Cloud-based Energy Efficient and Secure Service Provisioning System for IoT using Blockchain

Adeel Ahmed (adeelmcs@gmail.com)
The Islamia University of Bahawalpur Pakistan https://orcid.org/0000-0002-4034-6917
Saima Abdullah
Islamia University: The Islamia University of Bahawalpur Pakistan

Research Article

Keywords: IoT, Edge Computing, Cloud Computing, Blockchain, Energy Efficient, Security

Posted Date: July 20th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-606120/v1

Cloud-based Energy Efficient and Secure Service Provisioning System for IoT using Blockchain

Adeel Ahmed[1]. Dr Saima Abdullah[2]

Abstract

The energy consumption of the internet of things (IoT) routing protocol can affect the network life span. The high volume of data produced by IoT will result in transmission collision, security, and energy dissipation due to data redundancy because tiny sensors are usually hard to recharge after they are deployed. Generally, to save energy, data aggregation reduces data redundancy at each node by turning some nodes into sleep and some into wake-up mode. The main work is that to group the nodes with high data similarity using the fuzzy matrix. Then, data received from the member nodes at CH are analyzed using a fuzzy similarity matrix for clustering. In the next step, after clustering, some nodes are chosen from all groups as redundant nodes. The sleep scheduling mechanism is then applied to reduce data redundancy, network traffic jamming, and transmission cost. We proposed an energy-efficient data aggregation mechanism (EEDAM) secured by blockchain. The proposed system uses a data aggregation mechanism at the cluster level to save energy. Edge computing is used to provide on-demand trusted services to IoT without minimum delay. Blockchain is integrated inside a cloud server, so the edge is validated by the blockchain to provide secure services to IoT. Finally, we performed simulations to calculate the performance of the proposed mechanism and compared it with the conventional energy-efficient algorithms. The simulation results show that the proposed structural design can successfully reduce the amount of data, provide proper security to IoT, and extend the wireless sensor network (WSN).

Keywords IoT, Edge Computing, Cloud Computing, Blockchain, Energy Efficient, Security

---

[1]Adeel Ahmed

(Corresponding author)

Department of Computer Science & IT

The Islamia University of Bahawalpur, Punjab, Pakistan, 63100

Email: adeelmcs@gmail.com

[2]Dr. Saima Abdullah

Department of Computer Science & IT

The Islamia University of Bahawalpur, Punjab, Pakistan, 63100

Email: abdullahsaima@yahoo.com

I. Introduction

Nowadays, many network edge devices and real-world objects are integrated with wireless sensors to monitor and collect real-time data from the monitoring area. On the other hand, this architecture has changed with the invention of the IoT. Intelligent devices such as sensors, smart home devices, intelligent cars, industrial areas, and utility are communicated through the internet and integrated with data analysis capability. This paradigm has changed the way we live, play, and work. IoT devices formed a massive volume of the data stream at high speed. With flexible and efficient security service provisioning in cloud base architecture (Bhajantri & Mujawar, 2019) (Zhang et al., 2020), a vast volume of IoT device data formed by IoT cluster networks can be communicated to the remote edge cloud for further processing through the network (Lockl et al., 2020)(Apostolopoulos et al., 2020). However, the internet is not effectively efficient and not effectively scalable to deal with this massive IoT data volume. Also, the processing and transfer of necessary data are expensive, consuming vast bandwidth, energy, and time. Huge IoT data volumes are communicated to the cloud server at maximum speed to discover important information in a real-time environment. So there is a need to design an effective and secure architecture for local data processing to reduce the cloud server's processing load and the data redundancy at the cluster level of the WSN.

For emerging technology computing, fog and edge computing is a transparent structure that combines the working of cloud and IoT devices (Tange et al., 2020). Recently, cloud-based frameworks broadly researched due to the restricted computing resources of IoT devices and cloud services increasing demand. Currently, research shows that cloud servers are not providing satisfactory services to the end-user. Edge computing nowadays is considered the extension of the cloud server services. The use of edge transparent computing does the cloud server's processing and storage work at the network's edge; It can deliver faster services to the end-user, such as processing, storage, and networking. With emerging network technologies like edge, fog, and cloud, the IoT-constrained device's functionalities increase. There is a need for protocol and standard layer like edge computing that provides security services to IoT networks to control huge data volume generated by them. The existing cloud server centralized architecture in which IoT devices are connected with cloud servers through the internet for processing and storage purposes. It may contain transmission issues like a congestion problem, bandwidth problem, network congestion, delay, security, and a single point of failure. There is a need for decentralized architecture for IoT networks for local storage, computing, and protection to overcome these issues. There is some existing decentralized architecture for large-scale IoT networks to avoid these issues. However, security and privacy issues are not considered in this architecture (G. Singh, 2019)(Liu et al., 2019)(Rehman et al., 2019). We conclude a need for a paradigm for protecting the IoT devices from security threats, eliminate data redundancy and illegal service providers in the network from existing research.

With the limited resources and market scope, fog computing cannot provide efficient, reliable, and secure services to the end-user (Butun et al., 2018). IoT devices' future goals realize resources like scalable, protected, and with sufficient processing power. Decentralized cloud architecture must achieve the maximum objectives of IoT-constrained devices. Currently, blockchains are widely researched due to their growing demand in industry and decentralized property(L. Tseng et al., 2020)(P. Singh et al., 2020). The primary purpose of using blockchain

technology is to operate in a decentralized model in a proper secure manner. The current research indicates that the latest technologies like blockchains and bitcoins are the finance domain's future (Sharma et al., 2020)(Li et al., 2021).

The invention of the blockchains overcomes the limitation problem of centralized architecture. Blockchain provides excellent functionalities like security, decentralized architecture, and a transparent system. Blockchains are also used for secure and efficient data transmission. However, blockchain architectures for IoT devices cause low throughput, low latency, and delay-like issues. Current blockchain systems are using high processing power and storage.

On the other hand, IoT-constrained devices lack these resources. At present, different companies offering decentralized architecture and storage capacity. Recently, to overcome the server and maintenance cost problems, most of the organizations shifted to the cloud server. These things motivated us to trust the third party for cloud services like processing and storage. Due to the low cost of maintenance and storage, we must trust other parties for our encrypted sensitive data. Existing architecture working between the cloud server and the financial organization can be replaced with blockchain technology rather than third-party security, processing, and storage services. Blockchain-based cloud server architecture sells their extra storage capacity to renters, and they made payments through blockchain with proper security and trust. The world economic forum's survey predicted that by 2027 world GDP might be store 10% on blockchain infrastructure (C. Te Tseng & Shang, 2021). Due to blockchain infrastructure, secure service provisioning and safe edge computing devices are possible for end-users. This paper proposes a data aggregation architecture that maintains the edge server's validity state depending on the service provided to the end-user part of the IoT network and the end user's rating given to the edge. With the invention of blockchain technology, the network's risk of suspected activities is eliminated for edge servers to provide security services for IoT devices. The usage of edge computing for IoT devices at the edge of the network enhances cloud architecture work progress, throughput, and security. All the transaction occurs in the network are stored in cloud network infrastructure.

Currently, cluster techniques are primarily used in wireless sensor networks. Low-energy adaptive cluster hierarchy (LEACH) protocol for micro-sensor network organization increases energy efficiency and network life span proposed by Heinzelman (Heinzelman et al., 2002). An improved version of the LEACH protocol for selecting the cluster head and energy consumption balance (Chawra & Gupta, 2020). Dynamic sleep scheduling mode is better than fixed sleep scheduling can improve the network's lifetime (Venugopal et al., 2020), In cluster network itinerary-based to solve the spatial query processing problems to save network energy (Verma et al., 2020). For the aggregation of data cluster-based data analysis system is proposed (GAVIN WOOD, 2014). The sleep scheduling scheme (Khan et al., 2020) analyzes some factors, like node distance to cluster head, residual energy, coverage ratio, and schedule.

IoT-based clinical sensor data is managed for security using Blockchain technology. It helps for early treatment by using a smart contract between the patient and the health authority (Wang, 2020). A high-level Hybrid IoT method uses blockchain, cloud, edge, and fog to reduce the limitations of each architecture (Memon et al., 2020). Deep

Blockchain framework (Alkadi et al., 2020) is designed to protect IoT networks using smart contracts for security and privacy services. (Serrano, 2021) Presents the Blockchain Random Neural Network for the cybersecurity users and technique for the authentication, and saves the network from security breach using Blockchain infrastructure. Blockchain infrastructure is proposed to meet the dynamic user security requirements to access network supply in a 5G network environment (Aloqaily et al., 2021).

Route optimization and service assurance (ROSA) is proposed for low latency communication in industrial IoT network for energy efficiency (Njah & Cheriet, 2021). A comprehensive survey on the energy efficiency of medium access control for cellular IoT is presented on the source of energy dissipation (Shah et al., 2021). An adaptive channel (Chen et al., n.d.) and a QoS approach are proposed for IoT bidirectional communication for energy efficiency and green computing. Edge computing is used for enabling IoT for vehicle location detection rapidly (Xu et al., 2021). The Federated learning approach identifies the resource allocation, communication cost, privacy, and protection for edge data sharing using Blockchain (Nguyen et al., 2021). Edge computing has become an essential approach in IoT-based networks to store data on the cloud to reduce cloud server workload and real-time event detection (Puthal et al., 2021). Lockedge (Huong et al., 2021) proposed an edge cloud infrastructure that fulfills the edge layer's detection requirements for quick response. An energy-efficient Q-Learning-based data aggregation protocol is proposed for IoT to save energy. Data aggregation is used to eliminate the data redundancy in each node to reduce transmission time in wireless sensor networks. Furthermore, the proposed algorithm uses reinforcement learning to achieve maximum results (Yun & Yoo, 2021). A fuzzy logic-based protocol is proposed for the threat detection on real-time videos from the security and privacy point of view (Shifa et al., 1868)

Data transmitted by the cluster head can be penetrated and may contain security and privacy issues. The IoT constrained devices ' performance and functionalities increase by using rising modern technologies like edge computing, fog, Cloud, and Blockchain. For energy efficiency and security issues, architecture needs to provide energy-efficient security services for IoT-based networks. Network data transmission issues like blockage, network jamming, bandwidth, security, and response delay may happen due to the rapidly growing use of IoT devices. There is a considerable need for decentralized architecture to manage such security and energy-related issues from the IoT-based networks.

Research contributions: This paper proposes an energy-efficient cloud-based data aggregation system for IoT secured by blockchain infrastructure, an efficient, flexible, scalable, and secure cloud infrastructure including edge computing, a cloud server blockchain technology is used to provide security service to edge computing. Edge nodes are also used to gather, classify and analyze IoT data streams. Thus, edge computing plays a vital role in intelligent computing for data processing and convenience to security issues. The primary function of the research for this proposed architecture is given below.

- This paper proposes a decentralized cloud-based secure infrastructure based on the blockchain emerging technology, which provides secure, effective, low-cost on-demand services through edge computing to the IoT devices network. In our proposed architecture, a safe distributed edge node-based architecture using cloud and

blockchain is used to bring processing and storage power at the edge of the IoT constrained devices. As a result, the network traffic transmitted between cloud servers and IoT devices can be safe and smooth with minimum end-to-end delay. Thus, the primary purpose of edge computing is to provide secure services, storage, and computing resources to the IoT network.

- It also proposes to achieve energy efficiency by data aggregation using the fuzzy matrix to reduce the similarity degree and co-relation of the collected data from the IoT network to increase the network's lifetime by keeping the redundant nodes on sleep wake-up mode.
- The proposed system's performance compares with the existing system from different performance factors points of view.

Organization: The rest of the paper is organized as follows:

Section II discusses the need for blockchain technology and the transparent edge technology for secure service without delay for IoT-constrained devices. Section III presents the decentralized architecture using the blockchain emerging technology to validate the edge server and services provided to the IoT devices; Section IV presents the evaluation of the proposed decentralized architecture from a different performance metrics point of view. Finally, section V presents the future work and conclusion.

II. Preliminaries

A. Need for blockchain in cloud architecture

Blockchain is the new technology for security on the blocks. This unique idea has currently attracted researchers who have recognized blockchain technology for the cloud infrastructure's security services. The blockchain's need in the distributed cloud storage is given below.

- *Redundancy and decentralization*: Using the blockchain technique helps build a decentralized cloud data storage where data is stored in different nodes disbursed worldwide.
- *Resource services:* on the requested assistance from the intelligent IoT devices, the blockchain technology can facilitate the use of resources on-demand by the intelligent contract algorithm. After that, payment will automatically occur upon completion of the requested services.
- Security: using blockchain technology, each user manages its key, and every block of the blockchain stores an encrypted form of data. It also provides complete protection without the involvement of a third party.
- Reduction of cost: due to blockchain technology efficiency, security, and low cost of each host. With the comparison of the cost, blockchain cost is 2$ per terabyte per month, and Amazon S3 cost is 25$ dollar per terabyte per month.
- Quality of services: The blockchain technology can trace the use of the resources used to verify the client and service provider's service level agreement

B. Requirements for secure distributed infrastructure in an IoT scalable network using edge computing

Design a high-performance system using the edge computing scalable IoT network for secure services challenges and future requirements. The following system design principles must be taken for implementation:

- Flexibility: If some nodes fail, the processing should be continued on other working nodes.
- Efficiency: Users must receive excellent system performance even the computing nodes are very different.

- Easy to deploy: If the nodes are located on the different network edge, it allows the nodes to use without configuration.
- Adaptability: The network should accept all changing requirements to meet the user's future needs.
- Availability: Edge server and cloud availability are essential to meet the IoT network demands.
- Fault tolerance: The provisioning of the priority identification of fault tolerance are essential steps for the activity.
- Scalability: It is essential to design a decentralized IoT architecture to manage the future increase of devices and information they produce.
- Performance: Still, it is a big challenge to achieve linear performance from the decentralized IoT architecture.
- Security: Security is a vital goal in decentralized IoT architecture. Confidentiality and data security are the main key points to ensure network design.

C. Required principles for energy efficiency in IoT network

- Cluster organization: IoT networks are divided into clusters using a fuzzy matrix on the base high data similarity to save IoT network energy to prolong the network life span.
- Data aggregation: Data transmitted by the sensors may contain spatial correlation. By reducing the correlation, energy efficiency can be achieved for better network performance.
- Sleep schedule: In the sensor cluster, nodes can be grouped into the active and passive mode for data transfer due to the same monitoring area deployment to save nodes energy.

The previous section presented the expansion of the IoT-based decentralized architecture design principles for new communication infrastructure. We found that the existing cloud-based system can fulfill the user-distributed requirements for their work. Simultaneously, there are still growing demands of researcher communities for efficient processing power to process the enormous volume of data produced by the IoT and process different applications. Edge computing is an emerging technology that brings cloud storage and processing power at the IoT network's edge to fulfill the requirements. IoT devices are locally managed and enforce to implement different policies with an edge computing model. Edge computing is a local processing power to provide storage and processing power service to IoT devices. With the use of an edge server at the edge of the IoT network, IoT nodes' raw data can be locally analyzed categorized without network and cloud server involvement. Edge mitigates the cloud's computing power, storage, and network traffic and analyzes the IoT network's raw data. However, secure and efficient deployment of the edge nodes to facilitate the communication between the cloud server and edge nodes is always an open problem. The edge server deployment ensures that every IoT network can access the processing power everywhere without end-to-end delay and increased network traffic. This section proposes a novel energy-efficient data aggregation technique using blockchain emerging technology, edge computing, to meet the current and future requirements to provide secure services to IoT networks.

III. Architecture design workflow

Figure 1 presents the proposed decentralized system overview, organized into three different layers, i.e., IoT devices, edge server, cloud layer including Blockchain mechanism. The IoT devices collect data from the monitored public infrastructure and send it to the base station after filtering using the fuzzy matrix. The base station is located outside the IoT monitored area. IoT devices are location um-aware devices, and a unique id is assigned to all devices for identification. The sensor nodes detect signal strength and the estimated distance from the sender device and maintain the communication power adaptively for energy efficiency. All the IoT devices are capable of data fusion. It is assumed the collected data is relevant, perfect, and data packets can be of equal size for transmission over the network. Energy consumed for each round of data transmission can be calculated based on the IoT devices' data reception and communication. For the estimate of energy consumption, the First Order Radio is exploited. The energy consumed for transmission of N-bit packets from the sender to receiver at a distance (d) can be defined as

$$E_{Tx} \begin{cases} lE_{elec} + l\varepsilon fsd^2, d < d_0 \\ lE_{elec} + l\varepsilon mpd^4, d \geq d_0 \end{cases}$$

For monitoring of the controlled area, IoT nodes are circulated in the monitoring area. The data collected from this area contain spatial co-relation. To reduce energy usage, we will turn some nodes into sleeping mode. In addition, some nodes will be turned into a wake-up mode to save energy. Our work's primary focus is on a sleep schedule,

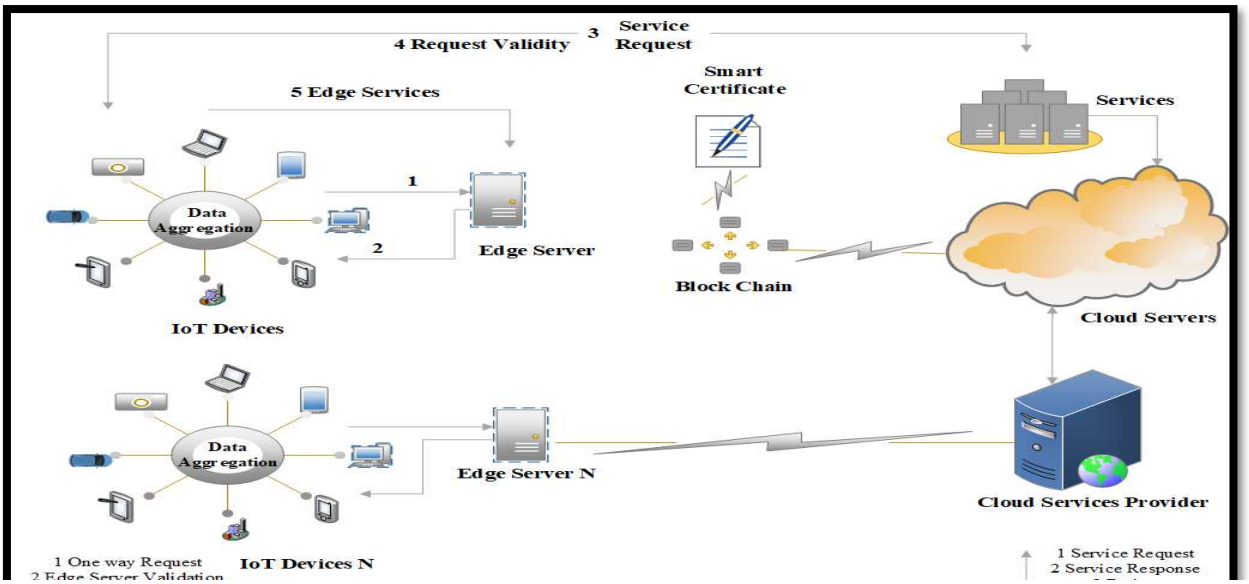

Figure 1 Proposed System Architecture

which is more critical for data redundancy and communication variance. By converting the node into a dormant state, sleep and scheduling methods will save a lot of energy. The main work is that to group the nodes with high data similarity using the fuzzy matrix. Data received from the member nodes at CH are analyzed for further extension. First, a fuzzy similarity matrix is made to make clustering. In the next step, after clustering, some nodes are chosen from all groups as redundant nodes. The sleep scheduling mechanism is then applied to reduce data redundancy, network traffic jamming, and transmission cost.

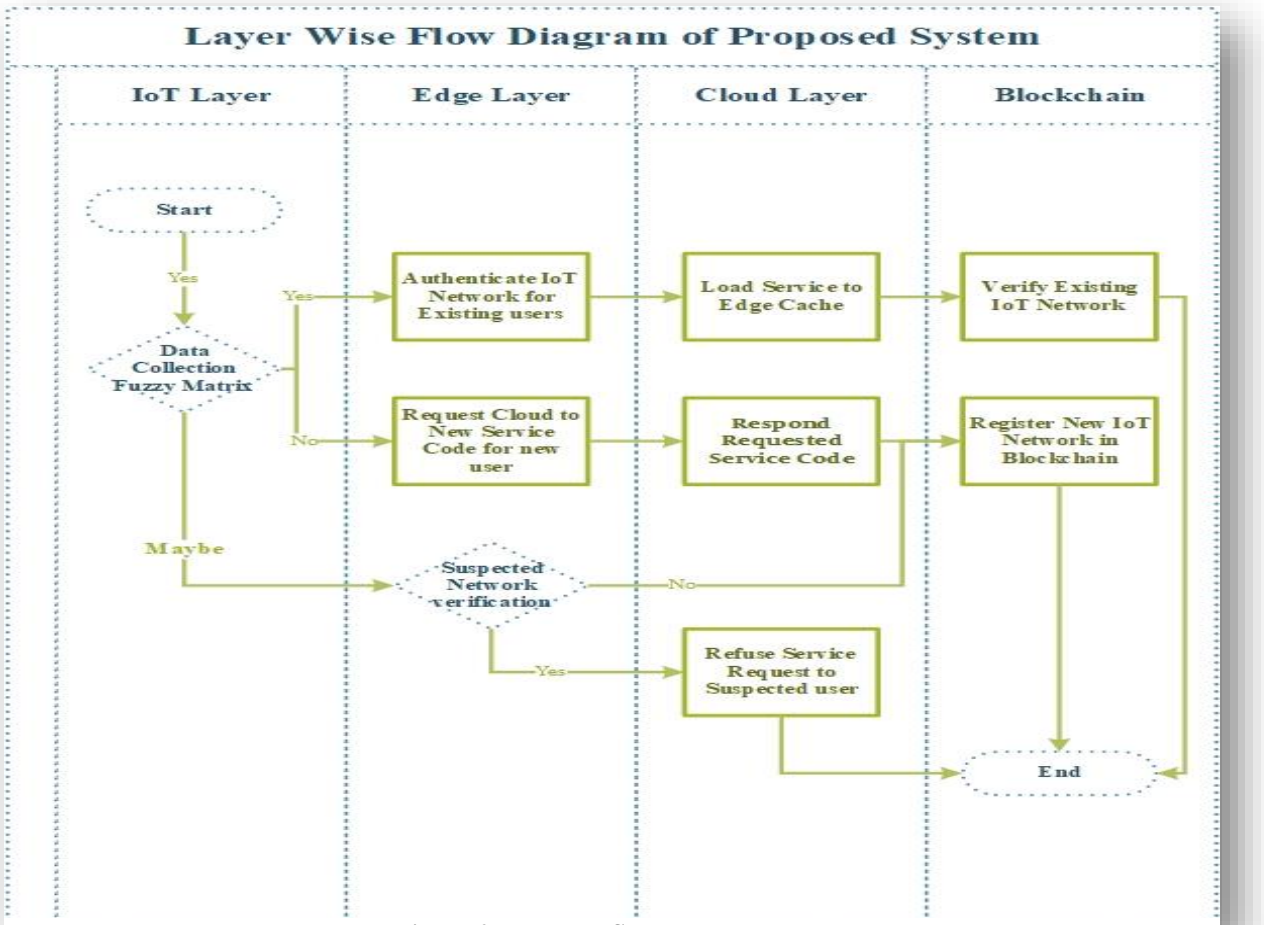

Figure 2 Proposed System Work Flow

The cooperation between two nodes, N_a and N_b can be calculated by the deployment distance using function calculate_Dis(a,b). The distance is much higher between the nodes than the data collected from the nodes assuming without spatial co-relation. Clustering is also done by using the fuzzy matrix for observed objects. Different classification results are obtained from different confidence levels to form a dynamic clustering network.

Suppose sensor network $N = \{N_1, N_2, \ldots N_n\}$ represents the number of deployed member nodes in the cluster, and n shows the total number of sensor nodes in the cluster. The data collection time from observed objects are divided into t intervals, and $D_{a,b}$ represents the data gathered by that member node S_a at time u. Thus, the data collected matrix can be defined as $D=(D_{ab})n*t$.

The next step is to transform matrix D into the matrix. First of all, standard and shift deviation transformation is implemented to normalized matrix elements that can be given as

$$d'_{ab} = \frac{d_{ab} - \bar{d}_b}{n_b}, (a = 1, 2.., n, b = 1, 2, .. n)$$

$$\bar{d}_b = \frac{1}{n}\sum_{b=1}^{n} x_{ab}, n_b = \sqrt{\frac{1}{n}\sum_{a=1}^{n}(d_{ab} - d_b)^2}$$

For $d'\alpha b \notin [0,1]$, it is necessary to build another process for the unique dimension.

$$d''_{ab} = \frac{d' - \min 1 \le a \le n\{d'_{ab}\}}{\max 1 \le a \le n\{d'_{ab}\} - \min 1 \le a \le n\{d'_{ab}\}}$$

The fuzzy correlation matrix $R=(d''ab)n \times t$ can be obtained.

By observing the spatial correlation of the data collected from those nodes, the similarity coefficient technique is used to build a fuzzy similarity matrix.

$$r_{ab} = \frac{\left|\sum_{k=1}^{t}(d_{ak}\ \bar{d}_b)(d_{bk} - \bar{d}_b)\right|}{\sqrt{\sum_{k=1}^{t}(d_{ak} - \bar{d}_a)^2}\sqrt{\sum_{k=1}^{t}(d_{bk} - \bar{d}_b)^2}}$$

$\lambda - trunction$ The matrix $R_\lambda = (r_{ab}(\lambda))$ is further reduced for related fuzzy matrices. Since R λ is a boolean matrix, the nodes' grouping depends upon the R's value λ is equal to 10r not. The particular rules for node grouping are as follows.

1. The nodes group will be maintained directly if the R and R λ matrix are equal.
2. If R λ is being converted into an equal Boolean matrix by following rules, grouping the nodes will not be applied.

In more detail, to get the nodes data similarity gap fuzzy matrix is used. By selecting λ_1=1 equal form of the class is created $[d_a]_R=\{d_a|r_{ab=1}\}$ for each d_a, the node d_b class attributes are mention if the condition is true.

By taking $\lambda_2(\lambda_2 < \lambda_1)$ the maximum value, the elements pair $(d_a\ d_b)$ with the similarity degree λ_2 can be found out from the matrix R, i.e $r_{ab} = \lambda_2$. So, by merging d_a and d_b in the equal grouping of λ_1 into one class, a similar collection on level λ_2 can be obtained. Let $\lambda_{1>}\lambda_{2>...}\lambda_k$ until S is merged into a single class. The number of categories for clustering K can be obtained.

The sensor nodes are divided into many groups based on the observed area's similarity degree after the clustering technique is applied. In every group, some nodes are selected redundant nodes to schedule for sleep to improve energy efficiency.

Let $d_a^{(a)}$ represents the number (i-th) of nodes in category V, and the number of nodes into category a can be defined ad $a = |d^{(v)}|, \sum_{a=1}^{k}|d^{(v)}| = n$ to measure the difference between the data being collected from the sensor nodes at time slot m. we have

$$Calculate\_Dis(n_a^{(v)}, d_b^{(v)}) = \sqrt{\sum_{a=1}^{t} (d_a^{(v)} - d_b)^2}$$

Information should not be lost when applied the sleep scheduling technique upon redundant nodes of the sensor nodes. The redundant nodes selection function is given below as.

$$n_*^{(a)} = \arg\min\{\sum_{a=a}^{v} \text{Calculate\_Dis}(n_a^{(v)}, n_b^{(v)})\}$$

Finally, $s_*^{(v)}$ it represents the nodes selected as redundant from the category.

Determine the Sensor nodes be selected to sleep.

For each CH

Build a garbage data matrix X;

Then the matrix D can be transformed into fuzzy matrix R;

The member nodes are grouped into K categories;

For each category V

For each node denoted as B, K belongs $n^{(v)}$

Calculate confidence distance Calcualte_Dis ($n_a^{(v)}$,$n_b^{(v)}$) between the data from node $n_a^{(v)}$,$n_b^{(v)}$)

$n_*^{(v)}$ = agr{**SUM** Calculate_Dis ($n_a^{(v)}$,$n_b^{(v)}$)}

End for

End for

Obtain redundant nodes set {R_1,R_2,……..R_t};

For each node belongs to {R1, R2…R_t}

Send Schdule_MSG (CH_id, id, Status_flag)

Receive Schdule_MSG_ACK;

End for

End for

IV. Experimental Analysis & Results

This section discussed the simulation evaluation results on different experimental environments of our proposed model. The proposed model evaluates different performance metrics points of view. In this work, EEDAM was compared with two protocols, EEHS (Paul & Sao, 2011) and ESSM (Wan et al., 2018). The detailed evaluation parameters are described in Table **1**. Edge server accuracy also assesses through the IoT device's feedback. As

shown in Figure 1, IoT devices are connected with an edge server for the service request, and the edge server is further associated with the cloud server for security and service code requirements. In blockchain technology, gas is the unit of how much transaction is executed in a period. The transaction is the set of activities that are performed in the blockchain environment. Every activity that is performed in the blockchain environment uses has gas consumption. Suppose more resources consuming in blockchain than more gas be destroyed than the normal blockchain task process—some gas consumption rates in blockchain technology already defined in the ethereum yellow paper (GAVIN WOOD, 2014).

One gas consumption= four gwei (one eth= 1000000000 GWEI)

3.1 Experimental Analysis: In this section, we analyze the efficiency and effectiveness of our proposed system through experiments. We simulated cloud servers on a single physical machine. Each of them behaves as an arbitration node in the consortium blockchain, which has the highest power as miners. We also simulated many edge devices to serve client nodes. There also exist IoT devices layer which requests to the edge server for specific service. The details of the cloud, edge, and IoT client devices are given in Table **2**. In Figs. **3** and **4,** the experimental results are shown. The values of the parameter α can be from 0.2, 0.5, and 0.8. It can also be observed that when the value is 0.5, the performance of the energy mean and variation are better than other conditions. It is because of the smaller value of the parameter α . As the value of the α is large, the distance factor becomes more critical.

Table 1Simulation Experiment Parameters

Parameters	Value
Network interface	Wireless
Number of nodes	100
Initial energy in each node	0.5 J
Round duration	10 s
BS location	(200,100) m
Network size	100x100 m
Packet Size	512 (bytes)
Residual energy threshold %	0.35
Data rate	1 abs
Distance threshold	75 m
Idle power	13.5 mW
Sleep power	15 IW
E_{elec}	50 nJ bit
E_{DA}	5 nJ/bit/signal
ε_{mp}	0.0013pJ/bit/m^4
εfs	10 PJ/bit/m2

Table 2: Testing Devices Specifications

Parameters	Edge Node	IoT Node	Cloud Server (Inclouding Blockchain)
ROM	512 GB	256 MB	1 TB
RAM	8 GB	4 GB	16 GB
Network	100 Mbps	100 Mbps	100 Mbps
CPU core	Dual-Core	Single-Core	Quad-Core
OS	Fedora (Vanilla 3.38)	Ubuntu Mate (20.10)	CentOS 7.0
CPU Frequency	2.6 GHz	512 MHz	3.4 MHz

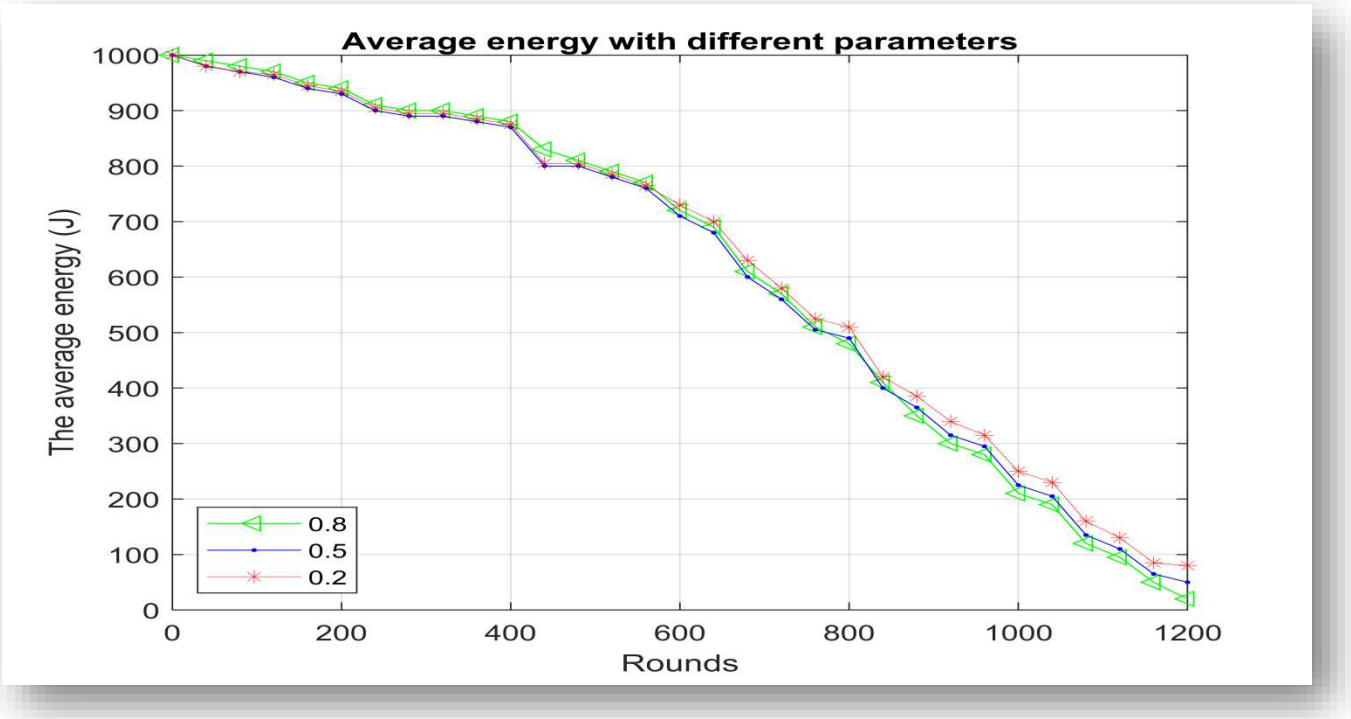

Figure 4 The average energy with different parameter

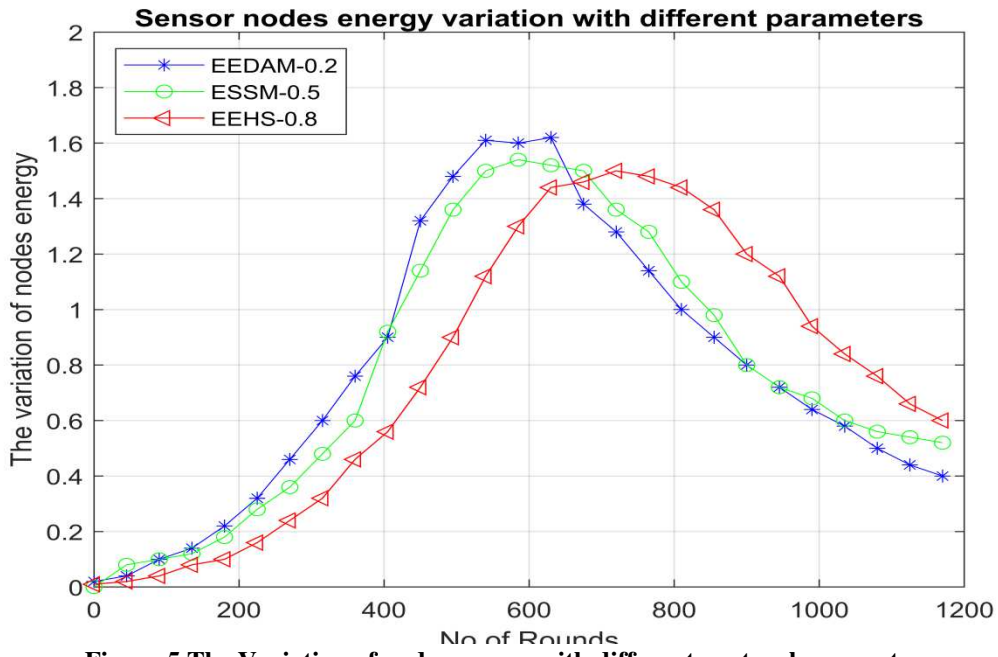

Figure 5 The Variation of nodes energy with different protocol parameters

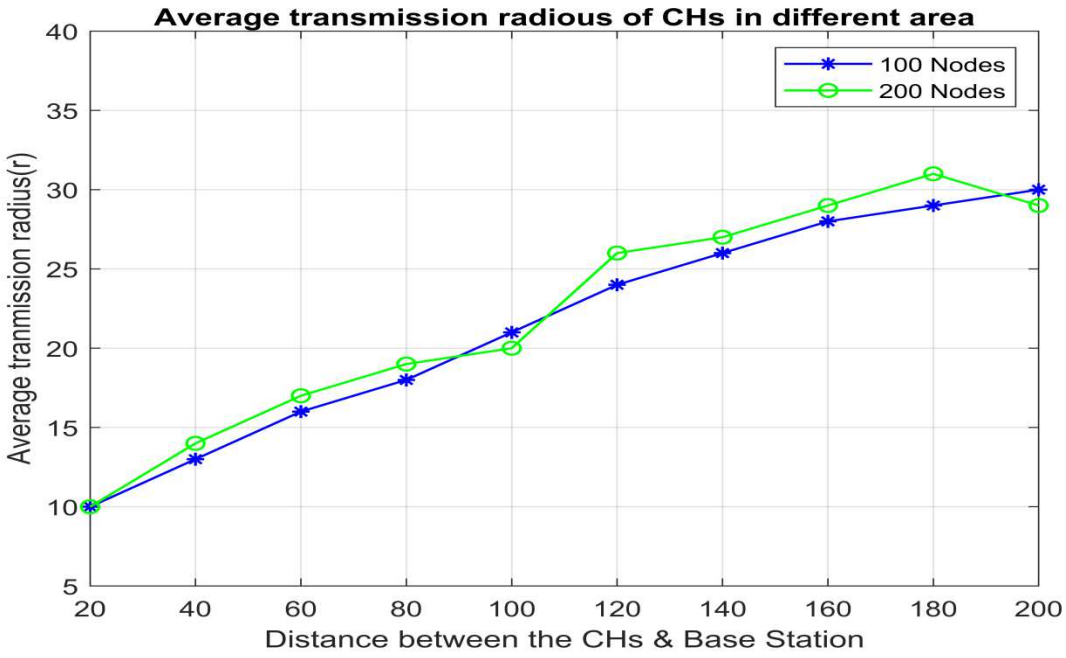

Figure 6 Average distance between sink and nodes

According to the previous analysis, select the parameter $\alpha = 0.5$ according to the different sensor node's densities. Then, the communication distance of the cluster head is analyzed, and the result is shown in Fig. **5**. It can be observed that the transmission radius of the CHs is smaller than other CHs near Sink. It is because the energy consumption by the CHs closely related to the distance between BS and CH in a single hope manner. Therefore, to save energy, fewer CHs should be distributed near the BS.

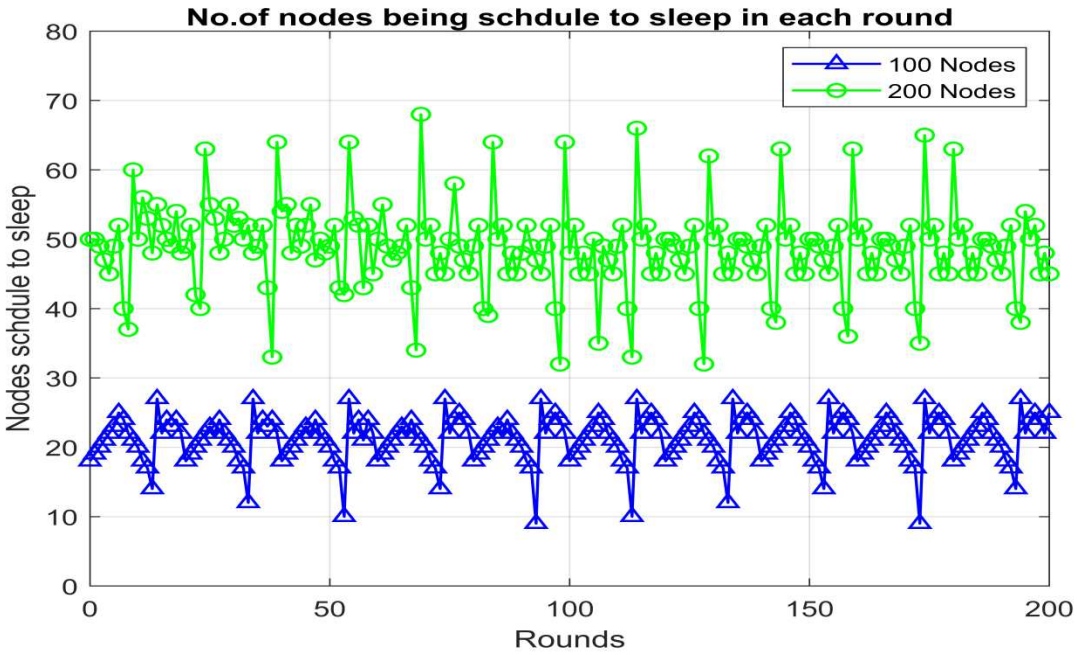

Figure 7 No of the sensor being schedule to sleep in each round of transmission

Furthermore, the average number of nodes is compared with different node densities in each round. For example, fig. 6 shows the number of dormant nodes is more than in low density. This is because due to the data correlation collected by the neighboring nodes, much higher and more dormant nodes being selected have subsequent data fusion. As a result, the number of nodes selected as redundant nodes scheduled to sleep is much higher. So as a result, we can find that the average number of dormant nodes at different densities is relatively stable, maintaining the average energy consumption among all nodes.

Next, the comparison between the CHs selection result is shown in Fig. 7 concerning node density. When the sensor node density is large, the number of CHs in EEHS is high than ESSM and EEDAM. The main reason is that EEHS main focus upon the cluster size overall energy consumption. It can be observed that the number of CHs selected by the EEDAM shows stability during many rounds and it is also not affected by the node density. Because of two factors: (1), The CHs selection is based upon the distance from BS and node's residual energy; (2) when the node's density is large and more redundant nodes are scheduled to sleep base on data correlation to save energy.

Figure 8 shows that the average time delay in data transmission. It can be observed that when the node's density is high, the time delay of the three algorithms is higher than the sparse node's density to increase the network throughput. In a single hope manner, CH aggregates the data from its member nodes and transmits it directly to BS. EEDAM can reduce time delay in the aspect of the efficiency of data transmission. Figure 9 shows data accuracy with a different number of nodes of EEHS, ESSM, and EEDAM. We can observe from the result as the number of nodes increases, data accuracy also increases. EEDAM shows the best performance in the aspect of data accuracy than EEHS and ESSM. In the proposed scheme, redundant nodes are selected based on the data correlation, and the

remaining nodes are enough to achieve the same level estimated level of data accuracy. Hence it is not compulsory to keep all nodes in active mode, which causes improved energy consumption improvement to achieve data accuracy.

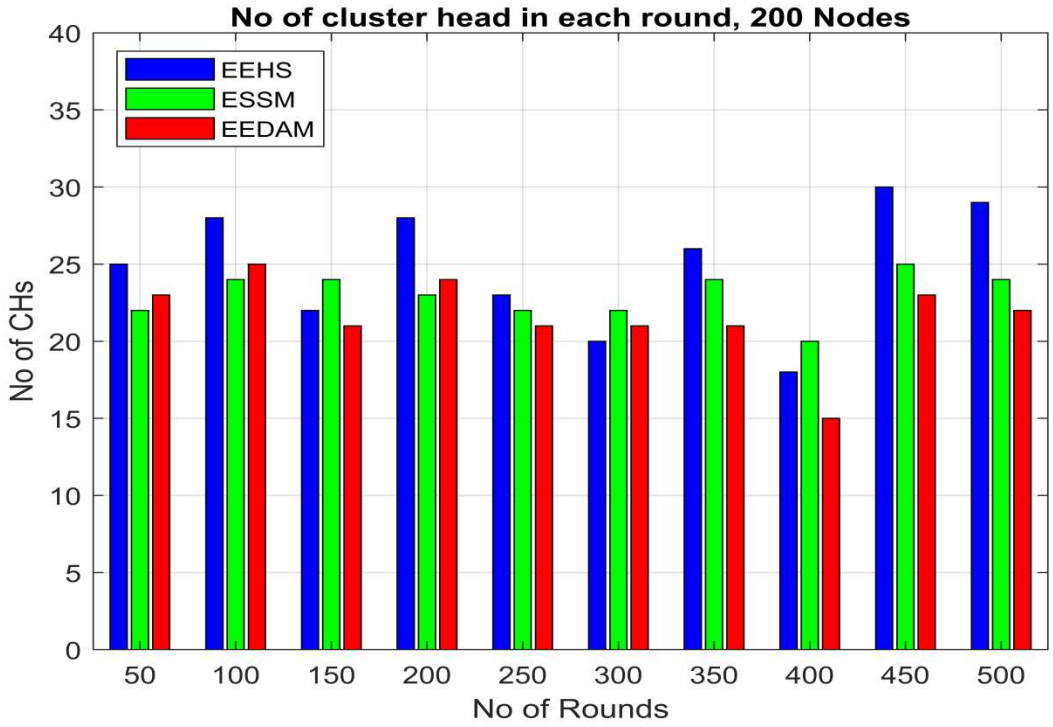

Figure 9 CHs selection comparison in each round, 200 Nodes

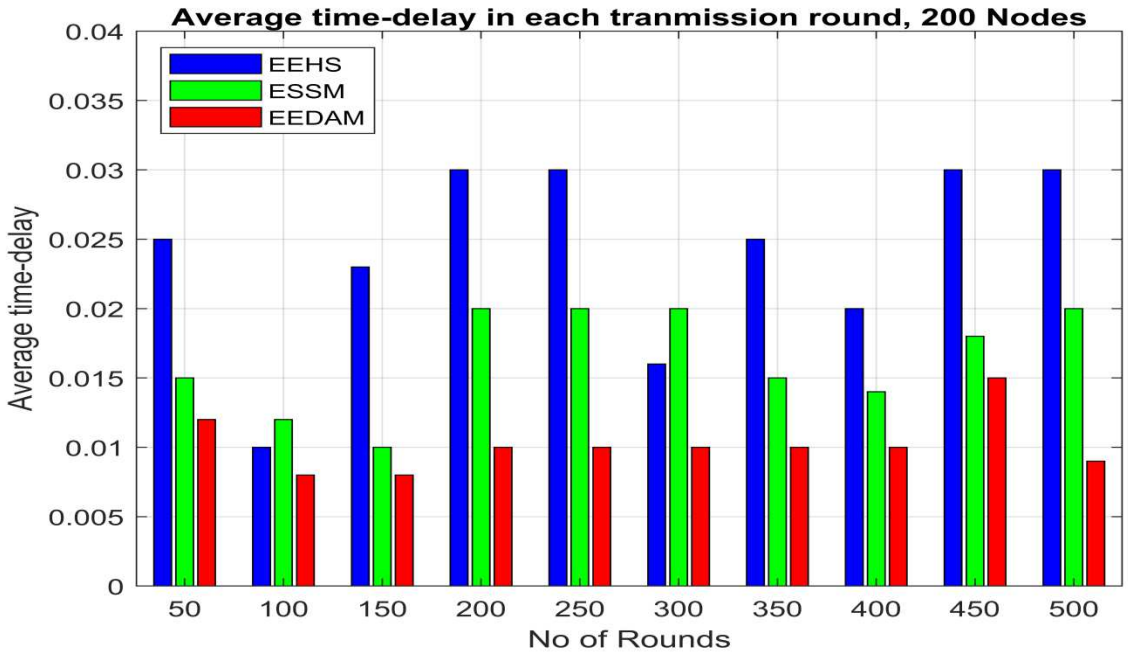

Figure 8 Average time delay in each transmission round

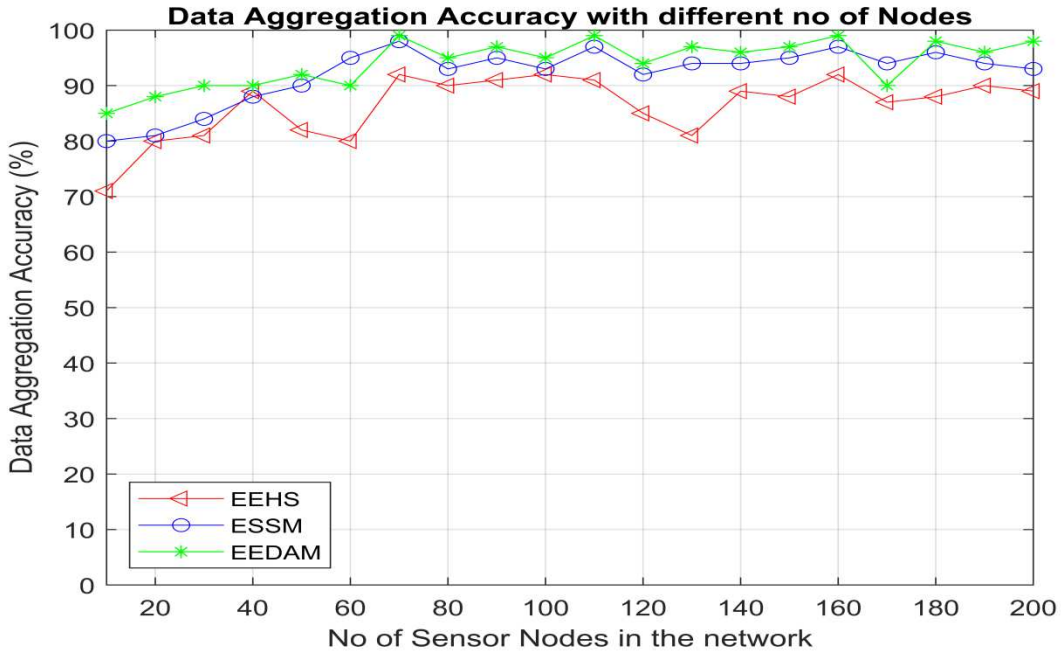

Figure 10 Data accuracy with different no of sensor nodes

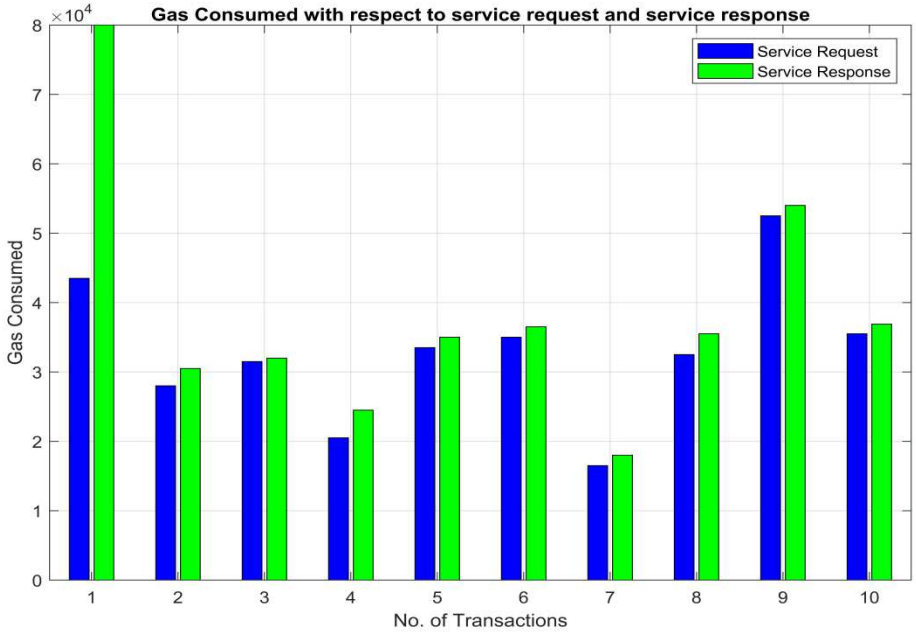

Figure 11 Gas consumed concerning service request & response

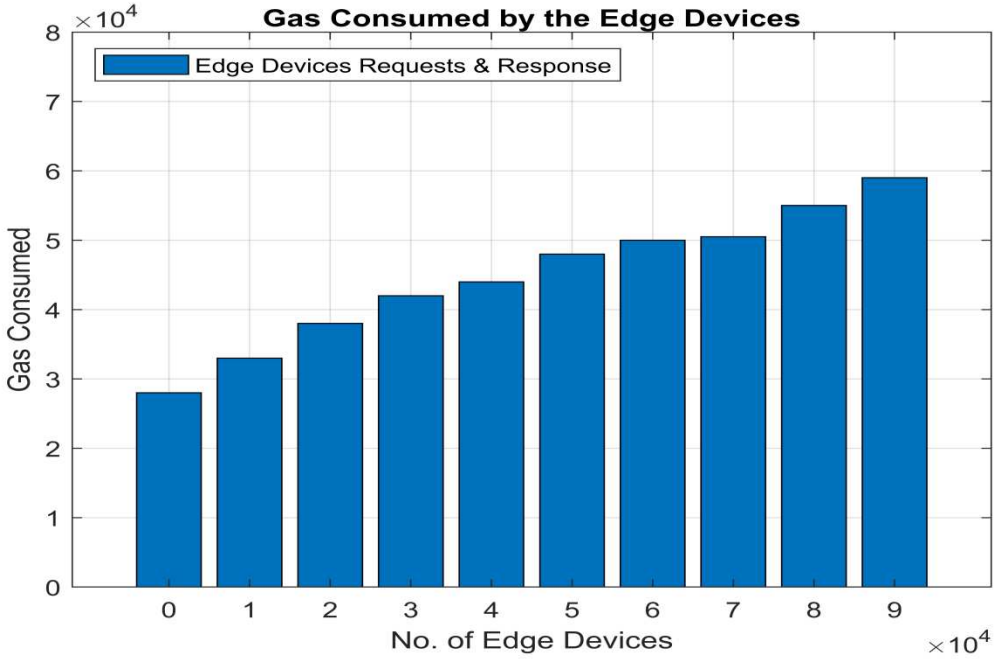

Figure 12 Gas consumed by the edge devices concerning service request & response

Figure **10** shows the analysis of the gas consumption of different service requests and responses. We take ten transactions having different services required by the IoT devices. The gas consumption depends on two different parameters the service size and the difficulty level of hash. As the essential service utilizes more bandwidth and resources, the gas consumption is also high than the average value. If the hash code generated by the hashing algorithm has many difficulties, more mining power is required, and execution time also increases. Fig. **11** shows the edge device's participation in the network and their gas consumption. When the IoT devices request to edge server for a service code at the start of the network, a small number of edge device requests are received at blockchain, and their gas consumption is not much higher. We simulate our proposed architecture EEDAM up to 100 edge devices. The results show there is a linear change in gas consumption concerning service requests and responses. Thus, the proposed system is scalable enough and achieves security by using blockchain emerging technology. With blockchain, no malicious edge device can communicate with the IoT network and the cloud server that contains blockchain technology.

After the IoT layer process work, the request will be sent to the edge server that will be deployed near the base station, authenticating the requesting IoT device. The IoT devices request the required service code to the edge server. Edge server looks in its cache memory which is used frequently and provide to the requested device.

Suppose the requested service code not in the edge server cache memory than the edge server request to the service code's cloud server. In the cloud infrastructure, blockchain is implemented. Cloud servers provide the requested service code to the edge server after the PoA process. Validation status and rating of the edge server given by the end-user will also store in the cloud server. For the security of the IoT-constrained devices from the un-trusted edge server, the edge server registration process is done at the cloud server to figure out the edge server validity. For the PoA of the edge server service code, the IoT device communicates with the cloud server and gets the hash code against the service code.

After this, an IoT device checks the hash code generated by the edge server and the cloud server. If the cloud server and IoT-constrained device cause both codes, then the service code request is valid, and it is also assumed that the edge server is not part of the malicious network. Validated states of the edge server are also updated in the blockchain. After getting the requested service code from the edge server, the IoT device gives the edge server feedback to encourage edge server usage in the network. The IoT devices' service feedback is stored in blockchain, which increases the edge server trust rating. With the Blockchain uses, security is achieved with Minimum overhead due to the edge server involvement.

III. Conclusion

This paper proposed an energy-efficient, secure, and data aggregation architecture that provides cloud-based architecture using Blockchain for IoT devices to meet the energy efficiency and security requirements. The edge server is used to reduce the cloud server load by providing the most frequently used service in its cache memory to serve the IoT devices. The proposed system is designed to protect IoT networks from malicious activities using blockchain technology and data co-relation reduction. Blockchain validates the edge server's validity and service provided by the edge server among the cloud server and IoT devices. The proposed system was also designed to support high availability. Real-time reduction, spatial data co-relation using fuzzy logic, high scalability, secures service provisioning, and low latency. Our performance evaluation results clearly show that our proposed model is energy efficient to offload the cloud server compared to traditional cloud servers using blockchain technology. It also indicates the model's effectiveness and efficiency and that it fulfills the essential design principles with minimum delay.

In the future, we will explore the various security and energy technique strategy of our proposed model for energy-efficient communication between the IoT devices at the edge of the core network.

IV. Declarations

Not applicable

V. Funding Not applicable

VI. Availability of data and material Data of the experiments and simulation available and can be provided on request

VII. Code availability code of the simulation is available

References

Alkadi, O., Moustafa, N., Turnbull, B., & Choo, K.-K. R. (2020). A Deep Blockchain Framework-enabled Collaborative Intrusion Detection for Protecting IoT and Cloud Networks. *IEEE Internet of Things Journal*, *4662*(c), 1–1. https://doi.org/10.1109/jiot.2020.2996590

Aloqaily, M., Bouachir, O., Boukerche, A., & Ridhawi, I. Al. (2021). Design Guidelines for Blockchain-Assisted 5G-UAV Networks. *IEEE Network*, *35*(1), 64–71. https://doi.org/10.1109/MNET.011.2000170

Apostolopoulos, P. A., Tsiropoulou, E. E., & Papavassiliou, S. (2020). Cognitive data offloading in mobile edge computing for internet of things. *IEEE Access*, *8*, 55736–55749. https://doi.org/10.1109/ACCESS.2020.2981837

Bhajantri, L. B., & Mujawar, T. (2019). A Survey of Cloud Computing Security Challenges, Issues and their Countermeasures. *Proceedings of the 3rd International Conference on I-SMAC IoT in Social, Mobile, Analytics and Cloud, I-SMAC 2019*, 376–380. https://doi.org/10.1109/I-SMAC47947.2019.9032545

Butun, I., Sari, A., & Österberg, P. (2018). Security implications of fog computing on the internet of things. *ArXiv*, *20201010*, 1–6.

Chawra, V. K., & Gupta, G. P. (2020). Load Balanced Node Clustering scheme using Improved Memetic Algorithm based Meta-heuristic Technique for Wireless Sensor Network. *Procedia Computer Science*, *167*(2019), 468–476. https://doi.org/10.1016/j.procs.2020.03.256

Chen, C., Fu, S., Jian, X., & Liu, M. (n.d.). *NOMA for Energy-Efficient LiFi-Enabled Bidirectional IoT Communication*. 1–30.

GAVIN WOOD. (2014). Ethereum: a secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*, *151*, 1–32.

Heinzelman, W. B., Chandrakasan, A. P., & Balakrishnan, H. (2002). An application-specific protocol architecture for wireless microsensor networks. *IEEE Transactions on Wireless Communications*, *1*(4), 660–670. https://doi.org/10.1109/TWC.2002.804190

Huong, T. T., Bac, T. P., Long, D. M., Thang, B. D., Binh, N. T., Luong, T. D., & Phuc, T. K. (2021). LocKedge: Low-Complexity Cyberattack Detection in IoT Edge Computing. *IEEE Access*, *9*, 29696–29710. https://doi.org/10.1109/ACCESS.2021.3058528

Khan, M. N., Rahman, H. U., Almaiah, M. A., Khan, M. Z., Khan, A., Raza, M., Al-Zahrani, M., Almomani, O., & Khan, R. (2020). Improving energy efficiency with content-based adaptive and dynamic scheduling in wireless sensor networks. *IEEE Access*, *8*, 176495–176520. https://doi.org/10.1109/ACCESS.2020.3026939

Li, Z., Zhong, R. Y., Tian, Z. G., Dai, H. N., Barenji, A. V., & Huang, G. Q. (2021). Industrial Blockchain: A state-of-the-art Survey. *Robotics and Computer-Integrated Manufacturing*, *70*(January). https://doi.org/10.1016/j.rcim.2021.102124

Liu, Y., Liu, A., Zhang, N., Liu, X., Ma, M., & Hu, Y. (2019). DDC: Dynamic duty cycle for improving delay and energy efficiency in wireless sensor networks. *Journal of Network and Computer Applications*, *131*(June 2018), 16–27. https://doi.org/10.1016/j.jnca.2019.01.022

Lockl, J., Schlatt, V., Schweizer, A., Urbach, N., & Harth, N. (2020). Toward Trust in Internet of Things Ecosystems: Design Principles for Blockchain-Based IoT Applications. *IEEE Transactions on Engineering Management*, *67*(4), 1256–1270. https://doi.org/10.1109/TEM.2020.2978014

Memon, R. A., Li, J. P., Ahmed, J., Nazeer, M. I., Ismail, M., & Ali, K. (2020). Cloud-based vs. blockchain-based IoT: a comparative survey and way forward. *Frontiers of Information Technology and Electronic Engineering*, *21*(4), 563–586. https://doi.org/10.1631/FITEE.1800343

Nguyen, D. C., Ding, M., Pham, Q.-V., Pathirana, P. N., Le, L. B., Seneviratne, A., Li, J., Niyato, D., & Poor, H. V. (2021). Federated Learning Meets Blockchain in Edge Computing: Opportunities and Challenges. *IEEE Internet of Things Journal*, 1–1. https://doi.org/10.1109/jiot.2021.3072611

Njah, Y., & Cheriet, M. (2021). Parallel Route Optimization and Service Assurance in Energy-Efficient Software-Defined Industrial IoT Networks. *IEEE Access*, *9*, 24682–24696. https://doi.org/10.1109/ACCESS.2021.3056931

Paul, S., & Sao, N. K. (2011). An energy efficient hybrid node scheduling scheme in cluster based wireless sensor networks. *Proceedings of the World Congress on Engineering 2011, WCE 2011*, *2*, 1775–1779.

Puthal, D., Mohanty, S. P., Wilson, S., & Choppali, U. (2021). Collaborative Edge Computing for Smart Villages. *IEEE Consumer Electronics Magazine*, *January*. https://doi.org/10.1109/MCE.2021.3051813

Rehman, M., Javaid, N., Awais, M., Imran, M., & Naseer, N. (2019). Cloud based secure service providing for IoTs using blockchain. *2019 IEEE Global Communications Conference, GLOBECOM 2019 - Proceedings*, *July*. https://doi.org/10.1109/GLOBECOM38437.2019.9013413

Serrano, W. (2021). The Blockchain Random Neural Network for cybersecure IoT and 5G infrastructure in Smart Cities. *Journal of Network and Computer Applications*, *175*(December 2020). https://doi.org/10.1016/j.jnca.2020.102909

Shah, S. W. H., Mian, A. N., Aijaz, A., Qadir, J., & Crowcroft, J. (2021). Energy-Efficient MAC for Cellular IoT: State-of-the-Art, Challenges, and Standardization. *IEEE Transactions on Green Communications and Networking*, 1–26. https://doi.org/10.1109/TGCN.2021.3062093

Sharma, P., Jindal, R., & Borah, M. D. (2020). Blockchain Technology for Cloud Storage: A Systematic Literature Review. *ACM Computing Surveys*, *53*(4). https://doi.org/10.1145/3403954

Shifa, A., Asghar, M. N., Ahmed, A., & Fleury, M. (2020). Fuzzy-logic threat classification for multi-level selective encryption over real-time video streams. Journal of Ambient Intelligence and Humanized Computing, 11(11), 5369-5397.

Singh, G. (2019). Internet-of-things with blockchain technology: State-of-the art and potential challenges. *Handbook of Multimedia Information Security: Techniques and Applications*, 775–795. https://doi.org/10.1007/978-3-030-15887-3_37

Singh, P., Nayyar, A., Kaur, A., & Ghosh, U. (2020). Blockchain and fog based architecture for internet of everything in smart cities. *Future Internet*, *12*(4), 1–12. https://doi.org/10.3390/FI12040061

Tange, K., De Donno, M., Fafoutis, X., & Dragoni, N. (2020). A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities. *IEEE Communications Surveys and Tutorials*, *22*(4), 2489–2520. https://doi.org/10.1109/COMST.2020.3011208

Tseng, L., Wong, L., Otoum, S., Aloqaily, M., & Othman, J. Ben. (2020). Blockchain for Managing Heterogeneous Internet of Things: A Perspective Architecture. *IEEE Network*, *34*(1), 16–23. https://doi.org/10.1109/MNET.001.1900103

Tseng, C. Te, & Shang, S. S. C. (2021). Exploring the sustainability of the intermediary role in blockchain. *Sustainability (Switzerland)*, *13*(4), 1–21. https://doi.org/10.3390/su13041936

Venugopal, K. R., T., S. P., & Kumaraswamy, M. (2020). LRTHR: Link-Reliability Based Two-Hop Routing for WSNs. In *QoS Routing Algorithms for Wireless Sensor Networks*. https://doi.org/10.1007/978-981-15-2720-3_2

Verma, R. K., Pattanaik, K. K., & Bharti, S. (2020). Query similarity index based query preprocessing mechanism for multiapplication sharing wireless sensor networks. *Telecommunication Systems*, *74*(4), 477–485. https://doi.org/10.1007/s11235-020-00667-9

Wan, R., Xiong, N., & Loc, N. T. (2018). An energy-efficient sleep scheduling mechanism with similarity measure for wireless sensor networks. *Human-Centric Computing and Information Sciences*, *8*(1). https://doi.org/10.1186/s13673-018-0141-x

Wang, D. H. (2020). IoT based Clinical Sensor Data Management and Transfer using Blockchain Technology. *Journal of ISMAC*, *2*(3), 154–159. https://doi.org/10.36548/jismac.2020.3.003

Xu, T., Wang, X., Su, T., Wan, L., & Sun, L. (2021). Vehicle Location in Edge Computing Enabling IoTs Based on Bistatic FDA-MIMO Radar. *IEEE Access*, *9*, 46398–46408. https://doi.org/10.1109/ACCESS.2021.3064849

Yun, W. K., & Yoo, S. J. (2021). Q-Learning-based data-aggregation-aware energy-efficient routing protocol for wireless sensor networks. *IEEE Access*, *9*, 10737–10750. https://doi.org/10.1109/ACCESS.2021.3051360

Zhang, P., Zhou, M. C., & Wang, X. (2020). An Intelligent Optimization Method for Optimal Virtual Machine Allocation in Cloud Data Centers. *IEEE Transactions on Automation Science and Engineering*, *17*(4), 1725–1735. https://doi.org/10.1109/TASE.2020.2975225