scientific reports

Check for updates

OPEN

Blockchain-enabled K-harmonic framework for industrial IoT-based systems

K. M. Baalamurugan[1], Prabu P.[2], Nebojsa Bacanin[3]✉, K. Venkatachalam[4], S. S. Askar[5] & Mohamed Abouhawwash[6,7]

Industrial Internet of Things (IIoT)-based systems have become an important part of industry consortium systems because of their rapid growth and wide-ranging application. Various physical objects that are interconnected in the IIoT network communicate with each other and simplify the process of decision-making by observing and analyzing the surrounding environment. While making such intelligent decisions, devices need to transfer and communicate data with each other. However, as devices involved in IIoT networks grow and the methods of connections diversify, the traditional security frameworks face many shortcomings, including vulnerabilities to attack, lags in data, sharing data, and lack of proper authentication. Blockchain technology has the potential to empower safe data distribution of big data generated by the IIoT. Prevailing data-sharing methods in blockchain only concentrate on the data interchanging among parties, not on the efficiency in sharing, and storing. Hence an element-based K-harmonic means clustering algorithm (CA) is proposed for the effective sharing of data among the entities along with an algorithm named underweight data block (UDB) for overcoming the obstacle of storage space. The performance metrics considered for the evaluation of the proposed framework are the sum of squared error (SSE), time complexity with respect to different m values, and storage complexity with CPU utilization. The results have experimented with MATLAB 2018a simulation environment. The proposed model has better sharing, and storing based on blockchain technology, which is appropriate IIoT.

The IIoT has been developing rapidly in industry and research. IIoT systems, the modern paradigm has a progression of smart technologies, contain various physical devices that are able to extract and share digitalized information. The intention of IIoT systems for smart applications enhances productivity, and real-time data more promptly for human interference[1]. Many cities, municipal governments, and communities are looking toward the technology of smart cities for the upcoming e-governance evolution. This digitally connected structure enables interactions for reducing the overhead. Also, organizations are highly dependent on the internet for their interaction in company meetings for business. Cloud service providers offer diverse services to industries with low-cost rents. Due to the expansion of cloud computing technologies, IIoT systems can be operated on a convenient platform with ease of maintenance. IIoT systems must control several machines in the network which paves the way for sufficient deployment of functions, storage benefits, and other computing performances[2]. To cope with these services in the IIoT system, new technologies are emerging exponentially in order to facilitate consumer interactions with those systems. Blockchain has been booming recently and it uses cryptography-based approaches to produce numerous associated blocks of data, with every block composed of information for validating the upcoming blocks. Security concerns are importantly dependent on Preserving privacy, non-temper ability, and distribution are features exhibited by blockchain which support deploying safe data-sharing during data transmission at the peer end[3].

[1]School of Computing Science and Engineering, Galgotias University, Greater Noida, India. [2]Department of Computer Science, CHRIST (Deemed to be University), Bengaluru, India. [3]Singidunum University, Belgrade, Serbia. [4]Department of Applied Cybernetics, Faculty of Science, University of Hradec Králové, 50003 Hradec Králové, Czech Republic. [5]Department of Statistics and Operations Research, College of Science, King Saud University, P.O. Box 2455, Riyadh 11451, Saudi Arabia. [6]Department of Mathematics, Faculty of Science, Mansoura University, Mansoura 35516, Egypt. [7]Department of Computational Mathematics, Science, and Engineering (CMSE), College of Engineering, Michigan State University, East Lansing, MI 48824, USA. ✉email: nbacanin@singidunum.ac.rs

IIoT security can be carried out in a number of ways, such as any of the employees can steal risky products, enter prohibited places, or crack data secrets by compromising or hacking the smart devices in the network. The alarm must be activated in all the entities located in dissimilar places. This clearly signifies that there is a demand to develop a number of frameworks against system controls.

Some organizations and businesses are still hesitant to adopt IoT. The 5G architecture for IIoT has been presented using three general application modes[4]. Several fields, such as the energy industry, healthcare, and internet-based vehicles have adopted blockchain to improve various processes. Existing studies on the safe sharing of data with blockchain have good improvement[5–7]. Although diverse studies have resolved the problems of privacy and security in with a privacy preservation method, the elements, the attributes and the scope of data to be shared are typically not deliberated. Every transaction has a transaction number, the address number, or the block number. Providing data sharing with data security, privacy using blockchain is important. To fulfill the aforementioned needs, blockchain must reach a consensus with advanced algorithms at the consensus layer as shown in Fig. 1 to provide the highest degree of data storage and sharing ability.

In this research work a data sharing framework based on blockchains' underweight data block algorithm and centroid-based community detection that focus on the similarity, distribution scope, and storage gain of the data to be shared. The IBM blockchain platform-based data-sharing environment has been framed to upload a vast amount of data which are collected from different IIoT devices and are made blockchain network-ready data. Based on the similarity and correlation of the gathered data, the clients are segregated. Hence before distributing the data, communities/clusters to be appropriate for sharing and retrieving are calculated by the proposed model. For best clustering performance, the Element-based K-Harmonic Means clustering algorithm has been proposed for decent community separation and for the scope of sharing. The sum of squared error is considered an effective measure for the divided clusters.

The traditional blockchain structure is presented in Fig. 2. A header and a body are the two fields of the data block[9–11]. The version number, previous block hash value, timestamp, number only used once (nonce) of the consensus layer, hash target, and Merkle in body block are stored in the header block. Overall transaction records with the transaction number are stored in the destination hashes, body block. Nonce are important fields in the traditional blockchain structure of the consensus process. Data consensus mechanism with Underweight Data Block algorithm, is applied to enable the solicitation of the blockchain technology and IIoT and to create an underweight data block. The UDB has previous block version number and hash value and block destination edge gateway, timestamp, hash value.

The data block is in Fig. 3. Thus, the UDB algorithm reduces delay and has good storage space. The main objectives is as follows:

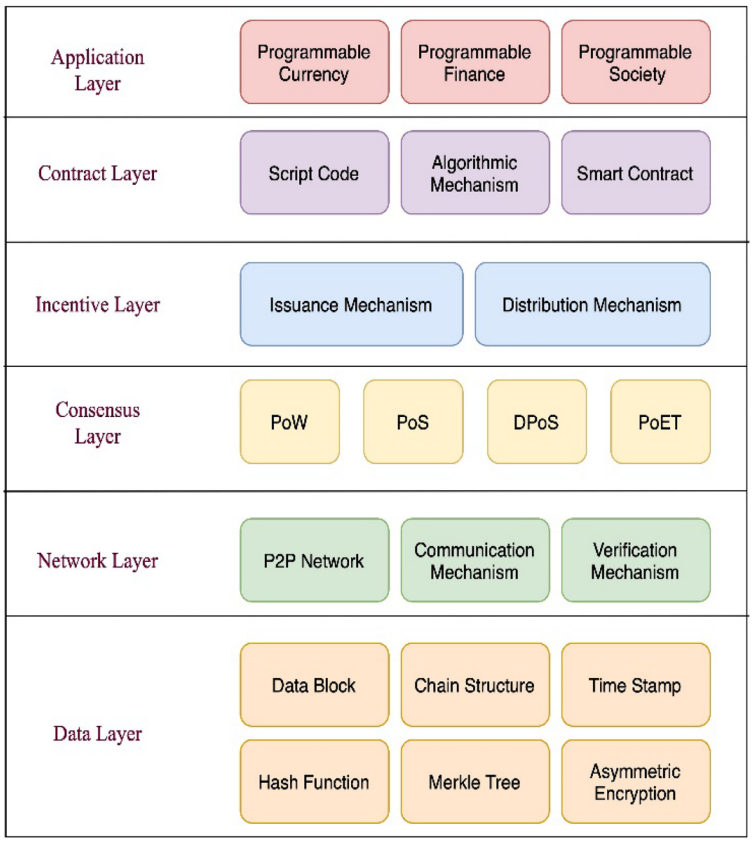

Figure 1. The layered infrastructure of blockchain technology[8].

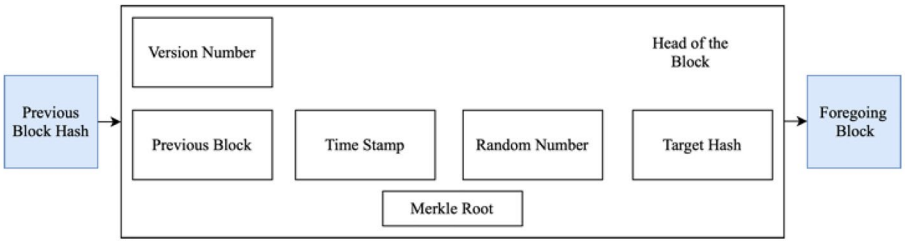

Figure 2. Basic data blockchain structure.

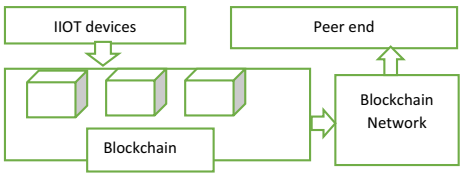

Figure 3. IIoT data blockchain structure.

- To build an expert framework for secure storing and sharing of data using Element-based K-Harmonic Means CA and UDB.
- To target the security of data broadcast in IIoT by implementing light weight consensus algorithm.
- To error for optimizing and judging cluster segregation.

The paper outlines is described in "Background study and preliminaries" section contains the background study and preliminaries to review about various techniques. The "Proposed research work" section defines the implementation of the proposed blockchain and K-harmonic algorithm based on IoT application. "Experimental analyses with simulation" section describes the result and discussion about the proposed system performance and finally the conclusion section highlights the improved result in "Conclusion" section.

Background study and preliminaries

Thakkar et al.[12] conducted study to feature out the working in blockchain platform "Hyperledger Fabric" and identified the likely functioning bottlenecks to develop a better picture of the blockchain model. Two phases of an approach were implemented. Ie, the Blockchain and protocol polices to secure the transaction services. The phase one goal is to comprehend the effect of a variety of configuration metrics such as block sizes, policy endorsements, and allocation of resources, channels, and state repository choices on the throughput and latency to deliver numerous strategies to constitute these performance evaluation factors that are aimed at identifying working hotspots and bottlenecks. Together IBM blockchain improvements are creates are transaction policy relates to defines the authentication rules. Observations made are transaction endorsement policy verification with consecutive policy validation inside a block. The CouchDB commit and the state endorsement were the three main bottlenecks. Phase two focused on optimizing Hyperledger Fabric version 1.0 based on their remarks, including simple optimizations parallelizing endorsement rule verification of a sevenfold improvement and aggressive caching for endorsement rule verification in the cryptography's component of a threefold improvement in performance. The upside is the enhancement of flaws in CouchDB while validating the commit, state phase of 2.5-fold improvement. The final throughput of the framework is improved with the combination of all optimizations. The downside is that Hyperledger cannot divide the clients on a community basis, which creates concerns about sharing data with the consumers.

Liang et al.[13] suggested user-centered data-sharing plan that highlights security insurance, identity management is implemented with the grouping chain. Healthcare data integrity is preserved; every record, validation and integrity proof is eternally extractable from the cloud repository and attached to the network of blockchain technology. A batching technique and tree-oriented data handling to process huge data sets of sensible health data are adopted. But, these plans do not focus on the attributes, elements for sharing. In the proposed framework, the IBM blockchain platform, the dynamic architecture of the grouping chain is embraced to confirm the security of data and to improve data-sharing performance.

Srivastava et al.[14] proposed the k harmonic weighing (KhmAW) technique to increase the analytical accuracy measure. The best community/feature identification is achieved over healthy and nonhealthy datasets. The effectiveness of the KhmAW is assessed with a vast number of previous cases. It was found that a KhmAW-oriented investigative system accomplishes the best quality outcomes compared to other clustering algorithms. Henceforth, it was determined that the KhmAW for enhancing the medical decision-making process and help medical staff concerning diverse diseases. The pitfall is that the handling of clusters with usually configured systems leads to storage difficulties, which may cause delays in query accessing among the clusters.

Yang et al.[15] described the adoption of data management with NDN-oriented service and secure data management was accomplished with blockchain technology. Consortium blockchain accomplishes blockchains with restricted centralism. Two types of nodes are considered in this work: representative nodes and contributing nodes. A proxy server of Fog Computing is replaced by a representative node. Fog Computing devices are replaced by contributing nodes. An NDN-related network was configured for an informal search of identifiers. The IP address of a device can be allotted with internet networks or system participation. A consolidated server is acquired to maintain data, complex for the network to efficiently treat the problems because of a greater number of users. Therefore, the author proposed a system highlighting improved security using blockchain as a way to divide and regain identifiers with fog network topology. Private identifiers are securely stored and handled through such an identifier division management structure. The downside is the identification of the device number, which can be easily found due to improper exposure division management.

The decentralized auditing in Ethereum developed by Fan et al.[16] has been proposed. By supplanting TPA with a planned smart agreement a decentralized inspecting plot (Dredas) is proposed, where anybody uses inspecting result from Ethereum without stressing over the semihonest TPA. In contrast with conventional evaluations, aside from having the option to perform conventional inspecting capacities, Dredas has two significant advantages over past work. To begin with, the irregular estimations of challenges are safer. Dredas picks the current nonce as an arbitrary seed to forestall any gathering in irregular qualities. Furthermore, so as to accomplish a protected, normal, proactive examination, the convention composes the inspecting into blockchain and utilizations of the number of squares on the Ethereum. Last, the information proprietor, client, and CSP provides brilliant contract as a store. Thus, it does not just restrain the injurious conduct of these three gatherings, but also makes them more sensible, in actuality. Dredas can be tuned to show that the calculation costs are reasonable and profitable, but it does not concentrate on the energy or fast retrieval of queries[17,18]. Reference[19] proposes a mutual authentication. The IoT based smart environment can authenticate and provide access. Security efficiency and privacy protection is provided with informal security analysis.

Proposed research work

The proposed work is a blockchain technology-enabled K-Harmonic clustering algorithm appended with an underweight data block-based secure data sharing and storing framework for IoT applications. IoT is gaining rapid growth and has limitations like privacy, data sharing issues, and security liabilities[20]. To invoke sharing and storing efficiency inside a single structure, the work is divided into two major layers.

Data sharing model based on blockchain and K-harmonic. To deliver fine-grained data distribution facilities, transactions saved into the blockchain repository are divided based on the privacy levels. The level of privacy contains data in public, cluster data in public, and data already encrypted for access. The public data bases on buy, sell can be categorized and provided. When users' share sensitive information, they must establish the information's level of privacy in the public area of the cluster, such that the information can be visible to all users who truly want to utilize it. Hence, the core work is to segregate the cluster sensibly by evolving a centroid-oriented community prediction algorithm. Figure 4 demonstrates the data-sharing framework constructed with blockchain. Three layers are invoked in the proposed framework: Data, Detection, and Blockchain layers. The data layer facilitates the gathering of information and is to be transmitted to the detection layer. Client clusters are created based on the similarity of their elements for accomplishing the scope of data sharing in an efficient way. The final layer of blockchain is accountable for preserving the detection of cluster results and the safe recording of transactions.

Communication process. The communication process for information exchange is outlined in Fig. 5. The association cycle comprises four stages: the initialization stage, identity approval stage, signature verification stage, and information sharing stage. In the statement stage, the key, ID of Client Server (CS) and Client (C) are mostly finished. The reason for the validation stage is to confirm the two players before setting up an association and trading data. Mark and the confirmation stage are liable for guaranteeing that information is not altered during transmission. In the information sharing stage, the customer is isolated into a few networks by the network location calculation, and the distribution degree is utilized as the file of iterative streamlining.

Stages of communication process. Initialization stage: The initialization stage mostly completes key generation for C, CS, ID events.

1. CAS (Certificate Authority Server) choses prime numeral g and double multiplicative sets, i.e., P1 and P2, is in order of g; P is for P1; p is for P2; and u is a bilinear map fulfilling u (P1, P1) = P2.
2. CAS arbitrarily produces m × n dimensional matrix two in number, i.e., B_{cs} and B_c and double m dimensional vectors per column, i.e., a_{cs} and a_c where $R(B_{cs}) <$ minimum {m, n}, as $B_{CS}\alpha_{CS}$

$$\mathrm{Bcs}\alpha\mathrm{cs} = \mathrm{acs}, \tag{1}$$

$$\mathrm{Bc}\alpha\mathrm{c} = \mathrm{ac}, \tag{2}$$

   have unlimited solutions. α_{cs} is the outcome of linear Eq. (1), α_c linear Eq. (2) solution.
3. In every CS_i, two private keys are randomly selected by CAS i.e., X_{i1} and $X_{i2} \in Y \times g$, and produces a pair of public keys, i.e., $Z_{i1} = X_{i1}P$ & $Z_{12} = X_{i2}P$. Two more private keys are randomly selected for CDS (Cluster Detection Server) by CAS.

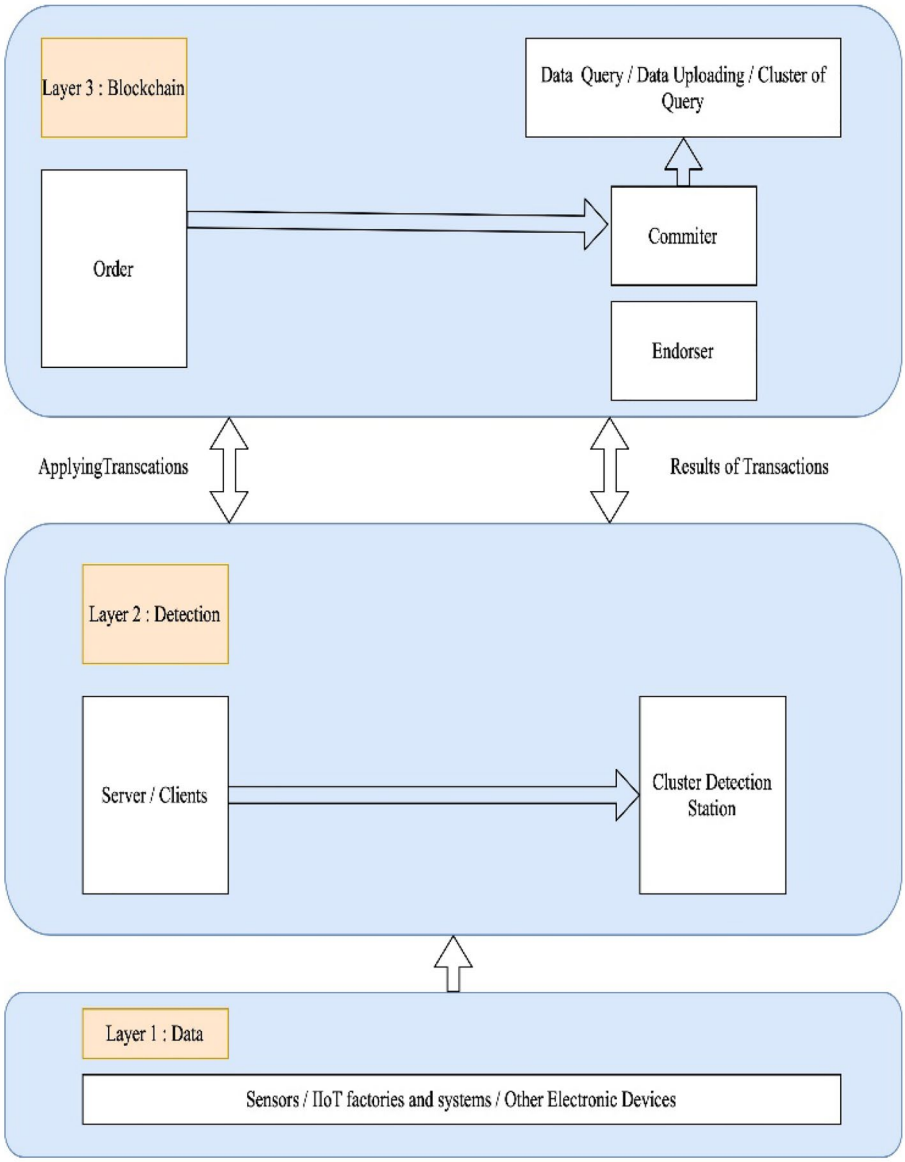

Figure 4. Blockchain-based data sharing structure.

Identity approval stage: The reason for the approval stage for parties to validate before the establishment of a connection and the exchange of information. Client C_j gets the verification message msg1 from CS_i and predicts co_{cj} by,

$$co_{cj} = co_1 \alpha_{ci}. \tag{3}$$

Client C_j does not comprise the parameters B_c and a_c. But, the parameter co_{ci} is calculated by C_j, which is equivalent to co_2 established from CS_i based on the equation,

$$coci = co1\alpha ci = rBc\alpha ci = rac = co2. \tag{4}$$

Equation (4) is verified, then the Eq. (5) is clearly acceptable.

$$H(\{(t1||co2||IDCSi)\}) = H(\{(t1||coci||IDCSi)\}), \tag{5}$$

means that the client C_j has been confirmed by the authority of client server (CS). After that, the client C_j initiates the verification message $msg2 = \{t_2, IDci, H(t_2||co_{ci}||IDCS_i)\}$ to CS_i; here, t_2 is the message timestamp for current message.

Signature verification stage: Information signature validation is used to make sure that the data has is not modified. The signature verification is with the client, CS is carried out with Eq. (6). After uploading the message and the signature into the system, the CDS retrieves the signature from the message β_{cj} of S_j, which it has

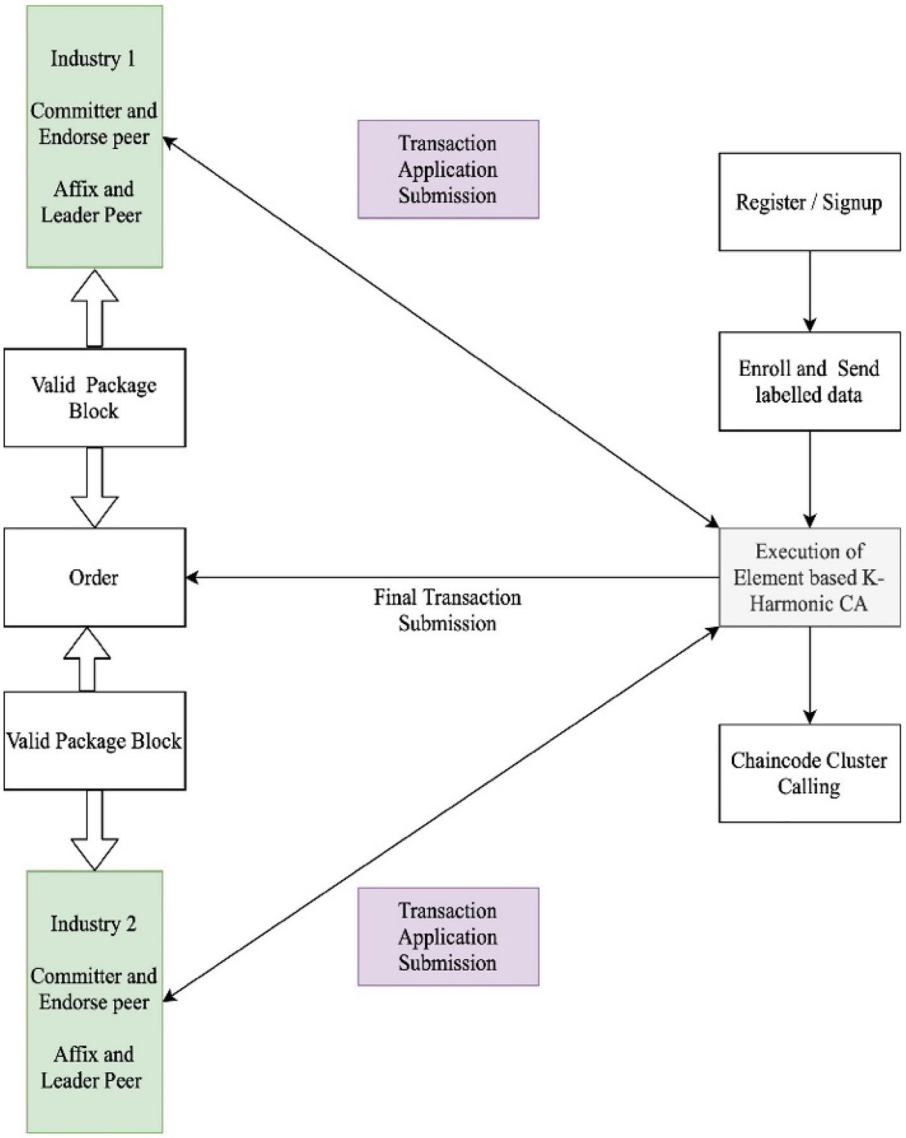

Figure 5. Blockchain-based communication process with clients.

obtained from C_j, and the validity of β_{cj} is then to be cross checked. CDS has to verify the exactness with the following equation,

$$u(Sj, P) = f(\gamma cj, Zi2)\, u(H(IDcj||\gamma cj||Sj), Zi1). \tag{6}$$

Element-based K-harmonic means clustering algorithm. Clustering is utilized on the basis of centroid-based clustering with element-based K-harmonic algorithm. This study utilized an improved K-harmonic bunching calculation to accomplish the clustering of customers. The K-harmonic[21] bunching calculation is appropriate for circumstances where the division procedure has no numeric operation. The definite community measure is portrayed with Algorithm 1: arbitrarily select k value points from n sample data from the population in k-harmonic; appoint the rest of the $n-k$ values for class at present best taken with harmonics as indicated by the rule of closest separation to the medoids; for all the values in the i_{th} class aside from the comparing harmonic/medoid values, compute the estimation of the model capacity in request for new harmonics, emphasize all prospects, and direct comparison with the base rule work as the new medoids; and rehash the above process until all the medoid values no longer change or have arrived at the set greatest number of emphases, after which it yields k-classes.

Algorithm 1 Separation of Clusters
Inputs: G, P
Output: A final
1: function of CLS (G,P)
2: /∗Initialization of the clusters' center∗/
3: Random Centers(G) = {Z}
4: /∗Start client allocation ∗/
5: for $P_i \in P$, $Zj \in Z$ do
6: if $\cos(P_i, Z_j) > \cos\theta$Max then
7: Sum the P_i to the cluster of Z_j
8: end if
9: end for
10: /∗Updating the clusters' center∗/
11: for the comm ∈ {Comm} do
12: Locate $C_i \in$ comm fulfilling Min$\{X_2(C_i)\}$
13: end for
14: /∗iterate till the cluster is not changing∗/
15: if C final!={Comm} then
16: start next upcoming round
17: end if
18: return C final
19: end the function

The cluster prediction algorithm proposed has been implemented with the K-harmonic clustering algorithm (CA). The vital performance measures considered in the algorithm are the contour-coefficient technique and the sum of squared error (SSE). But the assessment of the contour-coefficient technique is unsteady, so DISTRIBUTION DEGREE (DD) is applied instead. The SSE is utilized to evaluate the effect of clustering. The SSE is predicted with Eq. (7) and the DD is evaluated by Eq. (8).

$$SSE = \sum_{n=0}^{k} \sum_{\cos\theta \in Ci}^{n} [1 - \cos\theta]^2, \tag{7}$$

$$DD = \frac{\sum_{i,j=1,1}^{i,j=n,k} [WC_i \times N_{commj}]}{W_{total}}, \tag{8}$$

where W is the amount of cluster data in public that has been uploaded by the client; Wtotal is the amount of uploaded with the clients; N is the total number of clusters in the whole community; Ci is ith client; and comm is jth number of the community.

Underweight data block (UDB) algorithm. The consensus layer in the blockchain structure is a significant examination course in the field of blockchain innovation, that is, it is the means to accomplish agreement productively among hubs in a conveyed blockchain framework. In the bitcoin framework, the generally utilized instrument of proof of work (PoW), which is exceptionally subject to the registering intensity of the conveyed hubs, was utilized to guarantee the consistency of the bookkeeping measure. With the steady advancement of blockchain innovation, the Proof of Stake algorithm (PoS), Delegated Proof of Stake algorithm (DPoS) and other techniques as components of agreement and typified of the blockchain framework layer. To create an underweight score based on the mined property of blocks from the random Blockchain history 'w' depend on the frequency. Where 'ri' is the total block for generated window for Proof of Work,

$$\sum_{i=0}^{n} r_i = 1. \tag{9}$$

Each block is verified by the Key security by book keeping levels of access by transferring as tokens to access agreements.by defining the difficulty at each block access be beyond the underweight at 'K' mined from 'b' at each block

$$UDD_b = UW_b \times D_b = \sum_{k=1}^{l} r_k \times \sum_{k=1}^{l} d_k, \tag{10}$$

where 'rk' is the frequency level of access weight of each block from the mitigation at dk in each block K in length l at size of the individual block to verify before the decision.

Based on the hash rate, the optimum agreement be pa be valid at regulate point 'w/2' period at regular intensity level of access.

$$p_\alpha > p_o. \tag{11}$$

Based on each lock rate, the conditional b_α will be longer than original branch b_0. At the revealed time, UD of the original branch is,

$$UD_0 = D_0 \times \sum_{k=0}^{l} r_k^\circ = D_0 \times \left(\frac{1}{2} - \delta\right). \tag{12}$$

Underweight marginal frequency of access defined level is

$$UD_\alpha = \left(\frac{1}{2} + \delta\right) \times \frac{w-l}{w} \times D_\alpha. \tag{13}$$

That the difference is

$$\left(\frac{1}{2} + \delta\right) \times \frac{w-l}{w} \times D_\alpha > \left(\frac{1}{2} - \delta\right) \times D_0. \tag{14}$$

Because D_α and D_0 both sequences the derivation be access on hash ratio underweight w

$$\left(\frac{1}{2} + \delta\right) \times \frac{w-l}{w} > \left(\frac{1}{2} - \delta\right). \tag{15}$$

Be regularized at

$$\delta > \frac{l}{4w - 2l}. \tag{16}$$

Based on the minimal access fragment of blockchain be accessed by δ (w − 1) be make the decision subject to the verification. The noteworthy fragment in blockchain is that for decentralized framework, hubs with profoundly decentralized decision-making rights for an agreement on the legitimacy of exchanges in the square. In conventional blockchain innovation, guaranteeing agreement between hubs is profoundly subject to the processing intensity of the circulated hub, in particular, the PoW instrument. With that, IIoT frameworks are generally helpless in processing power. In this manner, this research appended an UDB algorithm in the blockchain framework for the IIoT model as shown in Fig. 6.

The UDB algorithm steps are given below:

- *Step_1* The final edge entry receives information, utilizes the function hash to compute the value for hash with respect to data, notes it in the block to be confirmed.
- *Step_2* The final edge entry has information to the verified block of data to the other edge entry point and awaits confirmation.
- *Step_3* The gateway edge, after receiving verified block starts searching for the earlier information block in its ledger.
- *Step_4* Cross check whether there is a succeeding block in the earlier block. If not, integrate the data block to be confirmed to the rear with earlier block and stay for the verification. If it occurs, continue to Step 5.

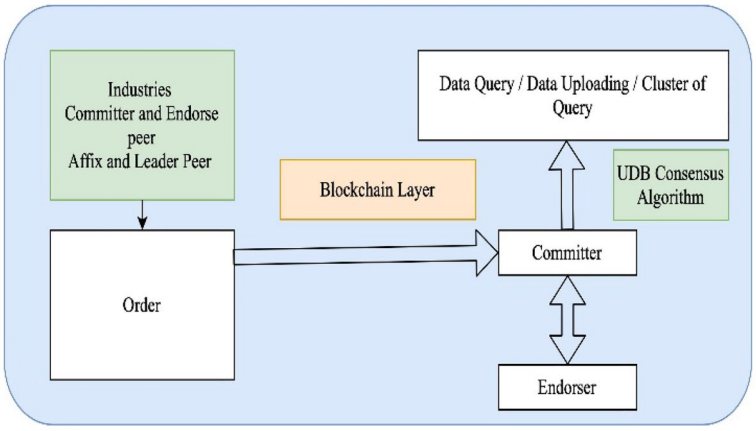

Figure 6. Blockchain consensus layer with UDB.

- *Step_5* Verify the similarity of the target edge entry and data block hashing rate of the earlier block, as the particular data block has to be confirmed. If it is similar, then return the confirmation report as true; if it varies, continue to Step 6.
- *Step_6* Persist with locating the target edge entry and conclude if the hash rate of the upcoming block is the similar block to verify. If so, then return the verification report as true; otherwise continue with the procedure until there is no arrival of any other block
- *Step_7* Inside the chain organization the blocks that are verified are associated with the equivalent positions in timestamp and stay for the confirmation
- *Step_8* The data blocks left in Step 4 and Step 7 for authentication reach threshold time of waiting, and the verification report is returned as false
- *Step_9* The target edge entry counts the confirmation outcomes returned from all other gateways. If the accurate number reaches 50% with number of the confirmed edge entries, then the information is noticeably accurate data sent to data center. Otherwise, the data are considered flawed information, are labeled with erroneous center.

The UDB algorithm uses a distributed IBM platform for blockchain on multiple edge entries. The broadcast strategy in the framework provides information consistency throughout the transmission. The underweight structure of the data block has improved over conventional blockchain technology structure.

Experimental analyses with simulation

The simulation has been in MATLAB 2018a simulation environment. The proposed clustering algorithm is related to K-harmonic centroid-based CA. The range of m directly influences the flow of the community algorithm. Supposing that m is selected perfectly, then the proposed algorithm will definitely converge with the threshold of the user. The algorithm has optimal solution in the local rather than the global. Based on the hypothesis of the k-harmonic CA framework, SSE will gradually increase with the increment in the m-value and the lessening DD of m-value will be qualitatively altered when k-value appears to be optimal. Prior to the appearance of the m optimal value, the SSE value will increase rapidly. Once the optimal k-value is reached, then the increasing drift of the SSE with k will be even. Hence, the finest m-value must be predicted by implementing the framework. The shift of the SSE value according to the m-value 2 for various algorithms like K-Means clustering algorithm, attribute-based K-means clustering algorithm, and K-medoids clustering algorithm against element-based K-harmonic means clustering algorithm (CA) are shown in Fig. 7 and Table 1.

The proposed element-based K-harmonic means clustering algorithm possesses noteworthy performance with a lesser query size mentioned at the origin of Figs. 7 and 8. The difference of 710 ms for m = 4 and 176 ms when m = 2 with the algorithm K-means; 339 ms and 58 ms against attribute-based K-means clustering algorithm;

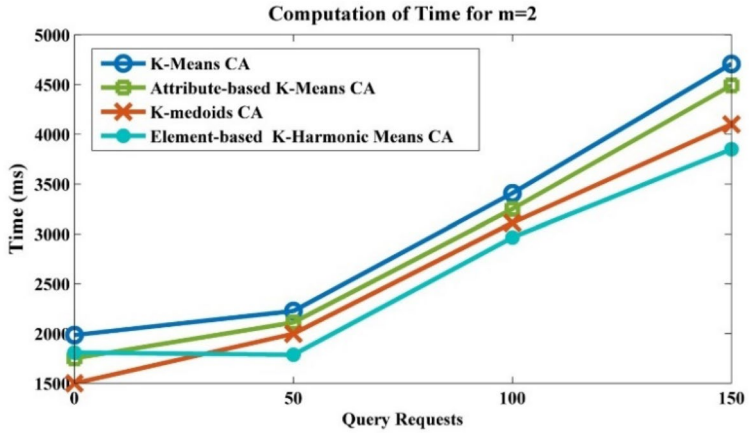

Figure 7. Computation of time for m = 2.

Query requests	Time (ms)			
	K-means clustering algorithm	Attribute-based K-means clustering algorithm	K-medoids clustering algorithm	Element-based *K*-harmonic means clustering algorithm
0	1985	1751	1500	1809
50	2226	2112	1998	1787
100	3408	3250	3111	2965
150	4707	4492	4100	3850

Table 1. Computation of time for M = 2.

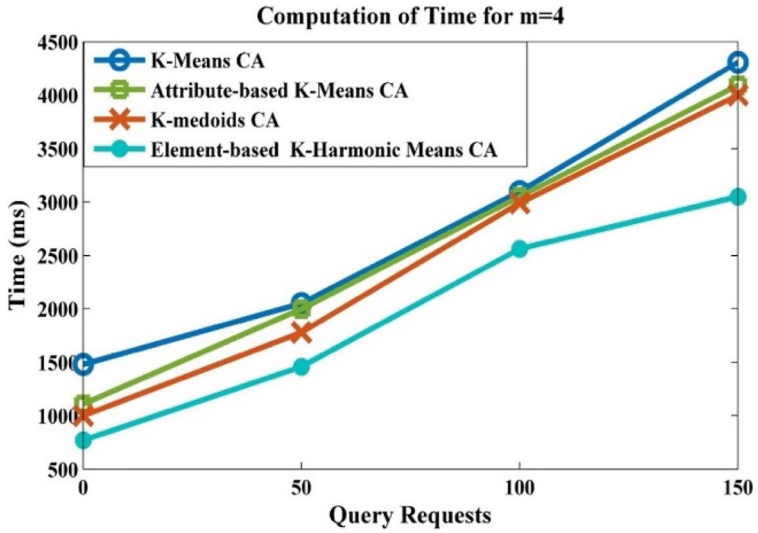

Figure 8. Computation of time for m = 4.

and 230 ms and 309 ms over the K-medoids clustering algorithm for m = 4 and m = 2, respectively. Hence the proposed approach is better.

The effect of the number of clusters on the performance is presented in Fig. 9. As the number of clusters reaches 1000, the CPU utilization reaches nearly 50% utility, indicating blockchain system has reasonable performance necessities has utility of the CPU (Table 2). In this simulation, numerous nodes are deployed on to the one server. Consequently, the performance blockage of the newly proposed work outcomes is very momentous from the server. Developing the server further in the proposed framework will achieve a significant improvement.

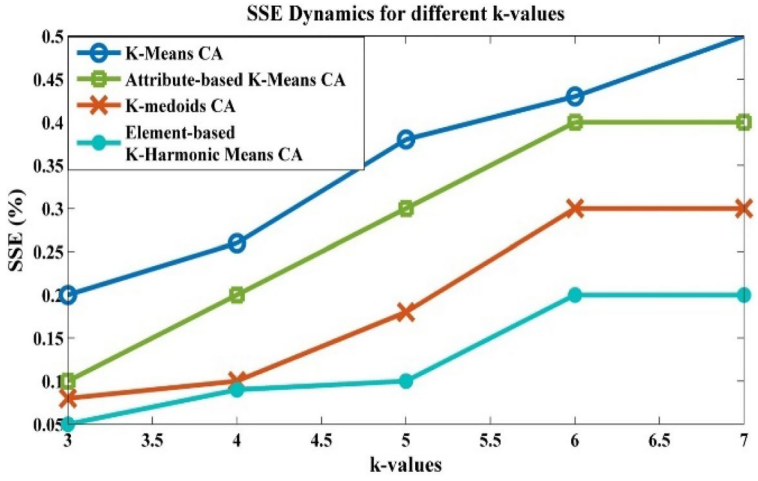

Figure 9. The effect of the number of clusters on the performance is presented.

Query requests	Time (ms)			
	K-means clustering algorithm	Attribute-based K-means clustering algorithm	K-medoids clustering algorithm	Element-based K-harmonic means clustering algorithm
0	1480	1109	1000	770
50	2051	1998	1780	1459
100	3098	3050	2990	2561
150	4307	4092	4000	3050

Table 2. CPU utilization.

With this, it is concluded that using the IBM platform for the blockchain network system can gradually reside with the requirements of today's business. Thereby, server functioning is not a vital bottleneck that restricts the deployment of blockchain systems, while blockchain provides various other benefits such as safety and trust of the framework.

Figure 10 shows the shift in SSE during clustering with different k/m values. Based on the concept of the proposed framework, in the k-harmonic method, SSE increases with the increment in k/m. From Table 3 it is clearly depicted that the SSE percentage is flattened at some point of k/m and after that there is no increase in the erroneous part of the prediction.

Figure 11 shows the connection between the occupancy of space and the algorithmic iterations count. The storage occupancy of the system increases with time, but the speed of increase varies and is compared with the existing three algorithms. The Proof of Work (PoW) has computational power of the edge entry that needs a significant storage area. In the 50th iteration, the balance space is 68% with the proposed UDB algorithm, but with the other existing algorithms, such as the Delegated proof of stake algorithm (DPoS), PoW algorithm, and Lightweight Data Consensus algorithm, 56%, 59%, and 62% of space is provided, respectively, as tabulated in Table 4. The DPoS method has blocks by choosing precise nodes for making sure of the consensus among them, although it cannot hold the space for a large size of data in the IIoT platform. Likewise, the existing algorithms are setting behind in some respects when related with the proposed UDB mechanism.

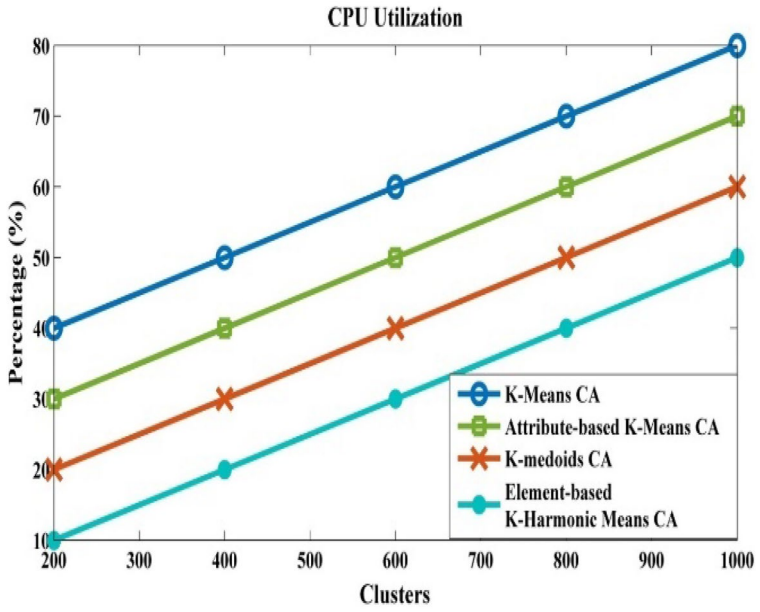

Figure 10. CPU utilization.

Clusters	Percentage (%)			
	K-means clustering algorithm	Attribute-based K-means clustering algorithm	K-medoids clustering algorithm	Element-based K-harmonic means clustering algorithm
200	40	30	20	10
400	50	40	30	20
600	60	50	40	30
800	70	60	50	40
1000	80	70	60	50
k-values	SSE (%)			
	K-means clustering algorithm	Attribute-based K-means clustering algorithm	K-medoids clustering algorithm	Element-based K-harmonic means clustering algorithm
3	0.2	0.1	0.08	0.05
4	0.26	0.2	0.1	0.09
5	0.38	0.3	0.18	0.1
6	0.43	0.4	0.3	0.2
7	0.5	0.4	0.3	0.2

Table 3. SSE dynamics for different k/m values.

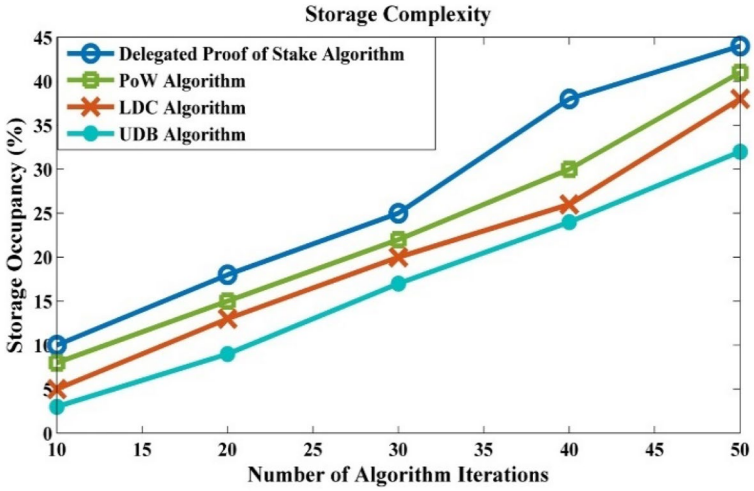

Figure 11. Storage complexity.

Number of algorithm iterations	Storage occupancy (%)			
	Delegated proof of stake algorithm	PoW algorithm	LDC algorithm	UDB algorithm
10	10	8	5	3
20	18	15	13	9
30	25	22	20	17
40	38	30	26	24
50	44	41	38	32

Table 4. Storage complexity.

Conclusion

With the development in the volume of IIoT devices with cloud computing enhancement, distributed management systems must be utilized by businesses. While acquiring the IIoT platform, there is a back seat to full-fledged data sharing and the proper storage of data beyond the security impacts. This research study has provided a considerable structure of blockchain for the enhancement of the aforementioned issues. The development of an element-based K-harmonic means clustering algorithm (CA) is proposed for effective data sharing among entities, along with the underweight data block (UDB) algorithm for overcoming the complexity of storage space.

The parameters evaluated for predicting the system performance are time complexity with respect to $m = 2$ and $m = 4$ values, sum of squared error (SSE), and storage complexity with CPU utilization. The simulation was performed with using MATLAB 2018a simulation environment. The anticipated model provides better sharing and storing based on blockchain technology for IoT. The utility of CPU and storage occupancy is nearly 30% less than the previous blockchain frameworks. Additionally, this research study can be extended to propose an increased network featuring security using blockchain as a mechanism to divide and re-establish identifiers. Susceptible identifiers has been securely stored and maintained via the identifier division management IIoT system which prevents the identification of a particular user.

Data availability

The datasets used and/or analysed during the current study available from the corresponding author on reasonable request.

Received: 8 February 2022; Accepted: 16 May 2022
Published online: 18 January 2023

References

1. Rathee, G., Sharma, A., Kumar, R. & Iqbal, R. A secure communicating things network framework for industrial IoT using blockchain technology. *Ad Hoc Netw.* **94**, 101933 (2019).
2. Zhang, W., Wu, Z., Han, G., Feng, Y. & Shu, L. Ldc: A lightweight dada consensus algorithm based on the blockchain for the industrial internet of things for smart city applications. *Futur. Gener. Comput. Syst.* **108**, 574–582 (2020).
3. Ritzdorf, H. *et al.* Toward shared ownership in the cloud. *IEEE Trans. Inf. Forensics Secur.* **13**(12), 3019–3034 (2018).
4. Wang, Y. Industrial structure technology upgrade based on 5G network service and IoT intelligent manufacturing. *Microprocess. Microsyst.* **81**, 103696 (2021).

5. Kang, J. *et al.* Toward secure blockchain-enabled internet of vehicles: Optimizing consensus management using reputation and contract theory. *IEEE Trans. Veh. Technol.* **68**(3), 2906–2920 (2019).
6. Balaji, V. *et al.* Combining statistical models using modified spectral subtraction method for embedded system. *Microprocess. Microsyst.* **73**, 102957 (2020).
7. Sathesh, S. *et al.* Computer vision based real time tracking system to identify overtaking vehicles for safety precaution using single board computer. *J. Adv. Res. Dyn. Control Syst.* **12**, 1551–1561 (2020).
8. Yu, Z., Liu, X. & Wang, G. A survey of consensus and incentive mechanism in blockchain derived from P2P. In *2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS)*, 1010–1015. https://doi.org/10.1109/PADSW.2018.8645047 (2018).
9. Drugman, T. & Alwan, A. Joint robust voicing detection and pitch estimation based on residual harmonics. Preprint at http://arXiv.org/2001.00459 (2019).
10. Benbouhenni, H., Boudjema, Z. & Belaidi, A. Indirect vector control of a DFIG supplied by a two-level FSVM inverter for wind turbine system. *Majlesi J. Electr. Eng.* **13**(1), 45–54 (2019).
11. Zheng, Z., Xie, S., Dai, H.-N., Chen, X. & Wang, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **14**(4), 352–375 (2018).
12. Thakkar, P., Nathan, S. & Viswanathan, B. Performance benchmarking and optimizing hyperledger fabric blockchain platform. In *Proc. MASCOTS*, 264–276 (IEEE, 2018).
13. Liang, X., Zhao, J., Shetty, S., Liu, J. & Li, D. Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In *Proc. PIMRC*, 1–5 (IEEE, 2017).
14. Srivastava, A. K., Kumar, Y. & Singh, P. K. Computer aided diagnostic system based on SVM and K harmonic mean based attribute weighting method. *Obes. Med.* **19**, 100270 (2020).
15. Yang, H.-K., Cha, H.-J. & Song, Y.-J. Secure identifier management based on blockchain technology in NDN environment. *IEEE Access* **7**, 6262–6268 (2018).
16. Fan, K., Bao, Z., Liu, M., Vasilakos, A. V. & Shi, W. Dredas: Decentralized, reliable and efficient remote outsourced data auditing scheme with blockchain smart contract for industrial IoT. *Futur. Gener. Comput. Syst.* **110**, 665–674 (2020).
17. Wang, W. *et al.* Blockchain-based reliable and efficient certificateless signature for IIoT devices. *IEEE Trans. Ind. Inform.* **18**, 7059. https://doi.org/10.1109/TII.2021.3084753 (2022).
18. Senthil Kumar, T. & Sivanandam, S. N. An improved approach for detecting car in video using neural network model. *J. Comput. Sci.* **8**, 1759–1768 (2012).
19. Song, J., Han, Z., Wang, W., Chen, J. & Liu, Y. A new secure arrangement for privacy-preserving data collection. *Comput. Stand. Interfaces* **80**, 103582. https://doi.org/10.1016/j.csi.2021.103582 (2022).
20. Madala, H. R. & Ivakhnenko, A. G. *Inductive Learning Algorithms for Complex Systems Modeling* (CRC Press, 2019).
21. Cui, Z., Cao, Y., Cai, X., Cai, J. & Chen, J. Optimal LEACH protocol with modified bat algorithm for big data sensing systems in Internet of Things. *J. Parallel Distrib. Comput.* **132**, 217–229 (2019).

Acknowledgements

Researchers Supporting Project number (RSP2023R167), King Saud University, Riyadh, Saudi Arabia.

Author contributions

N.B. and K.V.—prepared manuscript draft; M.A. and S.S.A.—simulation; K.M.B. and P.P.—review and editing. M.A. and S.S.A.—experimental findings validation; N.B.—data pre-processing.

Funding

This Project is funded by King Saud University, Riyadh, Saudi Arabia.

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to N.B.

Reprints and permissions information is available at www.nature.com/reprints.

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