# ESDAM - Efficient and Secure Data Aggregation against Malicious Nodes in Iot Environment

**Veerabadrappa, Girisha M N, P M Booma**

***Abstract*—*Rapid expansion of IoT technologies and their devices has created the considerable convenience in the daily lives of the people. Modernization of technique in IoT has allowed them to perform just more than sensing that directly means the more energy consumption. It is a known fact that most of the IoT devices have the limited power supply and hence it is an obvious need to design the energy efficient model. Despite of IoT devices being so useful in daily life and in other industries, data security is one of the primary concern in the fields of IoT application such as healthcare, agriculture, defense etc., and it is a challenging task to provide the data security in these fields. In past, several methods have been proposed to address this challenge, however, either they failed to provide the security or they lack from the efficiency. In this paper, it introduces a methodology named as ESDAM (Efficient and Secure Data Aggregation against Malicious Nodes) that provides better security with improved efficiency. The proposed methodology is parted into two methods, which helps in discerning the malicious nodes. First method, is through extending coordinates and the second method, is through surveilling the adjacent nodes. Extensive simulation has been performed by applying various constraints through persuading various number of malicious and performance metrics such as energy utilization, number of failed nodes, packet mismatch rate and packet discern rate. The performance evaluation of the simulation results proves that proposed methodology performs better than the existing methods.***

***Index Terms*—*IoT Security, Malicious Nodes, Secure Data Aggregation***

## I. INTRODUCTION

IoT i.e. Internet of Things is said to be the self-configured network as it interconnects the particular objects or the things that are present in the network. An object means the item which is present in the real world and capable enough to provide the communication chain [1]. The communication helps in transmission of data in the given paths by taking the help of network. Hence, it is meant to say that the main aim of IoT model is to connect the things in real world. In a simple words, IoT can be defined as the Network of interconnected objects or things. All of the IoT object can be transmittable either physically or virtually and each of these objects are associated with ID.

IoT has revolutionized the normal lifestyle by providing the convenience for various application and through the research, it has been found out that by the end of 2020, the IoT would hold the market of nearly 1.7 trillion dollar and 50 billion connected things [2]. IoT has several application such as in healthcare [3]–[5] agriculture [6]–[8], defense [9] and others. Wireless IoT is capable of interconnecting the embedded devices and these type of devices are mostly battery oriented, hence, they has limited function, such as, computation, processing and transmission. This phenomena has led the IoT to be used in almost everyplace, some of them includes E-healthcare, Smart cities [10] and Smart homes [11]. IoT possesses variety of characteristics in various areas, however, everywhere they share similar wireless IoT essence. In general, any application can be named as the inter-connected network, which uses the IoT devices. Things that are interconnected contains variety of data and these data can be anything from being the behavior of user to the private information. In case of such dynamic and distributed environment the IoT services can be a major threat where the data might be compromised and which might affect the end user. This damage can occur in various ways such as data modification, data leaking, data tapping and data destroying.

IoT possesses variety of characteristics in various areas, however, everywhere they share similar wireless IoT essence. In general, any application can be named as the interconnected network that uses the IoT devices. Moreover, IoT devices interconnects variety of multimodal data and these data can be anything from being the behavior of user to the private information. In case of such dynamic and distributed environment the IoT services can be a major threat where the data might be compromised and which might affect the end user. This damage can occur in various ways such as data modification, data leaking, data tapping and data destroying. The Fig. 1, shows the data aggregation technique model. It has several parts such as devices, clusters, aggregator and base station. Here, the device sense the data and sends it to the aggregator where the data aggregation takes place. Later, the aggregated data is sent to base station and through base station, it is sent to cloud storage from there end user can access the data.

### 1.1 *Architectural view of IoT*

The Fig.1 shows the complete IoT model, it has four distinctive component such as Sensors, Gateway, Cloud Server and End User [12].

*Sensors:* Sensors are the small devices, which is used for .sensing the environment sensor can be of multiple type such as temperature,

**Revised Manuscript Received on December 30, 2019.**
***** Correspondence Author

**Veerabadrappa***, Data Warehouse Engineer in The Banking Domain of Software Industry, Malaysia.

**Girisha M N,** Master of Engineering in Bioinformatics from Department of CSE, UVCE College of Engineering affiliated to Bangalore University

**Booma Poolan Marikannan,** Lecturer in School of Computing, Asia Pacific University of Technology & amp; Innovation, Malaysia.

pressure motion detection, proximity and others. Moreover, several sensors can be combined to work just more than sensors, smartphone is one of the best example, and it has several sensors.

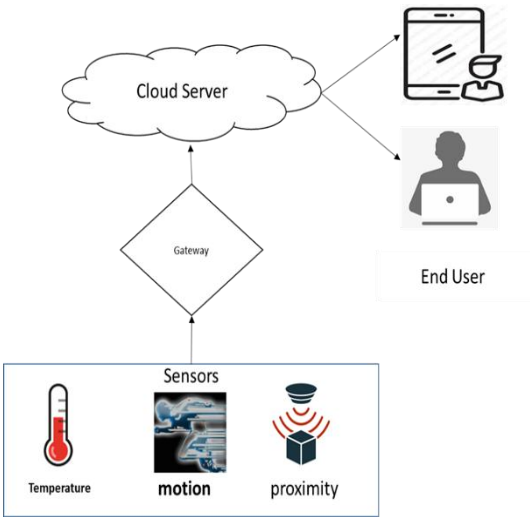

**Figure 1 IoT architecture**

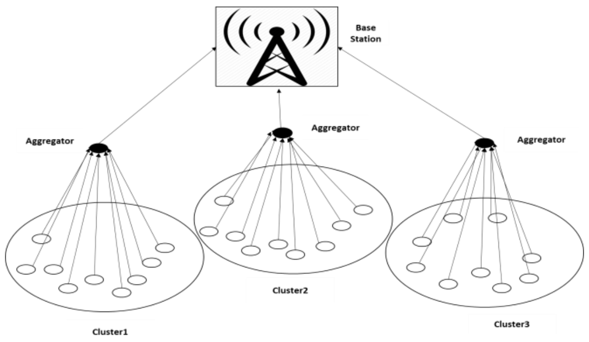

**Figure 2 Data Aggregation Model**

A *Gateway:* Once the data is sensed it needs to be stored and it is stored in the cloud, however to, send the data into cloud medium is required and this can be done through the gateway.

B *Cloud server:* This is one of the important part as the data sensed might be huge, hence cloud platform is used for storing the data.

C *End User:* Intuitive apps helps the end user for monitor- ing and controlling the devices.

### 1.2 *Motivation and Contribution*

IoT applications requires the IoT devices to send huge amount of data from one place to another and all these collected data needs to be transmitted directly. However, these sensor nodes are energy constraint and they need a processing technique which can help in conserving energy, hence, the Data Aggregation technique was introduced [13]. DA (Data Aggregation) is one of the technique, which helps in reduction of energy consumption and increases the network lifetime. Meanwhile in IoT, the sensors are power constrained, hence, Data Aggregation was introduced, the main idea behind data aggregation is to collect the data and aggregate it in efficient manner. Efficient data aggregation helps in eliminating re- dundancy and reducing the amount of data transferred [14]. However, data aggregation may degrade the service metrics of IoT, such as, fault tolerance, latency and accuracy. The aggregator nodes are prone to various attacks, one of the most concerned attack is compromising of nodes and it is one of the important security concern [15]. In compromising of nodes attack, the data might be tempered, as the false data might be injected and this leads to violation of data privacy [16]. This phenomena has led the researcher as well as industries to develop a methodology to secure the data.Hence, this paper propose a methodology named as ESDAM (Efficient and Secure Data Aggregation against Malicious Nodes) that uses two distinctive methods to secure data. First method, is Coordinates Extension and second method, is surveilling through the adjacent node. ESDAM has the following contribution in IoT Security:

- The data aggregation is done securely and smoothly.
- ESDAM is two step method, first is through the coordi- nate extension and through surveilling the adjacent node and it helps in discerning the malicious nodes.
- ESDAM provides the secure environment for IoT.
- It detects the malicious nodes effectively when compared with other methods.
- ESDAM is best energy utilized method when the nodes fails i.e. when the node is dead.
- ESDAM discern the malicious node.
- Persuades the various number of malicious nodes for evaluation of ESDAM methodology.
- ESDAM outperforms the existing method in consideration of eminent parameter such as, MNDR(Malicious Node Discern Rate) and MPMR(Malicious node packet mismatch Rate).

## II. LITERATURE SURVEY

As Data Aggregation in IoT has one of the major role to play in processing the data, hence, a lot of research has been done in the past for secure data aggregation. Some of the important methodologies has been surveyed in this research work.

The present broadcast protocols that is authenticated [17] need sensors of IoT to verify the data of broadcast with the key revealed by their gateway in upcoming interval of time. This produces an authentication delay, and every single sensor has to store all packets that are unauthenticated within its buffer. Even in scenario where a delay is allowed, there is some limit for the buffer size of IoT devices. However, there is no security for privacy of messages that will be broadcast and no protection design that is proven formally. Privacy protection infrastructure based on interaction, for example, [18], are approaches based for preventing the operations and deactivating the operation that are unauthorized. This privacy protection method utilizes levels of privacy preventing to stop accessing the data, which are sensitive. This protects operations that are unauthorized on IoT data. Solutions of Public Key, for example, as described in system introduced in [19], activate prevention of data for IoT devices.

They utilize IoT gateway to gather information from sensors and use encryption accordingly to the information, manage user access and protective transmission algorithms for gaining important privacy and protection needed for data, which are sensitive. Additionally, the interest is getting more to join and help theoretical forensic-by-model as shown in [20]. In the present method of access control that is based on EBA [21], [22], sensors are required to encrypt IoT information with EBA method. User that is having the policies of access control can decrypt the information that is encrypted. Anyways, EBA methods [23] usually generates more computation and are tough to develop in IoT devices and wireless sensors with some range of energy and capacity of computation.

The control method of data access takes help of encryption method of homomorphic offered by cryptosystem of Paillier

[24] to make sure the access is privacy protected for IoT information. To use the information, the client needs a secret and public key set ($sk$, $pk$) for cryptosystem of Paillier. The key can be possibly controlled and given with CA (Certificate- Authority). To access the information, the client sends a request containing the clients identity, query (along with time window), execution to be done on the information and private, public key set. In our implemented method, the aim is to offer analyzed information to the client without disclosing the actual information to both in between the client and server. The channel of communication between client and access layer of information is considered to be a protective channel and the access layer of information utilizes some kind of access control same as [21], [22]. If the clients request clears the sign authentication and fulfills the policies of access control, the access layer of information will execute the Algorithm-1 to fill the corresponding information. Based on CP-EBA, alternative fine-grained method of ac- cess controlling for IoT devices was introduced in [22]. This method permits only policies that are based on AND. In [24], author introduces a system, which is based on identity that prevents information of the location of IoT devices while in emergency cases. In this method, every single client interacts with others with the help of VID (Virtual-ID) that is not having any actual data about the client. In this infrastructure, privacy of the client can be prevented very well as they transmit only VIDs to interact, and VID is not specified and cannot be linked to clients. The information of the location will be transmitted to the client only when the authentication is successfully done. In IoT, authenticating identities of the devices are important to stop access that are not authorized to private information of client, and permit the access only for authorized clients. In [25], author introduces a protocol for authentication for IoTs. In the introduced protocol sensors are end nodes, and every node has an exclusive global address for linking via internet. To obtain a session key, cryptograms for PK and SK is assumed for IoT platforms, but they have some issues like cryptograms for SK needs huge memory to hold key chains and cryptograms for PK utilizes more power. Later in [26] the security concern was solved through authentication mechanism i.e. X.509 digital certificates, the digital certificates were capable of encrypting, hashing and then the certificates were created to secure the data. However, the generation of digital certificates is quite complicated. In [27], author introduces an ECC (Elliptic-Curve-Cryptosystem) dependent key obtaining approach applicable for IoT platform. The analysis of outcome shows that the introduced protocol can protect man-in-the middle, replay, eavesdropping and key control attacks. In [28], [29] for security the private data is stored in the separate server that tries to ensure the confidentiality, integrity and availability of the data. The data are also stored in the fog server, this dual storage helps in retrieving the data easily, however, this fails to provide the security as well as privacy. Similarly [30], [31] introduced a method based on the signature and it helps in securing the data multi-source IoT system. Here, the multi source network were used and it holds the security assumption under q-SDG. Signature scheme does holds well for the security purpose. However these mentioned method faces from several issue such as in case of high frequency data it fails to provide the desired security in terms of location privacy. Other issue is that the identity of the user can be impersonated for uploading the malicious data. In [32] mainly focused on the preserving the privacy of health data from the various source by providing the fair incentives, here advanced method of cryptographic schemes were used in order to support the data confidentiality while the data transmission takes place. Moreover to achieve the fair incentive , ID-based signature were used which detects the replay attacks and guarantee the privacy. Here three layer DA framework were approached first is for saving the computation load , second is adding noise with the differential privacy and later encrypt the data. In the third layer the CC(Cloud cener) aggregates the data and decrypts it. However the main disadvantage was that the privacy violation. In [33] proposed a model named as LBOAMax which tries to acieve the secure aggregation based on the data location. Here the Max data are aggregated first then LBOA Top-K and the LBOA Sum was proposed to obtain the Top-K as well as the sum aggregated, this scheme tries to achieve the secure aggregation based on the location and focuses on the location privacy protection. Moreover [34] worked to achieve the secure data aggregation multifunctional DA method through the ML approach is proposed, this supports the huge range of SAF(Statistical Aggregation function). [35] proposed the model for the network aggregation, a particular scheme of secret sharing and crypto model were introduced through this scheme only the particular cloud server can compute the aggregated data, however, a portion of the working cloud servers are compromised. Later [36] proposed a ADA(Anonymous Data Aggregation) to secure the participants identity, this allows the aggregator to gather the participants data without the identification of any other data.

In the above literature survey, we have observed that enormous research work has been performed and some of them does provide the security, however all these above discussed method have failed on one or another parameter, such as, some of the method are complex in nature, some of them are not secure or some of them lacks from efficiency. Henceforth, after the extensive survey we have designed and developed a methodology named as ESDAM based on the adjacent node surveillance.

ESDAM not only helps in achieving the secure data aggregation in IoT environment but also to achieve it in In next section we are going to discuss ESDAM methodology

## III. PROPOSED METHODOLOGY

### *3.1 System Model*

Assume, a particular network where the nodes are organized into various clusters as well as consider the connected cluster with number of nodes(devices). The data is aggregated from the cluster, it is important to note that the data has to be private, i.e. data is not exposed to any of the node. A network of the virtual network is constructed with logical link where the network are constructed over one another to exchange the data. The virtual link created is proceed as the undirected graph, that consists of node set, logical links and adjacent set. In the proposed model, all the nodes have been organized into the various clusters using the clustering algorithm where each cluster is connected by two nodes and the data is aggregated from all the nodes in the given clusters. An overlay network is designed to construct the same two different nodes that chooses the other node as adjacent node for data exchange among them. Later the overlay network is modeled as the undirected graph. As shown in Fig. 3 the proposed system model has three phases of execution:

- *Phase-I*: We achieve the data aggregation, in initial stage the data is not shared as it might contain the private data which also includes adjacent node.
- *Phase-II*: We perform the ESDAM that helps in securing the data and detecting the malicious nodes and it discards the malicious node.
- *Phase-III*: Final Phase involves reducing the energy con- sumption and achieving the optimized model through various parameter and constraints.

After completing all three phases, plot the results and evaluate the performance of the proposed system with well defined parameters such as energy utilized, number of failed nodes and packet discern rate.

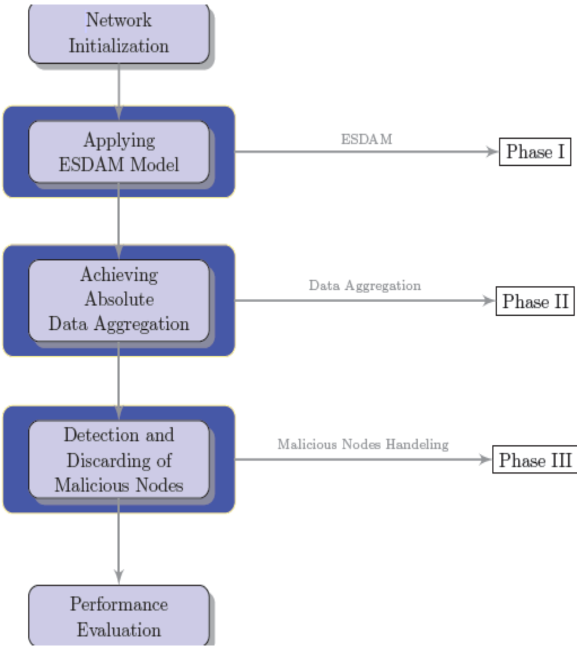

**Figure 3 system Model**

Consider any undirected graph $Z = (X, Y)$ where, denotes the node set and $Y$ denotes the Edges. Now consider the node $u$ with neighbour set $Neigh_u$, here, $v \in Neigh_u$ if and only if $(v, u) \in Y$. Moreover, node u has the information about the neighbour set$Neigh_u$, however it has to be noted that they do not have complete knowledge about the topology. Consider initial state of the node as $m_u(0)$ positive set integer, positive set integer is denoted by $P^+$, henceforth lets consider the below equation i.e. equation 1. In the initial state, the node has confidential information and the aggregated data only shows the statistics of whole node such as variance, average and sum. This scenario does not show the privacy of the node when it comes to the large network.

$$||m||_\infty = max\{|m_u|\} \qquad (1)$$

### *3.2 Aggregation Generation (Additive Aggregation)*

The proposed methodology extracts required aggregation, which is known as additive aggregation as stated in the following equation (2).

$$\sum_{u=1}^{S} m_u(0) \qquad (2)$$

Listed below are problem solutions:

- At first, the aggregation are obtained in a distributed manner.
- Moreover, the initial information is hidden from each
- other so that the privacy can be maintained.
- The cost has to be minimized. Here, the cost directly
- refers to the communication cost and the computation cost.
- At last, the secure mechanism is developed such that the
- malicious nodes gets detected in case of any abnormal behaviour.

At first, add noise to ongoing state in each iteration which is shown in equation 2. Here, $m_u^+(It)$ is the particular state at iteration $It$. $N_u$ be the noise which is added to secure the data, $It$ is the iteration which sets the distribution

$$m_u^+(It)\text{=}\ m_u(It) + N_u(\mathrm{It}) \qquad (3)$$

The average is computed in the following equation.

$$m_u(It+1) = AWT_{uu} m_u^+(It) + \sum AWT_{uv} m_u^+(It), u \in X, v \in X \qquad (4)$$

$AWT$ is the average weight.

$$AWT_{uv} = \begin{cases} [1 + \max\{[Neigh_u], [Neigh_v]\}]^{-1} & v \in Neigh_v \\ 1 - \sum_{o \in Neigh_i} V_{mr} & u = v \\ 0, & else \end{cases} \qquad (5)$$

ESDAM is introduced in order to secure the data. Noise are added to its current state and this takes place each time. Whenever the communication is done, it clearly means that each node will broadcast to its given neighbour which is given in following equation i.e. equation 3 is written in matrix form as given in the below equation.

$$m(It+1) = NW(m(It) + N(It)) \quad (6)$$

Here $N$ and m belongs to the $P_n$ and $P_{nXn}$ belongs to $P_{nXn}$and this satisfies the below equation i.e.

$$\text{U}=[u_1, u_2, u_3, \dots \dots, u_n]^T \quad (7)$$

$$N=[N_1, N_2, N_3, \dots \dots, N_n]^T \quad (8)$$

$$NW=[\text{A}WT_{uv}]_{nXn} \quad (9)$$

Above equation is the average computation algorithm, moreover if $N(It)$is null then the average $NW$ is obtained exponentially since the is the randomly determined process

$$\lim_{It\to\infty} m_u(It)= \bar{m}, \text{u} \in Y \quad (10)$$

Moreover, equation 10, $\bar{m}$ can be defined through the equation 11.

$$\bar{m} = n^{-1} \sum_{u\in Y} m_u(0) \quad (11)$$

It is well known fact that the value of noise cannot be zero, hence it should be designed in such a way that the value should not be zero due to security process. Moreover, AWSN (Additive White Gaussian Noise) makes sure that the average algorithm is obtained. However, the malicious nodes tends to add the noise without any condition and this leads to the performance degradation.

### *3.3 Data Aggregation against Malicious Nodes*

In this section of the research develops and design ESDAM that deals with the malicious nodes. The main purpose here is to secure the privacy of data while monitoring on to the nodes for being malicious. Hence, in order to achieve this ESDAM implements two sub methodology, firstly, it extends the dimension called as D-Extension and secondly, is to perform the Surveillance of nodes though its adjacent nodes.

### *3.3.1 Coordinate Extension*

At first, each node is parted into two distinctive parts that is given through the following equation.

$$m_u^1(0) = RV_U + \frac{1}{2} m_u(0) \quad (12)$$

$$m_u^2(0) = \frac{1}{2} m_u(0) - RV_u \quad (13)$$

$RV_u$ is random variable that has been picked up randomly $\left[-\frac{\theta}{2}\,\omega, -\frac{\theta}{2}\,\omega\right]$ and $0 < \omega < 1$, hencethe aggregator equation is as follows

$$m_u(0) = m_u^1(0) + m_u^2(0) \quad (14)$$

Moreover the aggregator node divides the UG (Undirected Graph) $Z = (X, Y)$ into the other two UG-subgraph which is given by $Z_a$ and $Z_b$, meanwhile $Z_a$=$(X, Y_1)$ and $Z_b$=$(X, Y_2)$ where$(Y_1,\ Y_2) \in Y$. Later the set of adjacent node set $P_u^x$ and $u = 1{,}2$. Moreover the nodes computes the weights and $AWT_{uv}$ and the node transmit $m_u^1(0)$ and $m_u^2(0)$ to the particular neighbor $P_u^1$ and$P_u^2$.

$$m_u^{x\prime}(It) = m_u^x(It) + \omega_u^x(It) \quad (15)$$

Now let us consider $\overline{m_u}$ which is the estimated approximation of $m_u^1(0)$ and $PE_m$ is the Error Prediction and it can be known as the adjacent. Moreover, statistic set $stat_u^x$

$$stat_u^x\text{=\{x,} \quad AoN_u^x, AoN_v^x, \overline{m_u} \quad (0), \quad (16)$$
$$PE_m, m_u^{x'}(It), m_v^{x'}(It)\ \}$$

Where$v \in P_u^x$, $AoN_u^x, AoN_v^x$ indicates the adjacent nodes an it is used for surveilling. surveilling method involves the detection as well as discard the malicious nodes, now a particular aggregator node chooses any nodes to surveillance the adjacent node. The main advantage is when the particular node sends the message to secure the other node then the aggregator node has to pass only the topology information to the chosen nodes and this makes sure that the chosen nodes have the $stat_u^x$ knowledge i.e. Node $u$ have the complete access about the node $v$ and how the updation takes place is available for node $u$ .Next is to detect the malicious nodes. Let us assume that the aggregator randomly chooses a node to monitor neighbor node.

### *3.3.2 Adjacent node surveilling*

Assume that the aggregator randomly chooses a node to monitor neighbor node, once such request are received the given three scenarios are checked, let's consider to be the neighbor node u of the node v satisfies the below equation.

$$\omega_v^x(It)\text{=}m_v^{x\prime}(It) - [\text{A}WT_{vv}^{x} m_v^{x\prime}(It-1) + \quad (17)$$
$$\textstyle\sum_{r \in B_n^e} AWT_{nr}^x\, m_r^{x\prime}(It-1)]$$

Where $|\omega_m^e(l)| \le \frac{1}{2}\alpha\rho^l$ and $V_n^r$ is computed using the equation 3 for$l \in B^+$.

$$m_v^+(0) - \widehat{m_v}(0) \le \tfrac{5}{4}\alpha\rho \quad (18)$$

$$\frac{m_v'(0)}{2} - m_v^{x\prime}(0) \le \frac{5}{4\alpha\rho} \quad (19)$$

If the equation 17,18 and 19 satisfies then the node is correct node else it is considered to be te malicious nodes. If it is reported as the malicious node then that particular node is dissolved and hence it does not affect the aggregation. Here, equation 17 makes sure that each iteration constitutes average process and the distortion added rots, equation 18 makes sure that the malicious nodes are bounded through the estimation error and equation 19 makes sure of that all the mentioned rules are followed.

Based on these equations the Data Aggregation (DA) algorithm is written.

### *3.3.3 Secure DA algorithm*

The algorithm is designed for securing the data. Here, at first step-7 is induced and let the threshold iteration be the square of n, this makes sure that for absolute aggregation. Moreover, the below equation is initialized.

$$|m_u(It) - m_v(It)| \leq \; O \text{ for } \forall v \in \; P_u \qquad (20)$$

The above equation is used for terminating the iteration In proposed algorithm, the two neighbour sets are given, as the input and the expected output are the updated states. Hence, in the given algorithm if the three equation passed the normal nodes are passed.

```
Algorithm 1 Secure Data Aggregation Algorithm
Step1: start
Step2: random vectors are generated such that the given elements can be choosen from the [-$\frac{\theta}{2}\ \omega, \frac{\theta}{2}\ \omega$ ]
Step3: Initialize $m_u^1(0)$ and $m_u^2(0)$ using the equation
Step4: Initialize $m_u'(0)$ using equation 1 and $m_u^{e\prime}(0)$ using equation 8
Step5: In case if the aggregator chooses the node $u$ to monitor the nodes
Step6: the aggregator provides the all the information such as $x, mal_r^x, mal_v^x, P_v^x$
Step7: let' s initialize $\tau_u^x(0) = \omega_m^x(0)$ and also initialize $It = 1$
Step8: initialize $It = 1$ while $It \; < \; Threshold\ \_iteration$
Step9: use Received and Information Set $m_v^x(It-1)$ and $set_n^e(It-1)$ are used for monitoring
Step10: If the particular node follows the three equation 8,9 and 10 as the criteria then the node is normal node else can be declared as the malicious nodes
Step11:update the below equation $m_u^x(It) = \; AWT_{uu}^x m_u^{x\prime}(It - 1) + \sum_{r \in P_u^x} AWT_{uu}^x \, m_l^{x\prime}(It-1)$
Step12:Initialize $m_u(It)$= $m_u^1(It) + m_u^2(It)$ and choose $\tau_u^x(It)$ and $\omega_u^x(It)$ according to the below equation. $\omega_u^x(It)$<= $\omega_u^x(It) - \; \delta_i^v(It-1)$.
Step13: using the equation 8 lets initialize $a_m^e(l)$
Step14: transmission of $m\,_u^x(It)$ and $v$ to their corresponding neighbors
Step 15 : Increment $It$ by 1
Step16: end
```

### *3.3.4 Accuracy*

Using the proposed methodology we analyze the constraints on malicious nodes, moreover the security of the model is analyzed. Let $m_u(0)$ be the initial states of malicious node $u$ and let's assume that malicious nodes $u$ uses $\widetilde{m_u}(0)$ instead of $m_u(0)$ while computing the $\overline{m_u}(0)$ and $m_u^{x\prime}(0)$ then this leads to the false computation of $m_u'(0)$ and $m_u^{x\prime}(0)$ <= $\frac{\theta}{2}\omega$ . $m_u^{-v}(0)$ would be the false initial state and it satisfies $|\overline{m_u^x}(0) - \; m_u^{x\prime}(0)| < \; = \frac{\theta}{2}\omega$ for $x = 1{,}2$.Moreover from the our methodology, we achieve the consensus and the malicious nodes and while evaluation which is discussed in the next section and hence the agreement has been achieved while maintaining the gap between the nodes is maintained.

## IV. PERFORMANCE EVALUATION

This section evaluates the proposed agreement based algorithm.In order to achieve such scenario the C# is used as a programming language with the help of the Sensoria simulator [37]. Sensoria is a fully pledged wireless sensor network (WSNs) simulator and been preferred by researchers over other WSN simulators due to its useful features. It is component based simulator that provides rich graphical user interface and simulates almost all scenarios from small to large scale WSNs. Also, it provides simulation results in various formats that can easily configured to include different simulation details and with increased accuracy. The computer has the configuration of 8 GB Ram and 2GB Nvidia Graphics on the Windows Operating System. Microsoft Visual Studio V17 is used as IDE for writing and evaluating the code. Table I shows the proposed model configuration, the WSN network is simulated that contains 100 nodes in the area of dimension 50mX50m, introduced the malicious nodes in multiples of 10 till 40 nodes. The scenarios are simulated using two base stations with the initial energy of 0.2J.

ESDAM methodology is evaluated by considering various parameters and constraints based on the count of failed nodes, energy usage by nodes and comparative parameters that measures how many malicious nodes defined and how manypackets mismatched. Moreover Table 1 depicts the model configuration.

**Table 1 Model Configureation**

| | |
|---|---|
| Area of the Network | 50m * 50M |
| Number of nodes | 100 |
| Malicious nodes induced | 10, 20 , 30 and 40 |
| Number of Base Station | 2 |
| Initial Energy | **1.2** *J* |

### 4.1 Number of Failed Nodes

In order to evaluate the data aggregation algorithm, the experiment is performed with one of the eminent parameter NoF (Number of Failed) nodes that effects the model efficiency directly. The more number of failed nodes indicates the low performance of model. The Quality of Service(QoS) is decreased by the number of failed nodes and it is most important to evaluate for proving the effectiveness of algorithm. As shown in Fig. 4 graph is plotted with the failed nodes along with malicious nodes persuading against simulation time. Here, X axis is simulation time in seconds, whereas Y axis indicates the failed or dead nodes. From the graph 4 it can be clearly observed that proposed methodology identifies the dead nodes effectively for varying malicious nodes presence in network. Similarly, as shown in Fig. 5 graph is plotted for the failed nodes against the malicious nodes. where, X axis is the malicious nodes persuading and Y axis is the dead nodes. From the plot 5 it can be observed that as the malicious nodes are increased then the proposed framework identifies more dead nodes that is most useful measure.

### 4.2 Energy utilized

By Nature WSN nodes are battery power devices and tiny devices. Hence, energy efficient data aggregation methodologies are most essential that increases the lifetime of the node. Energy Utilization is the term used for minimizing the amount of energy needed for productivity and services. The graph shown in Fig. 6 depicts the energy utilization when the malicious nodes are present in the network. The X-axis indicates the number of malicious nodes persuade and Yaxis indicates the energy utilized in units of milli joules(mj)and the graph clearly shows the linear increment in energy consumption over the number for malicious nodes increased in network.

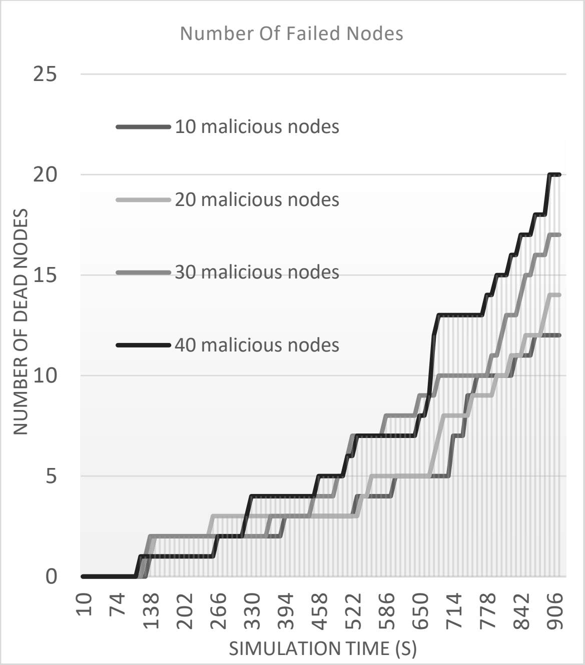

**Figure 4 Dead Nodes vs Simulation Time**

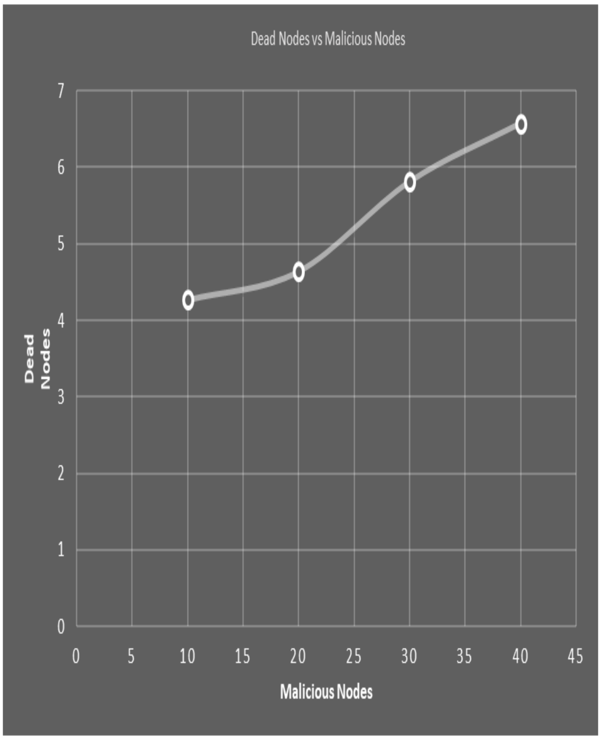

**Figure 5 Dead Nodes vs Malicious Nodes**

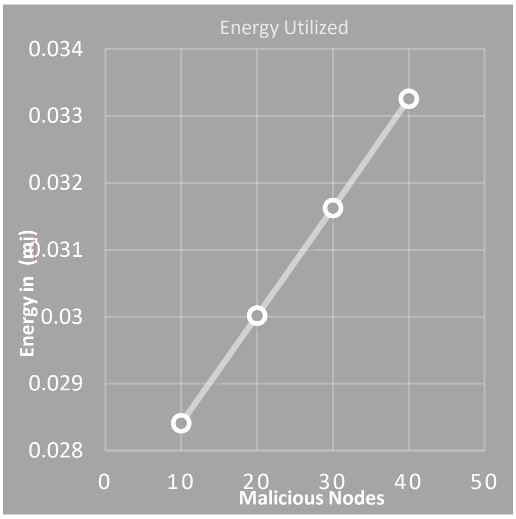

**Figure 6 Energy vs Malicious nodes**

#### *4.2.1 Comparison Analysis*

The comparative analysis is performed along with the parameter evaluations which provides useful measurement criteria to evaluate the proposed methodology. The Malicious Node Discern Rate and Malicious Packet Mismatch Rate parameters are analysed over the number of persuade malicious packets and the results are mentioned in following sections.

#### 4.2.1.1 Malicious Node Discern Rate

Malicious Node Discern Rate (MNDR) is one of the parameter, which is considered for the evaluation of our proposed algorithm. Discern rate is defined as the identification of discerning malicious nodes. Increase in number of malicious packet identification discern yields the better efficiency of the system and to be considered more secured method. In graph shown in Fig. 7 depicts the MNDR, in the graph Y axis is malicious nodes as 10, 20, 30 and 40 malicious nodes whereas X axis has the malicious packet. The results have been plotted for both existing system and our proposed system and it clearly shows the comparative increment in identification of discern malicious packets as more number of malicious nodes were persuaded into the system.

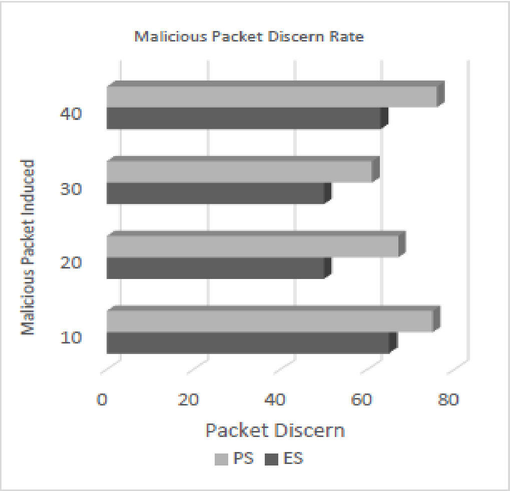

**Figure 7Malicious Packet Induced vs Packet Discern**

#### 4.2.1.2 Malicious Packet Mismatch Rate (MPMR)

Another evaluation parameter is the Malicious Packet Mismatch Rate and it shows that model fails to identify the malicious nodes, the lesser mismatch shows the better efficiency of the model. In the graph shown in Fig. 8 that is plotted malicious packet persuade against the packet mismatch, where X axis depicts the malicious packet mismatch, Y axis depicts the malicious nodes persuaded. The graph shows that proposed system has the less packet mismatch rate is compared to the existing methodology [38], as the number of malicious packet persuaded increased.

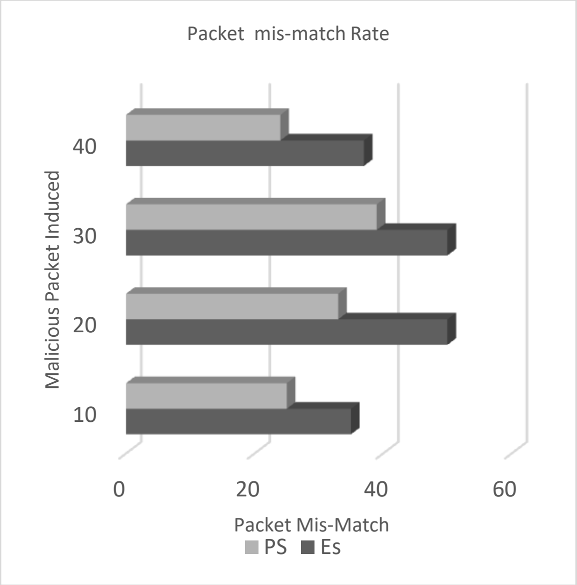

**Figure 8 malicious Packet Induced Va Packet Mis-Match Rate**

## V. CONCLUSION

In this research paper, the proposed ESDAM framework evidently addresses security in the IoT environment. At the same time, the proposed methodology ESDAM also highlights the security concern which is raised with the malicious nodes while sharing the data through two methods. First method, is by dimension extension and second method, is through adjacent node surveillance. Through adjacent nodes we get the error bound due to the malicious nodes. Moreover, for evaluation extensive simulation has been done and the analysis of results shows that proposed model is more secure and efficient than the existing models. Though this research works ensures the security but still many open issue exists, such as, how it performs under the various constraints. Hence, in future with the help of ESDAM mechanism, a novel method can be prepared in such a way that no nodes are malicious and thiscan achieve absolute security in IoT environment. In future work, evaluation of ESDAM needs to be considered through the constraints such as failure of first device, failure of certain number of devices and other constrains.

## REFERENCE

1. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," Future generation computer systems, vol. 29, no. 7, pp. 1645–1660, 2013.
2. G. Davis, "2020: Life with 50 billion connected devices," pp. 1–1, Jan 2018.
3. L. Catarinucci, D. De Donno, L. Mainetti, L. Palano, L. Patrono,

a. M. L. Stefanizzi, and L. Tarricone, "An iot-aware architecture for smart healthcare systems," IEEE Internet of Things Journal, vol. 2, no. 6, pp. 515–526, 2015.

4. [4] E. Luo, M. Z. A. Bhuiyan, G. Wang, M. A. Rahman, J. Wu, and M. Atiquzzaman, "Privacyprotector: Privacy-protected patient data collection in iot-based healthcare systems," IEEE Communications Magazine,

a. vol. 56, no. 2, pp. 163–168, 2018.

5. [5] S. Amendola, R. Lodato, S. Manzari, C. Occhiuzzi, and G. Marrocco, "Rfid technology for iot-based personal healthcare in smart spaces," IEEE Internet of things journal, vol. 1, no. 2, pp. 144–152, 2014.
6. [6] J. Ruan, Y. Wang, F. T. S. Chan, X. Hu, M. Zhao, F. Zhu, B. Shi, Y. Shi, and F. Lin, "A life cycle framework of green iot-based agriculture and its finance, operation, and management issues," IEEE Communications

a. Magazine, vol. 57, no. 3, pp. 90–96, 2019.

7. [7] O. Elijah, T. A. Rahman, I. Orikumhi, C. Y. Leow, and M. N. Hindia, "An overview of internet of things (iot) and data analytics in agriculture: Benefits and challenges," IEEE Internet of Things Journal, vol. 5, no. 5, pp. 3758–3773, 2018.
8. M. C. Vuran, A. Salam, R. Wong, and S. Irmak, "Internet of underground things in precision agriculture: Architecture and technology aspects," Ad Hoc Networks, vol. 81, pp. 160–173, 2018.
9. T. Abdelzaher, N. Ayanian, T. Basar, S. Diggavi, J. Diesner, D. Ganesan, R. Govindan, S. Jha, T. Lepoint, B. Marlin et al., "Will distributed computing revolutionize peace? the emergence of battlefield iot," pp. 1129–1138, 2018.
10. H. Rajab and T. Cinkler, "Iot based smart cities," 06 2018.
11. C. Paul, A. Ganesh, and C. Sunitha, "An overview of iot based smart homes," in 2018 2nd International Conference on Inventive Systems and Control (ICISC), Jan 2018, pp. 43–46.
12. Z. Zhu, R.-G. Huang et al., "Study on the iot architecture and accesstechnology," in 2017 16th International Symposium on DistributedComputing and Applications to Business, Engineering and Science (DCABES). IEEE, 2017, pp. 113–116.
13. B. Pourghebleh and N. J. Navimipour, "Data aggregation mechanisms in the internet of things: A systematic review of the literature and recommendations for future research," Journal of Network and Computer

a. Applications, vol. 97, pp. 23–34, 2017.

14. Y. Lu, P. Kuonen, B. Hirsbrunner, and M. Lin, "Benefits of data aggregation on energy consumption in wireless sensor networks," IET Communications, vol. 11, no. 8, pp. 1216–1223, 2017.
15. N. Labraoui, M. Guerroui, M. Aliouat, and T. Zia, "Data aggregation security challenge in wireless sensor networks: a survey," Ad hoc & Sensor Networks International Journal, vol. 12, no. 3-4, pp. 295–324, 2011.
16. A. Ayadi and S. Sassi, "Privacy in the age of internet of things: Challenges and prospects," in 2016 Global Summit on Computer & Information Technology (GSCIT). IEEE, 2016, pp. 48–53.
17. A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "Spins: Security protocols for sensor networks," Wireless networks, vol. 8, no. 5, pp. 521–534, 2002.
18. A. Samani, H. H. Ghenniwa, and A. Wahaishi, "Privacy in internet of things: A model and protection framework," Procedia Computer Science, vol. 52, pp. 606–613, 2015.
19. C. Doukas, I. Maglogiannis, V. Koufi, F. Malamateniou, and G. Vassilacopoulos,

a. "Enabling data protection through pki encryption in iot m-health devices," in 2012 IEEE 12th International Conference on Bioinformatics & Bioengineering (BIBE). IEEE, 2012, pp. 25–29.

20. M. Paul, M. S. Hossain, M. M. Rahman, Q. A. Khaliq, and S. Rahman, "Chemodynamics of cypermethrin insecticide in summer country bean ecosystem in bangladesh," Research Journal of Environmental Toxicology, vol. 10, no. 1, p. 50, 2016.
21. S. Yu, K. Ren, and W. Lou, "Fdac: Toward fine-grained distributed data access control in wireless sensor networks," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 4, pp. 673–686, 2010.
22. P. Picazo-Sanchez, J. Tapiador, P. Peris-Lopez, and G. Suarez-Tangil, "Secure publish-subscribe protocols for heterogeneous medical wireless body area networks," Sensors, vol. 14, no. 12, pp. 22 619–22 642, 2014.

23. R. L. Cramer, Advances in Cryptology-EUROCRYPT 2005: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings. Springer Science & Business Media, 2005, vol. 3494.
24. C. Hu, J. Zhang, and Q. Wen, "An identity-based personal location system with protected privacy in iot," in 2011 4th IEEE International Conference on Broadband Network and Multimedia Technology. IEEE, 2011, pp. 192–195.
25. J. Liu, Y. Xiao, and C. P. Chen, "Authentication and access control in the internet of things," in 2012 32nd International Conference on Distributed Computing Systems Workshops. IEEE, 2012, pp. 588–592.
26. S. Karthikeyan, R. Patan, and B. Balamurugan, "Enhancement of security in the internet of things (iot) by using x. 509 authentication mechanism," in Recent Trends in Communication, Computing, and Electronics. Springer, 2019, pp. 217–225.
27. S. Kalra and S. K. Sood, "Secure authentication scheme for iot and cloud servers," Pervasive and Mobile Computing, vol. 24, pp. 210–223, 2015.
28. T. Wang, J. Zhou, M. Huang, M. Z. A. Bhuiyan, A. Liu, W. Xu, and M. Xie, "Fog-based storage technology to fight with cyber threat," Future Generation Computer Systems, vol. 83, pp. 208–218, 2018.
29. J. Li, X. Chen, S. S. Chow, Q. Huang, D. S. Wong, and Z. Liu, "Multi-authority fine-grained access control with accountability and its application in cloud," Journal of Network and Computer Applications, vol. 112, pp. 89–96, 2018.
30. C. Wang, J. Shen, Q. Liu, Y. Ren, and Y. Li, "A novel security scheme based on instant encrypted transmission for internet of things. Security and communication networks," 2018.
31. T. Li, W. Chen, Y. Tang, and H. Yan, "A homomorphic network coding signature scheme for multiple sources and its application in iot," Security and communication networks, vol. 2018, 2018.
32. W. Tang, J. Ren, K. Deng, and Y. Zhang, "Secure data aggregation of lightweight e-healthcare iot devices with fair incentives," IEEE Interne of Things Journal, 2019.
33. J. Zhang, Y. Zong, C. Yang, Y. Miao, and J. Guo, "Lboa: Locationbased secure outsourced aggregation in iot," IEEE Access, vol. 7, pp. 43 869–43 883, 2019.
34. W. Jia, H. Zhu, Z. Cao, X. Dong, and C. Xiao, "Human-factor-aware privacy-preserving aggregation in smart grid," IEEE Systems Journal, vol. 8, no. 2, pp. 598–607, 2013.
35. S. Han, S. Zhao, Q. Li, C.-H. Ju, and W. Zhou, "Ppm-hda: privacypreserving and multifunctional health data aggregation with fault tolerance," IEEE Transactions on Information Forensics and Security, vol. 11, no. 9, pp. 1940–1955, 2015.
36. Q. Li and G. Cao, "Providing efficient privacy-aware incentives for mobile sensing," pp. 208–217, 2014.
37. J. N. Al-Karaki and G. A. Al-Mashaqbeh, "Sensoria: A new simulation platform for wireless sensor networks," pp. 424–429, 2007.
38. J. He, L. Cai, P. Cheng, J. Pan, and L. Shi, "Consensus-based dataprivacy preserving data aggregation," IEEE Transactions on Automatic Control, 2019.

## AUTHORS PROFILE

**Name** Veerabadrappa
Qualification M.E (Computer Science),
Specialization Computer Science
Email Id veeru4998@gmail.com

Veerabadrappa is currently working as a Data Warehouse Engineer in the banking domain of Software Industry, Malaysia. He has 5+ years of working experience in Software Industry. Veerabadrappa received his Master of Engineering in Computer Science and Engineering from Bangalore University and recevied Bachelor of Engineering in Information Science and Engineering from Vishwesharaia Technological University. He is UGC NET and KSET qualified. He has worked on various real-time projects of Banking, Insurance and ERP domains. His research interests are towards the area of IoT, Artificial Intelligence, Big Data, Data Analytics and Visualization and Image Processing.

**Name** Girisha M N
Qualification M.E (Computer Science),
Specialization Computer Science

Girisha M N received his Master of Engineering in Bioinformatics from Department of CSE, UVCE College of Engineering affiliated to Bangalore University and received Bachelor of Engineering from Vishwesharaia Technological University. Girisha has 7+ years of Software Industry experience especially in the development background on various projects in Financial, Infotainment and Healthcare domains. He also has expertize on different programming languages, tools and methodologies.

**Name** Booma Poolan Marikannan
Qualification M.S (Computer Science)
Specialization Computer Science

Booma Poolan Marikannan is now working as a lecturer in School of Computing, Asia Pacific University of Technology &amp; Innovation, Malaysia. Booma received her Doctorate in Computer Science and Engineering from SRM University, India, Masters and Undergraduate with the specialization of Computer Science and Engineering Science from Anna University, India. Her research was in enlarging efficient disease identification system with the help of Machine learning techniques. She received a best paper award in one of the ISI journal during 2014 for one of her research paper. She also received a Best Supportive Teacher award during 2015. She is SME in the field of Data Science. Booma has 10+ years of teaching experience in various area under Computer science and she excels impressively. She has been invited as guest speaker for several talks on Machine Learning and conducted several workshops related to Machine Learning. Her research interests are towards the area of Machine Learning, Big Data, Data Mining, Data Analytics and Visualization, Artificial Intelligence, Image Processing and Health care &amp; IT. She is also an active IEEE and IET member.