# Trust-based Key Management Conglomerate ElGamal Encryption for Data Aggregation Framework in WSN using Blockchain Technology

T.G.Babu[1]
Research Scholar
Vels Institute of Science,
Technology and Advanced Studies, Chennai, India

Dr.V.Jayalakshmi[2]
School of Computing Sciences, Vels Institute of Science,
Technology and Advanced Studies
Chennai, India

***Abstract*—In wireless sensor networks (WSN), data aggregation is a widely used method. Security issues like data integrity and data confidentiality became a significant concern in data aggregation when the sensor network is deployed in a hostile environment. Many researches may carry out several works to tolerate these security issues. However, there were some limitations like delay, the arrival rate of packets, and so on. Hence, to overcome the existing problems, this approach offers a blockchain-dependent data aggregation scheme in WSN. The main intention of the proposed work is to generate a certificateless key generation so that the proposed system's secrecy rate is improved. The use of blockchain is employed for security purposes, and it enables the user to acquire the information stored internally in an effortless manner. Initially, deployment of sensor and base station (BS) is carried out, followed by node registration at which the public/private keys are generated. The computation of private hash values is carried by performing certificateless key generation. After that, the formation of blockchain is made using the PoW (Proof of Work) detection algorithm followed by the aggregation of data. In the data aggregation process, Elgammal based cryptographic approach is introduced to acquire member data, perform aggregation logic, and transfer the aggregated data. Finally, cluster-based routing is established with the use of Knapsack based cluster routing strategy. The performance investigation of the proposed system is estimated and the outcomes attained are compared with the existing techniques in terms of arrival rate, average delay, and the delay ratio of the packets. The investigation illustrates that the suggested approach is better than the traditional techniques.***

***Keywords*—Wireless sensor networks; data aggregation; PoW detection scheme; blockchain technology; cluster formation; key generation; security; delay ratio***

## I. Introduction

Generally, WSN comprises disseminated micro-devices named sensors that might embed and have innumerable detection capabilities or sensing capabilities. The risks that face security of WSN arise from inside and outside a network frequently. The suitable network nodes are es negotiated and enforced to act as malicious nodes. The security-related issues resolving has a thoughtful influence on the development and design trends of WSNs and consist of extensive consideration that attracts in the traditional works [1]. The WSN sensors are compact generally and thus utilize the constrained resource of battery. This sensor, in turn, aggregates data and thus transmits it to the targeted location called base station (BS). The data received at BS are analyzed to create the decision for various prescribed applications like IOT based products. This node operates or functions as a repeated one to transmit data to the sink and other nodes. Moreover, the power source of WSN should be adequately utilized as this could not be exchanged or recharged. This WSN basis is exaggerated by numerous constraints like energy efficiency, scalability, fault tolerance, and so on. The WSN sensor, in turn, exhausts energy mostly in two ways that are sensing environmental parameters and the transmission of data to the base station over sensor nodes. The insufficient source of power is observed as the important problem in wireless sensor networks, and henceforth the node failure and network failure rise [2]. Additionally, the usage of optimal energy in the framework of WSN is required for attaining more performance and a high lifetime. Therefore, sensors grouping as corresponding clusters has been utilized for reducing the drainage of network energy and thus to enhance the reliability of the network. Several methods have been carried out with respect to sensor network construction with the solutions presented for resolving issues related to layer and the protocols that connect some things like scalability, optimum use of energy resources in sensors, environment, energy consumption, error tolerance, change in network regulations, low cost and so on. These problems are being addressed by various researchers [4]. One such advantage of employing data aggregation is that the data was to be transmitted in an efficient way with negligible latency of data. Various data aggregation algorithms have been presented so far to enhance the sensor network lifetime. The inadequate power source are regarded as the key issue in wireless sensor network and hence the network failure and node failure arises. Further the optimal energy usage in WSN is needed for obtaining high lifetime and more performance. So grouping of sensors into the corresponding clusters has been employed for decreasing the network energy drainage and thereby to increase the network reliability. Every Cluster possess Cluster Head and an effective framework like our proposed system is required to reduce the consumption of energy. Security enhancement is also a challenging issue of WSN at the time of aggregation. Here we study and propose a secure cryptosystem based on blocking of data. The blockchains invention overwhelms the constraint issue of a centralized manner. Blockchain offers admirable functionalities similar to decentralized architecture, a transparent system, and security. Also, Blockchains are employed for efficient and secured data transmission [3, 4]. Though, blockchain frameworks for IoT strategies might cause lower latency, lower throughput, and delay-related issues. The present system on blockchain employs storage and high processing power. The huge amount of heterogeneous data in blockchain IoT, such as WSN outcomes in the consumption of huge energy at the time of data transmission from various sources [5-7]. Moreover, the major dispute in data aggregation is the data heterogeneity in the network. Therefore, there is a need to enhance the network security since WSN are prone to various attacks like injection attacks, repay attacks, and tampering attacks, and so on. Several works have been employed to address the existing issues over data privacy and security in blockchain-based IoT. The presented scheme aims at proposing an efficient framework for node registration and formation of blockchain using data aggregation and cluster-based routing. The blockchain formation is carried using a PoW detection algorithm along with data aggregation. Each cluster, in turn, possesses a cluster head for reducing energy consumption. The presented technique employs data aggregation using Elgammal based encryption which enables effective data aggregation model.

### A. Contribution

The main intention of the proposed work is:

- To generate a certificateless key generation such that the secrecy rate of the proposed system is improved.
- To employ blockchain technique security purpose using PoW detection algorithm and is integrated with data aggregation scheme.
- To form a cluster based on the cluster-based routing protocol.

### B. Organization

The residual portion of this manuscript is systematized as shown: Section II is the illustration of various existing techniques review. Section III is the depiction of a detailed explanation of the proposed mechanism. The analysis of the proposed system performance is shown in Section IV. Lastly, the conclusion and future enhancement are narrated in Section V.

## II. Related Work

In this section, various existing techniques employed are reviewed. In this [8], the author presented a scheme of blockchain-based multi-WSN authentication models. The IoT nodes were categorized as cluster head nodes, base stations, and ordinary nodes as per their variations inability that was formed as hierarchical networks. The blockchain network is thus constructed with two varied kinds of nodes that form a hybrid blockchain scheme that includes public and local chains. In this hybrid model, the mutual authentication identity of nodes at several scenarios of communication was realized, the operation of ordinary node identity authentication was accomplished by means of local blockchain, and the identity authentication of cluster head node was realized in the public blockchain. The security and performance analysis illustrates that the performance and security of the scheme offer comprehensive security with an enhanced rate of performance. This [9] suggested a protocol of extremely secured CAKE (codeword Authenticated Key Exchange) that depends on one-way verification along with OTP (one-time-password) verification. This protocol was then related to other traditional schemes of mutual verification that portray substantial energy and time consumption reduction. The presented protocol in turn supports privacy, mutual authentication, and integrity and thus could counter various attacks such as replay attack, offline guess occurrence, impersonation attack, DoS attack, and so on and thus preserves forward secrecy perfect and creating the etiquette an appropriate one for several WSN applications.

In [10] developed a scheme of the blockchain-dependent framework with decentralization integrated with the privacy preservation and authentication in WSN aided IoTs. The registration, certification, and revocation process was utilized intended for the base station (BS) and sensor nodes communication in the cloud framework. In this approach, the CHs transmit information gathered at the base station. Meanwhile, BS saves entire key constraints on the disseminated blockchain, and a huge amount of data was then transferred to the cloud for storage purposes. The certificates that were revoked of all malicious nodes were then eliminated by BS from the blockchain. The proposed system performance was examined in terms of authorization delay, communicational and computational overhead, certification delay, and detection accuracy—the comparative outcome and the security authentication aid the advantage of the projected scheme over traditional ones.

In [11] utilized technology of blockchain for building the incentive scheme of nodes as per the storage of data for WSN. In this approach, data storing nodes were satisfied with digital money. If the information kept by the node were huge, then recompense would be more. However, two blockchains were constructed. One was employed for storing data of each node, and the other was to control the data access. Also, the proposed scheme adopts the data possession that was provable for replacing the proof of work (PoW) in the original bitcoins for carrying out the storage and mining of new data blocks that reduces the computing power greatly on comparing the PoW scheme. The conserving hash function was also necessary for comparing the new blocks and stored blocks of data. Thus, the new data could be stored in a node that was closest to previous data, and only varied subblocks were stored. Therefore, the node's storage space in the network was reduced greatly.

In [12] discussed the survey of an in-depth blockchain-based approach for the detection of malicious nodes, an examination of exhaustive blockchain technique integration with the WSN (BWSN), and insight for this novel approach. The contribution of blockchain for WSN was also explained in this survey, which includes aggregation, along with auditing, information analysis storage, auditing, event logs, and the offline query process. Thus, the presented schemes examine the centralized models of WSN for the security problems together with the blockchain discussion for the management of security like preserving information integrity, ensuring node longevity, guaranteeing privacy, and so on.

In [13] suggested a blockchain-dependent scheme of data provenance (BCP) which was compression-free, at which provenance was kept on nodes together distributivity with the packet path, and the BS could retrieve on-demand provenance through the inquiry method. The edge computing-dependent network monitoring comprised of H-nodes (high-performance nodes) was organized near or above WSN that retains the WSN data provenance in the blockchain-dependent dataset. The authenticity, provenance, and security were then protected. Both experimental outcome and simulation analysis represents that the proposed BCP scheme was much effective in terms of energy and secured on comparing the distributed provenance of data.

In [14] suggested an energy-effective decentralized mechanism of trust with the use of the blockchain-dependent solution for multi-mobile code on behalf of sensing the interior attacks in the SN (sensor node) enabled IoT. The outcome validates improved concert of presented technique over traditional ones with 43.94% and 2.67% a reduced amount of overhead message in the Greyhole and blackhole attack circumstances correspondingly. Likewise, the detection time of malicious nodes was decreased by 20.35% and 11.35% at both Greyhole and blackhole attacks. These two factors show a dynamic part in enhancing the lifetime of the network.

In [15] presented a massive blockchain-enabled IoT data collection (MIDC) intellectual context for supporting the security, efficiency, and trust of the huge collection of data for the huge-scale varied WSNs. Specifically, a series of novel framework technology was presented. Initially, a huge scale heterogeneous WSN concerted individuality so as to guarantee a reliable source of data. Next, the scheme of Ranked massive aggregation of data so as to collect massive IoT data in a secured and efficient manner. Thirdly, the blockchain-dependent massive management of IoT data systems was depicted for constructing trust over various parties. The simulation analysis and the experimental prototype prove the framework's effectiveness.

In [16] presented a novel scheme of data aggregation depending on the clustering of node and extreme machine learning scheme (EML) for reducing the erroneous and redundant data. The analysis, along with the real-time databases, represents that the presented scheme outdoes the prevailing system consistently in relation to data clustering accuracy and efficiency of energy in WSN.

In [17] suggested a privacy preservation and energy efficiency algorithm CBDA (chain-dependent data aggregation). In this scheme, sensor nodes were systematized as a network topology of the tree. The leaf nodes of the tree were reconnected successively with one another to form several chain network topologies. The suggested approach CBDA attains less consumption of energy and higher accuracy of aggregation at the time of data aggregation. The simulation outcomes attained were compared with traditional ones, and attained outcome reveals that the presented scheme outperforms other traditional mechanisms.

In [18] presented a scheme of new ring-dependent in-network data aggregation to solve existing issues. The network was then portioned as rings, and the aggregated data was executed from outside to inside as a ring form. The analysis shows the effectiveness of the presented scheme.

[19] projected an energy-effective mechanism of data aggregation (EEDAM) that was protected by a technique of blockchain. The suggested technique employs a mechanism of aggregation of data at the level of the cluster for saving energy. The edge computation was employed for offering trusted on-demand services to the IoT deprived of the lowest delay. Since the blockchain was united inside the cloud server, the edge was authenticated by blockchain for offering secured services to IoT. At last, the performance simulation was estimated, and the proposed system performance was compared with traditional algorithms. The outcomes show that the projected operational strategy was reduced effectively and offers security to IoT, which extends WSN.

## III. Proposed Work

A detailed narration on the proposed system methodology is depicted in this part. The overall flow of the proposed mechanism is shown Fig. 1.

### A. *Deployment of Sensor and Base Station*

*1) Network model:* Blockchain technology was utilized for designing DWSNs based on WSN for achieving trustworthiness. This technique comprises of huge stationary numbers or sensor nodes moving and the BS, which assigns partial certificateless public/private pair of keys to the nodes. There were two kinds of SN's: (1) the nodes having huge storing space, communication capabilities, and computing termed as $H_{ss}$ -sensors, which comprises of consent network. (2) nodes having lower storage space, communication capability, and computing termed as normal node called $L_{ss}$-sensors.

Let us assume that there were N number of nodes in the WSN with $N_H$ $H_{ss}$ -sensors and $N_L L_{ss}$--sensors, here, $N_T = N_H + N_L$ and $N_H$" $N_L$. From WSN perspectives, the network is divided into a number of clusters as per the region at which the CHs are $H_{ss}$-sensors and the cluster member are the L-sensors. From the blockchain viewpoint, H-sensors act like a node of consensus that forms a blockchain network termed stake blockchain. Owing to the analysis like storage, communication, and computation, $L_{ss}$ -sensors remain just normal or ordinary nodes that will not participate in any consensus part. This is worth noticing that the BS, a unified device, might not link consensus, consequently $H_{ss}$-sensors might form a system that is decentralized, and the management of key does not depend on the base station BS. This BS role is to assign a unique individuality simply to each node. The node Id $L_{ss}^i$ is employed for indicating the $H_{ss}$--sensor $H_{no}^i$. The key generation center (KPC) that is hosted by BS, in turn, generates the parameters of the community system and consequently issues the certificateless private/public pairs of keys for each WSN s node. In the model of the network, a pairwise key recognized by certificateless public/private key is then spitted among the two nearby nodes, whereas the cluster key is being distributed among the nodes in the cluster. Fig. 2(a) and 2(b) indicates the Sensor establishment of the network model.

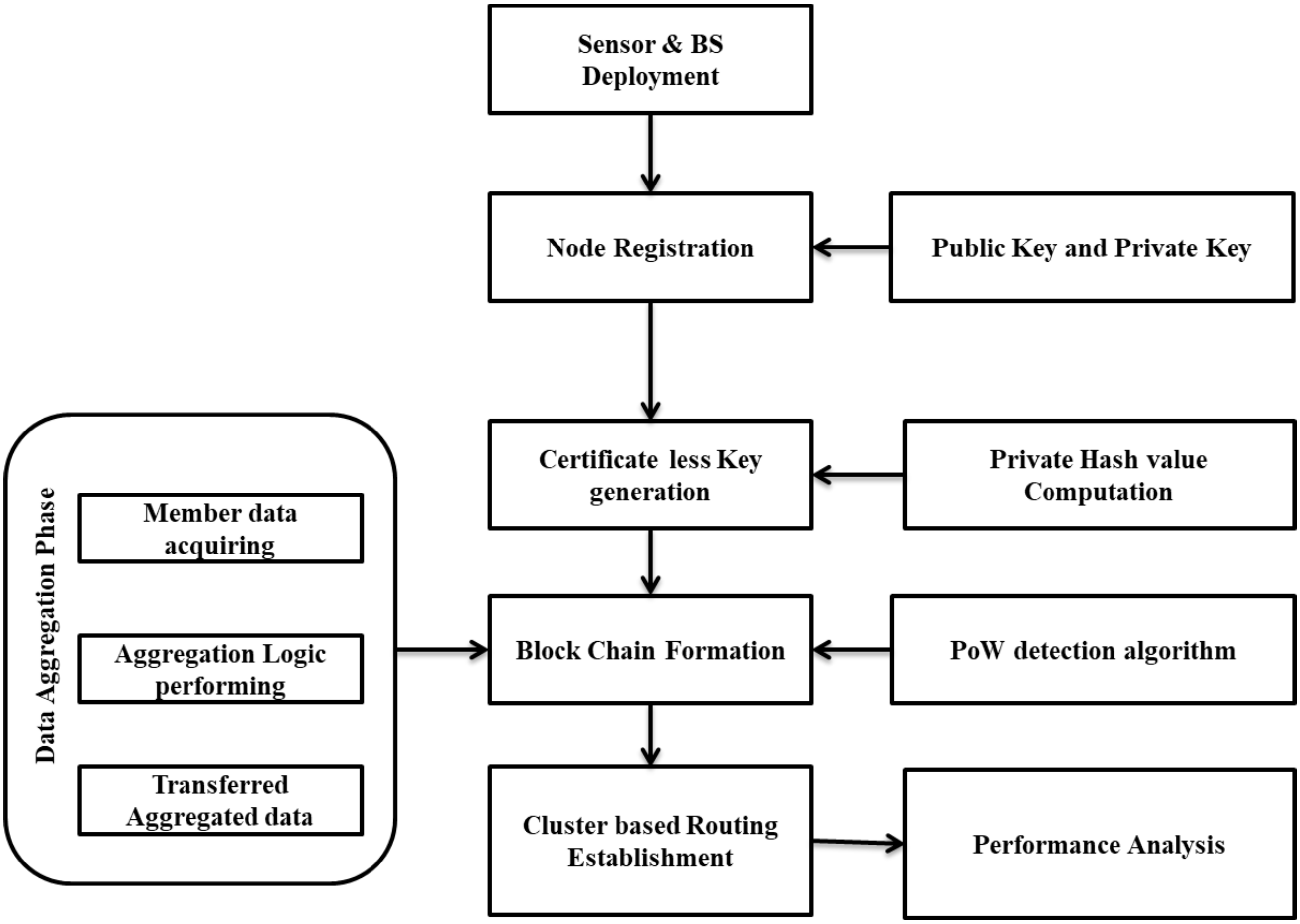
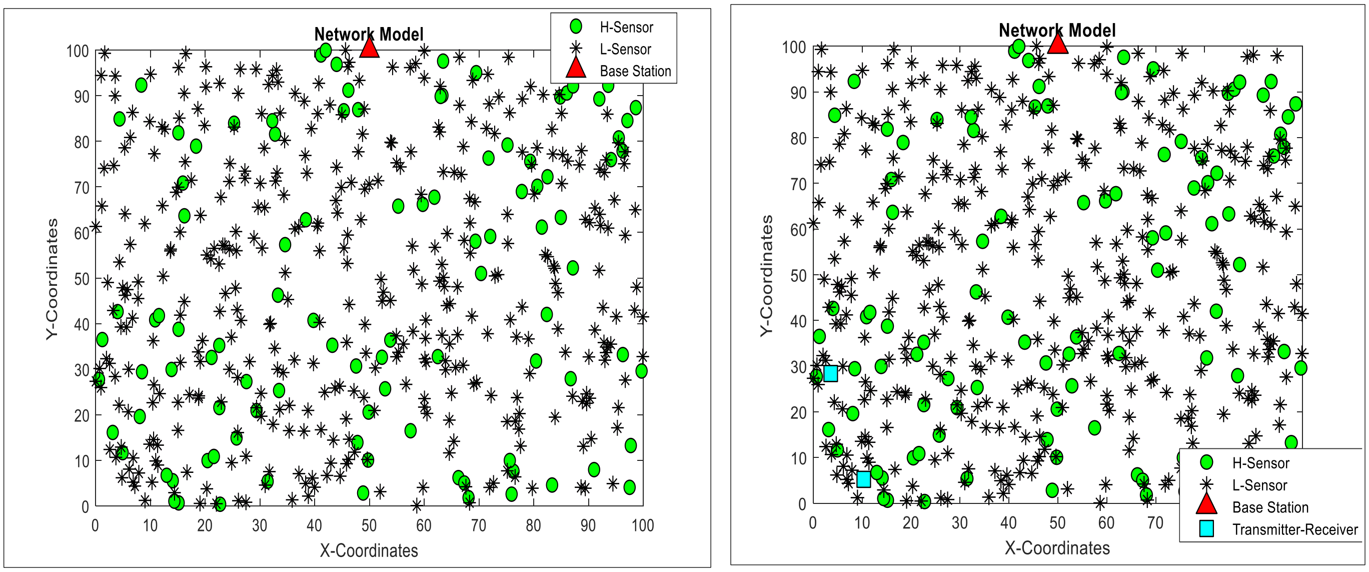

Sensor & BS Deployment
Node Registration
Public Key and Private Key
Certificate less Key generation
Private Hash value Computation
Block Chain Formation
PoW detection algorithm
Cluster based Routing Establishment
Performance Analysis
Data Aggregation Phase
Member data acquiring
Aggregation Logic performing
Transferred Aggregated data

Fig. 1. Overall Workflow of the Proposed System.



(a)

(b)

Fig. 2. (a) Network Model Deployment, (b) Deployment of the Network Model.

*2) An Attack model:* It was supposed that the opponent could not perform impersonation and cloning attacks however could perform several other attacks like pseudo-BS attack, interruption attack, etc., at the system setup. It is too assumed that BS might be impersonated or invaded. Moreover, once the nodes are captured, the adversary could augment a malicious node to the network for playing a legitimate node termed as an impersonation attack. Likewise, this technique presents the following requirements on security in the management of secured keys:

*a) Backward and Forward secrecy:* the node that has been logged out or else logged out by force might not lead to taking part in the communication of the cluster. However, this could not attain session information and could not be able to send a valid packet that is encrypted. Backward security refers to the new member that could not decrypt the information of the session before it joins.

*b) Resistance in contradiction of impersonation and cloning:* the technique should have the function of node substantiation or detect the malicious node for preventing in contradiction of node impersonation and cloning occurrences.

*c) Resistance in contradiction of pseudo BS attack:* once the adversary generates the pseudo-BS, this could not affect the registration of the node.

The presented scheme too prevents the BS and the compromised nodes from collaborating for reaching the stealing data and controlling the network's goal.

### *B. Registration of Node*

After the deployment of the network, the BS, in turn, generates the system parameters and thus aids H-sensor nodes in registering the nodes. The legitimate nodes list is being maintained by blockchain technology.

*1) System parameters generation:* At BS, KPC selects the $n$-bit prime $q_n$ thus recognizes the tuple $\{H_q\ , \mathrm{E}/H_q\ , \mathrm{G_q}, P\}$, here $n \in Z+$. After that, the KPC, in turn, computes the public key of the system $K_{pub} = K_{pr}P$, here $K_{pr}$ is a master private key and $K_{pr}\ \in Z_q$ . Simultaneously, there consists of a cryptographic hash function as $\{H_a, H_b, H_c, H_d\}$. Consider that t is the symmetric key length and the base station, in turn, publishes $\delta = \{H_q\ , \mathrm{E}/H_q\ , \mathrm{G_q}, P, H_a, H_b, H_c, H_d\}$ too retains secret of $K_{pr}$.

*2) Generation of session less private/public key:* The base station employs $L_{ss}^i$ for indicating the exclusive uniqueness of each $L_{ss}$-sensor $L_{no}^i$ , then employs $H_{ss}^i$ for denoting each H-sensor's $H_{no}^i$ Unique identity. After that, the certificateless private/public key generation was described for $H_{ss}^i$ which are the similar functions applied for $L_{ss}^i$. Next, the entire node $H_{no}^i$ chooses a $H_{ss}^x \in Z_q$ secret value by computing $PH_{ss}^i = K_{pr}H_{ss}^iP$ . The KPC is then utilized for generating public/private keys of the $H_{no}^i$ over the $H_{ss}^i$ input parameters and $PH_{ss}^i$. Besides, a KPC in turn selects $H_{ss}^r \in Z_q$, which is the BS's private key and too termed as skBS by returning the partial private/public key pair $(H_{ss}^R, H_{ss}^d)$ on computation as shown:

$$H_{ss}^R = H_{ss}^r P \tag{1}$$

$$H_{ss}^d = H_{ss}^r + K_{pr} \tag{2}$$

$$H_{ss}^d = H_{ss}^r + K_{pr} hash_0(H_{ss}^i, H_{ss}^R, PH_{ss}^i) mod\ q \tag{3}$$

Here, $H_{ss}^R$ termed as a BS's public key and called as $pk_{BS}$.

Once $H_{ss}^i$ takes ($H_{ss}^R$ , $H_{ss}^d$ ), this will authenticate whether the subsequent calculation grasps.

$$H_{ss}^d P = H_{ss}^R + hash_0(H_{ss}^i, H_{ss}^R, PH_{ss}^i) K_{pub} \tag{4}$$

In case the above equations are true, then $H_{ss}^i$ sets the full public key $pkH_{ss}^i$ = ($PH_{ss}^i$ , $H_{ss}^R$ ), full private key $sk_Y$ = ($H_{ss}^d$, $H_{ss}^x$), and thereby records RHj as the BS's public key termed $pk_{BS}$.

*3) Generation of Genesis Block:* Once the generation of keys for entire nodes is accomplished, the BS distributes information to the entire $H_{ss}^i$ -sensor nodes through the message $msg$ that consist of a list of registration comprised of identifiers and the public keys of those nodes over $msg =< setup\ , pk_{BS}\ , sk_{BS}(hash_0(\varphi), \varphi)$.

The H-sensor node utilizes $pk_{BS}$ verified beforehand for verifying $pk_{BS}$ And signature. In case the successful verification is being inscribed to the innovative block through the witness node (one $H_{ss}^i$-sensor node) underneath the PoW scheme. Formerly, the witness node broadcasts the block instantly, and once over 50% of the consent node authenticates over the block, it specifies that this was noted on the mechanism of blockchain. The block produced initially is too termed as the block of genesis.

In case the authentication fails, the H-sensor nodes broadcast the warning messages $Warn_{msg}$ regarding the hacked base station or else the pseudo-BS attack. Those warning messages are then collected in the message pool by the witness node. As soon as over 50% of the nodes broadcast a piece of comparable warning information, the message is written to a new block by the witness node by propagating them to the other nodes for the purpose of verification. Till the nodes more than 50% verify and pass new 0block, this is chained as their individual blockchain nearby. This means that BS is being negotiated and therefore requires some human interventions for checking and recovering the BS. This is worth notable that in case the genesis block is not being linked to the local blockchain, H-sensor is simply required to link a new block that stores the warning data to the local blockchain. Else, owing to the blockchain's tamper-proofing property, $H_{ss}^i$-sensor relates the new block afterward the block of genesis; this means the blockchain that comprises H-sensors is termed trust mechanism, and the entire blockchain information could not be modified.

### *C. Secure Key Management Scheme*

The construction of secured key management is described in a detailed manner depending on the blockchain that comprises various phases. This is the system design's epitome that includes node registration. Table I represents the list of notations, grouping, and movement. Also, the solutions for presenting the deterministic detection of compromised nodes are also offered. The common model is that a blockchain to be the trusted database that offers protected decision making. This is a reliable database, and reliably it stores the variations in the sensor state. The major notations for this scheme are illustrated:

TABLE I. NOTATIONS LIST

| Notation | Definition |
|---|---|
| BS | Base Station |
| $q_n$ | $n$ bit prime number |
| $K_{pub}$ | Public key of KGC<br>$K_{pub} = K_{pr}P$ |
| $K_{pr}$ | Master private key |
| $P$ | An additive cyclic group's point generator $G_P$ |
| $Z_q$ | Group of integers that are multiplicative |
| E | An elliptic curve |
| $H_q$ | $a, b, x, y$ are the elliptic curve parameters |
| $pk_X$ | Any node's full public key $n_X$,<br>$pk_X = (P_X, R_X)$ |
| $sk_Y$ | Any node's full private key $n_X$,<br>$sk_X = (d_X, pr_X)$ |
| $M_{XY}$ | Pairwise master key between $n_X$ and $n_Y$ |
| $m_{XY}$ | Pairwise encryption key between $n_X$ and $n_Y$ |
| $CK_i$ | Cluster key which is distributed between nodes of the $i^{th}$cluster |
| $H_{mac}(mes, key)$ | Message authentication code using hash computation with message $mes$ and key $key$ |
| $E_{key}^{sym}(mes)$ | Algorithm of symmetric key encryption for encrypting the messages $mes$ with $key$ key |

### D. Formation of Blockchain using PoW Detection Algorithm and Data Aggregation

Blockchain mechanism is a distributed, trusted record that is very appropriate for the P2P systems and thus functional for the protection of privacy and social networks. Moreover, due to the establishment of high-cost blockchain among the resource constraint $H_{ss}$ --sensor nodes, a mechanism of consensus, is much critical for resolving the issue of excessive consumption of resources can resolve the issue of unnecessary consumption of a resource was very critical.

The system of consensus acts as a blockchain technology core; hence several great kinds of research on the mechanism of consensus have emerged. Though the consumption of resources is small in Paxos and Raft algorithm, the nodes can't be able to reach a consensus if there is a malicious attack like random process errors. Likewise, the PBFT scheme does not have good scalability. Therefore, an algorithm of proof of work (PoW) is employed in WSNs. This avoids the consumption of a huge amount of computational power and has the process of a faster-producing block in the blockchain. On the other hand, lower consumption of energy is highly suitable for WSN. Because of the quick speed of block production, H-sensor nodes could reach consensus quickly and thus makes a decision on the issue. Also, this proposed algorithm makes the blockchain system more scalable for connecting sensor nodes. By means of this approach, it is contentious in relation to decentralization degree and having the features of trust from the cryptographic and mathematical systems that are highly helpful for constructing the dispersed management of key with trustworthiness. By considering the traditional WSN scenarios, the proposed one makes a compromise option for trust-based requirements.

The PoW detection scheme illustrates a system that needs a non-significant but feasible quantity of effort for determining the malicious nodes or malicious use of computing power like sending spam emails or injecting denial of service (DoD) attacks. This concept was adopted to secure digital money and was introduced by Hal Finney in 2004 from the idea of "reusable proof of work" using the SHA-256 hashing scheme. It is considered that the most trustworthy approach for achieving consensus in blockchain technology, and it helps in attaining decentralization, thereby ensuring transaction validation. Thus, the use of this detection algorithm helps in identifying malicious activities both in the base station and nodes.

### E. Aggregation of Data using Elgammal Approach

This technique employs the Elgammal scheme for data aggregation, which employs encryption and decryption phases. For the cluster head selection, encryption has been processed. The cluster member developed was employed for the data acquisition and cluster weight determination. On performing the logic of aggregation, the members are subjected to the phase of data aggregation. The aggregated data transferred is being subjected to the analysis of performance for the estimation of the proposed scheme. Also, Knapsack based energy efficient protocol has been employed in the proposed method for the formation of the cluster. Thus, from this, the shortest path prediction was estimated by means of establishing route establishment with the energy-optimized path.

The process of Elgammal encryption is the system of a public-key cryptographic scheme that utilizes asymmetric key encryption for the purpose of communication among two parties and thus for encrypting the messages [20]. The data aggregation-based Elgammal encryption system is defined below. In this, the algorithmic steps for encryption, data aggregation, and decryption of the aggregated data has been described as shown:

The input of the data aggregation algorithm is sensor data $S_N^D$ and the output will be aggregated data $D_{aggr}$, encrypted data $S_i^C$ and decrypted data $S_i^{Decry}$ . Initially, the key generation process takes place at which the large prime numbers p will be chosen, and the primitive root is estimated as follows:

$$p_r = mod(g, p) \tag{5}$$

Then, the m, n are chosen randomly among the limit of $(1 \leq m \leq p - 2)$ and $(1 \leq n \leq p - 2)$ correspondingly. The secret integer is computed as follows:

$$c = mod(g^m, p) \tag{6}$$

The combined public keys are represented by $\{p, g, c\}$, followed by private keys as {m, n}. The data sensed is then encrypted with the public keys, and the following process is carried out in the encryption process performance as shown:

$$s = g^n\ (mod\ p) \tag{7}$$

$$S_i^C = S_i^D . c^n (mod\ p) \tag{8}$$

$//S_i^C$ is the cryptography text.

After that, the process of data aggregation is performed for the entire sensed information by,

$$D_{aggr} = S_i^{C_1} + S_i^{C_2} + \cdots + S_i^{C_t} \tag{9}$$

Finally, the decryption is carried out for the aggregated data as:

$$s^m = c^n (mod\ p) \tag{10}$$

$$S_i^{Decry} = D_{aggr} . \overline{c^n} (mod\ p) \tag{11}$$

### F. Cluster Formation using Knapsack based Protocol

The proposed system employs an energy-efficient protocol based on Knapsack to enhance overall system performance and cluster formation. This approach provides a fast variation for memory overhead, low network utilization, low processing, and dynamic link conditions, which thus uncast the destinations routing in the Ad hoc networks. Fig. 3 indicates the cluster formation of our proposed system.

The Knapsack with the energy-based approach is employed for the process of cluster formation. In this, the input is the Sensor nodes $S_N$ , Base station $BS$, sensors data $S_N^D$ and the output will be selected Cluster head $CH_i$, selected cluster member $CM_i$. At first, the entire number of nodes N are being deployed in the dimensions of network $M * M$. The entire elements in the established network are in the stationary mode only, and the nodes deployed energy are not recharged back that are in the heterogeneous environment. The entire sensor nodes are employed as a power control for the varying transmit power amount. The entire nodes are termed as BS locations that are located at the sensor field. Each sensor node has the unique identity $S_{id}$ . The energy usage for the transmission of the sensed packet $S_N^D$ at distance $d_i$ is represented as

$$E_{Tx}(m, d_i) = \begin{cases} mE_{elec} + m\delta_f d_i^2 d_i \le \rho \\ mE_{elec} + m\delta_m d_i^4 d_i > \rho \end{cases} \tag{12}$$

Here

$\delta_f$ – the free space

$\delta_m$ – multipath fading channel model

$E_{elec}$ – electronic energy that depends on some factors includes the modulation and digital coding

$\rho$ – threshold distance

The energy consumption taken for receiving such packet is shown as:

$$E_{Ry}(m) = m * E_{elec} \tag{13}$$

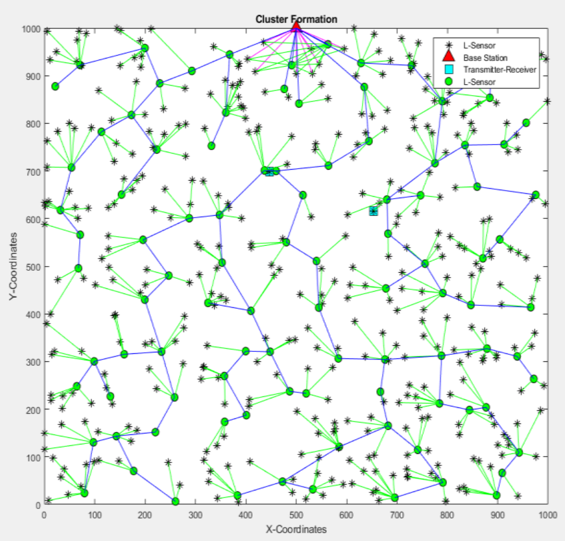


Fig. 3. Cluster Formation.

Based on the probability, the random nodes are selected by,

$$S_R = \frac{p_{sr}}{1 - p_{sr}(r\ mod(\frac{1}{p_{sr}})} \tag{14}$$

Here,

$p_{sr}$ is the percentage of neighbor nodes number

Then, the neighbor node selection based on the Euclidean distance is illustrated as shown:

$$d_i = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2} \tag{15}$$

$$dr = d_i - d_j \tag{16}$$

$d_i$ – distance between random nodes and member nodes.

$d_j$ – distance between random nodes and base station $BS$.

The number of nodes for each sensor is found, and the set is formed with respect to distance as.

$for\ i = 1: N$

$for\ j = 1: N$

$$d_i = \sqrt{\left(x_i - x_j\right)^2 + \left(y_i - y_j\right)^2} \tag{17}$$

$if\ d_i < \ \varphi$ // $\varphi - sensing\ range$

$CM\{i\} = \{j\}$ // $CM$ –cluster member group

Finally, the CH selection is generated based on the multi-objective fitness function attained from the knapsack problem having two parameters like residual energy and the sensing range $\varphi$

$$fit_{val} = c_1 \left[\frac{E_{res}^m - E_{res}^i}{E_{res}^m}\right] + c_2 \left[\frac{\varphi^m - \varphi^i}{\varphi^m}\right] \tag{18}$$

Here, $E_{res}^m$ – maximum residual energy.

$E_{res}^i$ – residual energy for sensors.

$\varphi^m$ – maximum sensing range.

$\varphi^i$ sensing range of each sensor.

$c_1$&$c_2$are the constant value with a random number.

The list of those members and the information on formed CH will be stored in the routing table, and the routing table is utilized for selecting the second CH once certain rounds are completed. The presented approach employs a simple model for communication energy consumption. Based on the receiver and transmitter distance, the multipath fading channel or the free space method was employed.

The required energy to transmit packets over that distance was established in the above-mentioned steps. The energy consumption of receiving the packets is found in the next step. Afterward, the random deployment, random number of nodes were selected on the probability basis for the chosen node $S_{R.}$ Depending on the provided equation, the random nodes are selected. On following this, the neighbor nodes are determined based on the Euclidean distance, which thus offers distance among the member and random nodes.

## IV. Performance Analysis

The performance is estimated and the outcomes attained are related to the traditional mechanisms to verify the efficiency of the projected strategy.

Fig. 4 is the comparative analysis of the packet's arrival rate. The average delay of the packets in a slot-wise manner is estimated, and the outcomes of the proposed scheme. We compared with the existing techniques like TB-BP, QL-BP, RLBC, and Blockchain MDP [21]. The analysis shows that the proposed system delivers a good outcome by giving a reduced range of delay rates.

Fig. 5 illustrates a comparative estimation of the arrival rate of the packets vs. the average delay of packets (slots) with 50% malicious node presence. The proposed system delay is estimated and is correlated with the existing techniques like TB-BP, QL-BP, RLBC, and Blockchain MDP. The comparative analysis represents that the proposed mechanism offers a lower delay rate with a 50% malicious node. Thus, the system is effective than others.

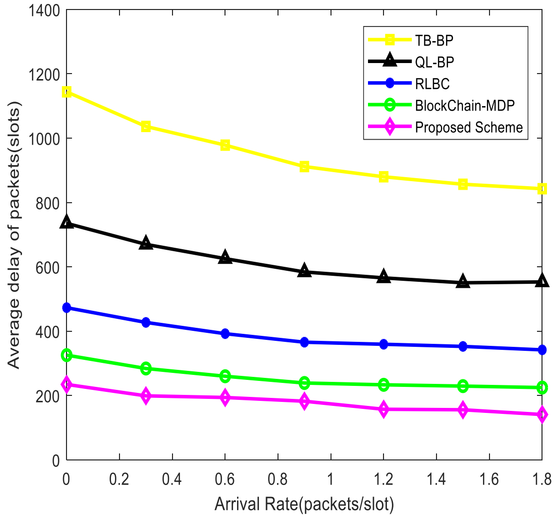


Fig. 4. Comparative Estimation of the Arrival Rate of the Packets.

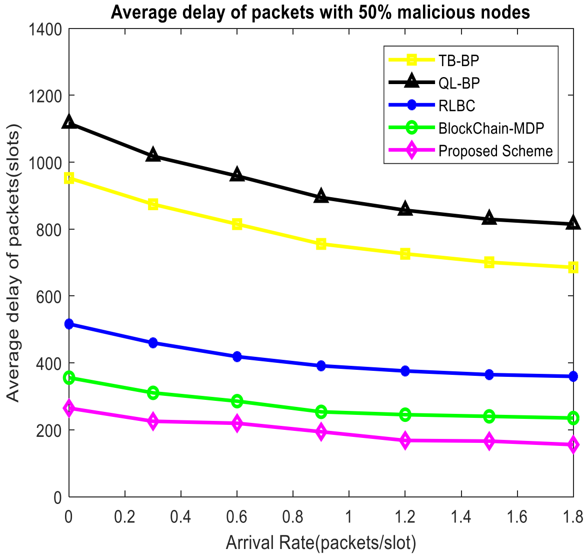


Fig. 5. Comparative Estimation of the Arrival Rate of the Packets with 50% Malicious Nodes.

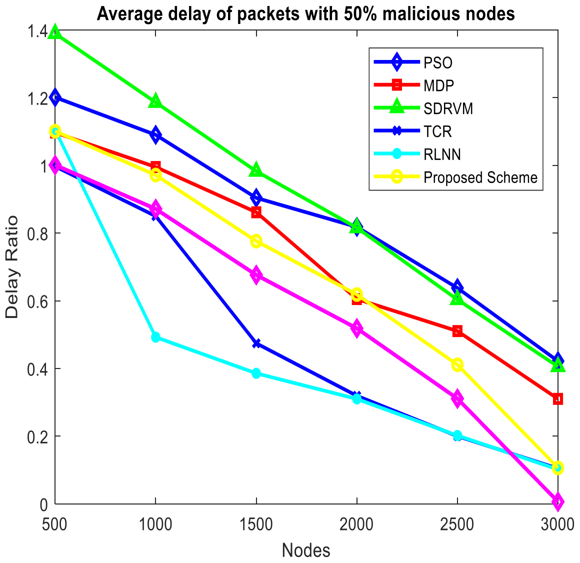


Fig. 6. Comparative Estimation of Delay Ratio of the Packets.

The overall delay ratio of the proposed detection system is estimated. The proposed scheme will indicate the outcomes attained and compared with the traditional mechanisms like PSO, MDP, SDRVM, TCR, and RLNN [22] in Fig. 6. The analysis shows that the existing system has a higher delay ratio, whereas the proposed scheme offers a better delay ratio than other existing methods. Therefore, the proposed approach is said to be an effective one in comparing the other traditional techniques.

## V. Conclusion

A blockchain-based data aggregation scheme was presented along with the certificateless key generation. The significant contribution of the proposed work was to generate the certificateless key, which provides the expiring time of key, and to employ blockchain technique with the use of PoW detection scheme integrated with data aggregation procedure.

Then the formation of the cluster was carried out by the routing protocol. Thus, the use of blockchain and key generation aids in secured storage and transmission of packets. The performance analysis was carried out in terms of the packet's delay ratio, average delay, and arrival rate. The outcomes attained were compared with existing techniques, and the effectiveness of the proposed scheme over existing methods was projected. In future we aim to enhance the proposed approach with high level cryptosystems with cure the energy efficient.

## REFERENCES

[1] X. Wang, S. Garg, H. Lin, G. Kaddoum, J. Hu, and M. S. J. I. I. o. T. J. Hossain, "A secure data aggregation strategy in edge computing and blockchain empowered Internet of things," 2020.

[2] I. Mosavvar and A. Ghaffari, "Data aggregation in wireless sensor networks using firefly algorithm," Wireless Personal Communications, vol. 104, no. 1, pp. 307-324, 2019.

[3] L. Zhu, K. Gai, and M. Li, "Blockchain and Internet of Things," in Blockchain Technology in Internet of Things: Springer, 2019, pp. 9-28.

[4] M. Kaur and A. J. A. H. N. Munjal, "Data aggregation algorithms for wireless sensor network: a review," vol. 100, p. 102083, 2020.

[5] S. Ghai, V. Kumar, R. Kumar, and R. Vaid, "Optimized Multi-level Data Aggregation Scheme (OMDA) for Wireless Sensor Networks," in Mobile Radio Communications and 5G Networks: Springer, 2021, pp. 443-457.

[6] B. VANASWI and S. Suresh, "Secure Data Aggregation Technique for Wireless Sensor Networks in the Presence of Various Attacks."

[7] R. Aishwarya, S. S. J. A. i. N. Babu, and A. Sciences, "Privacy-preserving access control on data aggregation for wireless sensor networks," vol. 11, no. 6 SI, pp. 224-232, 2017.

[8] Z. Cui et al., "A hybrid blockchain-based identity authentication scheme for multi-WSN," vol. 13, no. 2, pp. 241-251, 2020.

[9] P. S. Mehra, M. N. Doja, and B. J. I. J. o. C. S. Alam, "Codeword Authenticated Key Exchange (CAKE) lightweight, a secure routing protocol for WSN," vol. 32, no. 3, p. e3879, 2019.

[10] R. Goyat et al., "Blockchain-based data storage with privacy and authentication in Internet-of-things," 2020.

[11] Y. Ren, Y. Liu, S. Ji, A. K. Sangaiah, and J. J. M. I. S. Wang, "Incentive mechanism of data storage based on blockchain for wireless sensor networks," vol. 2018, 2018.

[12] R. L. Kumar, F. Khan, A. L. Imoize, J. O. Ogbebor, S. Kadry, and S. J. I. A. Rho, "Blockchain-Based Wireless Sensor Networks for Malicious Node Detection: A Survey," 2021.

[13] Y. Zeng, X. Zhang, R. Akhtar, and C. Wang, "A blockchain-based scheme for secure data provenance in wireless sensor networks," in 2018 14th International Conference on Mobile Ad-Hoc and Sensor Networks (MSN), 2018, pp. 13-18: IEEE.

[14] N. Tariq, M. Asim, F. A. Khan, T. Baker, U. Khalid, and A. J. S. Derhab, "A blockchain-based multi-mobile code-driven trust mechanism for detecting internal attacks in the internet of things," vol. 21, no. 1, p. 23, 2021.

[15] L. Zhang, F. Li, P. Wang, R. Su, and Z. J. I. I. o. T. J. Chi, "A Blockchain-Assisted Massive IoT Data Collection Intelligent Framework," 2021.

[16] I. Ullah and H. Y. J. J. o. S. Youn, "Efficient data aggregation with node clustering and extreme learning machine for WSN," vol. 76, no. 12, 2020.

[17] S. Hu, L. Liu, L. Fang, F. Zhou, and R. J. I. A. Ye, "A novel energy-efficient and privacy-preserving data aggregation for WSNs," vol. 8, pp. 802-813, 2019.

[18] J. Zhang, P. Hu, F. Xie, J. Long, and A. J. I. A. He, "An energy-efficient and reliable in-network data aggregation scheme for WSN," vol. 6, pp. 71857-71870, 2018.

[19] A. Ahmed and S. Abdullah, "Cloud-based Energy Efficient and Secure Service Provisioning System for IoT using Blockchain," 2021.

[20] M. K. Al-name and S. M. Ali, "Improved El Gamal public-key cryptosystem using 3D chaotic maps," Bulletin of Electrical Engineering and Informatics, vol. 10, no. 1, pp. 404-411, 2021.

[21] J. Yang, S. He, Y. Xu, L. Chen, and J. J. S. Ren, "A trusted routing scheme using blockchain and reinforcement learning for wireless sensor networks," vol. 19, no. 4, p. 970, 2019.

[22] M. Revanesh and V. J. T. o. E. T. T. Sridhar, "A trusted distributed routing scheme for wireless sensor networks using blockchain and meta - heuristics - based deep learning technique," p. e4259, 2021.