Received January 1, 2022, accepted January 22, 2022, date of publication January 25, 2022, date of current version February 1, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3146295

An Energy-Efficient Data Aggregation Mechanism for IoT Secured by Blockchain

ADEEL AHMED, SAIMA ABDULLAH, MUHAMMAD BUKHSH, ISRAR AHMAD, AND ZAIGHAM MUSHTAQ
Department of Computer Science, Faculty of Computing, The Islamia University of Bahawalpur, Bahawalpur, Punjab 63100, Pakistan
Corresponding author: Muhammad Bukhsh (muhammadbukhsh316@gmail.com)

ABSTRACT The Internet of Things (IoT) is getting important and interconnected technologies of the world, consisting of sensor devices. The internet is smoothly changing from an internet of people towards an Internet of Things, which permits various objects to connect to another wirelessly. The energy consumption of the IoT routing protocol can affect the network life span. In addition, the high volume of data produced by IoT will result in transmission collision, security issues, and energy dissipation due to increased 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 mode and others into wake mode. Therefore, it is important to group the nodes with high data similarity using the fuzzy matrix. Then, the data received from the member nodes at the Cluster Head (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 costs. We have proposed an Energy-Efficient Data Aggregation Mechanism (EEDAM) secured by blockchain, which uses a data aggregation mechanism at the cluster level to save energy. As edge computing is used to provide on-demand trusted services to IoT with 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 the IoT, and extend the wireless sensor network (WSN).

INDEX TERMS Edge computing, blockchain, energy efficiency, security, IoT systems, availability, wireless sensor networks.

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. Consequently, this architecture has changed with the invention of the Internet of Thing (IoT). The IoT includes intelligent devices, such as sensors, smart home devices, intelligent cars, industrial areas, and utilities, which can communicate through the internet and are integrated with data analysis capabilities. This paradigm has changed the way we live, play, and work. IoT devices account for a massive volume of data streams at high speeds. With a flexible and efficient security service provisioning the cloud base architecture [1], a vast amount of IoT device data formed by IoT cluster networks can be communicated to the remote edge cloud for further processing through the network [2], [3]. However, the internet is not effectively efficient and scalable, so it cannot deal with this massive volume of IoT data. Also, the processing and transfer of necessary data is expensive, consumes 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 cloud and IoT devices [4]. Recently, cloud-based frameworks were

The associate editor coordinating the review of this manuscript and approving it for publication was Arun Prakash.

broadly researched due to the restricted computing resources of IoT devices and the increasing demand for cloud services. Currently, research shows that cloud servers are not providing satisfactory services to the end-user. Edge computing is considered the extension of the cloud server services. The use of edge transparent computing executes the cloud server's processing and manages storage 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, IoT-constrained device's functionalities increase. There is a need for protocol and standard layers, like edge computing, to provide security services to IoT networks to control the huge amount of data generated by them. The existing cloud server is a 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 congestion problems, bandwidth problems, delays, security issues, or a single point of failure. Therefore, there is a need for a decentralized architecture for IoT networks to establish local storage, computing, and protection to overcome these issues. Currently, there are some existing decentralized architectures for large-scale IoT networks. However, security and privacy issues are not considered in this architecture [5]–[7]. We conclude, from existing research, that there is a paradigm for protecting the IoT devices from security threats, eliminating data redundancy and illegal service providers in the network. With the limited resources and market scope, fog computing cannot provide efficient, reliable, and secure services to the end-user [8]. IoT devices' future goals require resources, like the ability to be scalable, protected, with sufficient processing power. Therefore, decentralized cloud architecture must achieve the maximum objectives of IoT-constrained devices. Currently, blockchain is widely researched due to its growing demand in the industry and decentralized property [9], [10]. The primary purpose of using blockchain technology is to operate in a decentralized model in a properly secure manner. The current research indicates that the latest technologies, including blockchain and Bitcoin, are the finance domain's future [11], [12].

The invention of blockchain overcomes the limitation problem of centralized architecture; it provides excellent functionalities, like security, decentralized architecture, as well as a transparent system. Blockchain is also used for secure and efficient data transmission. However, blockchain architectures for IoT devices causes low throughput, low latency, and delay-like issues, as current blockchain systems are using high processing power and storage. On the other hand, IoT-constrained devices lack these resources. At present, different companies offer decentralized architecture and storage capacity. Recently, to overcome the server and maintenance cost problems, most of these organizations have shifted to cloud servers. These changes motivated us to trust the third party for cloud services for processing and storage. In addition, due to the low cost of maintenance and storage, we must trust other parties for encrypting our sensitive data. Existing architecture that works 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 can sell their extra storage capacity to renters, who can make payments through blockchain with established security and trust. The world economic forum's survey predicted that by 2027, 10% of the world's GDP might be stored on blockchain infrastructure [13]. 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 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, providing 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 these transactions that occur in the network are stored in cloud network infrastructure. Currently, cluster techniques are primarily used in wireless sensor networks. The low-energy adaptive cluster hierarchy (LEACH) protocol, proposed by Heinzelman, is a micro-sensor network organization which increases energy efficiency and a network's lifespan, [14]. There is an improved version of the LEACH protocol for selecting the cluster head and enabling an energy consumption balance [15]. In addition, the dynamic sleep scheduling mode is better than the fixed sleep scheduling method, as it can also improve the network's lifetime [16]. The aggregation of a cluster-based data analysis system is proposed by [17]. The sleep scheduling scheme [18] analyzes some factors, like node distance to cluster head, residual energy, coverage ratio, and schedule. A two-tier distributed fuzzy logic-based protocol (TTDFP) is proposed to enhance the data aggregation operations in multihope wireless sensor network. For better use of energy clustering is used [19]. [20] Proposed a modified an energy efficient clonal selection algorithm (CLONALG-M) for rule-based clustering algorithms. Security aspect in wireless sensor network is most important. How the security requirements, efficiency aspect and accuracy can be affected by each attack in WSN's. A defense system and security attacks in WSN's are discussed to fulfill the security requirements [21].

The 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 [22]. A high-level hybrid IoT method uses blockchain, cloud, edge, and fog to reduce the limitations of each architecture [23]. A deep blockchain framework [24] is designed to protect IoT networks using smart contracts for security and privacy services. [25] presents the Blockchain Random Neural Network for cyber security users and the technique for the authentication, which saves the network from security breaches using blockchain infrastructure. Blockchain infrastructure is proposed to meet the dynamic user security requirements to access network supply in a 5G network environment [26]. Route optimization and service assurance (ROSA) is proposed for low latency communication in an industrial IoT network for energy efficiency [27]. A comprehensive survey on the energy efficiency of medium access control for cellular IoT is presented on the source of energy dissipation [28]. An adaptive channel [29] and a QoS approach are proposed for IoT bidirectional communication for energy efficiency and green computing. Edge computing is used for enabling the rapid detection of vehicle locations within IoT [30]. The Federated learning approach identifies the resource allocation, communication cost, privacy, and protection for edge data using blockchain [31]. 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 [32]. Lockedge [33] proposed an edge cloud infrastructure that fulfills the edge layer's detection requirements to ensure a 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 [34]. Data transmitted by the cluster head can be intercepted and may contain security and privacy issues. The IoT constrained devices' performance and functionalities rise by using increasingly 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 occur 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 within the IoT-based networks.

Research contributions:

- This paper proposes an energy-efficient and secure system for IoT based devices. 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 the convenience of security issues.
- A fuzzy based algorithm is also used for data aggregation in the IoT layer to reduce redundancy and network traffic, which in turn, will increase the system's performance.
- The most frequently used services will be provided to the requesting IoT devices present in the cache of the edge server.
- Blockchain infrastructure is also used for the registration process of newly requesting IoT devices. After the registration process, the requested service code is provided through the cloud server to the IoT system.

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

Section II discusses the related work. Section III presents the decentralized architecture using the emerging technology of blockchain to validate the edge server and services provided to the IoT devices from the proposed energy efficient data aggregation system; Section IV demonstrates the simulation results and performance from different points of view. Finally, section V suggests future work and the conclusion.

II. RELATED WORK

The cloud and IoT is widely used to check the excellence and rank of the water reservoir in real-time; currently, it is used to monitor and acquire the dam health to prevent the need to take action. In the proposed research, cloud node based IoT sensors will collect data and transmit them to the dam management system. This system is blockchain-based architecture, which offers security, confirmation, storage, data integrity, traceability of the deliverance job within the monitoring cloud system and reimbursement of all stakeholders that are liable for the delivery and sensing tasks [35]. Currently, there is an emphasis on the addition of cloud, fog computing, and edge computing infrastructure with IoT to support its execution and intensive computing applications. Many real-world systems try to aid such additions, relating to independence, security, supply management, and multiple application processing. This research proposes an integration framework named fog bus that will facilitate end to end IoT fog computing, edge computing, and cloud computing integration, which can help developers assemble IoT applications, while also allowing users to process different request at the same time and control their components [36].

In recent years, IoT has been implemented in many real-world applications, like fast shipping and smart city infrastructure, to ensure the accessibility and convenience of human life. With the increase in the use of IoT end-devices, a vast amount of sensing data is produced from IoT based networks. In the analysis of significant data issues, artificial intelligence plays an essential role in delivering scalable results in big real-world data. The vital purpose of this research is to develop artificial intelligence and a blockchain-based mechanism to analyze significant real-world data. The proposed system is a blockchain-based intelligent IoT framework, which supports real-world applications by converging blockchain technology and AI [37].

Medical care is an essential part of human life, leading to a remarkable rise in data issues regarding preventive health measures. For better treatment and diagnosis processes, health care specialists adopt IoT based wearable mechanisms; therefore, using IoT devices for remotely monitoring patient treatment and care is common nowadays. However, these architectures also cause many privacy and security issues related to data transmission. The proposed research system is blockchain-based to provide the security of this data concerning health management, as well as analysis of the big data from healthcare to end delays in the treatment process and ultimately save patients' lives. Modern blockchain-based systems for IoT end-devices are based on a circulated environment, which is secure and suitable for advanced cryptographic primitives [38]. The old blockchain-based technology data transmission methods in IoT have low-security mechanisms and high processing costs with a significant amount of data produced, which is difficult to manage. This research proposes a blockchain-based dynamic, secure data communication mechanism, which is designed to recognize reliability, similar to power data communication. Moreover, the system has a suitable arrangement in sharing management and decentralization [39]. Edge computing plays an important role in smart computing for data processing and the convenience of security issues. The proposed system solves the aforementioned security problems by using a blockchain-based mechanism with reproduction coding to improve the reliability and security issues of the stored data in edge computing. A worldwide blockchain in the cloud service provisioning layer and a local blockchain is established within the IoT. Moreover, the data encryption scheme used to increase the consistency of data storage spaces in blockchain also facilitates a technique for verification and validation, which has standards of data to guarantee the reliability of the data stored in the global blockchain provides security to resource constrained devices IoT from external attacks. Optimal usage of the blockchain in IoT environment is that it reduces computation power for energy efficiency. Local edge server directly connected with the block chain for validation and verification of the IoT devices. All processing power done by the edge server, in this regard energy efficiency increase in resource constrained IoT devices [40].

IoT based mechanisms provide vital real-world applications, such as control systems, smart devices grids, privacy and security, and observation systems, which are very dependent on cloud-based system networks. However, the IoT end-devices collect data from the environment and forward it to cloud-based modules above the wireless family for data storage, data analysis, and decision-making. Furthermore, the transmitted data becomes insecure within the cloud storage. In this research, a blockchain-based protected data provisioning architecture for a cloud-based IoT network uses the public property of the blockchain technology's smart contracts [41]. There are two conventional data trade methods: data hosting and the data aggregation model. The above mentioned two trading methods cause data owners to become doubtful of communicating on different systems over the wireless sensor networks. In this paper, the researchers propose a solution for data sharing, which replaces smart contracts using secure blockchain technology and machine learning, The data communication smart contract using blockchain technology effectively scores the trust of the third data sharing agent [42].

Fog computing is a new architecture that enables the communication between the cloud and the intelligent edge computing devices placed at the edge of the wireless communication network. The fog platform has many properties popular with IoT based systems, like easy access to data, minimum latency, and location discovery. Data collection is a familiar aspect of IoT-based networks. On the other hand, data transmission in fog enabled IoT environments is a big issue for security and privacy of aggregated sensitive data. The proposed system, (A device-oriented Anonymous Privacy-Preserving scheme) APPA, has confirmation for data transmission and aggregation in fog enabled IoT system [43]. Electric Vehicles Cloud and Edge (EVCE) is a convenient network model using wireless connections between heterogeneous traffic communications. There may be mutual information and energy relations, and there are many severe privacy and security issues for such a cross cloud platform and edge system. The proposed system is stimulated by blockchain data coins, with energy-related coins being used to attain the data contribution level and verification of effort. All privacy and security measures are offered to secure the network data traffic between edge computing and the cloud platform [44]. The utilization of the IoT has introduced many security issues when data is in a collection from the network cluster. Blockchain technology may increase the IoT's inherent privacy and security, data aggregation reliability, and data administration. This article proposes a data related method for on-chain data allotment in the IoT blockchain system. Moreover, a designed system for the data organizer using fuzzy logic for the calculation of the Rating of Allocation value requests different situation parameters, i.e., data, network and excellence [45]. This research facilitates a complete assessment of the latest technology in the significant development of implementing blockchain in smart home-based systems. This article also discusses the many latest blockchain-based applications for intelligent homes [46].

To address the security vulnerabilities in IoT based infrastructure, including reliability, certification, and accessibility, the authors of this research, propose a blockchain-based smart home access network that defends against possible attacks on IoT based smart homes. The system contains three different layers; gateway, device, and cloud platform layers. Blockchain is implemented in the smart home gateway layer wherein data is communicated in the shape of blocks to eliminate the issues of possible attacks [47].

Blockchain is a beneficial technology that has many uses other than the privacy and security of currency-related problems. This article is a literature review analysis on blockchain in IoT, which may still enforce a range of security and privacy issues and challenges. Moreover, this article recognizes the five critical mechanisms withdrawing consideration and problems that should be measured while implementing blockchain for IoT based architectures. This research also highlights the gaps that obstruct the creation of protected blockchain structures for IoT end-devices [48].

In the IoT, data blocks are collected and packetized from a variety of sensors, which are installed in different locations, with data being transferred across various networks. This paper proposes a packetized scheme for IoT devices, which uses ZigBee, which is an open international standard to tackle the single need of low-cost, low-power wireless IoT network. In the proposed system, data is collected, aggregated and bundled into a packet for transmission. The performance of these mechanisms is discussed, and the execution of the system is elaborated to demonstrate their validation and verification [49].

A blockchain platform is a circulated and decentralized ledger that consists of blocks of money transactions for data storage. Blockchain also guarantees tamper-proof storage of allowed operations. A big test in the development of blockchain is the hosting of the site for the storage blocks. This research evaluates the use of cloud computing and fog computing as hosting platforms for blockchain [50]. The authors of this research propose a lightweight blockchain platform called Light Chain, which is resource-efficient application for power-constrained IoT devices. Specifically, it presents green computing for stimulating the collaboration of the IoT policy, and a lightweight data mechanism called Light Block to update and transmit data contents. Moreover, it designs a new disparate block, which off-load passes through a filter to save from the limitless development of the blockchain ledger, which lacks blockchain monitoring [51]. The integration of blockchain and the IoT's primary purpose is to construct a protected and reliable communication infrastructure. Therefore, the main dispute is to recognize a suitable location for the blockchain in the present system of the IoT with minimum penalties. In this research, the blockchain-based DualFog-IoT mechanism has three design filters with external requirements at the entrance level, including real-time, non-real time, and hindrance liberal blockchain applications. The DualFog-IoT segregates the fog level into two parts: the fog computing cluster and the fog mining cluster. The fog cloud cluster is dedicated to the IoT based network for real-time transmission, while fog mining is committed to fixing network traffic of data transmission [52]. The recent expansion of the IoT and the ensuing outburst in data quantity formed by IoT is a significant issue. However, to manage this substantial volume of data provisions, central data stations, such as cloud computing storage spaces, cannot pay for the suspected source for the transmission. This article presents a new blockchain-based circulated cloud design with (SDN) software-defined networking, which enables the control fog computing at the edge of the network to fulfill the necessary design requirements. The proposed model distributes cloud infrastructure based on blockchain, which provides secure, low-cost, and on-request entrée to the most viable architecture in an IoT based network [53].

To overcome the edge failure problems, a latency aware algorithm, which replaces the edge with a new edge device for high availability and reliability for network traffic, has been established [54]. It proposes an energy efficient method with fault tolerance for the IoT system. It is a novel approach for the cluster broker selection by considering the backup sensor node when the head fails [55]. There is a need for blockchain in cloud architecture, which is the new technology for security on the blocks. This unique idea currently attracts researchers who have recognized blockchain technology for the cloud infrastructure's security services. The reasons for blockchains need for 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, which are disbursed worldwide.

Resource services: on the requested assistance from 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 their 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, there is increased security and low cost for each host. With the comparison of the cost, blockchains cost is $2 per terabyte, per month, and Amazon S3's cost is $25 per terabyte, per month.

Quality of services: The blockchain technology can trace the use of its resources to verify the client and service provider's service level agreement.

There are requirements for the securely distributed infrastructure in an IoT scalable network using edge computing. The design is a high-performance system using 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 a different network edge, the nodes must be used 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's 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 the decentralized IoT architecture. Confidentiality and data security are the main key points to ensure the network's design.

Required principles for energy efficiency in the IoT network:

Cluster organization: IoT networks are divided into clusters using a fuzzy matrix on the base with high data similarity to save the IoT network's energy to prolong the network's 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 active and passive modes for data transfer due to the deployment of the same monitoring area, which saves the nodes' energy.

The previous section presented the expansion principles of the IoT-based decentralized architecture for the new communication infrastructure. We found that the existing cloud-based system can fulfill the user-distributed requirements. Simultaneously, there are still growing demands within the researcher communities for efficient processing powers to process the enormous volume of data produced by the IoT and 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 enforced to implement different policies within an edge computing model. Edge computing provides storage and processing power services 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 and categorized without the involvement of the network and cloud server. The edge mitigates the cloud's computing power, storage, and network traffic and analyzes the IoT network's raw data. However, the secure and efficient deployment of the edge nodes to facilitate the communication between the cloud server and edge nodes is always a 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 the emerging technology, blockchain and edge computing, to meet the current and future requirements to provide secure services to IoT networks.

III. PROPOSED EEDAM FRAMEWORK

Figure **1** presents the overview of the proposed decentralized system, organized into three different layers, i.e., IoT devices, the edge server, the cloud layer, including the 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 of the IoT monitored area. The local base station is edge server which receives data from IoT devices. After receiving the service request from IoT device the edge server checks its cache for most recently used services, if the requested service exist in its cache, the edge respond immediately to the IoT device. If the service not exists in the edge server cache, then the edge server requests to cloud server for service request. After receiving the request from the edge server cloud server checks the requested service and edge server. After the validation of the edge server the cloud server register the requesting edge server and provides the required service with proper security. IoT devices are location unaware devices, and a unique id is assigned to all devices for identification. The sensor nodes detect signal strength, estimate the 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 that the collected data is relevant, perfect, and data packets can be of equal size for transmission over the network. The energy consumed for each round of data transmission can be calculated based on the IoT devices' data reception and communication.

A. PROPOSED EEDAM (AN ENERGY EFFICIENT DATA AGGREGATION MECHANISM FOR IoT SYSTEM) ALGORITHM

For the estimate of energy consumption, the First Order Radio [56] is exploited. The energy consumed for transmission of N-bit packets from the sender to receiver at a distance (d) can be defined as. Where E_{elec} is the dissipated energy used to transmit one bit by the transmitter and the receiver circuit, d is the transmission distance. εfs and εmp are the amplifying energy for multi path channel and free space architecture. So the energy being spent for receiving and transmission is given as [57].

$$E_{Tx}\begin{cases} lE_{elec}+l\varepsilon fsd^2, & d<d_0\\ lE_{elec}+l\varepsilon mpd^4, & d\geq d_0\end{cases} \tag{1}$$

For monitoring the controlled area, IoT nodes are circulated in the monitoring area. The data collected from this area contains spatial co-relation. To reduce energy usage, we will turn some nodes to sleeping mode. In addition, some nodes will be turned to wake mode to save energy. Our work's primary focus is on a sleep schedule, which is critical for data redundancy and communication variance. By converting the node into a dormant state, sleep and scheduling methods will save significant energy. The main work is 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 ensure 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. The cooperation between two nodes, Na and Nb, can be calculated by the deployment distance using function calculate_Dis(a, b). The distance is much longer between the nodes than the data collected from the nodes assuming there is no 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.

$$N=\{N_1,N_2,\ldots N_n\} \tag{2}$$

Suppose sensor network represents the number of deployed member nodes in the cluster, and n shows the total number

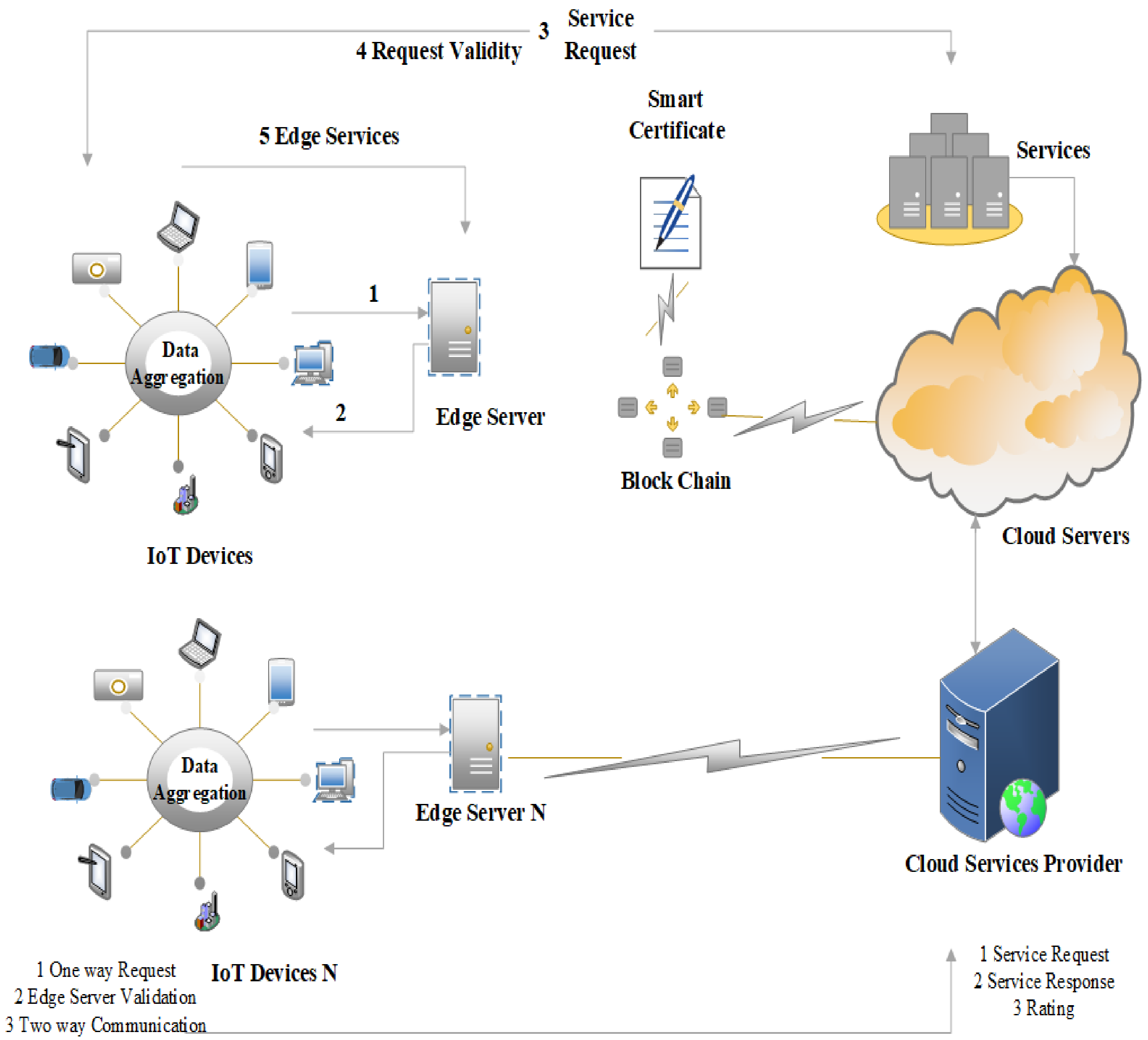

FIGURE 1. **Proposed system architecture.**

of sensor nodes in the cluster. The data collection time from the observed objects are divided into t intervals, and Da, b represents the data gathered by that member node Sa at time u. Thus, the data collected in the matrix can be defined as D = (Dab)n * t.

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

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

$$\bar{d}_b = \frac{1}{n}\sum\nolimits_{b=1}^{n} x_{ab}, \quad \mathrm{n}_b = \sqrt{\frac{1}{n}\sum_{a=1}^{n}(\mathrm{d}_{ab} - d_b)^2} \qquad (3)$$

For d′αb ∉ [0, 1], it is necessary to build another process for the unique dimension.

$$d''_{ab} = \frac{d' - \min 1 \le a \le n\{\mathrm{d}'_{ab}\}}{\max 1 \le a \le n\{\mathrm{d}'_{ab}\} - \min 1 \le a \le n\{\mathrm{d}'_{ab}\}} \qquad (4)$$

The fuzzy correlation matrix R = (d″ab)n × 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.

$$r_{ab} = \frac{|\sum_{k=1}^{t}(\mathrm{d}_{ak}\bar{d}_b)(\mathrm{d}_{bk} - \bar{d}_b)|}{\sqrt{\sum_{k=1}^{t}(\mathrm{d}_{ak} - \bar{d}_a)^2}\sqrt{\sum_{k=1}^{t}(\mathrm{d}_{bk} - \bar{d}_b)^2}} \qquad (5)$$

$\lambda - trunction$ 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 being equal to 10r. 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.

Essentially, to get a data similarity gap in the nodes, the fuzzy matrix is used. By selecting $\lambda_{1=1}$ equal form of the class is created $[da]R = \{dalrab = 1\}$ for each da, the node db class attributes are mentioned 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 da and db in the equal grouping of λ_1 into one class, a similar collection on level λ_2 can be obtained. $\lambda_1 > \lambda_2 > \ldots \lambda_k$ 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 as redundant nodes to schedule for sleep to improve energy efficiency.

$d_a^{(a)}$ represents the number (i-th) of nodes in category V, and the number of nodes into category a can be defined as:

$$a = |d^{(v)}|, \quad \sum_{a=1}^{k} |d^{(v)}| = n \tag{6}$$

to measure the difference between the data being collected from the sensor nodes at time slot m. we have:

$$Calculate\_Dis(n_a^{(v)}, d_b^{(v)}) = \sqrt{\sum_{a=1}^{t} (d_a^{(v)} - d_b)^2} \tag{7}$$

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

$$n_*^{(a)} = \arg\min\{\sum_{a=a}^{v} \text{Calculate\_Dis}(n_a^{(v)}, n_b^{(v)})\} \tag{8}$$

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

B. EEDAM ALGORITHM

The proposed algorithm energy efficient data aggregation mechanism has following 4 main processing operations regarding the time complexity.

A. In first processing operation clustering process and Cluster head selection (CH) of the nodes using fuzzy rule-based algorithm EEDAM is performed.
Cost: No. of nodes × CH's nodes
Mathematical bound
Member nodes = MN
CH's nodes = CHN
T (n) := O (CHN × MN)

B. Furthermore, in second processing operation distance calculation from CH's to member nodes is performed.
Cost: member's nodes: T (n) := O (CHN)

C. In the third step message transmission from member node to CH's is calculated.
Cost: no of member nodes
T (n) := O (CHN)

D. In the last step cost of number of member nodes schedule to sleep and schedule to active mode is calculated which is proportionally to the no of member nodes.
Cost: no of member nodes.
T (n) := O (CHN)
Proposed algorithm maximum operation cost is.
T (n) := O (CHN × MN)

E. As cluster formation, the energy efficient data aggregation mechanism algorithm in operation no 2 calculates the distance from CH's node to the member nodes.
Cost for each round: TR
Cluster Nodes: CHN
Member Nodes: MN
T (n) := O (TR (CHN × MN))
The maximum cost of energy efficient data aggregation mechanism algorithm is given below.
T (n) := O (TR (CHN × MN))

A fuzzy rule-based proposed algorithm has extra cost depending on the data aggregation from each node in the cluster is considered. The time complexity is improving against cluster formation, data aggregation, nodes schedule to sleep and active and message transfer from CH node to base station edge server with minimum time. The time of data aggregation is reduced and time efficiency is increased for message delivery to base station with accuracy. Worst time is accruing when edge server nodes become unavailable for message communication.

TABLE 1. Symbol and their related task.

Symbol	Related Task
d	Transmission distance
lE_{elec}	Dissipated energy for transmitter and receiver
εfs	Free space amplifier energy factor
εmp	Free space amplifier energy factor
$d0$	Threshold
N_a, N_b	Name of the Nodes
calculate_Dis (a,b).	For the calculation of deployment Distance
d'_{ab}	Data collected from member node
j	Time interval
$\mathbf{R}^{\lambda}$	Boolean Matrix
V	Category of redundant nodes
α	Parameter

Algorithm 1 Proposed EEDAM (An Energy Efficient Data Aggregation Mechanism) Algorithm

```
For each CH
        Build a garbage data matrix X;                    // Initialize threshold and DB with zero
        Then the matrix D can be transformed into fuzzy matrix 'R';
        The member nodes grouped into different 'K' categories     // random selection of Broker
For each category 'V'
        For each node nominated as 'B,' 'K' belongs to $n^{(v)}$
Calculate confidence distance Calculate_Dis ($n_a^{(v)}$, $n_b^{(v)}$) between the data from node $n_a^{(v)}$, $n_b^{(v)}$)
$n_*^{(v)}$ = agrSUM Calculate_Dis ($n_a^{(v)}$, $n_b^{(v)}$)
        End for
End for
obtain redundant nodes set {R, R2, ..., Rt};
For each nodes belongs to {R1, R2 ... $R_t$}
        Send Schdule_MSG(CH_id, id, Status_flag)
        Receive Schdule_MSG_ACK;
        End for
End for
```

TABLE 2. Simulation 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
Eelec	50 nJ bit
EDA	5 nJ/bit/signal
ε_{mp}	0.0013pJ/bit/m4
$\varepsilon\, fs$	10 PJ/bit/m2

TABLE 3. Testing devices specifications.

Parameters	Edge Node	IoT Node	Cloud Server (Including 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

IV. RESULTS AND SIMULATIONS

This section discusses the simulation evaluation results from different experimental environments of our proposed model. The proposed model evaluates the points of view of different performance metrics. In this work, EEDAM was compared with two protocols, EEHS [58] and ESSM [57]. The detailed evaluation parameters are described in Table 1. The edge server's accuracy also assesses 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 for how many transactions are 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 has gas consumption. Suppose more resources are consumed in a blockchain, then more gas will be used than the normal blockchain task process—some gas consumption rates in blockchain technology are already defined in the Ethereum yellow paper.

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

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. This cloud server behaves as a middle layer node in the consortium blockchain, which has the highest power as miners. As the cloud server receives the request from the edge node than cloud server take action and validate the edge server in the blockchain. We also simulated many edge devices to serve client's nodes. There also exist IoT devices with layers which request the edge server for specific services. The details of the cloud, edge, and IoT client devices are given in Table 2. In Figures 3 and 4, the experimental results are shown. Parameter α is variable that indicates the distance of node from base station. If the value is high than the distance factore becomes more critical and cause more

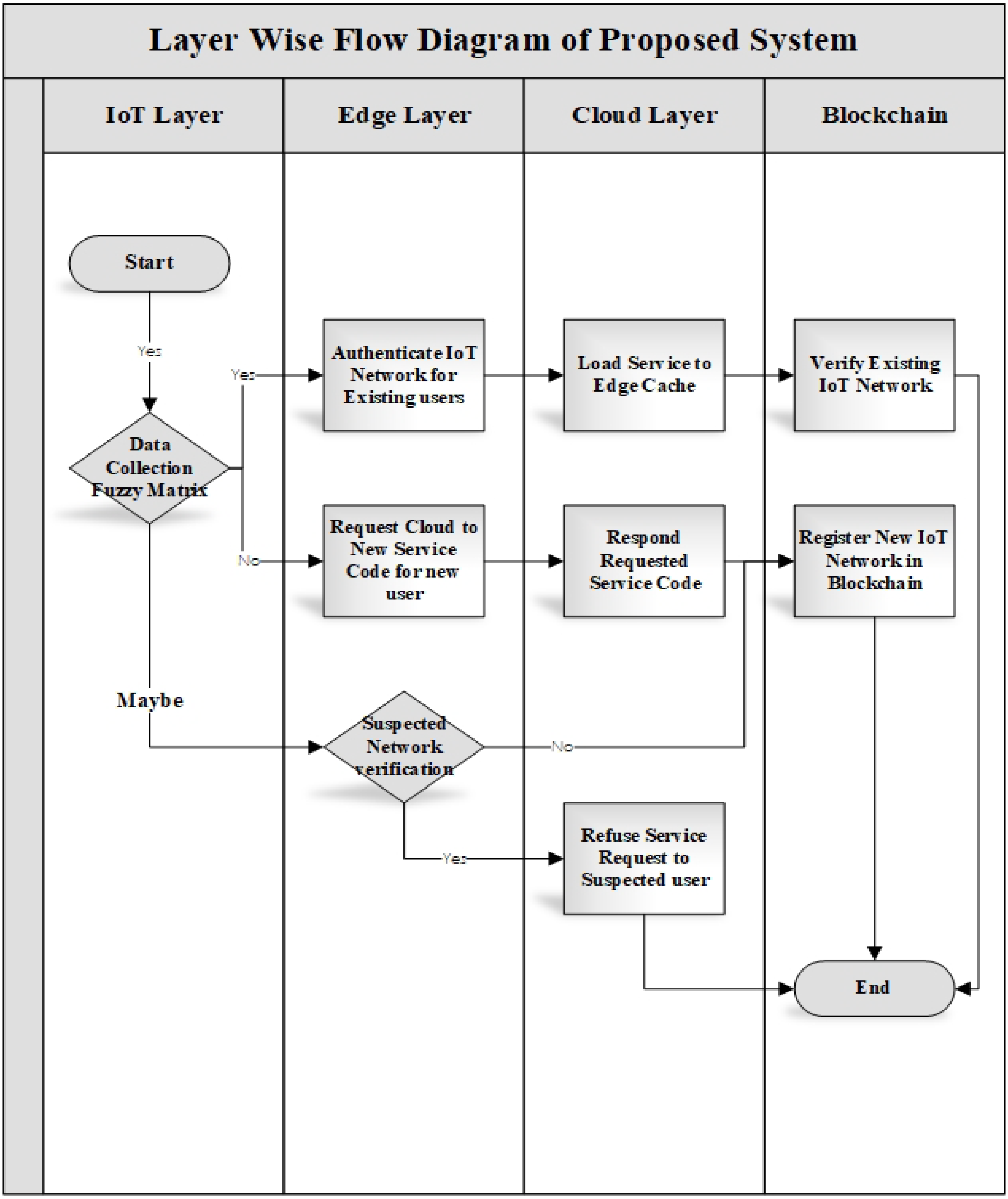
Layer Wise Flow Diagram of Proposed System
IoT Layer
Edge Layer
Cloud Layer
Blockchain
Start
Yes
Data Collection Fuzzy Matrix
Yes
No
Maybe
Authenticate IoT Network for Existing users
Request Cloud to New Service Code for new user
Suspected Network verification
No
Yes
Load Service to Edge Cache
Respond Requested Service Code
Refuse Service Request to Suspected user
Verify Existing IoT Network
Register New IoT Network in Blockchain
End

FIGURE 2. Proposed system work flow.

energy consumption. The values of 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. This is because of the smaller value of the parameter α. When the value of α is large, the distance factor becomes more critical.

According to the previous analysis, we can select 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 Figure 5. It can be observed that the transmission radius of the CHs is smaller than other CHs near Sink.

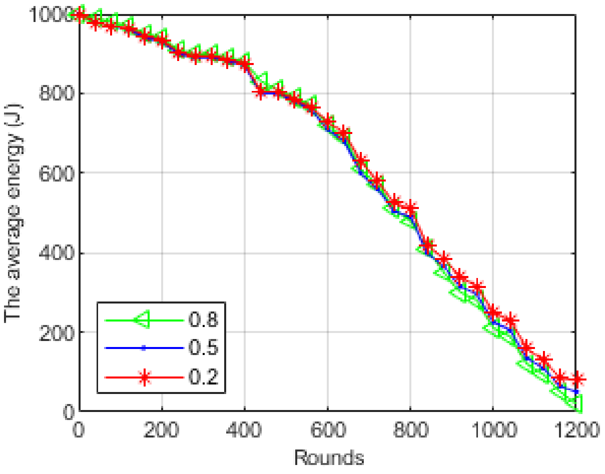

FIGURE 3. The average energy with different parameters.

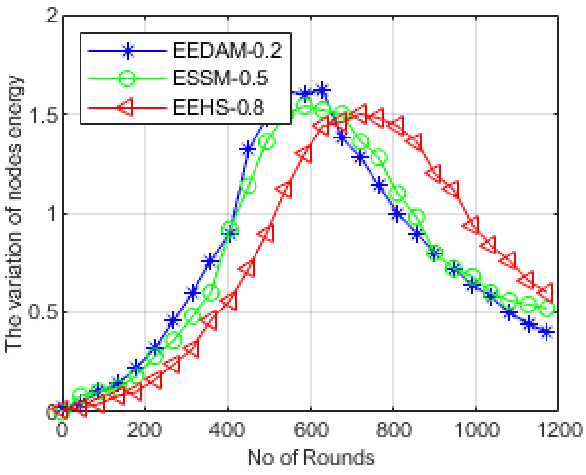

FIGURE 4. The variation of nodes energy with different parameters.

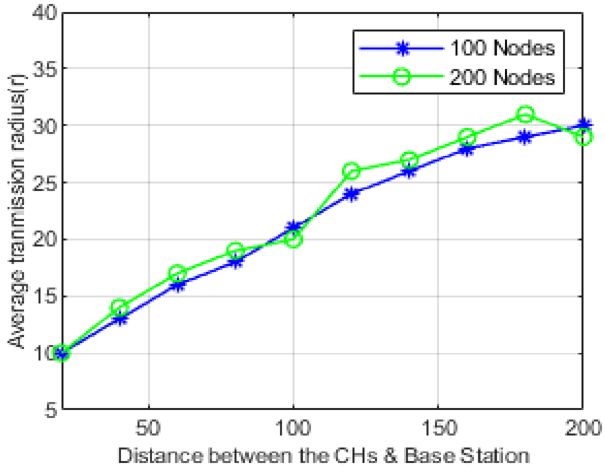

FIGURE 5. Average distance between source and sink.

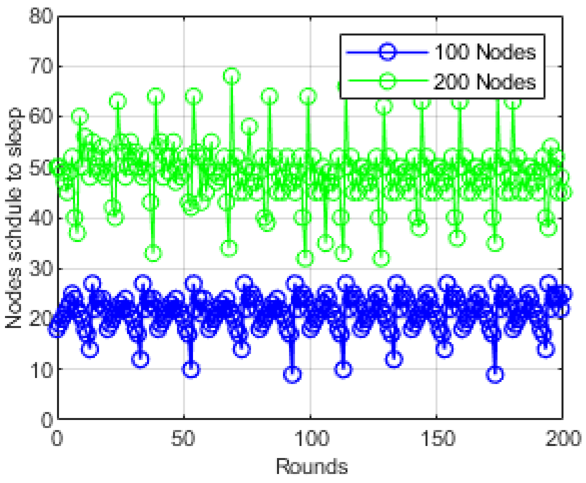

FIGURE 6. No. of the nodes being schedule to sleep in each round of transmission.

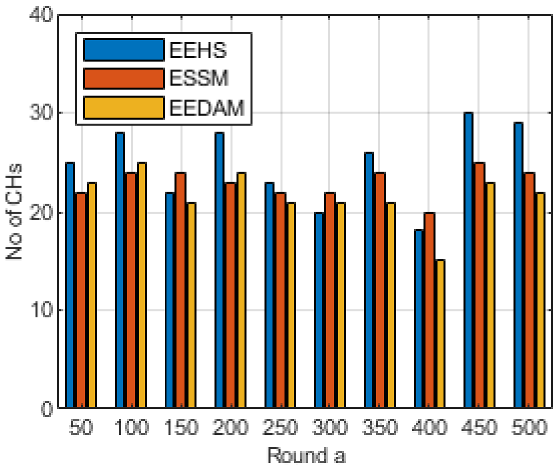

FIGURE 7. Average CHs selection from cluster 200 nodes.

It is because the energy consumption by the CHs is 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. Furthermore, the average number of nodes is compared with different node densities in each round.

For example, Figure **6** shows that the number of dormant nodes is more common compared to the low-density model. This is because due to the data correlation collected by the neighboring nodes, much higher and more dormant nodes are being selected to have subsequent data fusion. As a result, the number of nodes selected as redundant nodes which are scheduled to sleep is much higher. Therefore, we 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 concerning node density is shown in Figure 7&8 number of cluster selection each round (a) and round (b) on 200 and 400 nodes is shown. When the sensor node density is large, the number of CHs in EEHS is higher than ESSM and EEDAM. The main reason is that EEHS' main focus upon

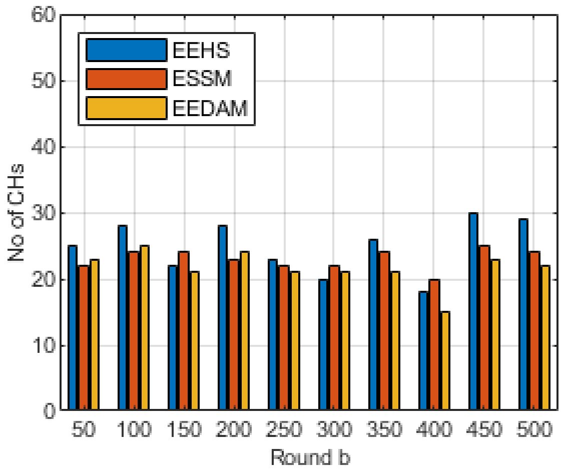

FIGURE 8. Average CHs selection from cluster 400 nodes.

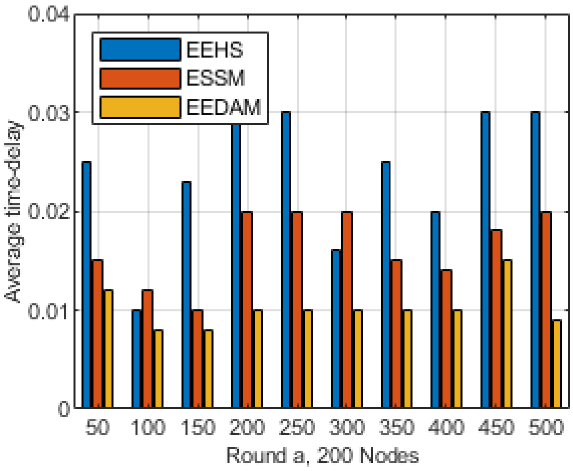

FIGURE 9. Average time-delay in each transmission round, 200 nodes.

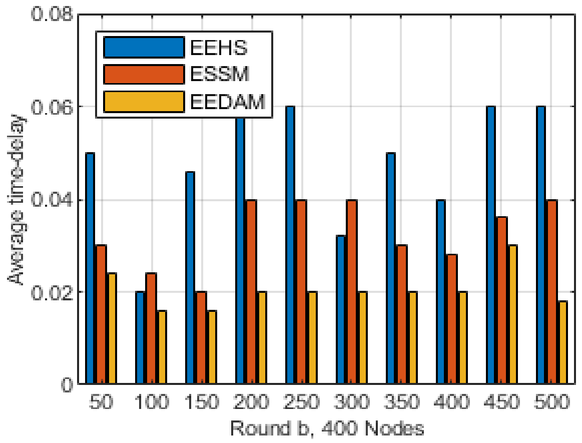

FIGURE 10. Average time-delay in each transmission round, 400 nodes.

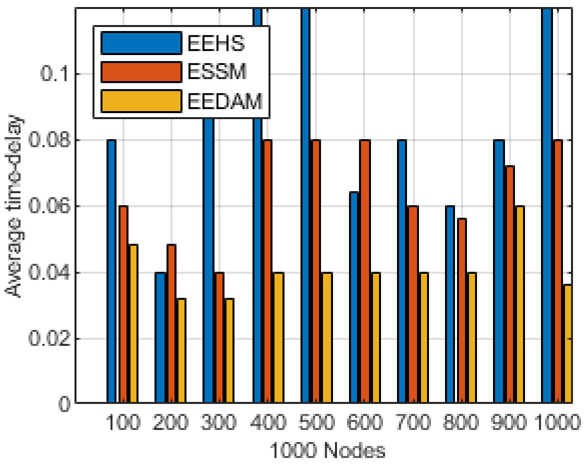

FIGURE 11. Average CHs selection from cluster 1000 nodes.

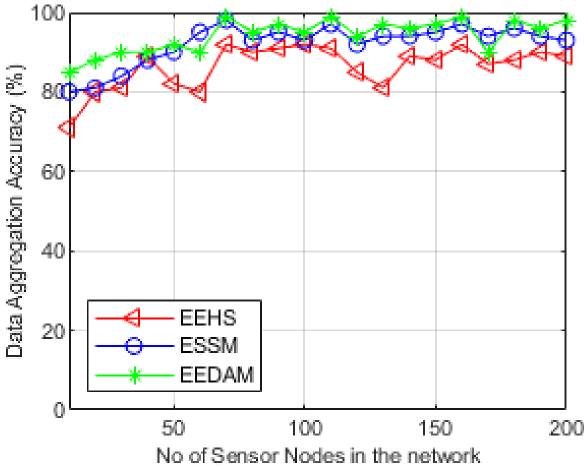

FIGURE 12. Data aggregation accuracy with different no. of nodes.

the cluster size is 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, more redundant nodes are scheduled to sleep based on the data correlation to save energy. The number of CH's selection is depending on number of rounds. In each rounds CH's selection is changed by the proposed mechanism.

Figure 9, 10 and 11 shows the average time delays in data transmission with nodes density 200, 400 and 1000. 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, which increases 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 the time delay with the efficiency of data transmission.

Figure **12** shows the data accuracy with a different number of nodes of EEHS, ESSM, and EEDAM. Data accuracy means during data aggregation process data is reduced and duplicated data is eliminated by fuzzy rule-based algorithm. After applying Fuzzy rule-based algorithm

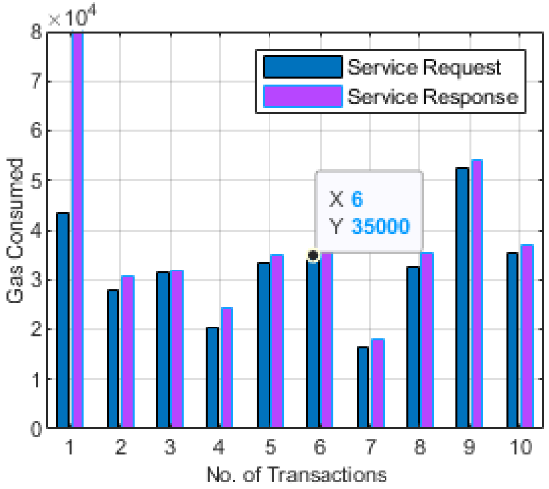

FIGURE 13. Gas consumed with respect to service request and response.

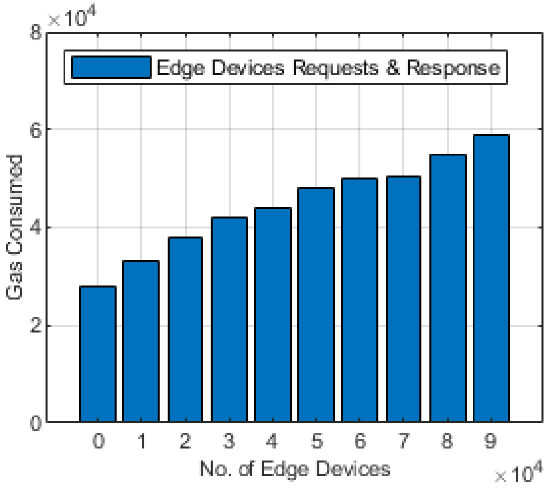

FIGURE 14. Gas consumed by the edge devices regarding services.

information received with maximum accuracy at base station. We can observe from the results that as the number of nodes increase, data accuracy also increases. That shows proposed system is scalable enough. EEDAM shows the best performance in the aspect of data accuracy compared to EEHS and ESSM. There is no limitation of nodes to measure the proposed system performance. A data accuracy experiment has done on 200 nodes. In the proposed scheme, redundant nodes are selected based on the data correlation, and the remaining nodes are enough to achieve the same estimated level of data accuracy. Hence, it is not compulsory to keep all nodes in active mode, which causes improved energy consumption, as well as data accuracy.

Figure 13 & 14 shows the analysis of the gas consumption of different service requests and responses. We took ten transactions using 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 essential services utilize more bandwidth and resources, the gas consumption is also higher than the average value. If the hash code generated by the hashing algorithm has difficulties, more mining power is required, and the execution time also increases. When the IoT devices requesting the edge server for a service code at the start of the network, a small number of edge device requests are received at the blockchain and their gas consumption is not too high.

We simulated our proposed architecture, EEDAM, in up to 100 edge devices. The results show that there is a linear change in gas consumption concerning service requests and responses. Thus, the proposed system is scalable enough as we increase the IoT nodes density.

And achieves security by using blockchain technology. With blockchain, no malicious edge device can communicate with the IoT network and the cloud server that contains the blockchain technology.

After the IoT layer process works, 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 requests to the edge server for required service code. The edge server looks in its cache memory, which is used frequently, to provide the requested device. Suppose the requested service code is not in the edge server cache memory, then the edge server requests the service code's cloud server. In the cloud infrastructure, blockchain is implemented. The cloud server provides the requested service code to the edge server after the PoA process. The validation status and rating of the edge server is given by the end-user, which will also be stored in the cloud server. For the security of the IoT-constrained devices from an un-trusted edge server, the edge server registration process is done at the cloud server to configure the edge server's validity. For the PoA of the edge server's service code, the IoT device communicates with the cloud server and gets the hash code against the service code.

After this, the IoT device checks the hash code generated by the edge server and the cloud server. In this proposed mechanism hash code is generate by the edge server and cloud server. In this regard energy consumption decrease by the IoT constrained devices. If the cloud server and edge device both create 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's trust rating. In using blockchain, maximum security is achieved with minimum overhead due to the involvement of the edge server.

V. DISCUSSIONS

Now days, the IoT depends the interconnection of different information technologies by using their connectivity ability.

Due to this the challenge of energy efficiency and cost of its deployment still exist. With the advancement in artificial intelligence coupled with IoT systems is providing lots of benefits in real-time applications connectivity. For the energy efficiency of such kind of applications [59] propose an improved dynamic clustering algorithm to address the energy efficiency issues. The proposed algorithm can be implemented in IoT applications which consist of different wireless sensor networks. To process the energy demand of each cluster of WSN's neural and copula theory is used, this also reduced data redundancy that caused by the construction of similar types of cluster. According the power requirements initially the nodes are divided into two clusters and compared with the set thresholds. The simulation results showed the proposed system effectiveness of information and use of communication energy efficiently in cluster.

The birth of 5G and arise of 6G enhance the development of next generation IoT for individual and industrial works more effective, efficient and profitable. The most important performance factor in 6G is smart network architecture and massive use of IoT applications which main relay on the automation and intelligence in industry. The authors [60] discourse the energy usage problems of massive use of IoT system with dynamic clustering network architecture using a multi agent system (MAS) for 6G industrial applications.

The proposed distributed artificial intelligence system to cluster the sensor nodes in the system to predict the main node and its location. For optimization back propagation neural network (BPNN) and convolutional neural network (CNN) are introduced. Furthermore, it distributes the network resources efficiently by analyzes the correlation of mutual cluster's node. This work is also reducing the resources wastage and improves the energy efficiency by eliminating the data redundancy.

With the advent of 6G is also performing key role for reliable transmission of sensor elements for IoT systems. The proposed work presented a novel mechanism for the implementation of distributed artificial intelligence (DAI) with neural networks for energy efficiency and overcome the intelligent transportation system challenges by introducing fast communication for inter cluster. This work also proposes new method for energy efficiency by implementation of hybrid approach of DAI and self-organizing Map (SOM). It also save the overall network energy and reduce the computation challenges [61].

VI. CONCLUSION AND FUTURE WORK

This paper proposed an energy-efficient, secure, and data aggregated architecture that provides a cloud-based system using blockchain technology for IoT devices to meet the security and energy requirements. The edge server is used to reduce the cloud server load by providing the most frequently used services in its cache memory to the IoT devices. The proposed system is designed to protect IoT networks from malicious activities using blockchain technology and data co-relation reduction. The blockchain validates the edge server's validity and the service provided by the edge server within the cloud server and the 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 in offloading the cloud server compared to traditional cloud servers using blockchain technology. It also indicates that the model is effective and efficient, and that it fulfills' the essential design principles with minimum delay.

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

REFERENCES

[1] L. B. Bhajantri and T. Mujawar, "A survey of cloud computing security challenges, issues and their countermeasures," in *Proc. 3rd Int. Conf. I-SMAC (IoT Social, Mobile, Analytics Cloud) (I-SMAC)*, Dec. 2019, pp. 376–380, doi: 10.1109/I-SMAC47947.2019.9032545.

[2] J. Lockl, V. Schlatt, A. Schweizer, N. Urbach, and N. Harth, "Toward trust in Internet of Things ecosystems: Design principles for blockchain-based IoT applications," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1256–1270, Nov. 2020, doi: 10.1109/TEM.2020.2978014.

[3] P. A. Apostolopoulos, E. E. Tsiropoulou, and S. Papavassiliou, "Cognitive data offloading in mobile edge computing for Internet of Things," *IEEE Access*, vol. 8, pp. 55736–55749, 2020, doi: 10.1109/ACCESS.2020.2981837.

[4] K. Tange, M. De Donno, X. Fafoutis, and N. Dragoni, "A systematic survey of industrial Internet of Things security: Requirements and fog computing opportunities," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2489–2520, 4th Quart., 2020, doi: 10.1109/COMST.2020.3011208.

[5] G. Singh, "Internet-of-Things with blockchain technology: State-of-the art and potential challenges," in *Handbook of Multimedia Information Security: Techniques and Applications*. Cham, Switzerland: Springer, 2019, pp. 775–795, doi: 10.1007/978-3-030-15887-3_37.

[6] Y. Liu, A. Liu, N. Zhang, X. Liu, M. Ma, and Y. Hu, "DDC: Dynamic duty cycle for improving delay and energy efficiency in wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 131, pp. 16–27, Apr. 2019, doi: 10.1016/j.jnca.2019.01.022.

[7] M. Rehman, N. Javaid, M. Awais, M. Imran, and N. Naseer, "Cloud based secure service providing for IoTs using blockchain," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2019, pp. 1–7, doi: 10.1109/GLOBECOM38437.2019.9013413.

[8] I. Butun, A. Sari, and P. Österberg, "Security implications of fog computing on the Internet of Things," 2018, pp. 1–6, *arXiv:1809.10492*.

[9] L. Tseng, L. Wong, S. Otoum, M. Aloqaily, and J. B. Othman, "Blockchain for managing heterogeneous Internet of Things: A perspective architecture," *IEEE Netw.*, vol. 34, no. 1, pp. 16–23, Jan. 2020, doi: 10.1109/MNET.001.1900103.

[10] P. Singh, A. Nayyar, A. Kaur, and U. Ghosh, "Blockchain and fog based architecture for internet of everything in smart cities," *Future Internet*, vol. 12, no. 4, pp. 1–12, Mar. 2020, doi: 10.3390/FI12040061.

[11] P. Sharma, R. Jindal, and M. D. Borah, "Blockchain technology for cloud storage: A systematic literature review," *ACM Comput. Surv.*, vol. 53, no. 4, pp. 1–32, Jul. 2021, doi: 10.1145/3403954.

[12] Z. Li, R. Y. Zhong, Z. G. Tian, H.-N. Dai, A. V. Barenji, and G. Q. Huang, "Industrial blockchain: A state-of-the-art survey," *Robot. Comput.-Integr. Manuf.*, vol. 70, Aug. 2021, Art. no. 102124, doi: 10.1016/j.rcim.2021.102124.

[13] C. Te Tseng and S. S. C. Shang, "Exploring the sustainability of the intermediary role in blockchain," *Sustainability*, vol. 13, no. 4, pp. 1–21, 2021, doi: 10.3390/su13041936.

[14] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Trans. Wireless Commun.*, vol. 1, no. 4, pp. 660–670, Oct. 2002, doi: 10.1109/TWC.2002.804190.

[15] V. K. Chawra and G. P. Gupta, "Load balanced node clustering scheme using improved memetic algorithm based meta-heuristic technique for wireless sensor network," *Proc. Comput. Sci.*, vol. 167, pp. 468–476, Jan. 2020, doi: 10.1016/j.procs.2020.03.256.

[16] K. R. Venugopal, S. T. Prakash, and M. Kumaraswamy, *LRTHR: Link-Reliability Based Two-Hop Routing for WSNs*. Cham, Switzerland: Springer, 2020.

[17] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum Project Yellow Paper, Ethereum Ethcore, Tech. Rep. EIP-150 Revision (a04ea02 - 2017-09-30), vol. 151, Apr. 2014, pp. 1–32.

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

[19] S. A. Sert, A. Alchihabi, and A. Yazici, "A two-tier distributed fuzzy logic based protocol for efficient data aggregation in multihop wireless sensor networks," *IEEE Trans. Fuzzy Syst.*, vol. 26, no. 6, pp. 3615–3629, Dec. 2018.

[20] S. A. Sert and A. Yazici, "Increasing energy efficiency of rule-based fuzzy clustering algorithms using CLONALG-M for wireless sensor networks," *Appl. Soft Comput.*, vol. 109, Sep. 2021, Art. no. 107510.

[21] S. A. Sert, E. Onur, and A. Yazici, "Security attacks and countermeasures in surveillance wireless sensor networks," in *Proc. 9th Int. Conf. Appl. Inf. Commun. Technol. (AICT)*, Oct. 2015, pp. 201–205.

[22] D. H. Wang, "IoT based clinical sensor data management and transfer using blockchain technology," *J. ISMAC*, vol. 2, no. 3, pp. 154–159, Jul. 2020, doi: 10.36548/jismac.2020.3.003.

[23] R. A. Memon, J. P. Li, J. Ahmed, M. I. Nazeer, M. Ismail, and K. Ali, "Cloud-based vs. blockchain-based IoT: A comparative survey and way forward," *Frontiers Inf. Technol. Electron. Eng.*, vol. 21, no. 4, pp. 563–586, Apr. 2020, doi: 10.1631/FITEE.1800343.

[24] O. Alkadi, N. Moustafa, B. Turnbull, and K.-K.-R. Choo, "A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks," *IEEE Internet Things J.*, vol. 8, no. 12, pp. 9463–9472, Jun. 2021, doi: 10.1109/jiot.2020.2996590.

[25] W. Serrano, "The blockchain random neural network for cybersecure IoT and 5G infrastructure in smart cities," *J. Netw. Comput. Appl.*, vol. 175, Feb. 2021, Art. no. 102909, doi: 10.1016/j.jnca.2020.102909.

[26] M. Aloqaily, O. Bouachir, A. Boukerche, and I. A. Ridhawi, "Design guidelines for blockchain-assisted 5G-UAV networks," *IEEE Netw.*, vol. 35, no. 1, pp. 64–71, Jan./Feb. 2021, doi: 10.1109/MNET.011.2000170.

[27] Y. Njah and M. Cheriet, "Parallel route optimization and service assurance in energy-efficient software-defined industrial IoT networks," *IEEE Access*, vol. 9, pp. 24682–24696, 2021, doi: 10.1109/ACCESS.2021.3056931.

[28] S. W. H. Shah, A. N. Mian, A. Aijaz, J. Qadir, and J. Crowcroft, "Energy-efficient MAC for cellular IoT: State-of-the-art, challenges, and standardization," *IEEE Trans. Green Commun. Netw.*, vol. 5, no. 2, pp. 587–599, Jun. 2021, doi: 10.1109/TGCN.2021.3062093.

[29] C. Chen, S. Fu, X. Jian, and M. Liu, "NOMA for energy-efficient LiFi-enabled bidirectional IoT communication," *IEEE Trans. Commun.*, vol. 69, no. 3, pp. 1693–1706, Mar. 2021.

[30] T. Xu, X. Wang, T. Su, L. Wan, and L. Sun, "Vehicle location in edge computing enabling IoTs based on bistatic FDA-MIMO radar," *IEEE Access*, vol. 9, pp. 46398–46408, 2021, doi: 10.1109/ACCESS.2021.3064849.

[31] D. C. Nguyen, M. Ding, Q.-V. Pham, P. N. Pathirana, L. B. Le, A. Seneviratne, J. Li, D. Niyato, and H. V. Poor, "Federated learning meets blockchain in edge computing: Opportunities and challenges," *IEEE Internet Things J.*, vol. 8, no. 16, pp. 12806–12825, Aug. 2021, doi: 10.1109/jiot.2021.3072611.

[32] D. Puthal, S. Mohanty, S. Wilson, and U. Choppali, "Collaborative edge computing for smart villages [energy and security]," *IEEE Consum. Electron. Mag.*, vol. 10, no. 3, pp. 68–71, May 2021, doi: 10.1109/MCE.2021.3051813.

[33] T. T. Huong, T. P. Bac, D. M. Long, B. D. Thang, N. T. Binh, T. D. Luong, and T. K. Phuc, "LocKedge: Low-complexity cyberattack detection in IoT edge computing," *IEEE Access*, vol. 9, pp. 29696–29710, 2021, doi: 10.1109/ACCESS.2021.3058528.

[34] W.-K. Yun and S.-J. Yoo, "Q-learning-based data-aggregation-aware energy-efficient routing protocol for wireless sensor networks," *IEEE Access*, vol. 9, pp. 10737–10750, 2021, doi: 10.1109/ACCESS.2021.3051360.

[35] S. B. H. Youssef, S. Rekhis, and N. Boudriga, "A blockchain based secure IoT solution for the dam surveillance," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2019, pp. 1–6, doi: 10.1109/WCNC.2019.8885479.

[36] S. Tuli, R. Mahmud, S. Tuli, and R. Buyya, "FogBus: A blockchain-based lightweight framework for edge and fog computing," *J. Syst. Softw.*, vol. 154, pp. 22–36, Aug. 2019, doi: 10.1016/j.jss.2019.04.050.

[37] S. K. Singh, S. Rathore, and J. H. Park, "BlockIoTIntelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence," *Future Gener. Comput. Syst.*, vol. 110, pp. 721–743, Sep. 2020, doi: 10.1016/j.future.2019.09.002.

[38] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT," *Sensors*, vol. 19, no. 2, pp. 1–17, 2019, doi: 10.3390/s19020326.

[39] W. Liang, M. Tang, J. Long, X. Peng, J. Xu, and K. Li, "A secure fabric blockchain-based data transmission technique for industrial Internet-of-Things," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3582–3592, Jun. 2019, doi: 10.1109/TII.2019.2907092.

[40] Y. Ren, Y. Leng, Y. Cheng, and J. Wang, "Secure data storage based on blockchain and coding in edge computing," *Math. Biosci. Eng.*, vol. 16, no. 4, pp. 1874–1892, Mar. 2019, doi: 10.3934/mbe.2019091.

[41] S. Ali, G. Wang, M. Z. A. Bhuiyan, and H. Jiang, "Secure data provenance in cloud-centric Internet of Things via blockchain smart contracts," in *Proc. IEEE SmartWorld, Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People Smart City Innov. (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, Oct. 2018, pp. 991–998, doi: 10.1109/SmartWorld.2018.00175.

[42] W. Xiong and L. Xiong, "Smart contract based data trading mode using blockchain and machine learning," *IEEE Access*, vol. 7, pp. 102331–102344, 2019, doi: 10.1109/access.2019.2928325.

[43] Z. Guan, Y. Zhang, L. Wu, J. Wu, J. Li, Y. Ma, and J. Hu, "APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT," *J. Netw. Comput. Appl.*, vol. 125, pp. 82–92, Jan. 2019, doi: 10.1016/j.jnca.2018.09.019.

[44] H. Li, R. Lu, J. Misic, and M. Mahmoud, "Security and privacy of connected vehicular cloud computing," *IEEE Netw.*, vol. 32, no. 3, pp. 4–6, May/Jun. 2018, doi: 10.1109/MNET.2018.8370870.

[45] W. Yanez, R. Mahmud, R. Bahsoon, Y. Zhang, and R. Buyya, "Data allocation mechanism for Internet-of-Things systems with blockchain," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3509–3522, Apr. 2020, doi: 10.1109/JIOT.2020.2972776.

[46] M. Moniruzzaman, S. Khezr, A. Yassine, and R. Benlamri, "Blockchain for smart homes: Review of current trends and research challenges," *Comput. Electr. Eng.*, vol. 83, May 2020, Art. no. 106585, doi: 10.1016/j.compeleceng.2020.106585.

[47] Y. Lee, S. Rathore, J. H. Park, and J. H. Park, "A blockchain-based smart home gateway architecture for preventing data forgery," *Hum.-Centric Comput. Inf. Sci.*, vol. 10, no. 1, Dec. 2020, doi: 10.1186/s13673-020-0214-5.

[48] D. Pavithran, K. Shaalan, J. N. Al-Karaki, and A. Gawanmeh, "Towards building a blockchain framework for IoT," *Cluster Comput.*, vol. 23, no. 3, pp. 2089–2103, Sep. 2020, doi: 10.1007/s10586-020-03059-5.

[49] M. Akash, B. Kumar, and P. Rana, "International journal of advance engineering and research," *Int. J. Advance Eng. Res. Develop.*, vol. 5, no. 3, pp. 434–439, 2018.

[50] M. Samaniego, U. Jamsrandorj, and R. Deters, "Blockchain as a service for IoT," in *Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData)*, Dec. 2016, pp. 433–436, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.102.

[51] Y. Liu, K. Wang, Y. Lin, and W. Xu, "LightChain: A lightweight blockchain system for industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3571–3581, Jun. 2019, doi: 10.1109/TII.2019.2904049.

[52] R. A. Memon, J. P. Li, M. I. Nazeer, A. N. Khan, and J. Ahmed, "DualFog-IoT: Additional fog layer for solving blockchain integration problem in Internet of Things," *IEEE Access*, vol. 7, pp. 169073–169093, 2019, doi: 10.1109/ACCESS.2019.2952472.

[53] P. K. Sharma, M.-Y. Chen, and J. H. Park, "A software defined fog node based distributed blockchain cloud architecture for IoT," *IEEE Access*, vol. 6, pp. 115–124, 2018, doi: 10.1109/ACCESS.2017.2757955.

[54] M. Bukhsh, S. Abdullah, and I. S. Bajwa, "A decentralized edge computing latency-aware task management method with high availability for IoT applications," *IEEE Access*, vol. 9, pp. 138994–139008, 2021, doi: 10.1109/ACCESS.2021.3116717.

[55] M. Bukhsh, S. Abdullah, A. Rahman, M. N. Asghar, H. Arshad, and A. Alabdulatif, "An energy-aware, highly available, and fault-tolerant method for reliable IoT systems," *IEEE Access*, vol. 9, pp. 145363–145381, 2021, doi: 10.1109/access.2021.3121033.

[56] D. Lee and K. Yoon, "An efficient spatio-temporal index for spatio-temporal query in wireless sensor networks," *KSII Trans. Internet Inf. Syst.*, vol. 11, no. 10, pp. 4908–4928, 2017, doi: 10.3837/tiis.2017.10.012.

[57] R. Wan, N. Xiong, and N. T. Loc, "An energy-efficient sleep scheduling mechanism with similarity measure for wireless sensor networks," *Hum.-Centric Comput. Inf. Sci.*, vol. 8, no. 1, pp. 1–22, Dec. 2018, doi: 10.1186/s13673-018-0141-x.

[58] S. Paul and N. K. Sao, "An energy efficient hybrid node scheduling scheme in cluster based wireless sensor networks," in *Proc. World Congr. Eng. (WCE)*, vol. 2, 2011, pp. 1775–1779.

[59] L. Manman, Q. Xin, P. Goswami, A. Mukherjee, and L. Yang, "Energy-efficient dynamic clustering for IoT applications: A neural network approach," in *Proc. IEEE 8th Int. Conf. Commun. Netw. (ComNet)*, Oct. 2020, pp. 1–7.

[60] A. Mukherjee, P. Goswami, M. A. Khan, L. Manman, L. Yang, and P. Pillai, "Energy-efficient resource allocation strategy in massive IoT for industrial 6G applications," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5194–5201, Apr. 2021.

[61] P. Goswami, A. Mukherjee, R. Hazra, L. Yang, U. Ghosh, Y. Qi, and H. Wang, "AI based energy efficient routing protocol for intelligent transportation system," *IEEE Trans. Intell. Transp. Syst.*, early access, Sep. 2, 2021, doi: 10.1109/TITS.2021.3107527.

ADEEL AHMED received the master's degree in computer science from The Islamia University of Bahawalpur, Pakistan, and the M.S. degree in computer sciences from the Virtual University of Pakistan. He is currently pursuing the Ph.D. degree with The Islamia University of Bahawalpur. His main research interests include edge computing, the IoT systems, energy efficiency, fuzzy logic, wireless networks, and blockchain. He serves as a reviewer for international journals.

SAIMA ABDULLAH received the Ph.D. degree from the Department of Computer Science and Electronic Engineering, University of Essex, U.K. She is currently an Assistant Professor with the Department of Computer Science and Information Technology, The Islamia University of Bahawalpur, Pakistan. She is a member of the Multimedia Research Group, DCS, where she has been involved in efficient and secure communication of multimedia data over future generation network technologies. Her main research interests include wireless networks and communications, future internet technology, and network performance analysis. She has authored around ten articles in the above research areas. She serves as a reviewer for international journals.

MUHAMMAD BUKHSH received the master's degree in information technology from the University of Education Lahore, Pakistan, in 2012, and the M.S. degree in computer sciences from The Islamia University of Bahawalpur, in 2016, where he is currently pursuing the Ph.D. degree. His main research interests include wireless networks and communications, ad hoc networks, the IoT systems, energy efficiency, edge commuting, high availability, blockchain, and fault tolerance.

ISRAR AHMAD received the bachelor's and master's degrees in computer science from the Virtual University of Pakistan. He is currently pursuing the Ph.D. degree with The Islamia University of Bahawalpur, Pakistan. His main research interests include the IoT systems, fog computing, high availability, and blockchain.

ZAIGHAM MUSHTAQ received the Ph.D. degree in computer science. He is currently working as an Assistant Professor with the Department of Computer Science, The Islamia University of Bahawalpur, Pakistan. He has worked on multilingual source code analysis, transformation of monolithic and legacy applications towards micro-services, and resolving heterogeneity across big data. His research interests include software engineering, reverse engineering, web services computing, and big data analytics.