Peer-to-Peer Networking and Applications (2021) 14:2858–2873
https://doi.org/10.1007/s12083-021-01115-4

Optimized dynamic storage of data (ODSD) in IoT based on blockchain for wireless sensor networks

Osamah Ibrahim Khalaf[1] · Ghaida Muttashar Abdulsahib[2]

Received: 28 October 2020 / Accepted: 1 March 2021 / Published online: 19 March 2021

Abstract

The Industry 4.0 IoT network integration with blockchain architecture is a decentralized, distributed ledger mechanism used to record multi-user transactions. Blockchain requires a data storage system designed to be secure, reliable, and fully transparent, emerged as a preferred IoT-based digital storage on WSN. Blockchain technology is being used in the paper to construct the node recognition system according to the storage of data for WSNs. The data storage process on such data must be secure and traceable in different forensics and decision making. The primary theme of the dynamic data security is therefore for rejecting exploitation of the unauthorized user and for evaluating the mechanism in tracing and evidence of system's data operation in a dynamic manner, growth and quality features under the stochastic state of the model; (1) a mathematical method for the secured storage of data in dynamic is built through distributed node cooperation in IoT industry. (2) the ownership transition feature and the dynamic storage of data system architecture are configured, (3) the emerging distributed storage architecture for blockchain-based WSN will substantially reduce overhead storage for each node without affecting data integrity; (4) minimize the latency of data reconstruction in distributed over storage system, and propose an effective and scalable algorithm for optimizing storage latency issue. In addition to this research, the system implements verified possession of data for replacing the evidence in original digital currency for mining and to store new data blocks that will be compared to the proof system, dramatically reduces computational capacity. The proposed ODSD framework has exceptional benefits for real-time applications while maintaining the security of the dynamic storage of data.

Keywords Blockchain · Secure Storage of data · Internet of Things · Authentication · Dynamic data · WSN

1 Introduction

The Wireless Sensor Network (WSN) [1] is recently becoming a very hot research area in communication, microelectronics, database, network, etc., due to its wide-area application prospects, and it incorporates various technologies, like sensing, wireless communication, and the computing. The physical targets have been tracked by different microsensors in real-time, generating a high density of data awareness at an individual rate. Even though the hardware implementation and real-time settings are different, the primary objective is for obtaining, distribute, and processing perceived data. The users, once again, will get valuable data information. Where WSN is a data-centered network and storage of data over nodes is, therefore, the critical challenge in WSN that needs to be described [2] . For end-users, the awareness of data is what they are concerned about, instead of the wireless sensor node as a whole and the WSN channels they form. The WSN also supports effective and reliable storage of data and access in a heterogeneous, insecure environment. Where storage energy and space of each node is small, the necessary research is a position of significant activity for data organization in WSN would be how efficiently storing of data in limited storage space [3].

The Internet of Things (IoT) [4] is connected to an exceptionally more quantity of devices connected with the internet.

This article is part of the Topical Collection: *Special Issue on Blockchain for Peer-to-Peer Computing*
Guest Editors: Keping Yu, Chunming Rong, Yang Cao, and Wenjuan Li

✉ Osamah Ibrahim Khalaf
usama.ibrahem@coienahrain.edu.iq

Ghaida Muttashar Abdulsahib
30834@uotechnology.edu.iq

[1] AI-Nahrain University Al-Nahrain Nanorenewable Energy Research Centre (NNERC), Baghdad, Iraq

[2] Department of Computer Engineering, University of Technology-Iraq, Baghdad, Iraq

Many research areas, like a business, education, medical care, the supply chain, with the input of multiple approved agencies, fresh data input can be created in the time factor, it is called as dynamic data. An important focus of research is by managing large data volume made by those digital storage components in a practical, cost-effective manner and safe—dynamic data and its operations for distinct forensics and decision-making necessary extensive protection and traceability [5]. Current features of dynamic data are as follows: Consistency, Time Sensitivity, Multi dimension, Availability, the analysis and testing of storage log metadata, investigation of unauthorized activities.

The storage of data over sensor nodes is, therefore, a fundamental challenge for WSN that needs to be resolved. For end-users, the data interpretation is what they are concerned about, instead of the member sensor nodes on its own and the WSN that clients are taken by individual comprise. Also, the WSNs under the heterogeneous, insecure environment, support effective and secured dynamic storage of data and access [6]. As storage energy and disk space of every sensor node is limited, fundamental research is a hot spot for data association in WSN would be how efficiently store the data in defined storage space. WSN normal operations involve neighborhoods nodes in the network. However, because of the limited resources, like storage space and energy, some network nodes can choose their performance. The whole WSN would not provide the standard service if most of the network node has greedy behavior, and it does not forward packets. Hence, the incitement of the selfish nodes is for cooperating and ensuring the regular functioning of the entire network have been the part of essential WSN research [7].

Traceability is an essential requirement for dynamic data integrity and reliability and is an essential manifestation of dynamic data availability [8]. Any efficient entity between the data source and the cloud computing center in the WSN edge network can run the edge computing platform for computing, storing, and implementing core technologies, delivering real-time, interactive, and intelligent service computing to end-users [9]. Besides, the combination of edge computing and the existing centralized processing model of cloud computing will effectively solve the cloud center and WSN network edge issue of big data processing. The traditional architecture [10] of blockchain allows every node to store its copy of all the blockchain data. Where the entire blockchain grows longer and uses more storage space where transactions are added with the tail of the blockchain, creating the challenge with storage scalability, the challenge of storage scalability might not be too significant for traditional blockchain applications like Bitcoin since the participants contain trial storage space (hard disk) [11]. In this paper, we're proposing distributed blockchain storage architecture for WSN. The elimination coding function made it feasible for substantially reducing the storage usage of every node without impacting the overall integrity of data. We also focus a latency-cost with trade-off optimization problem to decrease the latency of data reconstruction over this distributed storage system architecture and suggest an effective and scalable algorithm [12, 13]. We offer the following contributions in the description of ODSD:

(1) By examining the authentic functions of the individual node of the decision-making system in distributed node cooperation and the group games nature in specific industry backgrounds, this article proposes a consensus system for dynamic storage of data [14]. It guarantees the protection of dynamic data by consensus based on blockchain technology.
(2) To use blockchain and IoT integration for storage of data, we propose a distributed storage architecture that ensures the protection of data storage for WSN in edge computing.
(3) It is not a trivial task to ensure communication efficiency among sensor nodes on WSN.
(4) To find the optimization problem, we frame an optimization and scalable problem and to authenticate the efficiency of this algorithm through the simulation process while considering latency-cost trade-off [15].
(5) Moreover, if nodes have been storing a more significant number of data, it will obtain more benefits. We apply the established possession of data instead of the proof of original digital currencies when storing and extracting new data blocks are in progress.

2 Related work

The LEACH [16] protocol has been proposed for collecting data over a hierarchical WSN that randomly selects subset over nodes as the cluster heads and attaches different clusters to the other nodes according to measure the distances among nodes and cluster heads. The nodes transfer data to cluster heads over time, and the heads of the cluster process data and again send it to sink nodes. The LEACH protocol, whereby the WSN was coordinated into a chain network, has been enhanced by the PEGASIS method. Each node obtains data from the neighboring nodes and then forward it. The nodes in the sink simply select another node to connect with. During digital transmission from a node to the next node, the data is aggregated and, in the end, reaches the sink node. Thus, in PEGASIS protocol [17], the energy consumed is lesser over LEACH. A new protocol, an enhancement to LEACH protocol, was also introduced by Wang et al. and set the hard and soft threshold that can be dynamically changed, and it compares data collected for minimizing unwanted transmission of data. When data for the node is above the maximum threshold, data is broadcast and carried as a new threshold value. External storage focuses uniquely on the data acquisition by ignoring WSN storage of data capacity and demand for data nodes.The data is stored in network nodes in local storage, which requires minimal energy. Only send the query commands to the other nodes. The result has been transferred to the sink node. The later receives the node for querying and processing. This means that queries put away longer delays. The specific targeting diffusion method for storing data collected by nodes should be used in neighboring nodes where the sink nodes attain the information through transmitting *"Active Message"* to other nodes of WSN [18]. A gradient inside the network is generated by the node that received the post, points towards the sink node, and the node finds one, and sometimes more routes to the sensor node at the sink continue to perform the flood search and send data. The enhancement of the guided diffusion protocol is the Spatial and Energy-Aware Routing protocol. However, in this protocols, the request *'Msg'* is sent through the targeted region, based on the geographical location, the distribution of the *"Active Message"* is restricted to the target area, that further prevents flooding throughout the network and decreases route discovery overheads [19]. The local storage mechanism is rapid, and the approach focuses on the processing of the data requests and has less data description, which contributes to more energy in the query process. Blockchain integration and the IoT of Industry 4.0 [20] have gained more and more interest in recent years. The integration of IoT and Blockchain solves comprehensive studies of addressing various implementation situations, user trends, and future problems. It suggested blockchain-based network architecture for industrial IoT. This architecture first merged Smart-M3 and Blockchain, a previous information distribution platform, and then used smart contracts to offer trust between the IoT production network participants. Similarly, the implementation of smart deals from the blockchain with the IoT network has been investigated [21]. Thus, this work discovered many ways with IoT and Blockchain could be used together for allowing peer-to-peer communication and data sharing in an environment that is not trusting. Another novel blockchain-based distributed cloud architecture has been proposed that combines SDN, Fog Computing, and IoT, provides low-cost, stable, and on-demand access with IoT nodes. A variety of attempts are made for dealing with the scalability issue of storage in the blockchain. To monitor the portion of the full blockchain stored on each node, ElasticChain uses its duplicate-ratio-regulation model. ElasticChain boosts blockchain storage scalability to store only the part of the entire chain over each node, where its storage operation is not much high as redundant coding. The other recommended results that use a new combination of Shamir's secret sharing system, distributed storage codes, and private key encryption for creating a coding system that distributes blockchain information between node subsets. This coding system keeps storage space, compared to the convention elimination code process, it can lead to loss of data integrity. By merely using erasure coding to store blockchain data [22], researchers advised a low storage space requirement system for the distribution block in the blockchain. They also offered similar frameworks. Such frameworks, however, lack in-depth analysis about the collection or output enhancement of removal coding parameters.

There are many applications for intelligent computing coupled with the IoT, cloud computing, big data analytics, ML, DL, and AI. Smart medical care, for example, gathers information about the human body, temperature, nutrition, moisture, and motion through IoT sensors, which are uploaded to the cloud server [23]. When thousands of fragments of information from multiple databases, cloud computing tools are used to perform efficient ML and AI computations in order to data process information. Ultimately get a human health study, a balanced diet, and a realistic recommendation for exercise, pre-symptom disease prediction, etc [24].

The Blockchain tools are modern *'Distributed Accounting Method'*. Simple innovations like work delay, hash chain in production, reward systems have been implemented to circumvent the problems in conventional academics [25]. The problem of collaboration and social trust between the multi-parties has been almost correctly solved by decentralization and de-confidence. For maintaining a solution collectively for point-to-point value check and secure database and it transfers, *'Sharing Writing'* and *'Collective Involvement'* of information was achieved [26, 27]. The blockchain has been moved the importance of cryptography and the other realms as underlying encryption technology. Researchers have performed comprehensive research on blockchain technology includes protocol analysis and implementation in individual fields.

3 ODSD proposed model

3.1 Blockchain technology

The important components in the blockchain systems are essential in transaction data, important consensus mechanism, distributed ledgers, total and distributed network application, and stable distributed WSN network. And Fig. 1 illustrates the framework of blockchain technology. The underlying information is fixed into blocks, and in chronological order, each block is chained like a sequence, which is called the blockchain. A distributed ledger, it means a blockchain, is stored by every node over an entirely distributed network. The WSN protocol is used to communicate with each other within the WSN. It compromises processes, and both users will reach an agreement. These are the origins on which superior applications are created. Agent advances are in this system, the non-tampering blockchain data structure, job system

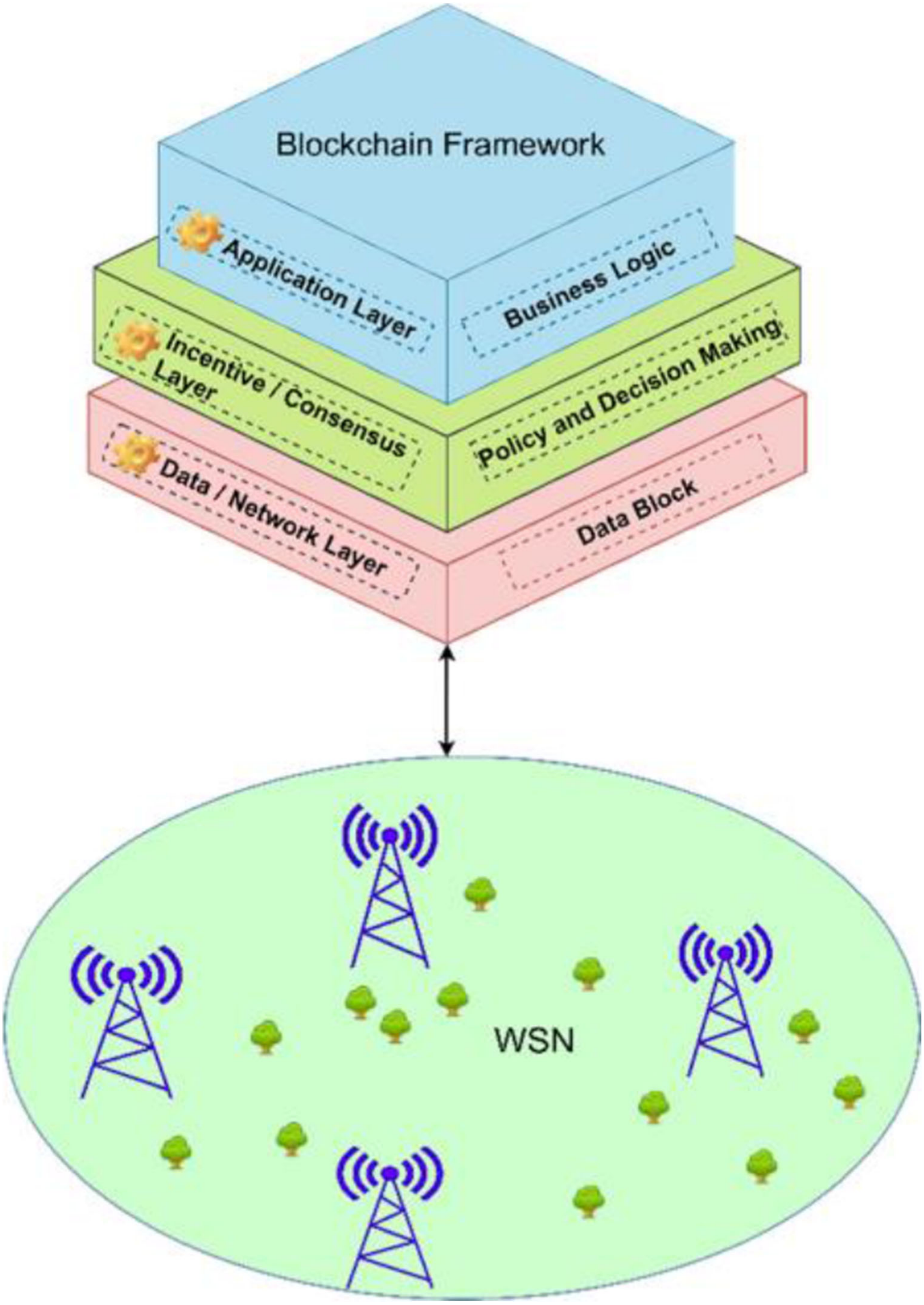


Fig. 1 A fundamental framework of blockchain technology for WSN

evidence, consensus process over a distributed network, and the progressively versatile smart transactions [28]. In specific, blockchain technology may be loosely divided into three groups: a consortium, private, and public blockchain, probably depends on the limitation of the sensor nodes in WSN.

(a) **Consortium Blockchain:** The chain of consortia is limited to alliance members. Applicable laws of the agreement formulate Read-write access verification and accounting credential. Blockchain data may be open or private and may be viewed as partially decentralized. Hyperledger is a blockchain consortium.

(b) **Private Blockchain:** Only private enterprises use private blockchains. According to the private organization's policies, read-write access authorization and login credentials are evidence.

(c) **Public Blockchain:** All users could examine and validate the transaction secretly and can also join in the consensus-making process. Bitcoin, for instance, is a public blockchain.

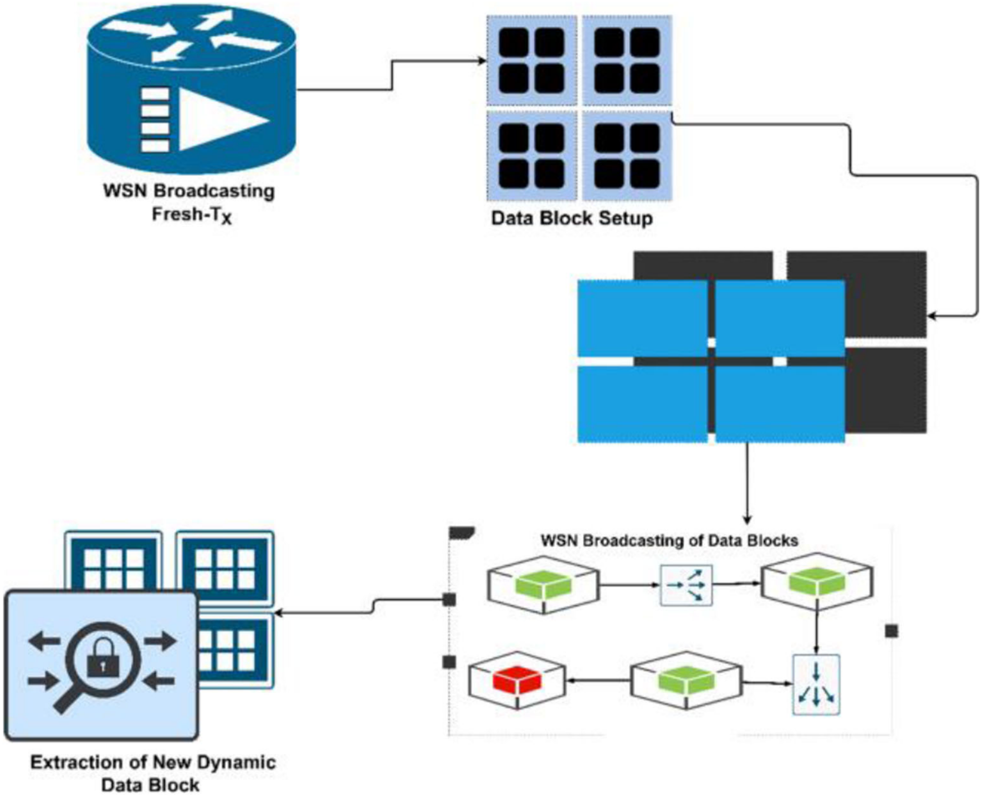
3.2 Process of a blockchain formation of ODSD

The formation ODSD method of a block will be characterized in Fig. 2 in the instance framework. Each node's account has the Hash Function (HF) of public-key (PUKY), and verification information is authorized by its private key (PRKY) [29]. The new traction T_X enhancement process has been distinguished by *"State Allocation Feature and Ownership State Statement"* and is broadcast over the WSN network. Each node in blockchain attends reliably over the router and collects a record of the transaction that has not yet been exhibited in the blockchain. The candidate validated blocks have been made; each node certifies the block decides if and received, like duplication and incorrect signature, there is invalid trading over the block. The block's checked results are broadcast again via the WSN, and the system will finally indicate the current consensus as *'New Block'* in according to the consensus method provided in this research paper in "Consensus model on node verification process," including it in the ledger via the previous block's header connexion. The most recent record is also the system's longest blockchain. The account node would broadcast it out to the entire network. Other network nodes can compare it to the local blockchain after it is obtained. If the length of the new chain is much extended, then it can replace the local blockchain.

3.3 ODSD of the data processing in WSN

Distributed consensus is the most crucial issue which needs to address for creating a complex data traceability system depends on blockchain technology based on a *"zero confidence."* However, the criteria of the public between anonymous situations and the rights to control the conditions for consensus are incredibly different. For instance, in systems with financial systems, the highly decentralized decision-making role, like Bitcoin, implement an economic incentive tool to allow each node to attain an agreement over the validity block of data efficiently. It makes it easy and powerful for freely joining nodes in the public blockchain. Dynamic data are typically based on internal business data that are closely linked with work processes, and also with consortium chain that allows only permitted nodes for participating is too appropriate for dynamic data management. In the monetary system, consensus features do not extend to the management of complex data under blockchain consortium. Under this chain of the consortium, the multi-party involvement has some prerequisites of the trust with interest towards restrictions. In this segment, we recommended where the core of distributed node benefit with a specific industry for making full cumulative utility of all nodes in distributed computing and environmental interaction by analyzing authentic motive in the decision-making [29]

Fig. 2 Creation of dynamic data blocks by blockchain process


WSN Broadcasting Fresh-T_X
Data Block Setup
WSN Broadcasting of Data Blocks
Extraction of New Dynamic Data Block

of a particular node during group game, by analyzing further about the boundary situations agreed by every node in the dynamic data traceability system.

3.4 ODSD blockchain storage of data for wireless sensor node

Multiple heterogeneous subsystems also make up the sensor network, and different network nodes had various capabilities over energy, computation, storage, and communication. In addition to these network nodes that use various sensor types, make types of data collected from modifying. The shared data storage system for the management and storage of data in the WSN should be implemented [30, 31]. The blockchain has the decentralization benefit. Also, storage of data based on decentring attributes can be achieved in WSN, where nodes need not be trusted utilizing encryption algorithms, timestamp, consensus mechanism, and tree structure. Each network node will store its data using the Merkle tree in the blockchain. The node data shall be contained in Merkle tree leaves. Each stored data point will become a block, and each node store the data that are connected to form a blockchain of data.

3.5 ODSD blockchain-based access control

We used blockchain for correct security storage to access the data stored in sink nodes. In authorized storage, transactions are included data callers, data owners, and a few added metadata. Each block of data is set for access rights, and it is time-limited. The right to access the data may be extended or removed by the data owner. Another node checks the privileges record via a corresponding distributed HF for any data retrieval request. Malicious nodes, potentially, will exchange data without authorization. Hence privileges of data are monitored. Unauthorized data access can be identified. Moreover, it will be removed from the network if the malicious node is found. The probability of such insecure access to the data is, therefore, minimal.

3.6 ODSD data security storage model in the WSN network

Redundancy is also implemented in storage systems to increase system reliability. The code deletion approach is getting more and more attention as an effective redundant strategy—popular delete code remedy for *(D_i, D_j)* maximum distance separable code, such as BCH. If data loss happens to a storage node, the original data may be recovered by redundant coding. Usually, the volume of data transmitted is greater than the node's storage capacity when a node recovers data loss—these findings in tremendous use of bandwidth. The recovering code of optimized fixed bandwidth proposed to solve the erasure code problem. As an enhancement to BCH code, regenerative code not only preserves the property of MDS erasure code but also substantially reduces the network bandwidth needed by incorporating the principle of network coding to fix unsuccessful data. This paper makes the data protection storage method in edge computing, based on the regeneration code and Blockchain (Fig. 3).

4 ODSD system model

It is considered that an extensive network node consists of $Node_1$ and $Node_2$ with flooded which message communication with the help of the relays ∊. All the participated nodes are the design of mobility like Euclidean planes, and it will be mentioned through three independent homogeneous probability (μ), the sensible method for the WSNs. The sources $Node_1$ are described by the Eq. (1)

$$\mu\{Node_1\} = \left\{\mathrm{P}_1\cdots\mathrm{P}_\mathrm{j}\right\} \tag{1}$$

where P_i, $\exists_i \in W$, represents the location of Node_1 source $N_1.\mu$, $Node_1$ has intensity σ_1, which represented the average number of the points per unit. As per Eq. (2)

$$\mu\{Node_1\} = \left\{\mathrm{Q}_1\cdots\mathrm{Q}_\mathrm{j}\right\} \tag{2}$$

with the intensity σ_2 representing location $\mathrm{Q_j}$, $\exists_\mathrm{i}\in\mathrm{W}$, of Node_2 the source N_2 and μ= $\{\mathrm{R}_1\ldots\ \mathrm{R}_\mathrm{k}\}$, $\exists_\mathrm{i}\in\mathrm{W}$, along with the intensity μ, location R_k of relay R_k.

Every node is represented and prepared along with the Single-Input-Single-Output sources, and target nodes ($Node_1$, $Node_2$) are in equal resources. Where all the nodes have been driven through Node Energy (NE) along with the initial energy level $NE_{1,}$ addition to this, relays should be capable of electromagnetic radiation by using Harvesting System (HS) separately with fixing antenna that is a specifically received antenna which is required to change RF energy into the direct electricity along with the efficiency η. The relay can harvest the electromagnetic energy, which emits through transmitting of source node N_1, with other relays and transmission (Fig. 4).

4.1 Hypotheses of distributed storage system

And we aim at the layer of the distributed storage system and achieve improved reliability and reduces the access delay. Let us consider the IoT cluster that consists of '*N*' number of sensor nodes. For its coherence, WSN holds the below Hypotheses (H):

> H_1: Every *'N'* node to be homogeneous, with every identical storage space.

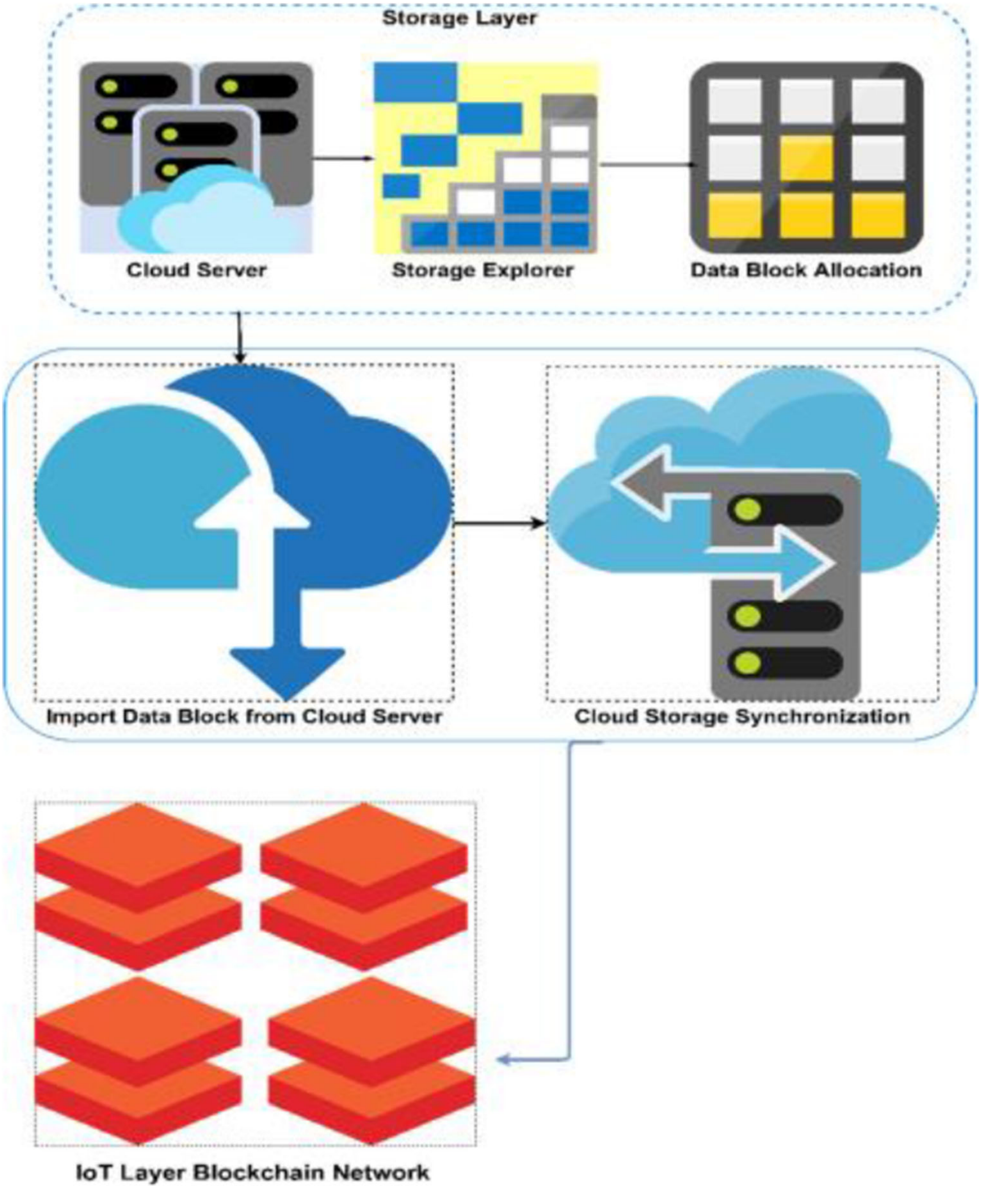

Storage Layer
Cloud Server
Storage Explorer
Data Block Allocation
Import Data Block from Cloud Server
Cloud Storage Synchronization
IoT Layer Blockchain Network

Fig. 3 The model storage of data based on Blockchain in WSN

H_2: When the IoT node fails to secure the information, the node will be damaged.

H_3: The number of nodes *'N'* is adequate for the enormous storage of data for keeping all files.

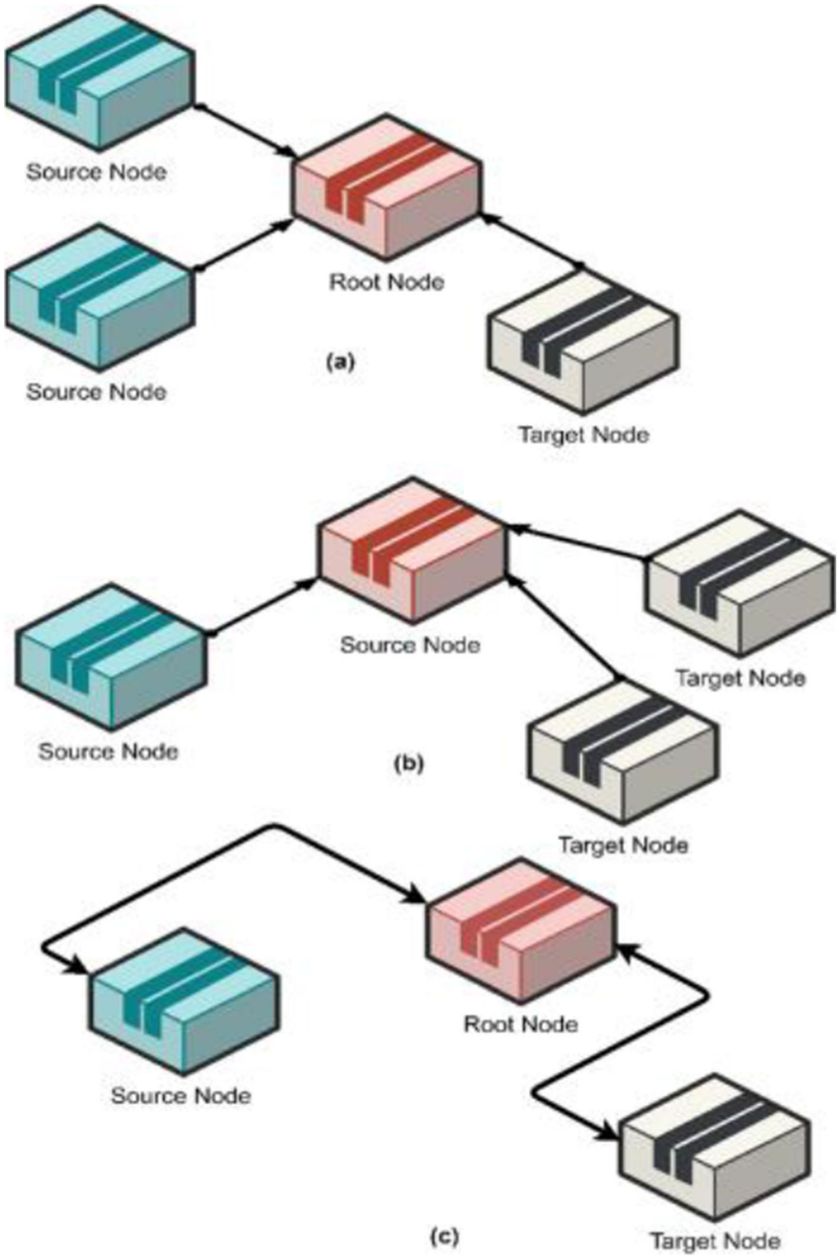
The aim of this distributed storage has to occupy the data series of Data Volume ($D_1, \cdots D_i$) across various selected nodes in a distributed way, though enabling reliable and fast recovery of the actual file when required. In this context, the term "Data Volume" signifies raw blockchain data created through the blockchain network. Where every file comprises a single/several blockchain data, it may decide by the system controller.

For distributing a series of Data Volume ($D_1, \cdots D_i$) that will be stored in IoT nodes, it can split every Data Volume into fixed-size chunks D_i, and then it uses a ($D_i, \ldots D_j$) Bose–Chaudhuri–Hocquenghem (BCH) codes for generating encoded chunks (D_i), including parity (D_i-D_j) fragment of file information. Depend upon the property of BCH coding, and original data will be recovered through collecting many numbers of D_j encoded chunks. Thus, the system model is indicated in Fig. 5.

In Fig. 6, the working model of the system is defined in the following steps:

1) This system reads the disk sector of the complete blockchain data D_i that are recently formed. The blockchain data were collected through the cloud server, using all the collected data, and then sent to the subordinate IoT node through the virtual machine.
2) These splits read data into the D_j fixed-size fragment of information on file and again utilizes the BCH method for

Fig. 4 Message distribution a) Route 1 (Node$_1$⇒∈) Route 2 (Node$_2$⇒∈) Route 3(Node$_1$⇒∈)



generating D_i encoded chunks; it includes parity information's D_i-D_j.

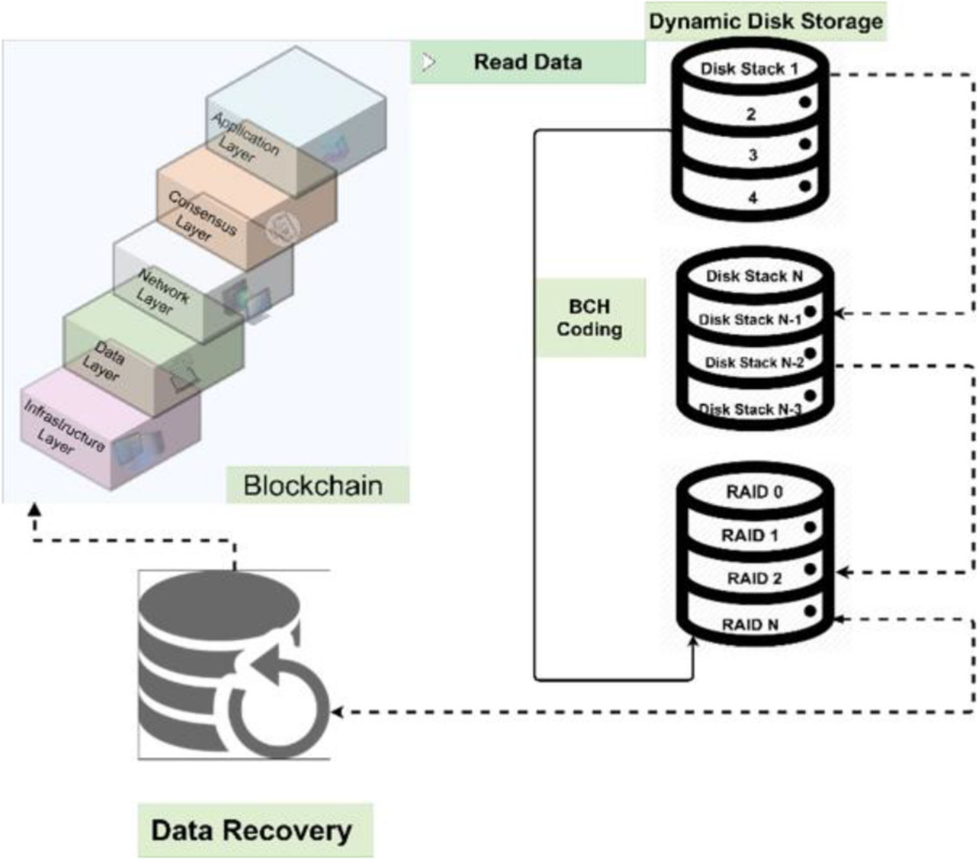
3) The systems also schedule D_i encoded chunks into many IoT nodes for storing data.
4) While blockchain receives a reading request, the system receives any D_j with different chunks, and it recovers the original blockchain data.

4.2 Description of scheme of ODSD

A new block of data can be broadcast, which will be processed in the sensor network. And for the data block, each network node calculates the Ownership of Data Verification (ODV) challenge. ODV method is used to verify if data is corrupted on the remote node. If the ODV is appropriately checked, the node will store the new data block, and the node can receive the benefit for storage of data block, i.e., a digital currency unit, as an outcome (Fig. 6). The proposed method is as termed in the following.

(i) A new data block $Message=\{Msg_1, \cdots Msg_n\}$ it has been stored, and the public key of the data publisher is represented by (G^x, U), and PR_k shows the private key; HF_1, It preserves hash function and the data publisher processes $\{HF1(Msg_i)\}$ and it creates authenticator Σ_i=(HF_i U^{mi})

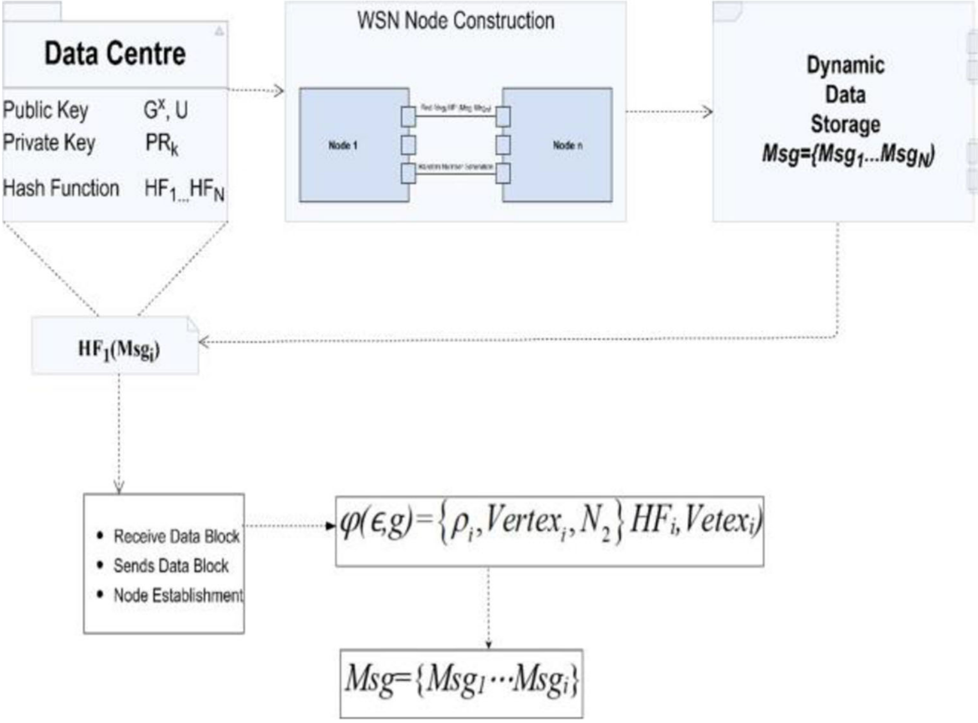
Fig. 5 System model for distributed storage system



PR_k with each subblock Msg_i; And the data request for the information is broadcasted through the WSN.

(ii) Each network node finding for stored sub-block message $Msg_i^{'}$ which is nearest to value depend on $HF_1(Msg_i)$, so

Fig. 6 Incentive mechanism based on ODV



that it provides, $HF_1(Msg_i)-HF_1(Msg_i^{'})\leq dif.$ Later, Random Number (RN$_i$) could be chosen principally for the sub-data block ($Block_i$) of the data block (Msg), represented as $DP=(\, Block_{i,}\ RN_i\,)$. The network node transmits $HF_1(Msg_i^{'}\ )$ and data distributor (server).

(iii) The data distributor accepts $HF_1(Msg_i^{'}\ )$ from each and every node, and it relates it with the $HF_1(Msg_i)$ value, for selecting $HF_1(Msg_i^{'}\ )$ value that is very close by to every $HF_1(Msg_i)$ data value, and it adds the network node $Block_j$ which sends $HF_1(Msg_j^{'})$ *data* value to the node-set $Node_1$.

(iv) The node in the network set $Node_2=(\in,\varepsilon)$, proving the resulting phrase: $\varphi(\epsilon,g)=\{\rho_i, Vertex_i, N_2\}HF_i,\ Vetex_i)$.

If it results in True, the data distributor can send data block $Msg=\{Msg_1\cdots Msg_i\}$ for every network node of $Node_2$ for data storing and to send node for digital currency feature. (v) By nature, the supporting HF, it will be detected that the real data block of every network node is in $Node_2$ has similar data for a new set of data block $Msg=\{Msg_1\cdots Msg_i\}$ so that it needs for storing the part which is not like real data. Therefore, by this method, it will be great to reduce the required storage space.

5 Performance analysis and verification of dynamic blockchain

The dynamic blockchain is proposed for consensus mechanism based on Node Validity (NV). This system allocates NV nodes through agencies, and it requires database local services that may not be altered, and it will restore at a given time. Dynamic data HF blocks can be transmitted and processed in any aggressive sensor nodes of WSN. Thus, all the nodes made up the dynamic storage of data systems, and it is tough to distribute the database. While another loss of data over every node will be validated by the test protocol, obtained through a portion of the HF nodes in the database. Where all other more gained energy nodes will be stored in the entire database at the same time, and the standard function of the whole database that would not affects suppose if any other node for a data block in dynamic will be destroyed and the performance results are verified and labeled below.

1.1 Algorithm for ODSD Block validity verification algorithm

Algorithm 1: Algorithm for ODSD Block validity verification algorithm

```
 INPUT: Blockchain X, New Entry Data Block Y; OUTPUT: ;
if blockchain X or New Entry Data Block Y does not exist then THEN;
 Return error;
 else
 end
 X = Correctness + X Blockchain Y THEN; Return Y;
 X= Incorrectness THEN; Return X;
 Start-Process;
 Function Validate Data Block (X, Y); X=Valid (Node);
 Y pow (Xs) THEN
 while (Valid=Node_N ) do
 end
 Add Node.
 ELSE
 X=Not Valid Return(X)
 }
  END IF
 Return(Y)
 ELSE
 {
  Return (Error)
 }
  END IF
 }
 }
 }
 }
  End Process
```

5.1 Lifetime of sensor node

In the end, transmission period $Time_{MSG}$, the node energy level of the relay, by not considering Energy Saving (ES) into account, is represented by Eq. 3.

$$EngerLevel(EL_{ES}) = EnergyLevel(EL_{ES})-MsgTime_s(U_r+Packet_{Time}) \quad (3)$$

EL_1 is the initial energy level of the system, U_r is the energy consumed at response mode, and the pact is the likelihood of the dynamic relay. In such cases, the relay has ES resources, and the energy level is represented by where EL provides the initial energy level, U_r is power consumption during the response phase, and the pact is the probability of the active relay. In such cases, that relay has ES capability, and its sensor node level is represented by Eq. (4)

$$EngerLevel(EL_{ES}) = EnergyLevel(EL_{ES})-MsgTime_s(U_r+Packet_{Time}) + \sum_{i}^{n}(Packet_{Time}) \quad (4)$$

where the $Packet_{Time}$ along with $Time=1\ldots N$ could be the rapidly harvested powers with the equivalent time slots and the origins of relay's node lifetime Msg_{max} for these two cases, correspondingly

$$Msg_{\max} = \left[\frac{EL_1}{Time_s(2U_r + Packet_{Time})} + \frac{EL_1}{Time_s(2U_r + Packet_{Time}) - Time \sum_i^n Packet_{Time}}\right] \tag{5}$$

The lifetime will become infinite due to the harvested energy is lost energy. The instantaneous harvested power through EMR that receives power over EHS through interferers, and scaled through efficiency σ of the harvester that is represented in Eq. (6)

$$Packet_{Energy} = \left\{\sum_{x=1} Packet_{Time} ES_x X^{-1}\right\} \tag{6}$$

5.2 Optimization solution

To apply convex relaxation, have to define two functions for optimization problem Eqs. (7) and (8)

$$HF_1(D_i, D_j) = \frac{1}{\prod}\left[\frac{D_i}{D_i - D_k}\right] \tag{7}$$

$$HF_2(D_i, D_j) = \frac{1}{\prod}\left[\frac{D_i + 1}{(D_i - D_k) + 1}\right] \tag{8}$$

The functions $HF_1(D_i, D_j)$and $HF_2(D_i, D_j)$have various properties. Initially, $HF_1(D_i, D_j)$ and $HF_2(D_i, D_j)$ are both decreasing the functions of $D_i(D_j)$. Next, $HF_1(D_i, D_j) + 1$. And the third, $(D_i - D_k) + 1$ due to the following inequalities, Eq. (9)

$$HF_1(D_i, D_j) = \frac{1}{\prod}\left[\frac{D_i}{D_i - D_k}\right] \le HF_2(D_i, D_j) = \frac{1}{\prod}\left[\frac{D_i + 1}{(D_i - D_k) + 1}\right] \tag{9}$$

That is $HF_1(D_i, D_j)$ and $HF_2(D_i, D_j)$ serve as upper and lower bounds of Limits (D_i, D_k), respectively. The data transmission delay of the upper and lower limit threshold is $HF_1(D_i, D_j)$;$HF_2(D_i, D_j)$ is depicted in Fig. 7. We assumed to set *Key=100; l=20;* $\varnothing$*=100;* ∂*=3* which are typical values and used in the evaluation chapter. Here, we can see the curve of $HF_1(D_i, D_j)$ and curve of $HF_2(D_i, D_j)$ together were n increases, which means the change ensues between the two bounds could be sufficiently small.

So $HF_1(D_i, D_j)$ and $HF_2(D_i, D_j)$ could be strong as necessary.

6 Performance evaluation of ODSD

6.1 Storage of data based on the global blockchain

These research investigations use Amazon S3. The response time of a distributed cloud storage service consisting of multiple cloud storage services is more reliable and quicker than a single cloud storage service. Since multiple copies of data are supported by blockchain-based cloud storage and can exploit the network capacity of multiple cloud storage providers, overcoming a single cloud server's bandwidth limitation.

When using regenerative code to repair failed files, the repair bandwidth, and disc I/O is reduced in the case of blockchain-based replica repair. And as the redundancy m increases, the decrease in bandwidth and disc I/O allows being repaired. Additionally, for both average repair bandwidth and average disc I/O, m can be effectively decreased. When, as decreases, rises, and grows the fastest is the standard deviation of the normal distribution of the target availability level. As a result, for highly accessible cloud storage devices, the bandwidth and disc I/O needed for repair would be dramatically reduced. If the server is less available, as a replica repair node, it can add a high-availability server to prevent large β_s that consume large quantities of storage space. Furthermore, due to the relative average repair bandwidth to total capacity, a decrease in average repair bandwidth often decreases total capacity. Therefore, as the alpha does not alter in the regeneration code, the rise of m would lead to an increase in total storage, the maximum increase in (β*-1*) Node α_1.

The computation of HF and the creation of the Merkle tree are efficient, requiring not too much computation and storage resources. In order to examine the effect on the data repair process of the heterogeneity of the processing node energy, we measured the impact of the Balance Energy coefficient of sensor nodes and the transmission and repair time of nodes on data. The higher the value of Balance Energy in the actual test phase, the longer the node will phase the information and data; the shorter, on the contrary. Figure 8 demonstrates how the entire process's repair time changes with the remaining resources. The greater the Balance Energy value, the more stable the node is, and the longer it takes to process data.

6.2 Evolution of delay-cost trade-off

The delay-cost trade-off of the different λ values is explored first. In this function, changes in λ value will reflect in the

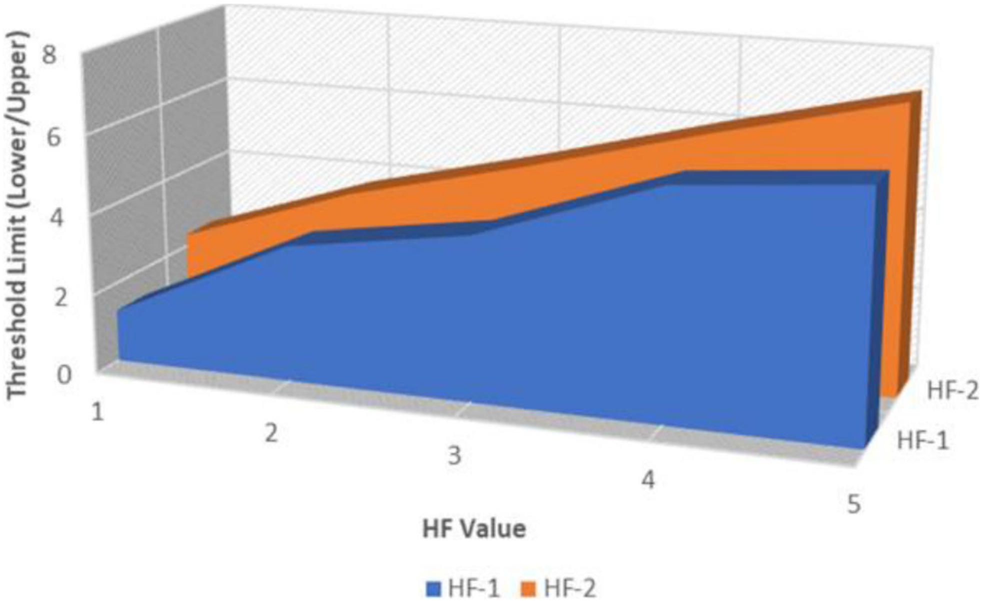


Fig. 7 Performance of threshold limits using HF_1 and HF_2

system trade-off situation. In Fig. 9 (a) (b) (c) (d), it illustrates the trade-off curves along with the cost function as *Stoage+ Threshold (0:0.5,0:6,0.5:0,1:0.5)* respectively. Each curve, the continuous change λ from 0 to 1, and it calculates corresponding delay and cost values. The results proved valuable insight over the system trade-off in the decision-making process.

Figure 10 shows all the three curves under the same coordinate that produces the relationship among various system trade-off clearer.

Besides, since the objective of our proposed distributed storage architecture based on BCH coding is to reduce space consumption over each blockchain network node while comparing with our proposed storage technique consumption with the conventional blockchain paradigms. In Fig. 11 for a comparison of storage space consumption based on simulation.

That is because our storage based on BCH coding has significant advantages over the conventional paradigm of blockchain storage. As can be inferred from Fig. 11, for each node, our design will save up to 91.18% storage space,

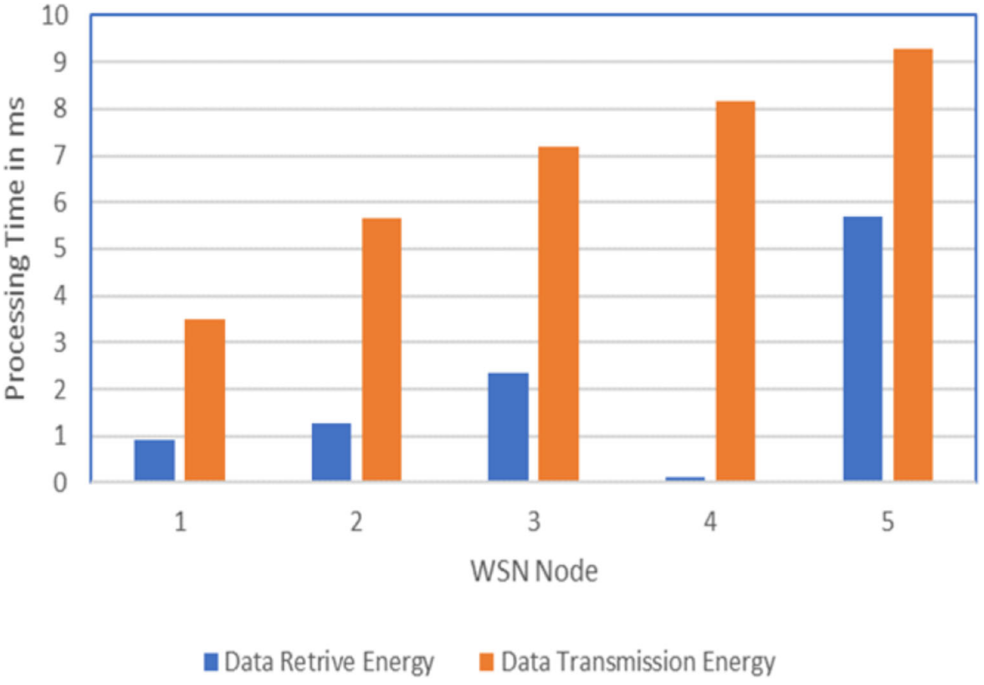
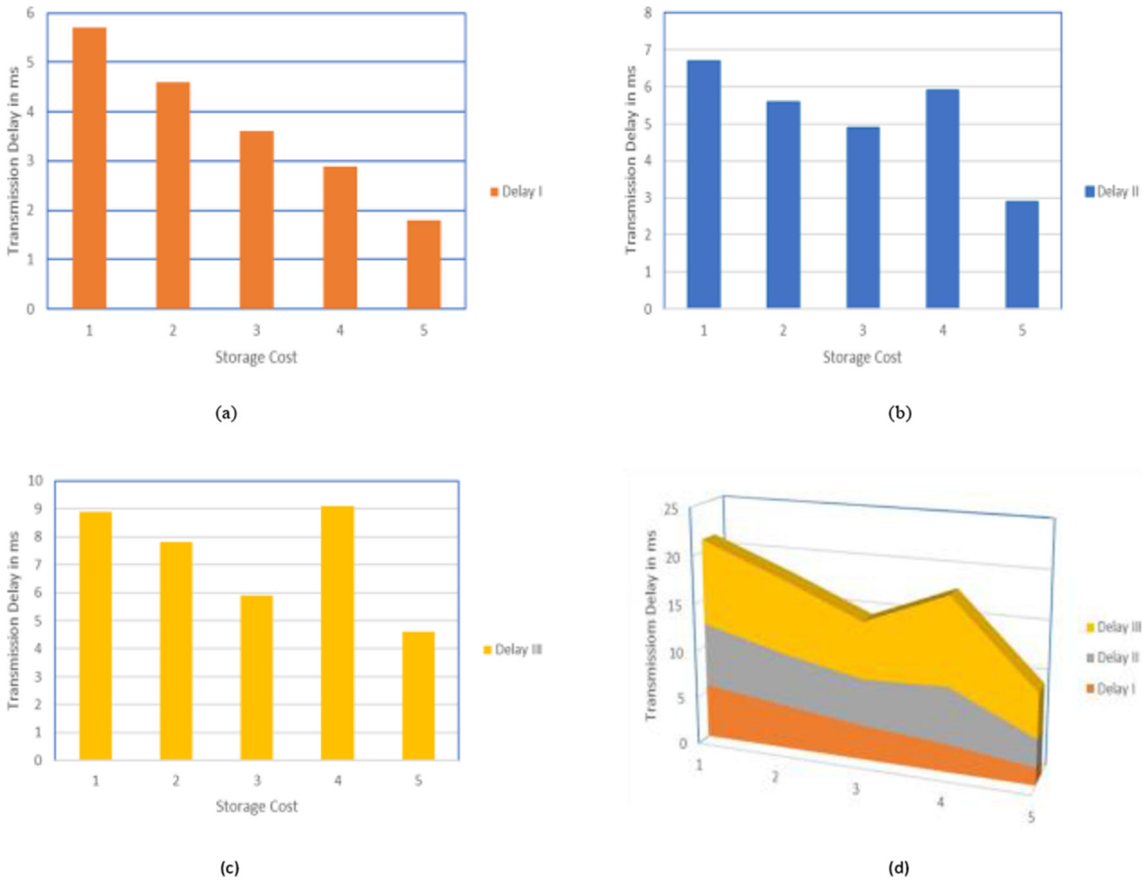


Fig. 8 Effect of Balance energy on data recovery and transmission



(a)

(b)

(c)

(d)

Fig. 9 Trade-off, (**a**) (**b**) (**c**) *Stoage + Threshold (0:0.5,0:6,0.5:0,1:0.5)*

eliminating the greatest obstacle to the incorporation of blockchain into the IoT network.

In addition, we could not concentrate only on the storage usage of each node as a distributed storage system, but also on the storage redundancy of the entire system. A balance exists between the usage of single node storage and redundancy of entire system storage. By encoding original data to more chunks, we can decrease the use of single node storage, but

Fig. 10 Performance of storage transmission delay and cost of HF

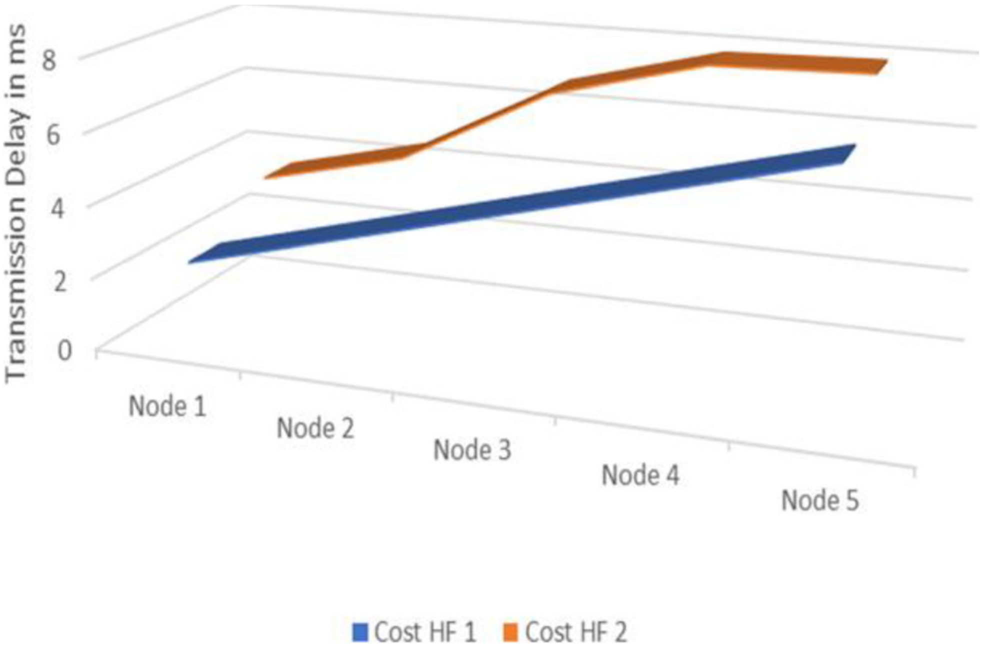
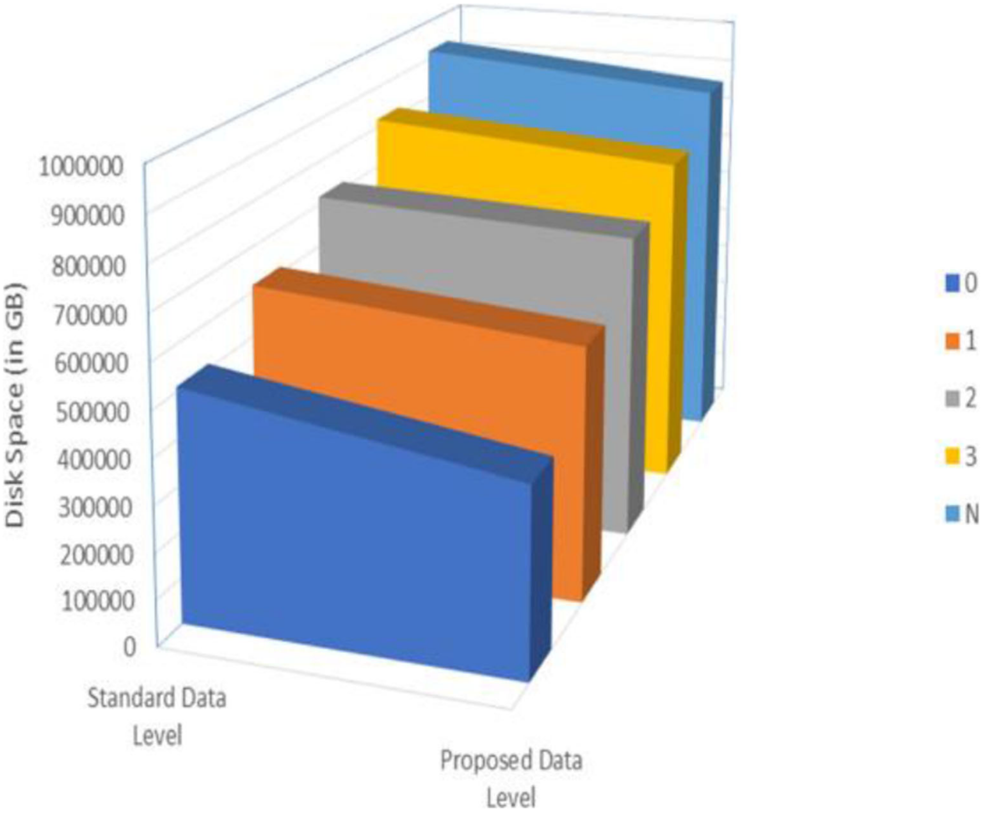


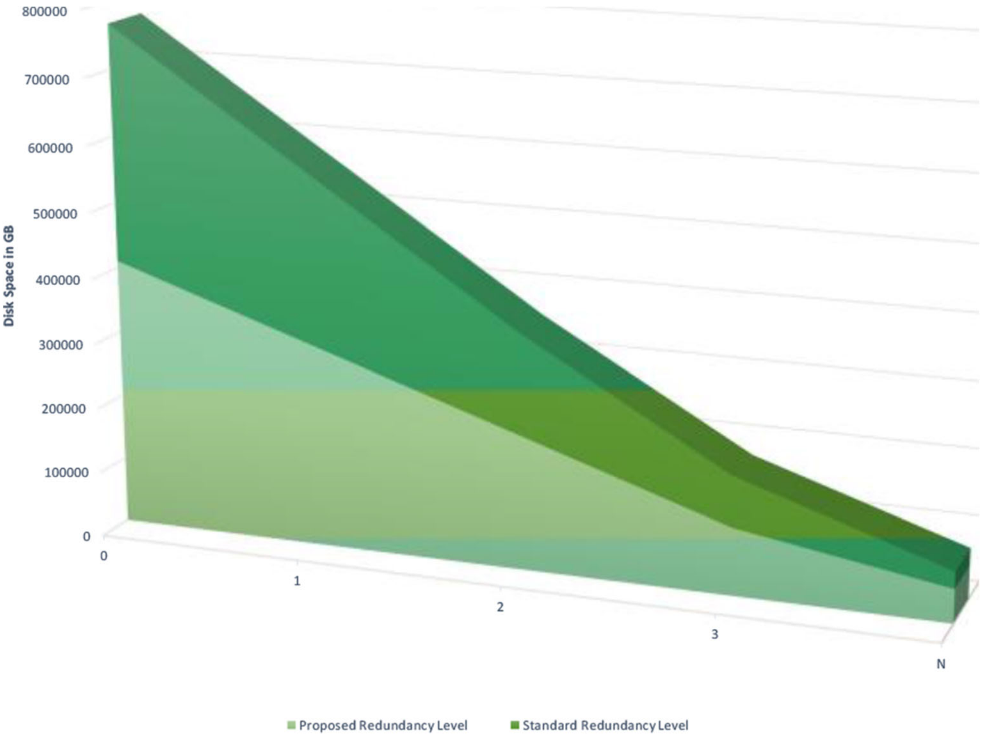
Fig. 11 Comparison analysis of disk storage standard vs. proposed



that will increase the overall redundancy of storage. Figure 12 indicted a storage redundancy of the WSN system.

We may infer from Figure 12 that overall storage redundancy is imported through our architecture is about 1.8 times,

Fig. 12 Storage redundancy comparison



which is very appropriate, given the massive storage space-saving of each node.

7 Conclusion

In this paper, based on the blockchain, the first incentive protection of node storage of data methods for WSN storage of data is constructed. Storage of data protection under edge computing has become an obstacle to its widespread use, affecting smart computing evolution. The incentive for digital currency can be collected through the storage of the data node, and as data hold to increase, the incentive for the implementation of the sensor node increases. We suggested a ODSD distributed storage Blockchain-IoT architecture based on WSN in this research work. It creates feasible to significantly reduce the overhead of storage for each node without affecting the overall integrity of data. We also proposed ODSD novel analytical methods for characterizing and analyzing the actions of wireless driven networks to accomplish WSN. In addition, the confirmed ownership of data in the proposed scheme is made to replace proof in the primary bitcoins that perform new data block storage and mining. It is stated that due to delay in data transmission, dynamic data blockchain becomes less likely to create multiple chains, including a length difference of more than 1.

Further, we determined a latency-cost trade-off optimization problem to minimize the latency of restoring data in distributed storage architecture and proposed an effective and scalable by the proposed method. The out- comes of the simulation show that the proposed model is achieved latency reduction of up to 87.19% while associated with other standard used for dis- tributed storage systems. Furthermore, our model will save up to 91.18% storage disk capacity for every node by reducing major drawbacks to incor- porating Blockchain into the IoT network. In the end, new data will be stored in node closes with current data due to the preservation of hash functions. And only the various subblocks are in stock. Hence the node storage space in WSN can be saved too.

References

1. Khalaf OI, Abdulsahib GM, Sabbar BM (2020) Optimization of wireless sensor network coverage using the bee algorithm. J Inf Sci Eng 36(2):377–386
2. Al-Mughanam T, Aldhyani THH, Alsubari B, Al-Yaari M (2020) Modeling of compressive strength of sustainable self-compacting concrete Incor- porating treated palm oil fuel ash using artificial neural network. Sus- tainability 12:9322
3. Subahi AF, Alotaibi Y, Khalaf OI, Ajesh F (2020) Packet drop battling mech- anism for energy aware detection in wireless networks. Computers, Ma- terials and Continua 66(2):2077–2086
4. Hadi TH, Joshi MR (2015) Handling ambiguous packets in intrusion detection. 2015 3rd International Conference on Signal Processing, 2015, pp. 1–7, Chennai, Communication and Networking (ICSCN)
5. Xiang X, Li Q, Khan S, Khalaf OI (2021) Urban water resource manage- ment for sustainable environment planning using artificial intelligence techniques. Environ Impact Assess Rev 86:106515
6. Yu K, Tan L, Aloqaily M, Yang H, Jararweh Y (2021) Blockchain-enhanced data sharing with traceable and direct revocation in IIoT. IEEE Trans- actions on Industrial Informatics. https://doi.org/10.1109/TII.2021.3049141
7. Khalaf OI, Abdulsahib GM (2020) Energy efficient routing and reliable data transmission protocol in WSN. International Journal of Ad- vances in Soft Computing and its Application 12(3):45–53
8. Feng C et al (2021) Efficient and secure data sharing for 5G flying drones: a Blockchain-enabled approach. IEEE Netw. https://doi.org/10.1109/MNET.011.2000223
9. Prasad SK, Rachna J, Khalaf OI, Le D-N (2020) Map matching algo- rithm: real time location tracking for smart security application. Telecom- munications and Radio Engineering (English translation of Elektrosvyaz and Radiotekhnika) 79(13):1189–1203
10. Yu K, Tan L, Shang X, Huang J, Srivastava G, Chatterjee P (1 March 2021) Effi- cient and privacy-preserving medical research support platform against COVID-19: a blockchain-based approach. IEEE Consumer Electronics. Magazine 10(2):111–120. https://doi.org/10.1109/MCE.2020.3035520
11. Yu K, Lin L, Alazab M, Tan L, Gu B (2020) Deep learning-based traffic safety solution for a mixture of autonomous and manual vehicles in a 5G-enabled intelligent transportation system. IEEE Transactions on In- telligent Transportation Systems. https://doi.org/10.1109/TITS.2020.3042504
12. Alkahtani H, Aldhyani THH, Al-Yaari M (2020, Article ID 6660489, 2020) Adap- tive anomaly detection framework model objects in cyberspace. Ap- plied Bionics and Biomechanics:14. https://doi.org/10.1155/2020/6660489
13. Khalaf OI, Abdulsahib GM, Kasmaei HD, Ogudo KA (2020) A new algorithm on application of blockchain technology in live stream video transmissions and telecommunications. International Journal of e- Collaboration (IJeC) 16(1):16–32
14. Salman AD, Khalaf OI, Abdulsahib GM (2019) An adaptive intelligent alarm system for wireless sen- sor network. Indonesian J Electric Eng Comput Sci 15(1):142–147
15. Ogudo KA, Muwawa Jean Nestor D, Ibrahim Khalaf O, Daei K (2019) A device performance and data analytics concept for smartphones. IoT services and machine-type communication in cellular networks. Symmetry 11:593
16. Khalaf OI, Abdulsahib GM (2019) Frequency estimation by the method of minimum mean squared error and P-value distributed in the wireless sensor network. J Inf Sci Eng 35(5):1099–1112
17. X. Zhang, L. Yang, Z. Ding, J. Song, Y. Zhai and D. Zhang, “Sparse Vector Coding-Based Multi-Carrier NOMA for In-Home Health Networks,” IEEE Journal on Selected Areas in Communications, vol. 39, no. 2, pp. 325–337, Feb. 2021, doi: https://doi.org/10.1109/JSAC.2020.3020679
18. Aldhyani THH, Alrasheedi M, Alqarni AA, Alzahrani MY, Bamhdi AM (2020) Intelligent hybrid model to enhance time series models for pre- dicting network traffic. IEEE Access 8:130431–130451
19. Dawle Y, Naik M, Vande S et al (2017) Database security using intrusion detec- tion system. Int J Sci Eng Res 8(2):30–34
20. Ning HS, Xu QY (2010) Research on global internet of things' developments and it's construction in China. Acta Electron Sin 11:2590–2599
21. Y. Ren, J. Shen, J. Wang, J. Han, and S. Lee, ‘Mutual verifiable provable data auditing in public cloud Storage,” J Int Technol, vol. 16, pp. 317–323, 2015

22. Yetgin H, Cheung KTK, Ei-Hajjar M, Hanzo L (2015) Network-lifetime maximization of wireless sensor networks. IEEE Access 3: 2191–2226
23. Shi N et al (2020) A Blockchain-empowered AAA scheme in the large-scale HetNet. Digit Commun Netw. https://doi.org/10.1016/j.dcan.2020.10.002
24. Jiang Q, Wei F, Fu S, Ma J, Li G, Alelaiwi A (2016) Robust extended chaotic maps-based three-factor authentication scheme preserving bio- metric template privacy. Nonlinear Dynamics 83(4):2085–2101
25. Sodhro AH, Pirbhulal S, Muzammal M, Zongwei L (2020) Towards Blockchain- enabled security technique for industrial internet of things based De- centralized applications. J Grid Computing 18:615–628
26. L. Zhao, G. Han, Z. Li, L. Shu (2020) Intelligent digital twin-based software-defined vehicular networks. IEEE Network, https://doi.org/10.1109/MNET.011.1900587
27. Liang Z, Zhao W, Hawbani A, Al-Dubai A, Min G-o, Zomaya AY, Gong C (2020) Novel online sequen- tial learning-based adaptive routing for edge software-defined Vehic- ular networks. IEEE Transactions on Wireless Communications. https://doi.org/10.1109/TWC.2020.3046275
28. Zhang J et al (2021) 3D reconstruction for motion blurred images using deep learning-based intelligent systems. CMC-Computers, Materials & Con- tinua 66(2):2087–2104. https://doi.org/10.32604/cmc.2020.014220
29. Zheng X, Ping F, Pu Y, Montenegro-Marin CE, Khalaf OI (2021) Recognize and regulate the importance of work-place emotions based on organizational adaptive emotion control. Aggression and Violent Behavior:101557
30. Dai H-N, Zheng Z (2019) Blockchain for internet of things: a survey. IEEE Internet Things J 6(5):8076–8094
31. Zhao L, Bi Z, Lin M, Hawbani A, Shi J, Guan Y (2021) An intelligent fuzzy- based routing scheme for software-defined vehicular networks. Computer Netw. https://doi.org/10.1016/j.comnet.2021.107837

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Osamah Ibrahim Khalaf is a Dr. in Al-Nahrain University/ Al-Nahrain Nanorenewable Energy Research Centre. He has hold many years of university-level teaching experience in computer science and network technology and has a strong CV about research activities in computer network.

Ghaida Muttashar Abdulsahib She is a Dr. in *Department of Computer Engineering/ University of Technology, Iraq*. She has hold many years of university-level teaching experience in computer science and network technology and has a strong CV about research activities in computer network.