Journal of Harbin Engineering University
ISSN: 1006-7043
Vol 45 No. 5
May 2024

Block Chain Based Access Control and Secure Cluster Based Data Aggregation for WBAN Networks

G. Sridevi Devasena,
Assistant Professor ,
Indian Maritime University,
Chennai Campus,
India

Abstract—The emerging technologies on wireless sensors, body area networks, data aggregation techniques, the cyber physical system and its privacy is considered as vital. The rapid growth in wireless communication has enabled a new generation of wireless sensor network. Thus, vital parameters of patients can be monitored through wearable and implantable biosensors integrated with wireless body area network, an intelligent and interdisciplinary area of medical domain. Cloud service provider operates for long-term storage and online/ offline processing where data in server are connected with WBAN through sensors. As patient's record consists of more sensitive information, privacy can be maintained by confidentiality, data aggregation and granular access control methods. Among all, WBAN network works effectively by focusing mainly on data aggregation. One of the fatal attacks in data aggregation troubles the network is considered to be more vulnerable. In this paper, WBAN network at the time of data access control and secured data aggregation should be proposed with block chain (PDB) and also faced difficulty. These methods have rights to access privilege to the security service of the network. Proper recognition of devices and permission to use network and service are ensured in addition to reflection of critical data packets from different nodes through sensor network in PDB scheme. Public key encryption probably provides higher level of security to data aggregation. Simultaneously, Detection of attacks creates secured aggregation technique which reduces cost of authentication by cryptographic assumptions. Thus, from entire proposal, analysis can be demonstrated for the resistance of security threats through PDB, user privacy, minimizing communication and computation overhead compared to existing methods.

Keywords—Blockchain, Wireless communication*, data aggregation, cryptography, Wireless body area network*.

I. Introduction

Recent progress in Cyber Physical Systems (CPS) has led to significant improvements in wireless sensing and transmission technology, resulting in enhanced environmental monitoring systems, real-time industrial monitoring systems, and improved healthcare monitoring systems. Among the innovative developments is the Wireless Body Area Network (WBAN), a small wearable device that facilitates the connection and transmission of essential physiological parameters of patients, including temperature, blood pressure, ECG, and more. This collect various information of the patient in a remotely basis and further process the local Processing Unit with privacy preserving secure protocol. Wireless body area network consists of n number of small sensors implanted or connected to the patient. The cost of storage and computation remains a crucial consideration in maintaining privacy and ensuring efficient healthcare monitoring systems. This is particularly vital in safeguarding sensitive data, especially when stored in cloud environments where multiple users may have access to it. To address this issue and minimize energy consumption across the physical network, effective solutions are sought to prevent data breaches and optimize overall system performance. Data aggregation process consists of sensor nodes and cluster head connected with various leaf nodes. Any kind of malicious attacks enter into the network can be identified by the nose.

One of the quickly developing innovation which isn't in that frame of mind of past techniques however makes headway in current conditions. It is, as a matter of fact, new figuring strategies

named as AI, far superior to design acknowledgment framework. Frequently, we utilize worked orders for the old hypothesis of PCs to learn specific assignment. Yet, as of late, most recognizable exploration worked out on man-made brainpower with additional emphasis to gain information from the PC. The outcomes can be anticipated as repeatability and unwavering quality will create a viable stage for assessment of AI and profound learning calculations.

AI calculations have a portion of the highlights like dealing with capacity, handling and consequently adjusting the numerical assessments for the constant datasets are enormous information. Consequently, it is considered as the piece of man-made reasoning with gigantic applications. By centering numerous ongoing advancements progressively applications, AI calculations works naturally and consequently diminish the slip-ups done by human calculations.

A genuine model for AI models were introduced, for example, ID of feline are canine picture. To distinguish the distinctions, feline and canine pictures are taken care of as contribution to the model. Then the right result is gotten by removing various highlights of pictures like shape, level, nose, eyes, and so on, trailed by executing arrangement calculation.

- The primary usage of data aggregation process in the wireless body area network provides high level of security at the edges.
- The approach presented, considered blockchain enabled wireless body area network with respect to data aggregation process.
- The proposed approach consider various technological constraints discuss in the previous applications such as computational cost reducing the complexity of the system approach improve and focuses on improving the energy and reducing the computation cost and complexity of the system.
- The proposed approach is implemented using Python simulator, where the WBAN network is virtually created. The rest of the paper the paper comprises a comprehensive literature study in Section II, where the chosen system tools and problem identifications are thoroughly examined in Section III. Section IV delves into the system architecture and provides a detailed explanation of the system design steps. The paper concludes with a discussion on future enhancements.

II. Background Study

I. Yakymenko et al ., (2020) the author presented a system in which EL-Gamal crypto algorithm is utilized. The system discusses various exponential modular multiplication values and complex operations are to be simplified using the EL-Gamal Crypto algorithm. Network models have complex cryptography enabled encryption processes to communicate the data securely.

W. Lu et al., (2021) the author presented a system lightweight privacy preserving data aggregation employed in smart grid applications. Data aggregation act as an important key factor in wireless communication technology. Various problems in the edge layers are resolved through edge block chain enabled data aggregation (EBDA) technique. By performing the system through the EBDA method, computational cost and complexity in communication is reduced.

M. Fan et al., (2019) the author presented a smart grid enabled data aggregation and regulation system in which blockchain mechanism is implemented. The process consists of regulating the system controlling the center grade operator and equipment control etc. the proposed approach considers power regulation feedback on smart systems. The System's Security Analysis and performance of the system are compared with various state-of-art approaches and further the Data integrity is being evaluated.

Y. Ming et al., (2019) The author presented a system where multi-dimensional data aggregation scheme is being discussed full stop the paper proposed and efficient privacy preserving model by using data aggregation methodology in smart grid is implemented. The Security Analysis discussed in the presented approach deal with the all kinds of privacy issues in the smart grid environment and proposed to reduce the computation cost.

N. Gai et al., (2020) The Other presented system were small grade adopted homomorphic encryption with randomised data aggregation technique is implemented. Privacy preserved smart grid environment is the prime goal of the system where local differential privacy based

random data processing is implemented. The presented approach improves the performance of the system and reduces the communication overhead. The computation cost is reduced by implementing the critical features of smart grid environment comparing with the conventional features. The demand on control centre managing is implemented here dynamically by adjusting the power supply price of the power.

J. Sarma et al ., (2019) The Other presented internet of things enabled wireless body area network for connecting various variable devices to a common biomedical platform. In order to manage the power utilisation prolonged continuous measurement of ECG systems the critical data and energy levels of storage systems or degraded. The presented approach reduces the power consumption focused on lightweight energy management system using w band the presented approach save up to 27% power consumption comparatively to various state of art approaches.

Y. Chen et al., (2019) The author introduced a system in which bilinear map pairing enabled secure protocol is implemented. Smart grid communication is applied widely in many sectors to provide secure privacy preserving wireless networks. Particularly in body area network privacy preserved data forwarding scheme is important in order to reduce the competition cost formal Security Analysis is being improved in the presented approach using pairing methodology.

Various existing systems are studied here; here the computational cost reduction is focused. To reduce the complexity in system communication overhead also important. Further based on the constraints available with the existing system, the proposed method is focused on improved network security through Data aggregation.

III. System Design

This model is uses Python toolset and the WBAN architecture is being simulated. The data is generated in a random manner. The python libraries are configured to achieve the data aggregation process. The secure authentication model is implemented using scientific computing toolbox, numerical computing toolbox, data analytical windows etc.

IV. Methodology

The design and implementation for the secure data aggregation using block chain (PDB) have been proposed and its issues were discussed in this paper. IoT network are more prone to vulnerabilities which are removed by this PDB. Hence Authentication Key Management (AKM) crypto system attributes PDB to aggregate the coded data across sensor nodes within their location. Access control keys are managed in such a way that service provider maintains compatible middleware security. Aggregation process well only when it ensures authenticated device and authorized network access to the service.

There are four different types of entities present in the system model are described in fig 1:

1.Patient Devices (PD)
2.CH
3.User (UK)
4.Trusted authority (TA)

Patient Devices [PD]: A set of medical devices are denoted as PD. The registered devices consist of sensors which collects secure data Di and send to the CH via access/ middleware layer. Security, data integrity and source authentication are some of the cryptographic operations performed by Di. The data usage are given to nearby UK by PDs.

2. Cluster Head [CH]: The computational and cloud storage to the edge of the end devices are supported here. Our proposal possess CH to aggregate user's data and performs functions like data integrity and source authentication which are aggregated, stored and forward to UK.

3. User (UK): The data packages from CH are given to UK then it took several intellectual decisions. The secret keys of UK about aggregated data are decrypted and send feedbacks to CHs.

4. Authority Center (AC): It is trusted party to generate System parameters (sp) and Master secret keys. Initially, public and Master secret keys are established to verify the user's identity based on their attributes. AC is not needed When key distribution ended in the data aggregation process.

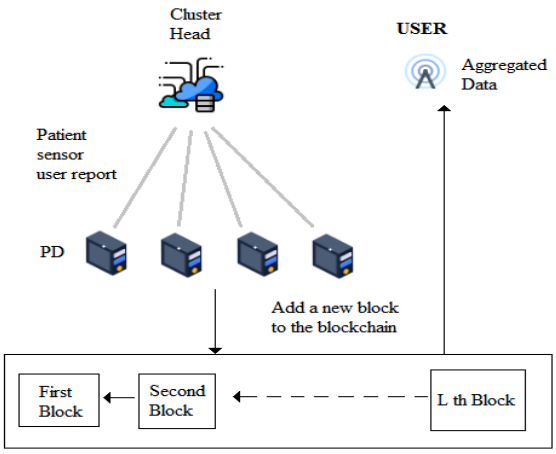

Fig. 1. System architecture of Proposed Data aggregated WBAN model

Fig. 1. Illustrate the System architecture of proposed Data aggregated WBAN model using Block chain technology.

Restricted Boltzmann machine algorithm choose the Cluster Head with the parameters like energy and buffer. Access control and secure data aggregation is processed followed by CH selection.

Buffer monitoring:

Let us consider B as a neighboring node, qj as the jth sample value of queue length at particular point and Q as the total number of queue length samples obtained at peak interval. With these parameters, we can calculate the average traffic load at node B as follows

$L_T(B) = (1/Q) * \sum_{j=1}^{n} qj$

At node B, qmax is defined as "the maximum length of queue interface at the MAC layer". Through this, Intensity function of traffic load is summarized as follows:

$L_{TI}(B) = (L_T(B) / qmax)$.

Finally, the expression for the true probability of packet due to neighbouring node B interms of overflowing queue can be modeled as

$PQ = 1- L_{TI}(B)$.

Energy calculation:

The equation for the "average dissipated energy" (ADE) is given by

$$ADE = \frac{Eni - Enf}{N(Di)}$$

At particular node, Eni and Enf are referred as initial and final energy. N(Di) represents the total count of data sets sent by the corresponding user to the neighboring nodes within the network.

Cluster head selection using RBM:

RBM is the self-learning technique to give an optimal CH through the parameters of buffer and energy. RBM algorithm is used in this protocol which has two layers: the visible layer with 'm' visible units denoted as V = v2, ..., vm, and the hidden layer with 'n' hidden units represented as h = h1, ..., hn. Weighted matrix (Wmn) and bias units of each node (Aim and bjn) are integrated with visible-hidden layer. Hence, the arrangement of RBM in the proposed protocol is considered as

$$C(V,H) = \sum_{i=1}^{m}\sum_{j=1}^{n} S_{m,n}\, h_n\, v_m - \sum_{i=1}^{m} a_{im}\, v_m - \sum_{j=1}^{n} b_{jn}\, h_n$$

$C(V,H) =$ Total weight of the RBM configuration

$S_{m,n}$ = connection strength between nodes 'm' and 'n' in the network

a_i, b_j = bias units of visible and hidden layers

v_m = visible unit

h_n = hidden unit.

In RBM, input feature vector (fv) = (senderip, destinationip, srcmac, destmac) and traffic trust vector (cv) = ($Node_{cong}$,$Node_{energy}$, $Node_{trust}$) training in the visible layer. Similarly for the identification of malicious routes, learning and processing of features and trust vectors take place in the hidden layer or processing layer. In addition to that, mapping of input data with network traffic occurs. During training period of vectors, joint probability distribution of both layer is represented as

$$J(V,H) = \left(\frac{1}{\phi}\right) * \exp\{-C(V,H)\}$$

The normalizing constant factor for the visible and hidden layers, denoted by ϕ, is provided as follows

$$\phi = \sum_{v}\sum_{h} exp - C[fv, cv], H[fv, cv, NIT_{nt-tf}]$$

where NIT_{nt-tf} is the new incoming network traffic pattern.

With the initial value of φ is 0, the model parameter assigning fails. Hence, iterative optimization depends on the alternative iteration algorithm can update the value of model parameter. The estimated value of φ i. φ i is the result of former sample training with sample Vi. The initial value of φi+1. φ i+1 gets changed for every model parameter and process repeats again and again until end conditions are satisfied. Self learning techniques are deployed in hidden layer as the computation of neighborhood true probability on the account of possible queue overflow. Fast learning algorithms are suitable in the interdependent layers. These restricted connections are not obeyed in other unsupervised Neural Network learning algorithms. There are two cases applicable for joint probability distribution to compute conditional probability distribution of two layers.

1. If we feed input value to visible layer as P (h_n/v_m) then hidden layer values are calculated.
2. If we feed input value to hidden layer as P (v_m/h_n) then visible layer values are calculated.

The same computations are processed under Gibbs sampling method whose input features are given by

$$GS\left(\frac{h_n}{v_m}\right) = \sum_v sigmoid(b_{jn} + v^T w{:}j)$$

Finally it is expressed as

$$O_{i,j}^{d}\ (t) = PQ_{i,j}(t) + \mathrm{ADE}\ (FN_i) + G_i$$

where FN_i is the number of forwarding packets from node i to node j, $PQ_{i,j}(t)\ is$ neighboring packet of true probability in terms of possible queue overflows and $E_{cons}(FN_i)$ is the energy utilization of neighboring nodes. Finally, MAX ($O_{i,j}^{d}\ (t)$) will be selected as Cluster head.

1. Access control and Secure data aggregation process:

A key management cryptosystem is a kind of protecting authority and allows to perform data access and computations on the encrypted data. Some of the challenging effect occur in secure aggregation due to public key encryption mechanism as it needs to equip with private key for higher security purpose. The effect of attackers can be filtered out by compromising unused nodes in the system. This limitation can exist high computational cost in both encryption and decryption technique. At last, bit size can be expanded during conversion of plain text and cipher text which causes high overhead and simultaneously the sensors energy gets depleted.

The main objective of using secure key generation approach is to focus effectively on managing and renewing keys for secure connection. It also guarantees the data integrity transmitted over an insecure channel. At two blocks of communication channel, symmetric encryption keys are generated due to synchronization and generation of local key. From this main characteristics, key selection will be changed during transmission to improve the security level.

Access Level: Some security mechanisms are specified to limit the network access. It functions like giving guarantee to the legitimate users for network and device access to tolerate the administrative task. e.g. remote control of IoT devices and network.

The proposed system can discuss about some of the malfunctioning data when aggregation and decryption is performed with fault tolerant sensing data. The threshold range of normal nodes can be altered by unauthorized data. The resultant causes high/ secure communication delays. Otherwise fault or missing data are sought from access control by the access/ middleware layer. Finally, data aggregation activity is stopped.

Bilinear mapping of "Composite order groups":

With security parameter $\tau \in Z^+$, as input, an algorithm $\mathcal{G}$ generates a tuple (p, q, G, G_1, e), where p,q are two random large prime number with τ- bit length, G, G_1 are two cyclic group with an order N = pq, and $e : G * G \rightarrow G_1$

The following are the properties of bilinear map:

1) Bilinear operation: $\forall u, v \in G$, and $a, b \in Z_N, e(u^a, v^b) = e(u, v)^{ab}$

2) Generating ability: if g is a generator of $G, e(g, g)$ is a generator of G_1 , and $e(g, g) \neq 1_{G_1}$;

3) Computing ability: $\forall u, v \in G$, acts as an efficient algorithm to compute $e(u,v)$.

Paillier cryptosystem:

Paillier cryptosystem [1] is an asymmetric encryption algorithm, whose additive homomorphism property should be achieved efficiently. It consists of three phases: key generation, encryption and decryption

1) Key generation: For the given security parameter $k \in Z^+$, choose two prime numbers $p, q,$ where $|p| = |q|$, and calculate $\lambda = lcm(p-1, q-1)$. Then we can define a function $L(u) = \frac{u-1}{N}$, where $N = pq$, and choose a generator of cyclic group g, then calculate $\mu = \left(L(g^2 \bmod N^2)\right)^{-1} \bmod N$ whose public key is (N, g), and the corresponding private key is (λ, μ) respectively.

2) Encryption phase Consider the plain text 'm' to select a random number $r \in Z_N^*$. Then, the ciphertext can be calculated as: $C = Enc(m) = g^m r^N \bmod N^2$.

3) Decryption phase：From the output of the ciphertext C, the plain text can be recovered with the private key (λ, μ) as: $m = D(C) = L(C^{\lambda \bmod N^2}) \times \mu \bmod N$.

Five phases are involved in this scheme are discussed below:

1. Initialization: System parameters, pair of private/ public key for CHs and input are generated by AC. At the corner point of the network, CHs are utilized to publish its public parameters.

2. Registration: PD chooses the registered identity in the block chain to AC using signature and private key. A pair of public and private key generation are highly possible. An effective registration of AC are acceptable even after the verification of signature.

3. PD data encryption and report: PD generates the particular signature for the uploaded data, then encryption takes place. Finally PD reports the cipher text, signature to its CH.

4. CH data aggregation and report: The validity of the cipher text are checked in each CH and aggregates it once text from PDs are valid. Again the process like generating signatures and reporting aggregated cipher text repeats through sink node to AC.

5. Decryption: From the block chain, validity CHs cipher text should be checked by sink and plain text are obtained from the decryption using secret key.

1. Initialization

To initialize the system, AC required to select certain parameters. At first, AC generates the parameters (p, q, G, G_1, e) in the input node by using algorithms. Next, AC chooses three random generators f, g and x of G, and calculate N and h where N = pq and h = xq. Next AC chooses the secure hash function $H: \{0,1\} * \rightarrow G$. Finally, AC publishes the public key $(N, G, G1, e, f, g, h, H)$ of the system, and the private key 'p' is maintained in confidential manner.

2. Registration

The AC chooses identity ID_{ES_i} which will be registered in the block chain, then generate the private/public keypair (y_i, Yi) for ES_i $(i = \{1, 2, \ldots n\})$, where $y_i \in (1, p)$ and $Y_i = h^{yi}$. Then, AC store the pair (ID_{ES_i}, Y_i) in the database, and (ID_{ES_i}, y_i, Y_i) in the ES_i. Finally, the edge server's CHs are deployed at the edge of the network to securely maintain their private keys.

When the user with $TD_{ij} (j = 1,2,..,l)$ want to access the location proximity edge server CHi, the registration phase will be carried out. The user chooses an identity $ID_{TD_{ij}}$, and generates the private /public keypair (y_{ij}, Y_{ij}), where y_{ij} is a

[1] M. Mohan, M. K. Kavithadevi and J. Prakash V., "Improved ElGamal Cryptosystem for Secure Data Transfer in IoT Networks," 2020 pp. 295-302

random number of bit length of $1 \sim \tau - 1$ and $Y_{ij} = h^{yij}$. Next $ID_{TD_{ij}}$ gets current timestamp t_{Reg} and calculates $Sig_{ij} = H(ID\_TD_{ij}||t_{Reg})^{y_{ij}}$, and submits $\{ID_{TD_{ij}}, t_{Reg}, Sig_{ij}, Y_{ij}\}$ to AC for registration. On receiving the request for registration, AC initially verifies the freshness of timestamp t_{Reg}, and next verifies $e(Sig_{ij}, h) = e(H(ID_{TD_{ij}}||t_{Reg}), Y_{ij})$. If it doesn't hold, the request is rejected by AC. Else, $ID_{TD_{ij}}$ registration is successful and $\{ID_{TD_{ij}}, Y_{ij}\}$ is stored in database and the corresponding ES_i. by AC

Besides, for a edge server ES_i and its l terminal servers $TD_{ij}(j = 1, 2, .., l)$, AC generates l random numbers $\{\pi_{i1}, \pi_{i2}, .. \pi_{il}\}$ from Z_N, and calculates $\pi_i = -(\pi_{i1} + \pi_{i2} + \cdots + \pi_{il}) \bmod N$. Then, AC assigns π_i to ES_i and π_{ij} to the corresponding $TD_{ij}\ (j = 1, 2, \ldots, l)$ secretly and these information are deleted.

3. PD data encryption and report

In this stage, each $TD_{ij}(j = 1, 2, \ldots . l)$ encrypts the message m_{ij} and generate the corresponding signature, then report it to its edge server $ES_i(i = \{1, 2, \ldots, n\})$.

We can collect the data consumption when $m_{ij} \in [0, T]$. In addition to this, TD_{ij} picks a random number r_{ij}, and the cipher text $C_{ij} = f^{\pi_{ij}}\ g^{m_{ij}} h^{r_{ij}}$ is calculated. Then, TD_{ij} gets the current timestamp t_{ij}, and generate a signature for the cipher text $\sigma_{ij} = H\left(ID_{TD_{ij}}\ \left||C_{ij}|\right|\ t_{ij}\right)^{y_{ij}}$ using its secret key y_{ij}. Finally, TD_{ij} report the message $\{ID_{TD_{ij}}, t_{ij}, C_{ij}, \sigma_{ij}\}$ to its edge server ES_i

4. CH data aggregation and report

In the stage, each ES verifies the message from PDs, and then aggregates , reports, and record the aggregation data into the new block. CH broadcasts this block, and other nodes in the entire network connect the block to their respective block chain. Then Sink can query the block in the block chain, and retrieve the aggregated data M. Here, we can take ES_i as an sample to demonstrate the phase.

Upon receipt of all the messages reported by $TDij\ (j = 1, 2, \ldots, l)$, meanwhile ES_i checks the validity of $ID_{TD_{ij}}$ and freshness of timestamp $t_{ij}\ (j = 1, 2, \ldots, l)$. is verified. The messages will be discarded if any of the process fails. Then ES_i performs the batch verification $e(\prod_{j=1}^{l} \sigma_{ij}, h) = \prod_{j=1}^{l} e(H\left(ID_{TD_{ij}}\ \left||C_{ij}|\right|\ t_{ij}\right), Y_{ij})$, which greatly reduces the $ES_i's$ computing speed and communication costs. If it doesn't hold, atleast one of the message reported by $TD_{ij}\ (j = 1, 2, \ldots, ;\ l)$ is not valid, and ES_i finds the invalid messages by checking $e(\sigma_{ij}, h) = e(H\left(ID_{TD_{ij}}\ \left||C_{ij}|\right|\ t_{ij}\right), Y_{ij})\ (j = 1, 2, \ldots, l)$ conversely, if the messages reported by $TD_{ij}\ (j = 1, 2, \ldots, l)$ are all valid, ES_iaggregates the received messages as follows $C_i = f^{\pi_i} \prod_{j=1}^{l} C_{ij}$. Next ES_i gets the current-timestamp t_i, and generate a signature for the aggregated data $\sigma_i = H(ID_{ES_i}||C_i||t_i)^{y_i}$. Finally, ES_i submits the message $\{ID_{ES_i}, C_i, \sigma_i, t_i\}$ to the Sink.

$$C_i = f^{\pi_i} \prod_{j=1}^{l} C_{ij}$$
$$= f^{\pi_i} f^{\sum_{j=1}^{l} \pi_{ij}}\ g^{\sum_{j=1}^{l} m_{ij}}\ h^{\sum_{j=1}^{l} r_{ij}}$$
$$= f^{\pi_i + \sum_{j=1}^{l} \pi_{ij}}\ g^{\sum_{j=1}^{l} m_{ij}}\ h^{\sum_{j=1}^{l} r_{ij}}$$
$$= f^{0}\ g^{\sum_{j=1}^{l} m_{ij}}\ h^{\sum_{j=1}^{l} r_{ij}}$$

$$= g \sum_{j=1}^{l} m_{ij} \, h \sum_{j=1}^{l} r_{ij}$$

5. Decryption

The number of n edge servers $\{ES_1, ES_2, \ldots, ES_n\}$ reports the receiving messages whose validity of ID_{ES_i} and freshness of the corresponding timestamp t_i $(i = 1, 2, \ldots, n)$ are checked by sink. If any one checking process fails, messages are removed. Sink computational costs and time are highly reduced by batch verification $e(\prod_{i=1}^{n} \sigma_i, h) = \prod_{i=1}^{n} e(H(ID_{ES_i} || C_i || t_i), Y_i)$. Sink can find out the invalid messages by checking $e(\sigma_i, h) = e(H(ID_{ES_i} || C_i || t_i), Y_i)$ $(i = 1,2, \ldots, n)$. If it doesn't hold, atleast one of the message should be reported by ESi (i = 1,2,....n). On the contrary, the message reported by ES_i $(i = 1,2, \ldots, n)$ are valid.

Sink checks the receiving messages validity as follows

$$C = \prod_{i=1}^{n} C_i = g \sum_{i=1}^{n} m_{ij} \, h \sum_{i=1}^{n} \sum_{j=1}^{l} r_{ij}$$

Since $h^p = (x^q)^p = x^{pq} = 1$,Sink can calculate by using the secret key p

$$V = C^p = \left(\prod_{i=1}^{n} C_i \right)^p$$

$$= \left(g \sum_{i=1}^{n} \sum_{j=1}^{l} m_{ij} \, . h \sum_{i=1}^{i} \sum_{j=1}^{l} r_{ij} \right)^p$$

$$= g^p \sum_{i=1}^{n} \sum_{j=1}^{l} m_{ij}$$

$$= \hat{g} \sum_{i=1}^{n} \sum_{j=1}^{l} m_{ij}$$

Where $\hat{g} = g^p$

Then, Sink can recover the aggregated plaintexts using discrete logarithm. The Pollard lambda method [1] from $TDs \sum_{i=1}^{n} \sum_{j=1}^{l} m_{ij}$ using discrete algorithm retrieve the original aggregated plaintexts by sink are mentioned in the above expression.

V. Results and Discussions

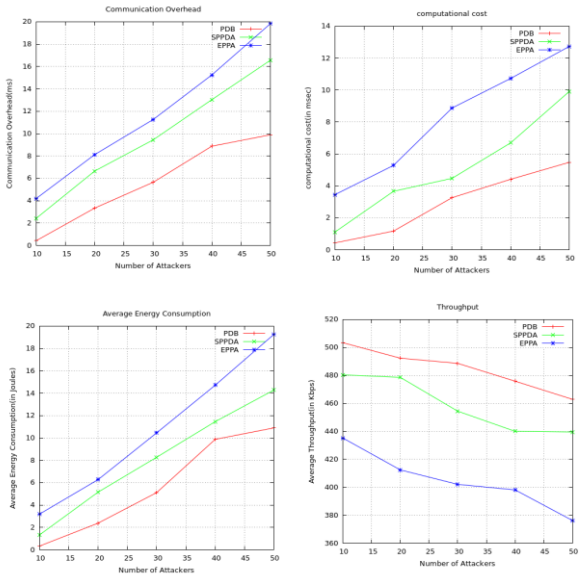

Fig. 3. Shows the system on attackers Compuattaion cost, communication over head, energy, throughput.

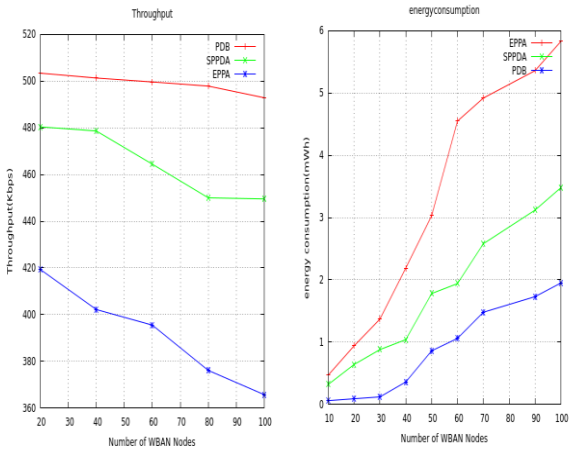

Fig. 4. Shows the system throughput, energy of Proposed PDB with respect to existing EPPA and SPPDA model.

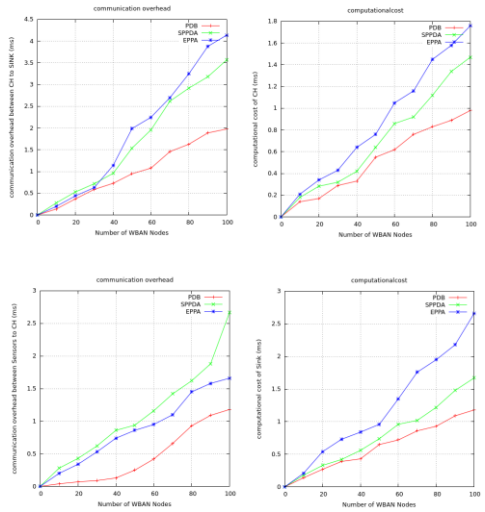

Fig. 5. Shows the system Compuattaion cost, communication over head, energy, throughput on PDB, EPPA, SPPDA models

Comparing with existing frameworks EPPA, SPPDA, the PDA achieved 10% lower computation cost, complexity os reduced. The proposed PDA model accomplished 1 as calculation cost that is 0.8 times not exactly the current EPPA model. The correspondence above is decreased to 2 contrasting the EPPA model, diminished by 1.5 contrasting and SPPDA model and so forth.

VI. Conclusion .

Wireless body area networks are recent trending research work, required to be optimized for improving the performance and response rate in the 5G communication world. Computation cost and Complexity of the design is the prime problem in the existing frameworks. The proposed approach utilized blockchain enabled high level privacy reserving secure communication model that considers data aggregation scheme. The presented paper is developed through scientific computing toolbox, numerical computing toolbox using python. The proposed PDA model achieved 1 as computation cost that is 0.8 times less than the existing EPPA model. The communication overhead is reduced to 2 comparing the EPPA model, reduced by 1.5 comparing with SPPDA model etc. further the presented work can be enhanced by implementing hybrid machine learning algorithms to provide better accuracy.

References

[1] I Yakymenko, M. Kasianchuk, O. Gomotiuk, G. Tereshchuk, S. Ivasiev and P. Basistyi, "Elgamal cryptoalgorithm on the basis of the vector-module method of modular exponentiation and multiplication," 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), 2020, pp. 926-929, doi: 10.1109/TCSET49122.2020.235572.

[2] M. Mohan, M. K. Kavithadevi and J. Prakash V., "Improved ElGamal Cryptosystem for Secure Data Transfer in IoT Networks," 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2020, pp. 295-302, doi: 10.1109/I-SMAC49090.2020.9243407.

[3] M. Fan and X. Zhang, "Consortium Blockchain Based Data Aggregation and Regulation Mechanism for Smart Grid," in IEEE Access, vol. 7, pp. 35929-35940, 2019, doi: 10.1109/ACCESS.2019.2905298.

[4] Y. Ming, X. Zhang and X. Shen, "Efficient Privacy-Preserving Multi-Dimensional Data Aggregation Scheme in Smart Grid," in IEEE Access, vol. 7, pp. 32907-32921, 2019, doi: 10.1109/ACCESS.2019.2903533.

[5] N. Gai, K. Xue, P. He, B. Zhu, J. Liu and D. He, "An Efficient Data Aggregation Scheme with Local Differential Privacy in Smart Grid," 2020 16th International Conference on Mobility, Sensing and Networking (MSN), 2020, pp. 73-80, doi: 10.1109/MSN50589.2020.00027.

[6] J. Sarma, A. Katiyar, R. Biswas and H. K. Mondal, "Power-aware IoT based Smart Health Monitoring using Wireless Body Area Network," 20th International Symposium on Quality Electronic Design (ISQED), 2019, pp. 117-122, doi: 10.1109/ISQED.2019.8697739.

[7] B. Cornet, H. Fang, H. Ngo, E. W. Boyer and H. Wang, "An Overview of Wireless Body Area Networks for Mobile Health Applications," in IEEE Network, vol. 36, no. 1, pp. 76-82, January/February 2022, doi: 10.1109/MNET.103.2000761.

[8] Y. Chen, J. -F. Martínez, P. Castillejo and L. López, "A Bilinear Map Pairing Based Authentication Scheme for Smart Grid

Communications: PAuth," in IEEE Access, vol. 7, pp. 22633-22643, 2019, doi: 10.1109/ACCESS.2019.2898376.

[9] I. Ali, Y. Chen, N. Ullah, M. Afzal and W. HE, "Bilinear Pairing-Based Hybrid Signcryption for Secure Heterogeneous Vehicular Communications," in IEEE Transactions on Vehicular Technology, vol. 70, no. 6, pp. 5974-5989, June 2021, doi: 10.1109/TVT.2021.3078806.

[10] V. Kumar, "A Bilinear Pairing Based Secure Data Aggregation Scheme for WSNs," 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), 2019, pp. 102-107, doi: 10.1109/IWCMC.2019.8766759.

[11] Fan Zhang. Charm-Crypto Benchmark, accessed on Jan. 1, 2017. [Online]. Available: http://student.seas.gwu.edu/~zfwise/crypto/report_1_4_1.pdf

[12] X. Lin, R. Lu, and X. Shen, ``MDPA: Multidimensional privacy-preserving aggregation scheme for wireless sensor networks,'' Commun. Mob. Com- put, vol. 10, no. 6, pp. 843 856, Jun. 2010

[13] J.-L. Beuchat, J. E. González-Díaz, S. Mitsunari, E. Okamoto, F. Rodríguez-Henríquez, and T. Teruya, ``High-speed software implementation of the optimal ate pairing over arreto Naehrig curves,'' in Pairing-Based Cryptography (Lecture Notes in Computer Science), vol. 6487. Berlin, Germany: Springer-Verlag, 2010, pp. 21 39.

[14] O. Kocabas, T. Soyata, and M. K. Aktas, ``Emerging security mechanisms for medical cyber physical systems,'' IEEE/ACM Trans. Comput. Biol. Bioinformat., vol. 13, no. 3, pp. 401 416, May 2016.

H. Yang, H. Kim, and K. Mtonga, ``An ef cient privacy-preserving authentication scheme with adaptive key evolution in remote health monitoring system,'' Peer-to-Peer Netw. Appl., vol. 8, no. 6, pp. 1059 1069, Nov. 2015