conference on Software Engineering and New Technologies, Dec 28, 2019 - Dec 30, 2019, Tunisia.

[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," 2019 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC), Tunis, Tunisia, pp. 209-213, 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, in IEEE Access, vol. 8, pp. 131397-131413, 2020.

[20] Ullah, I., Amin, N.U., Khan, M.A. et al., 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, 4 (2021).

[21] Aryan, Chaithanya Kumar and P M Durai Raj Vincent, Enhanced diffie-hellman algorithm for reliable key exchange, IOP Conference Series: Materials Science and Engineering 263, 2017.

[22] Y. Harbi, Z. Aliouat, A. Refoufi and S. Harous, Efficient End-to-End Security Scheme for Privacy-Preserving in IoT, International Conference on Networking and Advanced Systems (ICNAS), Annaba, Algeria, 2019.

[23] Harbi Y., Aliouat Z., Harous S., Bentaleb, A., Secure Data Transmission Scheme Based on Elliptic Curve Cryptography for Internet of Things, Proceedings of the 5th International Symposium, MISC 2018, December 16-18, Laghouat, Algeria, 2018.

[24] C. Quan, J. Jung, H. Lee, D. Kang and D. Won, Cryptanalysis of a chaotic chebyshev polynomials based remote user authentication scheme, International Conference on Information Networking (ICOIN), Chiang Mai, 2018, pp. 438-441.

[25] X. Guo et al., User Authentication Protocol Based On Chebyshev Polynomial For Wireless Sensor Networks, IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Chongqing, 2018.

[26] E. O. Adeyefa, L. S. Akinola and O. D. Agbolade, "A New Cryptographic Scheme Using the Chebyshev Polynomials, International Conference in Mathematics, Computer Engineering and Computer Science (ICMCECS), Ayobo, Ipaja, Lagos, Nigeria, 2020.

[27] M. T. Almalchy, V. Ciobanu and S. M. Algayar, Solutions for Healthcare Monitoring Systems Architectures, IEEE 16th International Conference on Embedded and Ubiquitous Computing (EUC), Bucharest, 2018.

[28] Shahidul Islam M, Islam MT, Almutairi AF, Beng GK, Misran N, Amin N., Monitoring of the Human Body Signal through the Internet of Things (IoT) Based LoRa Wireless Network System, journal of Applied Sciences, vol 9, pp. 1884, 2019.

Figures

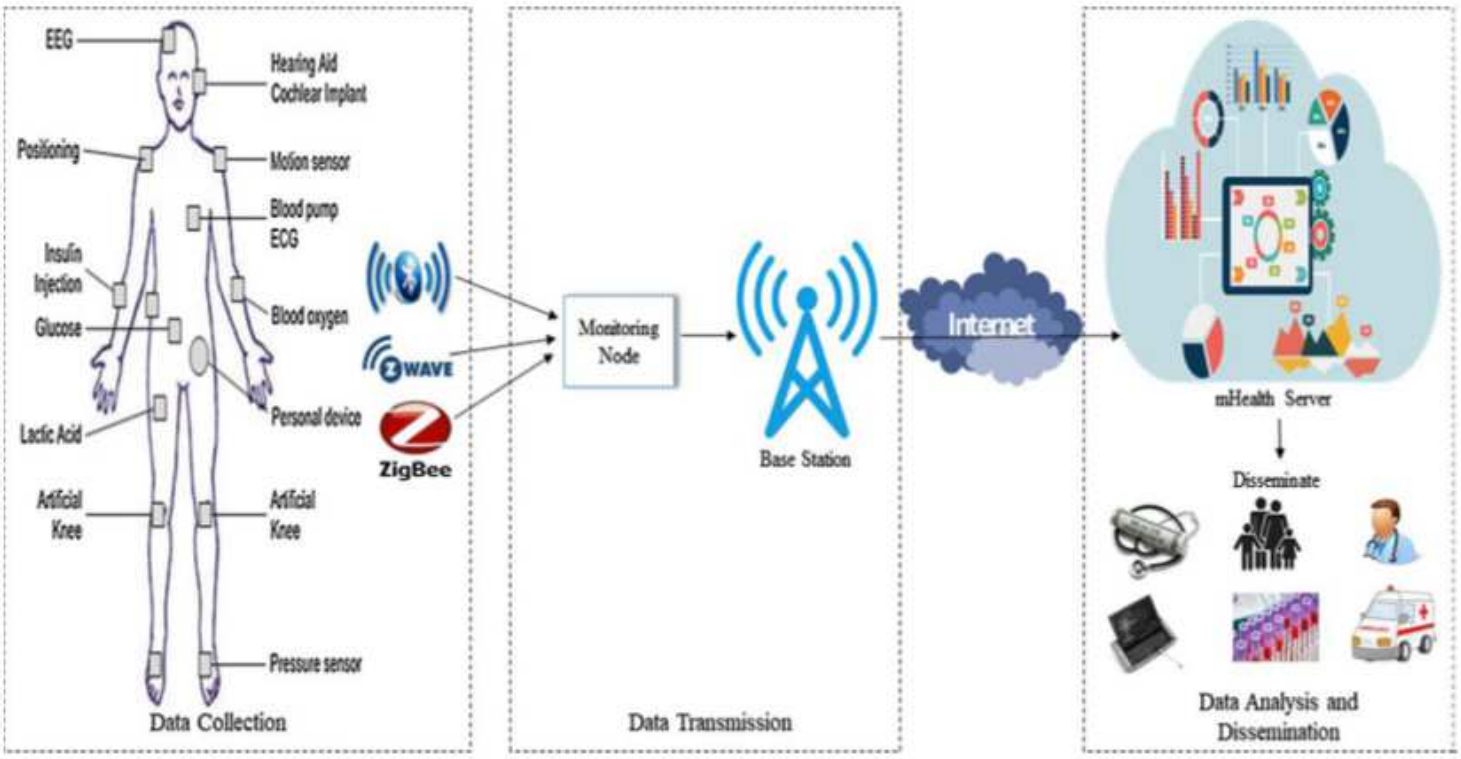

Figure 1

IoT-based healthcare monitoring architecture [3].

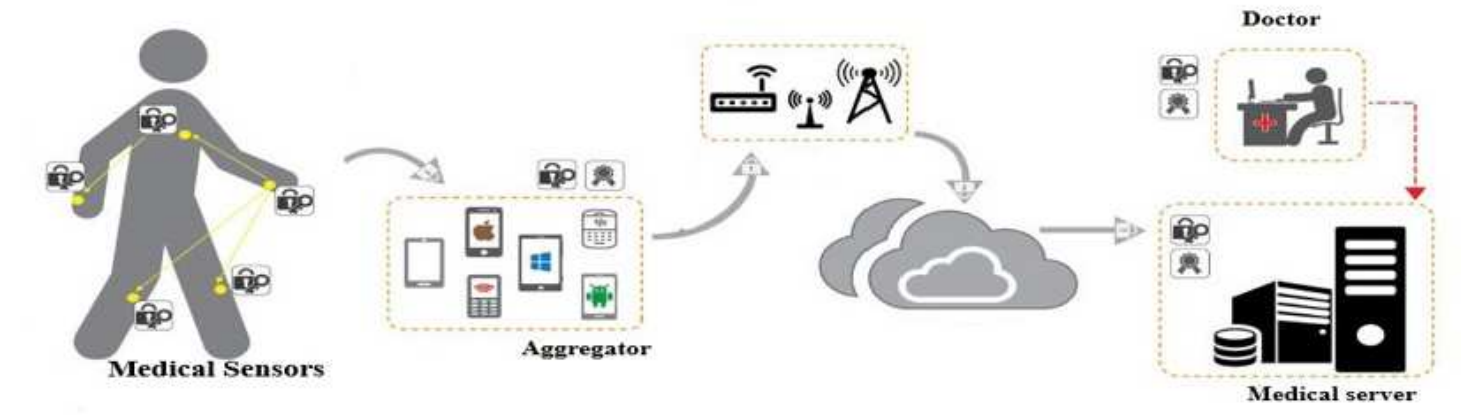

Figure 2

The proposed architecture for IoT-based healthcare

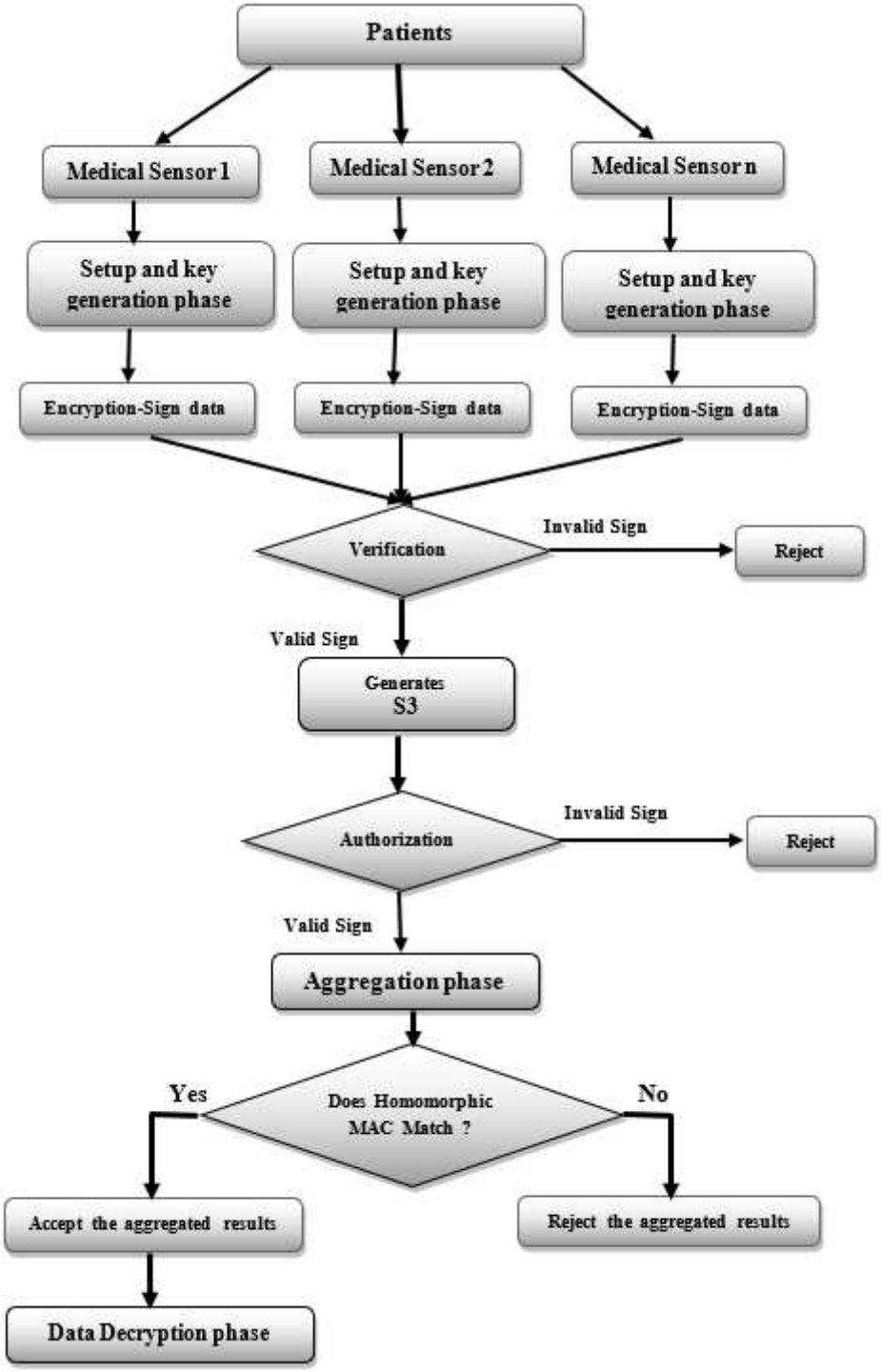

Figure 3

Concrete sequence flow diagram of the EPPDA.

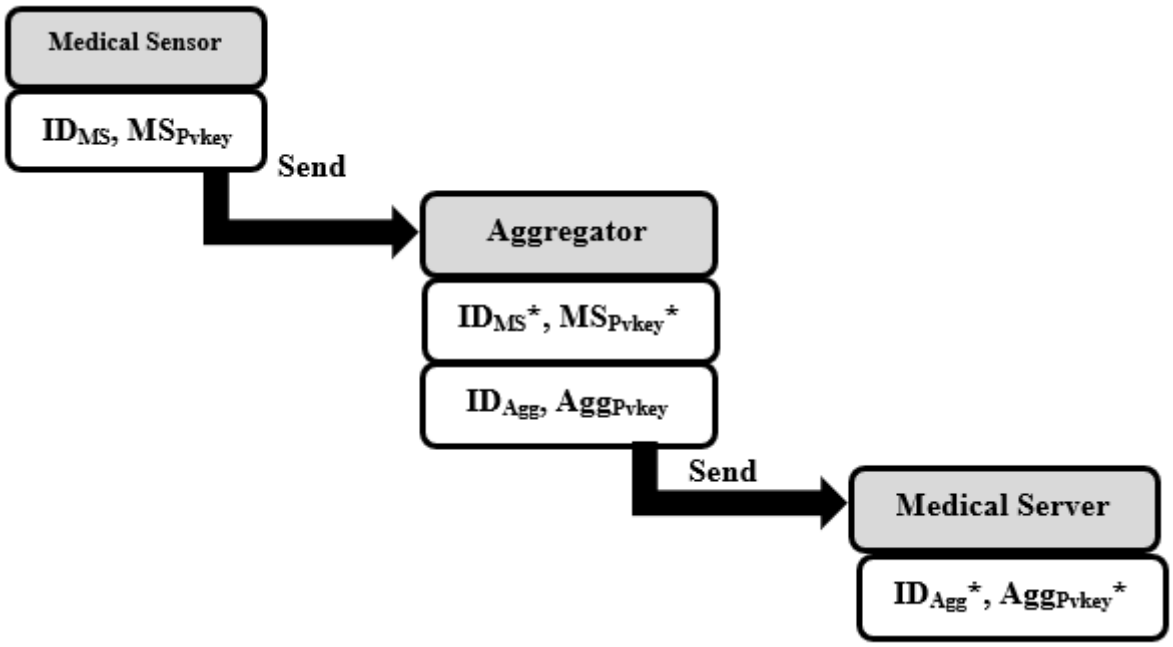

Figure 4

Setup and key generation phase of the proposed Solution

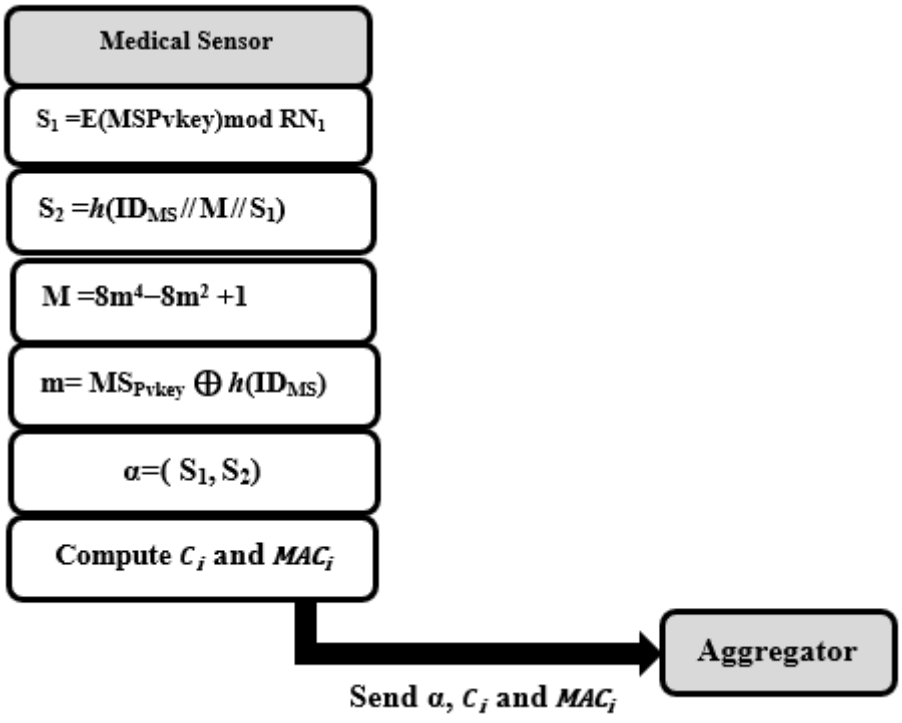

Figure 5

Encryption and Signing stages of the proposed Solution

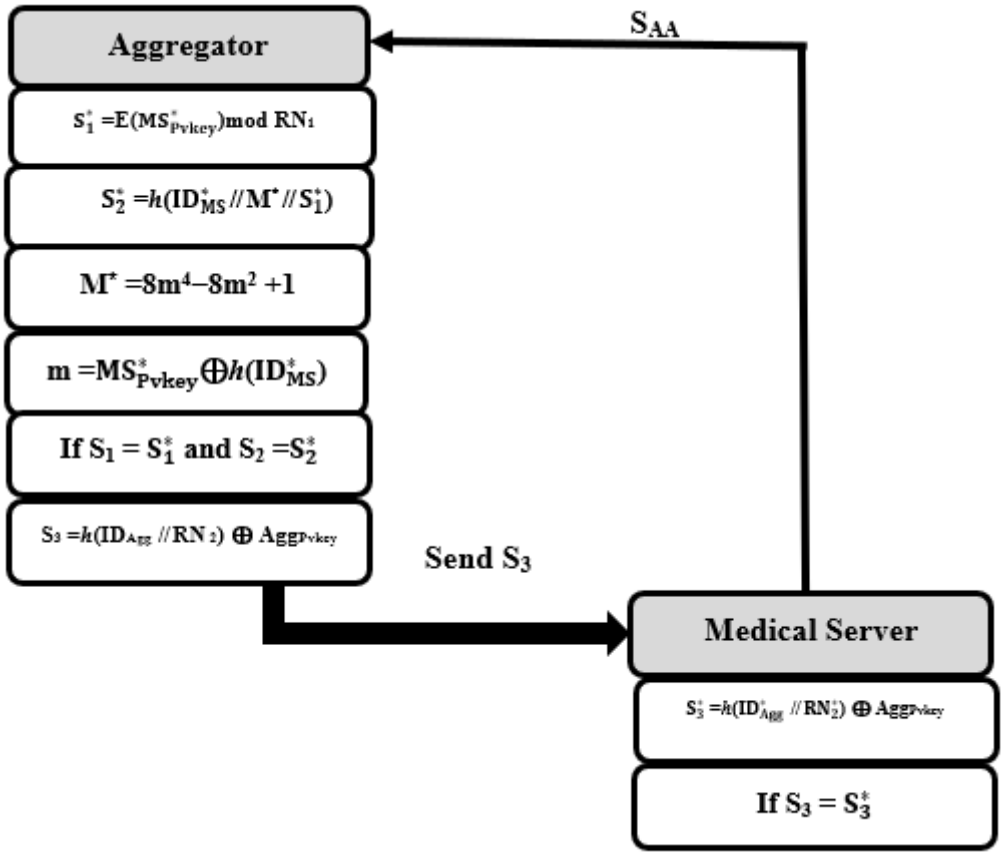

Figure 6

Verification Phase of the proposed Solution

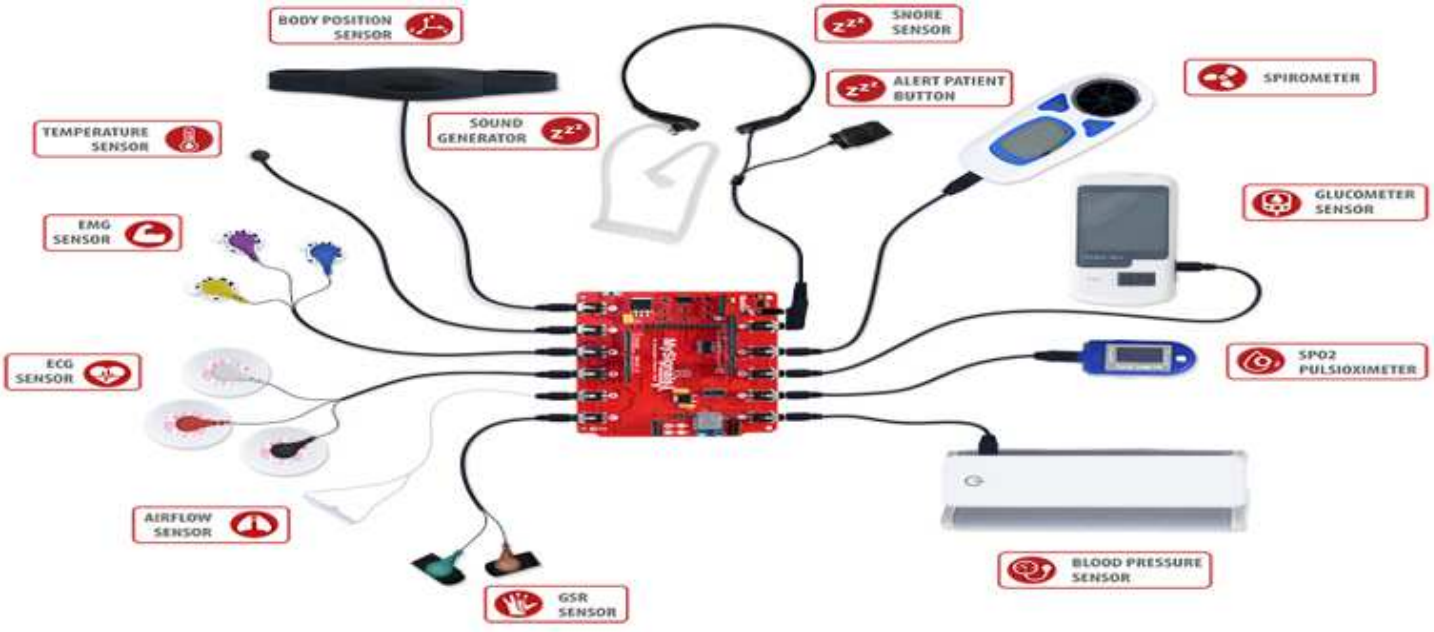

Figure 7

MySignals HW V2 platform [27].

Figure 8

MySignals with Sensor Nodes and WiFi Module.

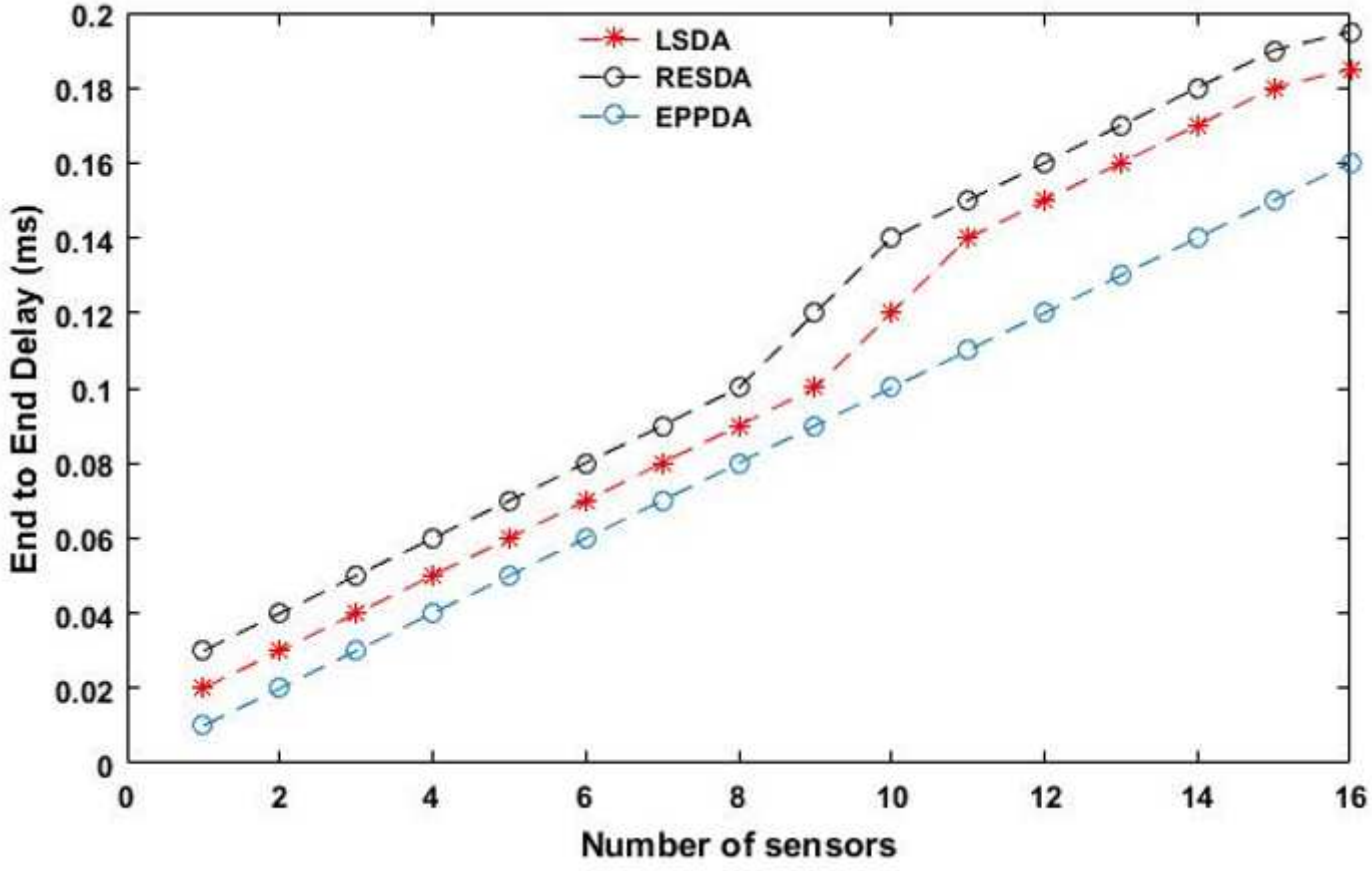

Figure 9

The End-to-End Delay

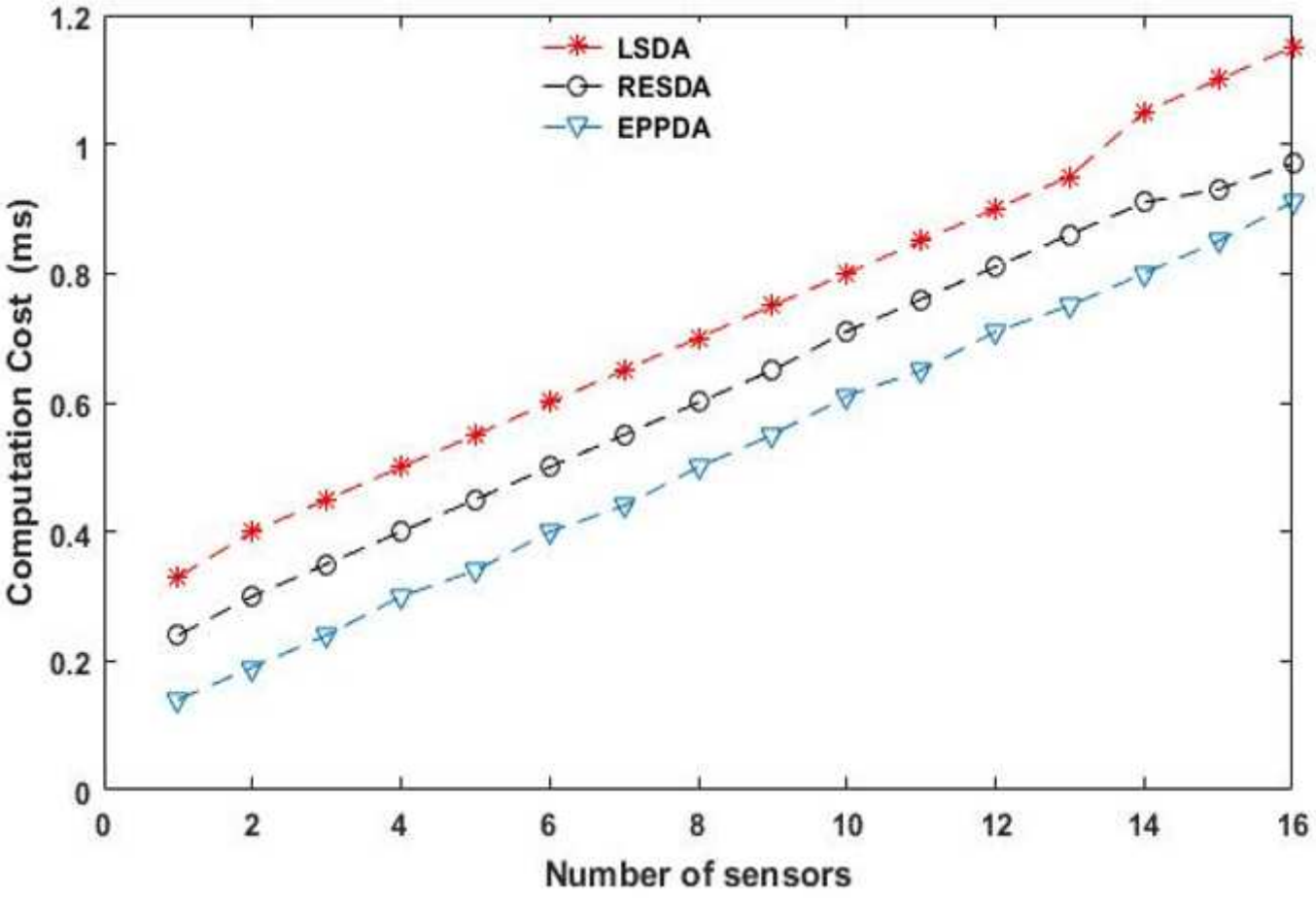

Figure 10

Computational cost

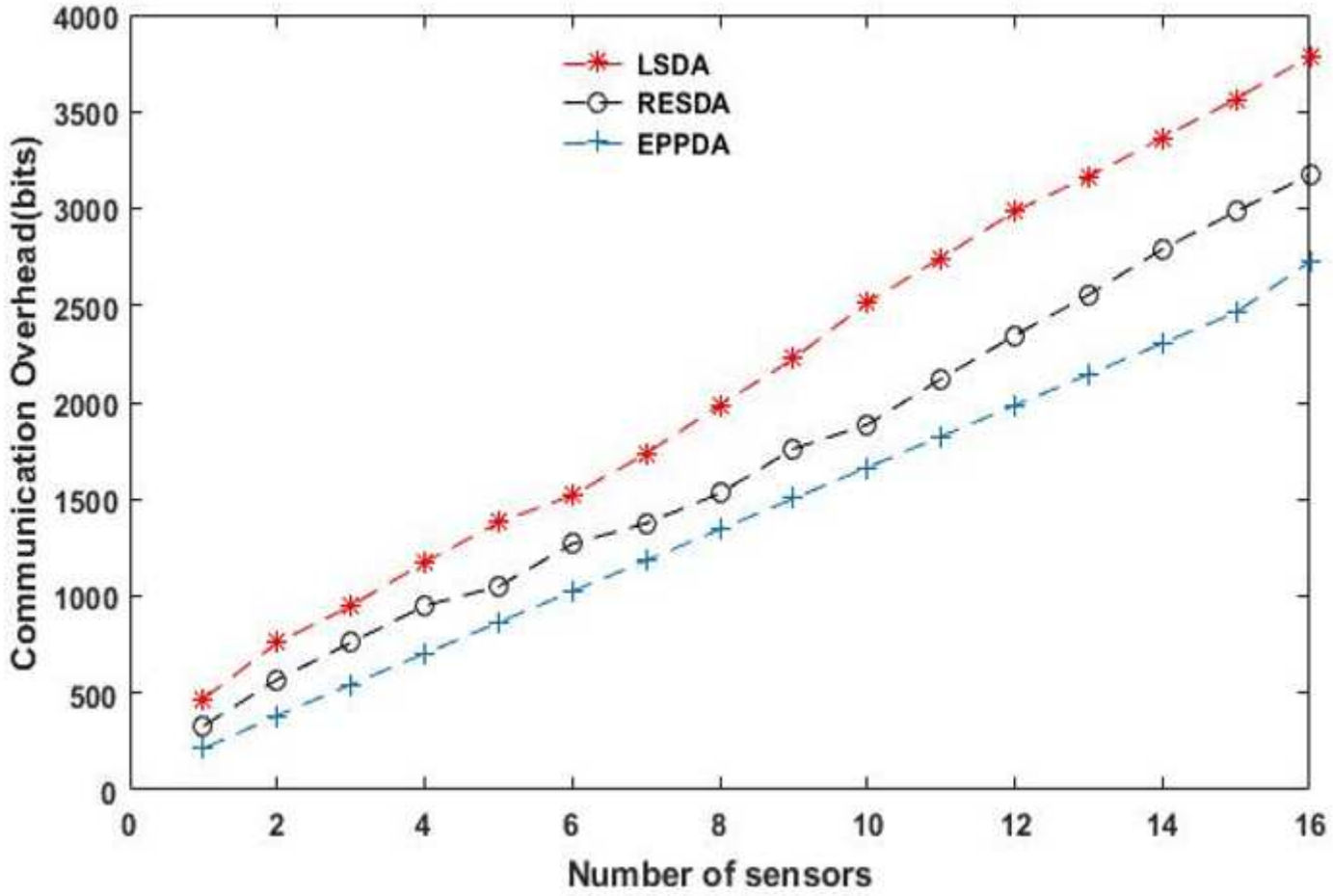

Figure 11

Communication Overhead

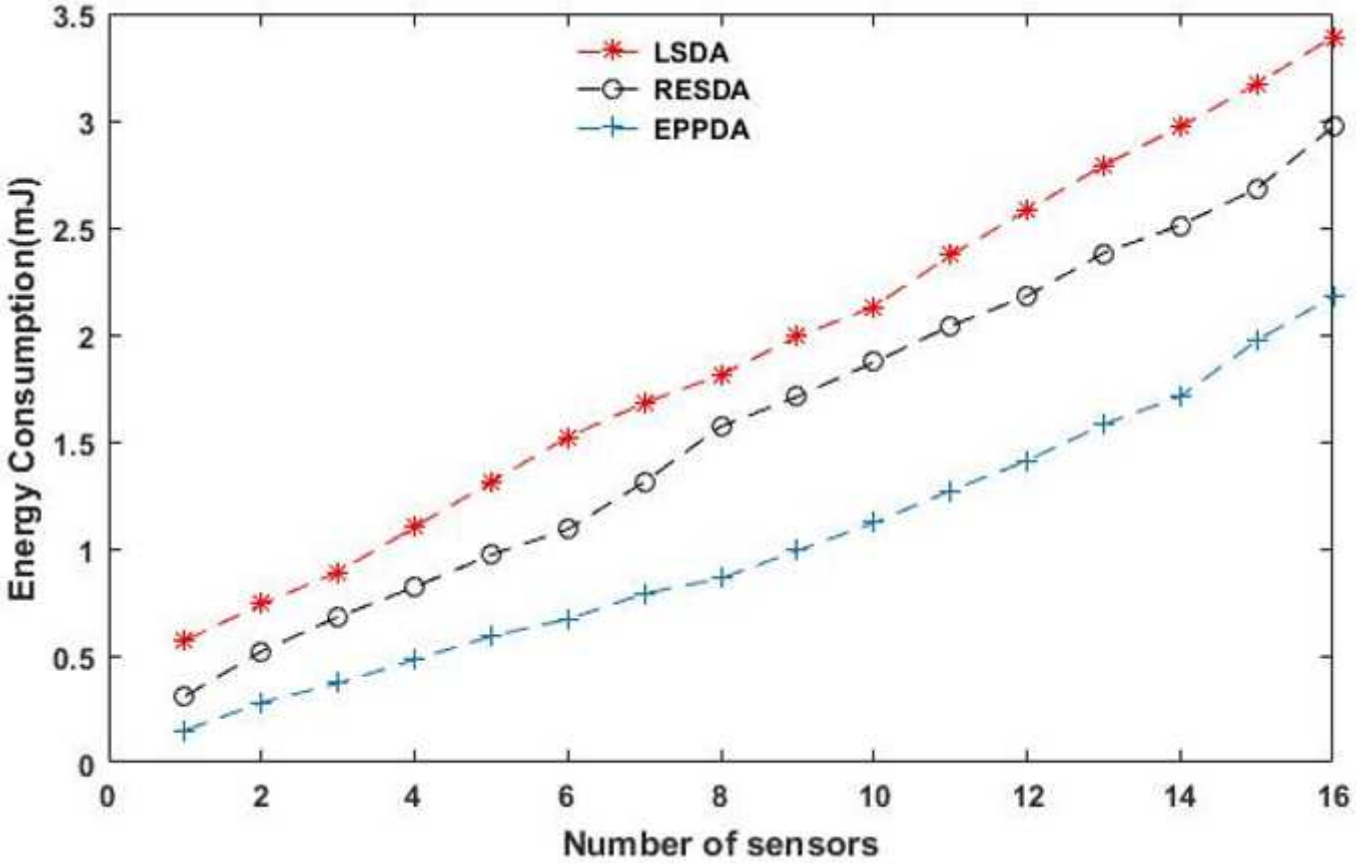

Figure 12

The total energy consumption.