Intelligent Automation & Soft Computing
DOI: 10.32604/iasc.2022.025665
Article

Tech Science Press

Aggregated PSO for Secure Data Transmission in WSN Using Fog Server

M. Manicka Raja[1,*] and S. Manoj Kumar[2]

[1]Department of Computer Science and Engineering, Hindusthan Institute of Technology, Coimbatore, 641032, India
[2]Department of Computer Science and Engineering, KPR Institute of Engineering and Technology, Coimbatore, 641048, India
*Corresponding Author: M. Manicka Raja. Email: mmanickraja21@outlook.com
Received: 01 December 2021; Accepted: 18 January 2022

Abstract: Privacy of data in Internet of Things (IoT) over fog networks is the biggest challenge in security of Wireless communication networks. In Wireless Sensor Network (WSN), current research on fog computing with IoT is gaining popularity among IoT devices over network. Moreover, the data aggregation will reduce the energy consumption in WSN. Due to the open and hostile nature of WSN, secure data aggregation is the major issue. The existing data aggregation methods in IoT and its associated approaches are lack of limited aggregation functions, heavyweight, issues related to the performance overhead. Besides, the overload on fog node will result in high latency, scalability, storage, degraded reliability and energy overhead. In order to overcome these issues, this proposed work has used two schemes for secure transmission of data over the network and reduce the energy consumption of the transmission. The secret data transferred between the IoT devices and the Fog server are transmitted through the aggregator node. If the aggregator node is placed far away from the Fog node, it may send the data to its neighbor aggregator. And it will append it with the current data and send it to the fog server through aggregator message receiving method. In addition to that, the fog server can extract the data through the fog message extractor method. In order to reduce the transmission cost and energy, Clustered Particle Swarm Optimization (CPSO) method is used to form the clusters. This proposed work can avoid the unnecessary energy consumption during the transmission and ensures secured aggregation so that the base station can know the origin of the sender and the validity of the received message. Therefore, the computation cost of the proposed work in authorization requires1MC+1H and the aggregation requires (n+2) MC+1H which is lesser than the existing methods.

Keywords: Wireless sensor network (WSN); fog; cloud; internet of things; aggregation; particle swarm optimization; energy consumption

1 Introduction

IoT is the emerging direction of the society and economy digitization where the objects and people are connected through wireless communication networks. It is mainly composed of sensors to generate the data and server to store, process and manipulating the data for bringing out better decisions [1–3]. Within it, large

volume of heterogeneous data are generated and communicated in bidirectional format. Due to its redundancy and lack of bandwidth, fog computing acts as a front-end service for the purpose of storing the distributed data generated from the IoT sensors based on the network storage and services. At the same time, it transfers it in to the cloud servers. There are various applications that are based on IoT which includes smart city [4,5], smart grid [6–8], smart healthcare [9,10], social network [11–14], smart phone [15], smart home [16], smart nation [17] and so on. It is undeniable fact that these applications have changed the human lifestyle in a smart way.

It is really a challengeable one to find an efficient data aggregation method which will satisfy the weakness of existing approaches with low communication cost, computational cost, recoverability, integrity and early filter of false injected data. To overcome all these issues, the proposed model is designed with the following contributions.

- Designs a fog assisted data aggregation method that utilizes peer to peer communication between the sensing devices and the servers. Initially, IoT sensing devices are clustered and the data from the sensing devices are aggregated by the Aggregator Node (AN) of its respective cluster.
- Aggregation node located nearer to the fog server transmits directly the encrypted data to the network server. The data from various AN that are located far away from the server are sent to its neighbor AN for transmission of data.
- Encryption and decryption are carried out using Asymmetric Paillier encryption method. AN aggregate the data with the proposed Aggregator Message Receiving Method (AMRM).
- Neighbor AN are found using the approach Clustered Particle Swarm Optimization (CPSO). This searching scheme finds AN which are nearer to the fog server as well as the source AN which will reduce the energy of the system.
- Fog server extracts the messages from AN using Fog Message Extraction Method (FMEM). This will help the model to monitor the data and save the values in local repository for a timestamp to ensure recoverability and also reduces the communication cost.
- Proposed model is evaluated with the existing schemes and provides the efficient data aggregation scheme with low computation cost, communication cost and minimum energy. Also, it ensures the functionalities such as recoverability, authorized aggregation, filter of false data rejection and data integrity.

Remaining sections of this paper are structured as follows: Section 2 discusses the related data aggregation schemes. Section 3 formulates the problem and the security model. Section 4 explains about the proposed efficient data aggregation method. Section 5 discusses the evaluation of proposed and existing data aggregation methods and Section 6 concludes with the merits of the proposed work with future directions.

2 Related Works

This section discusses the literature related to data aggregation method in IoT enabled WSN. Data Aggregation (DA) ensures for the security of message transmission with concatenation of data and avoids recurrent transmission. However, this will affect the energy consumption of WSN [18]. DA utilizes the multi hop path for the collection of data which involves intermediate nodes for data sharing. It will reduce the resource consumption and enhances the lifetime of the network [19]. Mainly, there are two kinds of data aggregation schemes. They include; arrangement-based DA and arrangement free DA. Particularly, the arrangement-based DA has no knowledge about the next hop sensor nodes. Whereas, the arrangement free DA is categorized as tree, cluster, flat network and grid-driven methods [20]. Efficient data aggregation with grouping of clusters has obtained better communication, where more than one node

is responsible for sharing the data between the peer and the distant nodes. Light weight-driven privacy preservation using data aggregation schemes are discussed in the referred articles [21–29]. The major problem is that the node selection for aggregation is the big challenge and even sometimes, there exists possibility of choosing inefficient nodes for consideration.

The proposed multidimensional secure data aggregation method involves in the discovery of neighbor key. The entire sensor nodes send the compressed data to the data aggregator. Moreover, the data is divided into two main parts using slicing mechanism and these data are exchanged in the two paths in different neighbor cluster heads until sink node has reached. With the consideration of lead and intermediate nodes, this method is also used for identifying the malicious node using locating mechanism. While sending the data, at certain point, the data is repeated and if the receiver has not received the final data, that particular node is identified as malicious node.

3 Problem Formulation and System Model

The proposed network structure is based on the cluster based aggregation method. The proposed network model of WSN is consisted of of large number of IoT sensor nodes that form a cluster and a common cluster head. Especially, each cluster communicates to the fog server through Aggregator Nodes (AN). In such case, IoT devices can transmit the data to assign AN through Peer to peer communication. Aggregator Node which is located far away from the fog server can transmit the data to the neighbor AN for the avoid of communication cost, threshold delay and sensing bottleneck which is considered to be the common issue in IoT enabled WSN. Huge number of sensing devices generates a large volume of data that leads the bottleneck. In Fig. 1 AN2 and AN3 are directly connected to the fog server. The AN1 is far away from the fog server. Then, the data transmission from AN1 to the fog server leads to the increase in the communication cost. Hence, AN1 can transmit the data to its neighbor aggregators such as AN3 or AN2 for its successful transmission. Within the cluster, all the neighbor sensing nodes of AN can encrypt the plaintext with its public key as $CT = E(PK, (M||R))$ to the Base station. At the same time, it is accounted as critical for the researchers in resolving these issues.

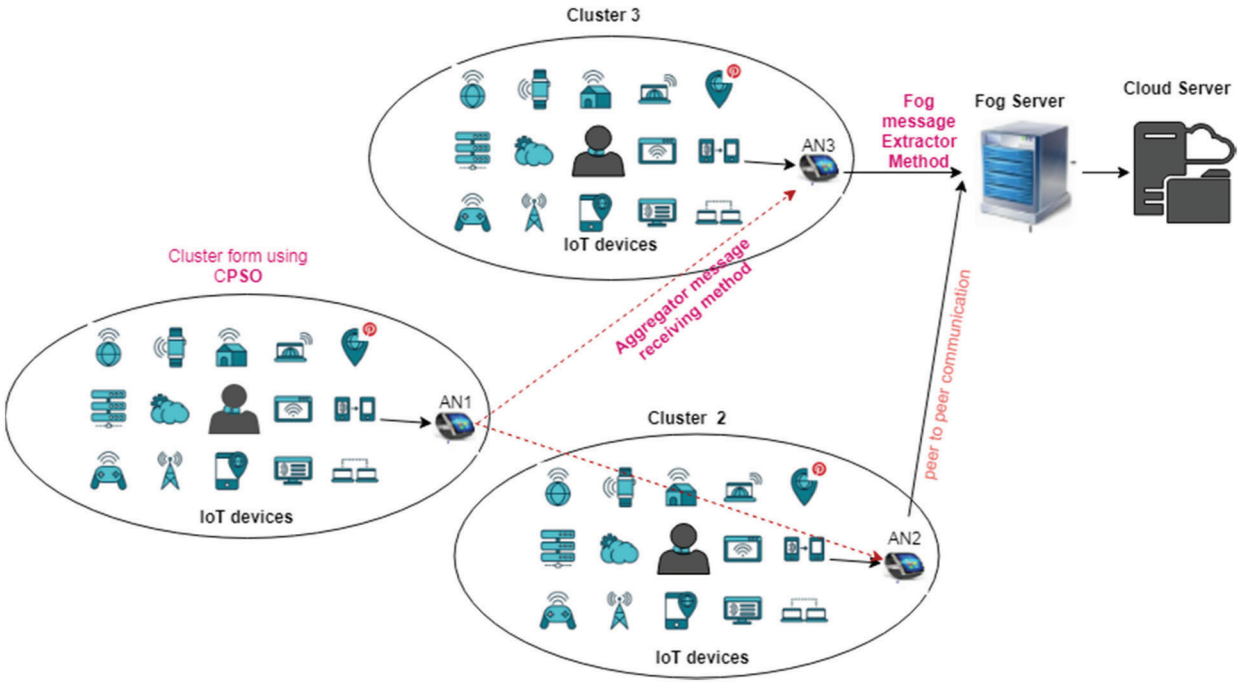

Figure 1: Overview of proposed system

Assume that the fog server is covered with m aggregators and each aggregator is composed of n IoT devices. The structure of Fig. 1 consists of three levels (level) such as Fog server (F), Cloud server (C) and Cluster which consists of IoT sensing devices and aggregator [30].

The proposed network is represented as direct acyclic graph $g_n = (n, l)$ where 'l' is the link between the nodes. Each node $n_i \in N$ with $i \in [0, N-1]$ which has the characteristics such as

- $Level_i$ in the network from 0 to level
- Capacity of CPU processing cpu_i in million instruction per second (MIPS)
- Capacity of memory ram_i in MB
- Energy consumption E_i^{idle}- energy of the device when it is not used and E_i^{max}- energy consumption of the device when it is used with maximum capacity.

Each link $l_p \in L$ that connects the nodes n_i and n_j with the following characteristics,

$$p = \begin{cases} (i, j) \ with \ \ i, j \in [0, N-1] & if \ peer \ to \ peer \\ (i, j_1, j_2, ..j_m) \ with \ j_m \in [0, N-1], \ m \in M \ if \ multi \ hop \end{cases} \quad (1)$$

Adversary Model

This adversary model considered the situations that are important for the data privacy during the data aggregation in the IoT enabled fog. AN is connected to the fog server that are fully trusted. The adversary model can also consist of certain characteristics as follows.

Design Objectives: Based on this system model and security needed, the objectives of the proposed work will derive secure, flexible and efficient data aggregation scheme with CPSO. For overcoming the attacks, the proposed work ensures security in terms of AN from one cluster to the neighbor AN that is chosen based on CPSO which will reduce the energy consumption of the network system. This secured energy efficient data aggregation scheme ensures the security constraints such as **Privacy preservation:** one device cannot infer the other device data to avoid collusion, **Authentication**: AN ensures that the received device is valid, **Data integrity**: AN detects the malicious activity by the adversary if it modifies or forges the data, **Efficiency**: with the implementation of CPSO, the proposed work is energy efficient and through aggregation, computational efficiency is ensured, **Flexibility**: the proposed work is convenient to add new IoT devices to the application.

4 Proposed Energy Efficient Data Aggregation Method

In order to ensure the data security among the network, the proposed system develops a secure data aggregation method which will overcome all the issues discussed in Section 3. The system mainly consists of four phases which are denoted in Fig. 2. In phase I, all the sensing devices can send the data to its respective AN using Homomorphic Encryption (HE) method. The sensing devices start the data transfer by encryption of data using the key which is preloaded and transfer it to AN which can further send the data to the fog server that are directly connected to AN. In Phase II, AN can receive the encrypted data from the device through AMRM. If AN is not connected to the fog server, nearby AN can be identified through the proposed CPSO scheme that is stated in Phase III. The fog server receives the data from AN using FMEM that is stated in Phase IV.

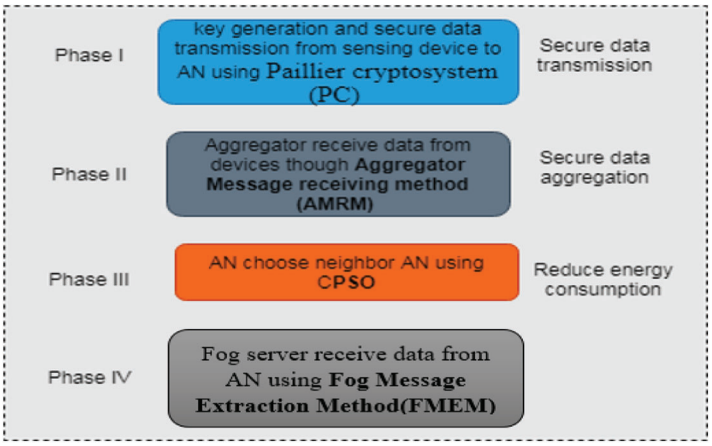

Figure 2: Proposed efficient data aggregation scheme

4.1 Phase I

The sensing devices encrypt the generated data and transfer to it's AN using Homomorphic Encryption method called Paillier Cryptosystem (PC) [31]. It is the asymmetric algorithm that provides secured and fast encryption and decryption. Based on Paillier Cryptosystem (PC), key generation, encryption and decryption are declared in algorithm 1.

Algorithm 1: (PC-encryption at sensor node)

Step 1: Key generation: Randomly, choose two prime numbers called p and q which are independent to each other as gcd(pq, $(p-1)(q-1)=1$)

- Calculate $t=pq$ *and* $\lambda=1$ cm, choose random integer number $g\epsilon Z_{t^2}^{*}$
- Ensure t divides g by checking the modular multiplicative inverse defined as

$$\mu = (G(g^{\lambda} \bmod t^2))^{-1} \bmod t \tag{2}$$

where $L(x)=x-1/t$

- Public key is (t, g) and private key is (λ, μ)

Step 2: Encryption: given plaintext p where $0 \le p \le t$ and random number r where $r \le p \le t$, ciphertext is calculated as

$$C = g^{p}.r^{t} \bmod t^2 \tag{3}$$

Step 3: Decryption: given cipher text c, plaintext is calculated as

$$p = G(c^{\lambda} \bmod t^2).\mu \bmod t \tag{4}$$

4.2 Phase II

The sensing device sends the message m with the concatenation of Node id (Nid), Timestamp T and encrypted data C_i with (λ, μ). In this phase, AN receives the encrypted message as cm_i from devices and concatenate the messages using Aggregator Message Receiving Method (AMRC). The sensor nodes which fulfill the querying scenario can be allowed sending to AN. Notations used in this algorithm are described in Tab. 1.

Table 1: Notations used

Notation	Description
N_i	Sensing device node id
T	Sensing device time stamp
h_i	Sensing device hash function concatenated with PC key
P	Plain text
K	Number of nodes send data to AN
CT_i	Encrypted cipher text by sensor device
CTm_i	Message sent by sensing node Ni to AN
ACT_m	Aggregated and encrypted message by AN
CA_j	Final aggregated message by AN
K_if	Key between sensing node and fog
m_i	Message extracted by fog
$H(Cm_i)$	hash function generated by Cm_i
$H'(Cm_i)$	Hash function of integrity check of Cm_i
D	Device
ANC	Aggregater node encryption

Algorithm 2: (AMRC)

Step 1: Initialize ANCp = null

Step 2: Receive $CTm_i = (N_i||T||D)$ from N_i

Step 3: if $T^{'} - T < \Delta t$ then

Step 4: if $H(CTm_i) == H'(CTm_i))$ *then*

Step 5: $$ACTm = ACTm||Cm_i \tag{5}$$

Step 6: else

Step 7: discard the message because of integrity violation

Step 8: End if

Step 9: else

Step 10: discard the message because of failure of newness

AN receives the Cyphertext (CT) message (m_i) called CTm_i from all the sensing devices where i is the node with ID. Now AN calculates the timestamp if the condition in step 3 is true, Cm_i is new or else it discards the message. In order to ensure the integrity, AN calculates the hash function of a received message and compares it with the original hash message [32]. If the condition mentioned in step 4 is true, AN aggregates all the messages received by the sensing device. Else the message is discarded. At the end, AN share the aggregated messages with the shared public key to the fog node as $CAj \oplus K(t_jg)$. It is the XOR operation of aggregated messages with the Key k generated using PC method.

4.3 Phase III

Neighbor AN node finds with CPSO if there is no peer to peer communication between AN and fog server. The aim of this phase is to place the set of AN in the heterogeneous network $AN = \{AN_0, AN_1, \ldots AN_{AN-1}\}$. Minimizing the cost function f with the constraint called $f: N^N \mapsto R$ which is the system total energy consumption E_C with the delay violation δ. The total delay violation is represented as,

$$\delta = \sum_{an_i \in AN} w_{an_i} \tag{6}$$

where

$$w_{an_i} = \begin{cases} 1 & if\ D_{an_i}^{max} < d_{a_i} \\ 0 & if\ not \end{cases} \tag{7}$$

Total energy consumption is the summation of energy of each node and communication network $E_T = E_N + E_C$.

4.3.1 Initialization of Population

Initially, the Particle Swarm $PS = \{x_0, x_1, ..x_{p-1}\}$ of size PS where $x_k \in P$ with T_{max} iteration. These particles are distributed in the search space. $\forall AN_i \in AN.\ x_k^0(i)$ uniformly takes AN_i aggregation nodes from the cluster. Velocities $v_k^0 = 1$.

4.3.2 Particle Position and Velocity Calculation

From Fig. 3, position of k th AN is the CPSO swarm as represented in $X_k^t \in AN^N$ where AN is the number of aggregation node vector with values $X_k^i \in [0,\ N-1] \forall i \in [0,\ M-1]$. $X_k^t(i) = r$ is the iteration t with AN_i is communicated to r^{th} cluster AN_z with $z \in [0, M-1]$ which is represented as

$$X_k^t(i) = r \Leftrightarrow Y_k^t(i,\ r) = 1 \wedge \forall j \in \{0,\ 1 \ldots N-1\} - \{r\},\ \ Y_k^t(i,\ j) = 0 \tag{8}$$

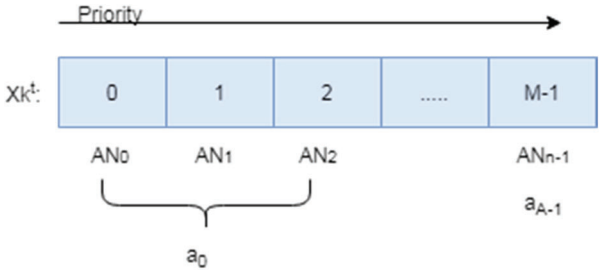

Figure 3: Position of k^{th} AN after t iteration

The particle velocity V_k is the $N \times M$ matrix which determines the motion speed of particle X_k. Each element of $v_k(i, j) \in R$ defines the possibility of connecting AN_i to cluster m_j. And the position of the particle is updated according to the following equations.

i) New velocity matrix is computed as,

$$v_k^{t+1}(i,\ j) = w^{t+1} v_k^t(i,\ j) + \varphi_1 w_1^{t+1}(i,\ j)[f(Pb_k^t) - f(X_k^t)] + \varphi_2 w_2^{t+1}(i,\ j)[f(Nb_k^t) - f(X_k^t)] \tag{9}$$

where, φ_1, φ_2-cognitive and social constant in the range [0, 4] and w_1, w_2–two matrices randomly [0, 1]. Pb –Personnel known best position, Nb-Neighbor best position. Particle representation of this vector format will reduce the memory space. The variable w influences the speed which lies between [0.5, 1] which denotes w_{low} and w_{high}. The variable w is updated using [33] stated in the

following equation,

$$w^t = w_{high} = \frac{(w_{high} - w_{low})}{T^{max}} \tag{10}$$

(ii) new particles position vector is updated as in Eqn

$$x_k^t(i) = r \Leftrightarrow v_k^t(i,\ r) = \max_{\forall j \in [0, N-1]} v_k^t(i,\ j) \tag{11}$$

(iii) Each $AN_i \in AN$ has its own subset of neighbor cluster AN and this network topology will reduce the placement possibility constraints of AN. If aggregation node ANi is not connected to AN in the cluster $m_j \in M$

$$\forall k \in [0,\ PS - 1],\ \forall t \in [0,\ T_{max} - 1] \Rightarrow v_k^t(i,\ j) = -\infty \tag{12}$$

4.3.3 Neighborhood Clustered Topology

It defines the Particle Swarm communication and finding the best search space for communication. In standard PSO, to find the global best solution, all the particles are exchanged with their possible solutions which lead to local optimum. To avoid this, search space is divided into sub groups called as the clusters and the communication is allowed in between the cluster aggregation nodes. This will deliver the best possible result when compared to the standard approach [34–36]. This neighbor network structure is represented in Fig. 4.

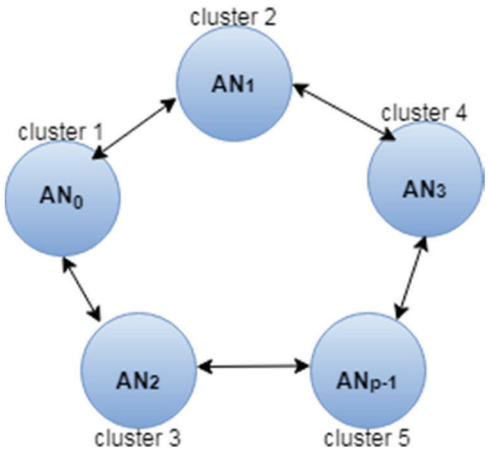

Figure 4: AN neighborhood network structure

In this network, AN from different clusters are communicated through AN to fog server. Aggregation node which is nearer to the fog server are selected from this network. AN, which is far away from the fog server will send its encrypted message. The messages are generated by the device to the fog server through neighbor AN that is found using this CPSO approach. Assume that AN0 and AN1 are far away from the fog server, the messages from cluster 1 is aggregated by AN0 and send through either AN1 or AN3 selected using CPSO approach as stated in algorithm 3.

Algorithm 3: CPSO–Neighbor AN selection

Input: Network nodes set N of size N, Set of AN of size M, P, T_{max}, φ_1, φ_2, w,w_1^0, w_2^0.

Output: Best possible placement vector called $G_{best,}$ Total energy E_T, total delay violations δ

Step 1: $V^0 = 1$, $P^0 =$ UniformInit (), $t = 0$ and $w^0 = 0.8$

Step 2: while ($t < T_{max}$) do

Step 3: for ($k \in [0, P-1]$) do

Step 4: for ($i \in [0, M-1]$) do

Step 5: for ($j \in [0, N-1]$) do

Step 6: if (m_j is authenticated device for AN_j) then

Step 7: $v_k^0(i, j) = 1$

Step 8: else

Step 9: $v_k^0(i, j) = -\infty$

Step 10: end if

Step 11: end for

Step 12: end for

Step 13: $Pb_k^0 = x_k^0$

Step 14: $Nb_w^0 = x_k^t$

Step 15: end for

Step 16: for ($x_k^t \in P^t$) do

Step 17: update velocity using Eq. (7)

Step 18: update position using Eq. (9)

Step 19: if ($(f(x_k^t) < f(Pb_k))$ then

Step 20: $Pb_k \leftarrow x_k^t$

Step 21: for $x_w \in neighbor(x_k)$ *and* $w = [0, P-1]$

Step 22: if ($(f(x_k^t) < f(Nb_w))$ then

Step 23: $Nb_w \leftarrow x_k^t$

Step 24: end for

Step 25: end for

Step 26: $$gbest \leftarrow x_r^t \leftrightarrow f(x_r^t) = \min_{\forall k,r \in [0,P-1]} f(x_k^t) \quad (13)$$

Step 27: i = i + 1;

Step 28: end while

4.4 Phase IV

Fog server receives the aggregated messages from all AN using FMEM. Then, the fog server is responsible for the decryption of the messages individually. Fog server then divides the aggregated data based on time stamp and extracts each AN data. FS extracts the aggregated message $ACTm_j = C'Aj \oplus K'(t_j g)$ by taking $C'Aj \oplus K'(t_j g)$. Hence, by using time stamp, encryption and

decryption method, hash function, each individual message of the sensing device mi is received as $m_i = CT_i \oplus K' t_i g$. Algorithm 4 explains these procedures in detail.

Algorithm 4: FMEM

Step 1: receive CAj $= ACTm_j \oplus K(t_j g)$

Step 2: if H (CAj) = =H′(CAj),

Step 3: $ACTm_j = \mathrm{C'Aj} \oplus K'(t_j g$ (14)

Step 4: for i = 1 to k

Step 5: extract $CTm_i = (N_i||T||D)$ from AN (15)

Step 6: if $T' - T < \Delta t$,

Step 7: extract ($\mathrm{CT_i}||\mathrm{h_i}$)) using decryption

Step 8: calculate $h_i = h(CT_i||K(t_j g)||T)$ (16)

Step 9: if $h_i = h_i'$ (*received hash*),

Step 10: $m_i = CT_i \oplus K' t_i g$ (17)

Step 11: save message to fog server local storage

Step 12: else

Step 13: integrity violation-discard message

Step 14: end if

Step 15: else

Step 16: newness failure-discard message

Step 17: end if

Step 18: end for

Step 19: else

Step 20: ACTm integrity violation-discard message

Step 21: end if

Fog server receives the aggregated cipher text of all the AN and considers XOR operation in step 3 with the key from algorithm 1. Until k which is the number of sensor nodes transmitting the data, it extracts the message in step 5 and checks the timestamp in step 6. If it is true, the hash value is calculated as in step 8. If the calculated hash and received hash value are equal, the original image is extracted using XOR operation as stated in step 10. Or else, the message is discarded due to integrity violation and newness failure. At the end of the execution of this algorithm, the fog node extracts the message sent by the AN and stores it in its local storage [37,38].

5 Performance Analysis and Discussions

This section discusses the evaluation performance of the proposed energy efficient data aggregation scheme called AMRM-CPSO-FMEM. The proposed scheme is evaluated in terms of functionality and cost which includes communication cost, computational cost and energy cost. Further, the method is

implemented in iFogSim [39], fog simulator with the CloudSim tool [40]. The proposed work is compared to the existing approaches such as Secure Privacy Preserving Data Aggregation (SPPDA), Concealed Aggregation Scheme for Multiple Application (CDAMA), Recoverable Concealed Aggregation (CDA) with homogeneous WSN (RCDA-HOMO) and Efficient Health Data Aggregation (EHDA) [41–43].

5.1 Evaluation of Functionality

Various data aggregation schemes functionality are evaluated such as recoverability, network false data filtering, peer to peer confidentiality, authorized aggregation and data integrity. Tab. 2 shows the evaluated results. Compared to the other existing approaches, the proposed scheme satisfies the extended functionalities.

Table 2: Performance evaluation and comparison of proposed system functionality

Methods	Recoverability	False data filtering	Confidentiality	Authorized aggregation	Data Integrity
SPPDA	Yes	No	No	Yes	Yes
CDAMA	No	No	No	Yes	Yes
RCDA-HOMO	Yes	No	Yes	Yes	No
EHDA	No	No	Yes	Yes	Yes
Proposed AMRM-CPSO-FMEM	Yes	Yes	Yes	Yes	Yes

5.2 Evaluation of Computational Cost (CC)

Computational cost is calculated based on the notations such as MC (Multiplication Cost), AC (one hop Addition Cost), E (cost of one modular Exponential) and H (cost of one Hash function). The comparison of existing and the proposed aggregation schemes CC are provided in Tab. 3.

Table 3: CC performance evaluation

Methods	Authorization	Aggregation
SPPDA	4MC + 2AC + 1H	(2n − 3)AC
CDAMA	2MC + 1AC	(n + 1)MC + nAC
RCDA-HOMO	4MC + 1AC + 1H	(2n − 2)AC
EHDA	2MC + 1H	(2n − 2)AC + 1H
Proposed AMRM-CPSO-FMEM	1MC + 1H	(n + 2)MC + 1H

From this evaluation, SPPDA requires 4MC+2AC+1H operations for its authorization phase in order to encrypt the data. For aggregation, the cluster head of each cluster requires (2n − 3) AC operations. For CDAMA, the authorization requires 2MC+1AC operations and the cluster head for aggregation requires (n + 1) MC+nAC operations. For RCDA-HOMO, each member node performs the authorization and requires 4MC+1AC+1H operations and (2n − 2) AC operations are required for the aggregation by the cluster head. For EHDA, each IoT device node performs the authorization which requires 2MC+1H operations and the aggregation by the needs of each cluster head (2n − 2) AC+1H operations. For the proposed scheme, each device node in the cluster needs 1MC+1H operations for encryption and for sending signature and AN in each cluster requires (n + 2) MC+1H operations. While comparing the

results, the proposed scheme needs less computational overhead for the data aggregation compared to the other existing approaches. The computational cost operations execution time called time cost is stated in Fig. 5. The computational cost of one IoT device is 0.00023 ms. For N number of IoT devices, time cost is n*(0.00023)ms.

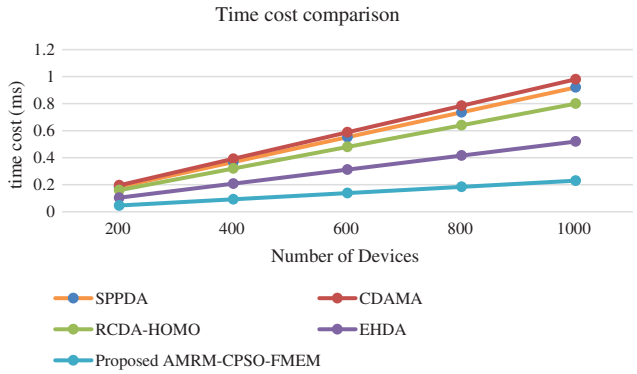

Figure 5: Total computational cost comparison of all IoT devices

In comparison to various aggregation schemes, the proposed data aggregation method requires less time for executing the computational operations for different number of IoT devices. To the maximum of 1000 IoT devices, the time cost of the proposed method is 0.23 ms. The total cost time of the compared approaches such as SPPDA, CDAMA, RCDA-HOMO, EHDA are 0.92, 0.98, 0.8, 0.52 ms respectively. Hence, the proposed efficient data aggregation scheme AMRM-CPSO-FMEM has obtained less cost for the execution of computational operations.

5.3 Evaluation of Communication Cost

In terms of exchange, the aggregated messages between the AN over the wireless network and the communication cost are calculated in terms of message exchange in bytes as shown in Fig. 6. In IoT enabled wireless network, the small message size requires the minimum communication cost. While sending the aggregated messages between the network, the proposed approach consumes its communication cost as 4000 bytes of data for transmitting 20000 bytes of data. Various existing approaches such as SPPDA, CDAMA, RCDA-HOMO, and EHDA are exchanged 5000, 5500, 6500 and 6000 bytes respectively. Comparatively, the proposed algorithm exchanges the data with low communication cost of 4000 bytes.

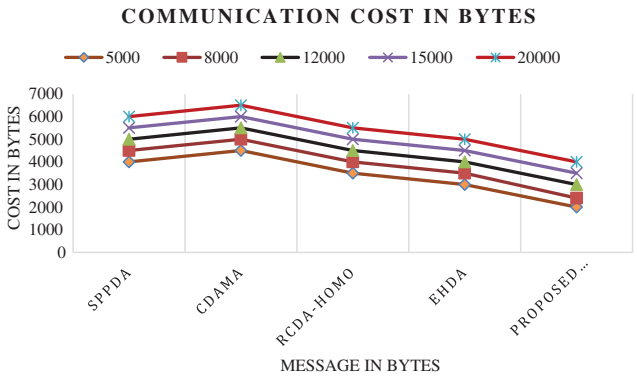

Figure 6: Comparison of communication cost in terms of bytes

5.4 Evaluation in Terms of Energy Consumption

Total energy consumption of various data aggregation schemes are calculated as in Eq. (16). The evaluated results are shown in Fig. 7.

$$E_T = (E_s * N) + (M * E_r) + (D * E_s) \tag{18}$$

where,

E_s-Energy of sending single message, E_r-Energy of receiving single message, N-total number of messages, M-total number of messages received, D-number of dropped packet

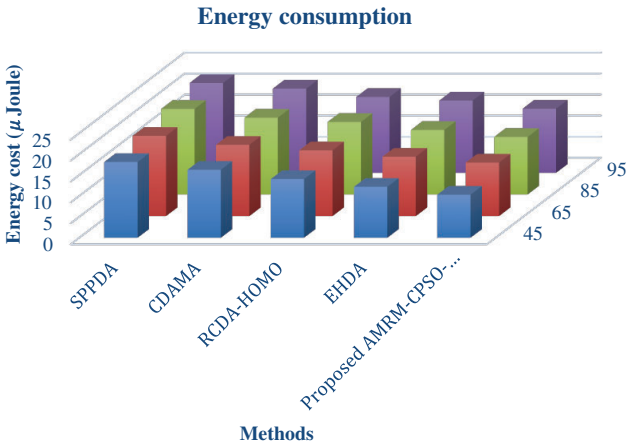

Figure 7: Comparison of energy consumption

While sending the maximum of 95 packets in the transmission, the proposed method consumes 15.261μ Joules of energy. The other existing approaches such as SPPDA, CDAMA, RCDA-HOMO, and EHDA consume 21.378 μ Joules, 20.029 μ Joules, 18.028 μ Joules and 17.209 μ Joules respectively. Some of the messages are dropped while sending the messages from AN to the server that is out of the communication range. AN can send the messages directly to the fog server or through neighbor AN using CPSO. This proposed approach consumes less energy due to the use of CPSO method. That is efficiently finding the next neighbor where the packet needs to forward in case of away fog server. At the same time, the searching time is also reduced due to the implementation of CPSO which will further reduce the energy of extra searching devices. This algorithm also finds AN that is nearer to the fog server and efficiently send the messages which will reduce the packet loss.

Energy consumption in terms of number of nodes in one cluster is evaluated as shown in Fig. 8. For the maximum of 100 nodes per cluster, the proposed scheme consumes 4.244 μ Joules. Various other existing approaches such as SPPDA, CDAMA, RCDA-HOMO, and EHDA consume 9.02 μ Joules, 8.387 μ Joules, 7.22 μ Joules and 6.028 μ Joules accordingly. Hence, in terms of all the evaluation processes, the proposed data aggregation approach is confidential, efficient and effective to deliver the message from IoT devices to Fog and Central cloud in secured manner.

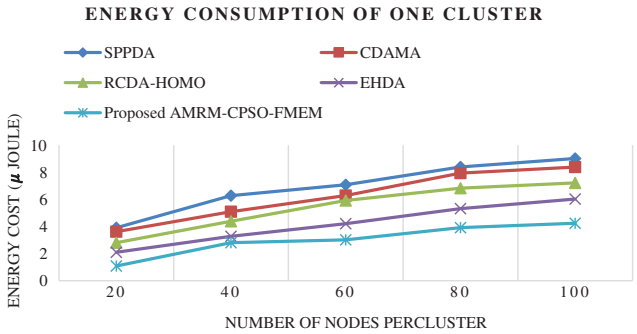

Figure 8: Energy cost of one cluster

6 Conclusion

In this paper, efficient and effective data aggregation scheme based on asymmetric Paillier Cryptosystem based encryption and decryption between the IoT devices data to aggregator is proposed. In order to ensure the efficiency of the data aggregation, the proposed method incorporates two methods between AN and fog server such as message received by aggregator from IoT device and message extracted by fog server from AN. In addition to that, this proposed scheme ensures the functionalities such as confidentiality, integrity, authorized aggregation and energy saving. The major features of the proposed work are (i) IoT devices are formed as cluster and for each cluster one aggregator node is created which will aggregate the data generated by the corresponding device node through AMRM. (ii) AN far away from the fog server is communicated to the neighbor AN using CPSO searching scheme which will reduce the time and energy cost and also ensures the confidentiality. (iii) Fog server can extract the encrypted data and decrypt the cipher text with the key and extract the messages using FMEM. With different kinds of evaluations, the proposed scheme is the best in terms of communication cost, computational overhead in terms of time and cost, functionality and energy consumption. In future, the proposed scheme is implemented with different region mobility of IoT sensing devices enabled fog.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] C. Cecchinel, M. Jimenez, S. Mosser and M. Riveill, "An architecture to support the collection of big data in the internet of things," in *Proc. 2014 IEEE World Congress on Services*, IEEE, Anchorage, AK, USA, pp. 442–449, 2014.

[2] M. Abu Elkheir, M. Hayajneh and N. Ali, "Data management for the internet of things: Design primitives and solution," *Sensors*, vol. 13, no. 11, pp. 15582–15612, 2013.

[3] C. Perera, R. Ranjan, L. Wang, S. U. Khan and A. Y. Zomaya, "Big data privacy in the internet of things era," *IT Professional*, vol. 17, no. 3, pp. 32–39, 2015.

[4] C. Hu, X. Cheng, J. Yu, Z. Tian, W. Lv. *et al.,* "Achieving privacy preservation and billing via delayed information release," *IEEE/ACM Transactions on Networking*, vol. 29, no. 3, pp. 1376–1390, 2019.

[5] A. Alkhamisi, M. S. H. Nazmudeen and S. M. Buhari, "A Cross-layer framework for sensor data aggregation for iot applications in smart cities," in *Proc. IEEE Int. Smart Cities Conf. (ISC2)*, pp. 1–6, Trento, Italy, 2016.

[6] A. Alrawais, A. Alhothaily, C. Hu and X. Cheng, "Fog computing for the internet of things: Security and privacy issues," *IEEE Internet Computing*, vol. 21, no. 2, pp. 34–42, 2017.

[7] Z. Cai and X. Zheng, "A private and efficient mechanism for data uploading in smart cyber-physical systems," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 2, pp. 766–775, 2018.

[8] H. Chunqiang, L. Hang, M. Liran, Y. Huo, A. Alrawais *et al.,* "A secure and scalable data communication scheme in smart grids," *Wireless Communications and Mobile Computing*, vol. 2018, pp. 1–17, no. 17, 2018.

[9] C. Hu, H. Li, Y. Huo, T. Xiang and X. Liao, "Secure and efficient data communication protocol for wireless body area networks," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 2, no. 2, pp. 94–107, 2016.

[10] T. K. Dasaklis, F. Casino and C. Patsakis, "Blockchain meets smart health: Towards next generation healthcare services," in *Proc. 2018 9th Int. Conf. on Information, Intelligence, Systems and Applications (IISA)*, Zakynthos, Greece, pp. 1–8, 2018.

[11] C. Hu, R. Li, W. Li, J. Yu, Z. Tian *et al.,* "Efficient privacy-preserving schemes for dot-product computation in mobile computing," in *Proc. 1st ACM Workshop on Privacy-Aware Mobile Computing*, ACM, Paderborn, Germany, pp. 51–59, July 2016.

[12] Z. Cai, Z. He, X. Guan and Y. Li, "Collective data-sanitization for preventing sensitive information inference attacks in social networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 577–590, 2018.

[13] Z. He, Z. Cai and J. Yu, "Latent-data privacy preserving with customized data utility for social network data," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 1, pp. 665–673, 2018.

[14] L. Huang, X. Fan, Y. Huo, C. Hu, Y. Tian *et al.,* "A novel cooperative jamming scheme for wireless social networks without known csi," *IEEE Access*, vol. 5, pp. 26476–26486, 2017.

[15] S. Egelman, A. P. Felt and D. Wagner, "Choice architecture and smartphone privacy: There's a price for that," *E-Economics of Information Security and Privacy*, pp. 211–236, 2013.

[16] T. Song, R. Li, B. Mei, J. Yu, X. Xing *et al.,* "A privacy preserving communication protocol for IOT applications in smart homes," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1844–1852, 2017.

[17] S. L. Hoe, "Defining a smart nation: The case of Singapore," *Journal of Information, Communication and Ethics in Society*, vol. 14, no. 4, pp. 323–333, 2016.

[18] Y. Huo, Y. Tian, L. Ma, X. Cheng and T. Jing, "Jamming strategies for physical layer security," *IEEE Wireless Communications*, vol. 25, no. 1, pp. 148–153, 2018.

[19] X. Zheng, Z. Cai and Y. Li, "Data linkage in smart iot systems: A consideration from privacy perspective," *IEEE Communications Magazine*, vol. 10, no. 2, pp. 12–20, 2018.

[20] C. Hu, W. Li, X. Cheng, J. Yu, S. Wang *et al.,* "A secure and verifiable access control scheme for big data storage in clouds," *IEEE Transactions on Big Data*, vol. 4, no. 3, pp. 341–355, 2018.

[21] L. Chen, R. Lu, Z. Cao, K. Alharbi and X. Lin, "Muda: Multifunctional data aggregation in privacy-preserving smart grid communications," *Peer-to-Peer Networking and Applications*, vol. 8, no. 5, pp. 777–792, 2015.

[22] C. Li, R. Lu, H. Li, L. Chen and J. Chen, "PDA: A privacy-preserving dual-functional aggregation scheme for smart grid communications," *Security and Communication Networks*, vol. 8, no. 15, pp. 2494–2506, 2015.

[23] H. Bao and R. Lu, "A lightweight data aggregation scheme achieving privacy preservation and data integrity with differential privacy and fault tolerance," *Peer-to-Peer Networking and Applications*, vol. 10, no. 1, pp. 106–121, 2017.

[24] R. Lu, K. Heung, A. H. Lashkari and A. A. Ghorbani, "A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT," *IEEE Access*, vol. 5, pp. 3302–3312, 2017.

[25] P. D. Patel, B. Pranav and V. Ravindra, "Data aggregation in wireless sensor network," *International Journal of Management, IT and Engineering*, vol. 2, no. 7, pp. 457–472, 2012.

[26] C. Zhang, C. Li and J. Zhang, "A secure privacy-preserving data aggregation model in wearable wireless sensor networks," *Journal of Electrical and Computer Engineering*, vol. 61, pp. 1–9, 2015.

[27] W. He, X. Liu, H. Nguyen, K. Nahrstedt and T. Abdelzaher, "Pda: Privacy-preserving data aggregation in wireless sensor networks," in *Proc. of the INFOCOM 2007 26th IEEE Int. Conf. on Computer Communications*, Anchorage, AK, USA, pp. 2045–2053, 2007.

[28] Y. H. Lin, S. Y. Chang and H. M. Sun, "Concealed data aggregation scheme for multiple applications in wireless sensor networks," *IEEE Transactions on Knowledge and Data Engineering*, vol. 25, no. 7, pp. 1471–1483, 2013.

[29] K. A. Shim and C. M. Park, "A secure data aggregation scheme based on appropriate cryptographic primitives in heterogeneous wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 8, pp. 2128–2139, 2015.

[30] Y. Huo, C. Hu, X. Qi and T. Jing, "LoDPD: A location difference-based proximity detection protocol for fog computing," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1117–1124, 2017.

[31] C. Hu, N. Zhang, H. Li, X. Cheng and X. Liao, "Body area network security: A fuzzy attribute-based signcryption scheme," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 37–46, 2013.

[32] Y. Huo, W. Dong, J. Qian and T. Jing, "Coalition game-based secure and effective clustering communication in vehicular cyber-physical system (vcps)," *Sensors*, vol. 17, no. 3, pp. 475, 2017.

[33] Y. Lu, Z. Zhao, B. Zhang, L. Ma, Y. Huo *et al.,* "A Context-aware budget-constrained targeted advertising system for vehicular networks," *IEEE Access*, vol. 6, pp. 8704–8713, 2018.

[34] C. Hu, Y. Huo, L. Ma, H. Liu, S. Deng *et al.,* "An attribute-based secure and scalable scheme for data communications in smart grids," in *Wireless Algorithms, Systems, and Applications (WASA)*, pp. 469–482, Berlin, Germany: Springer, 2017.

[35] H. Bao and R. Lu, "Comment on privacy-enhanced data aggregation scheme against internal attackers in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 1, pp. 2–5, 2016.

[36] N. Saputro and K. Akkaya, "Performance evaluation of smart grid data aggregation via homomorphic encryption," in *Proc. of the Wireless Communications and Networking Conf. (WCNC)*, IEEE, Paris, France, pp. 2945–2950, 2012.

[37] S. Maheswaran, P. G. Kuppusamy, S. M. Ramesh, T. V. P. Sundararajan and P. Yupapin, "Refractive index sensor using dual core photonic crystal fiber–glucose detection applications," *Results Phys*, vol. 11, pp. 577–578, 2018.

[38] S. Maheswaran, B. K. Paul, M. A. Khalek, S. Chakma, K. Ahmed, and M. M. Rajan, "Design of tellurite glass based quasi photonic crystal fiber with high nonlinearity," *Optik*, vol. 181, pp. 185–190, 2019.

[39] Z. Erkin, J. R. Troncoso-Pastoriza, R. L. Lagendijk and F. PerezGonzalez, "Privacy-preserving data aggregation in smart metering systems: An overview," *IEEE Signal Processing Magazine*, vol. 30, no. 2, pp. 75–86, 2013.

[40] R. Lu, "Privacy-enhancing aggregation techniques for smart grid communications," *Wireless Networks*, 2016.

[41] R. Lu, X. Liang, X. Li, X. Lin and X. Shen, "EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1621–1631, 2012.

[42] E. Shi, T. H. Chan, E. G. Rieffel, R. Chow and D. Song, "Privacy preserving aggregation of time-series data," in *Proc. of the Network and Distributed System Security Symposium, (NDSS)*, San Diego, California, USA, 2011.

[43] K. Alharbi and X. Lin, "LPDA: A lightweight privacy-preserving data aggregation scheme for smart grid," in *Proc. Int. Conf. on Wireless Communications and Signal Processing, WCSP*, Huangshan, China, pp. 1–6, 2012.