The Journal of Engineering

WILEY

IET The Institution of Engineering and Technology

ORIGINAL RESEARCH OPEN ACCESS

Scalable Consensus Algorithm and Storage in Decentralized Blockchain (SCSB) For Heterogeneous Internet of Things (IoT) Systems

Inderpal Singh[1] | Balraj Singh[1] | Muhammad Faheem[2,3]

[1]School of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab, India | [2]VTT Technical Research Centre of Finland, Espoo, Finland | [3]School of Technology and Innovations, University of Vaasa, Vaasa, Finland

Correspondence: Muhammad Faheem (muhammad.faheem@vtt.fi)

Received: 23 August 2024 | **Revised:** 30 June 2025 | **Accepted:** 8 July 2025

Funding: The authors would like to thank their affiliated universities and institutes for supporting this study.

ABSTRACT

The internet of things (IoT) is widespread in various real-time applications in developing smart environments. The involvement of numerous network devices and users in the system includes illegitimate and malicious entities. Also, the participation of numerous devices leads to scalability issues. The decentralized blockchain is one of the promising solutions to satisfy all the requirements of security. In this paper, a priority-based lightweight authentication and access control is designed for cloud-IoT (SCSB) with the assistance of decentralized blockchain technology. The SCSB design consists of the data owner (DO), data user (DU), trusted authority (TA), and cloud server. The cloud server manages a huge amount of data, hence, it receives multiple DU requests. The DO is also authenticated and then allowed to upload data. The data in the cloud is clustered and then stored, which is scalable in storage. In this work, density-based spatial clustering applications in noise (H-DBSCAN) is presented with a hybrid distance measure. The validation of multiple requests into the blockchain is conducted using novel proof-of-authentication, which selects a trusted node for validation. To ensure secure data upload, the priority, i.e., the confidentiality level of data, is predicted from the dual fuzzy algorithm, and then the data is secured. For a high confidential level and low confidential level, a lightweight TWINE algorithm and differential privacy are incorporated. The use of lightweight algorithms and parallel processing algorithms in dual fuzzy enables it to operate with numerous devices while utilizing limited resources and time, which solves the scalability issue. The proposed SCSB shows better performance results than the previous research algorithms.

1 | Introduction

Heterogeneity in the IoT defines the support provisioned for a variety of devices with the incorporation of different types of technologies for connecting the Internet. This communication is ubiquitous, which is spread across the use of multiple applications. In general, IoT devices are equipped with limited power and capabilities, where the heterogeneous IoT devices operate on an appropriate set of protocols, standards, and technologies [1–4]. The heterogeneous devices include sensors, actuators, thermostats, and others.

The IoT with heterogeneous devices gathers a huge amount of data that differs in severity based on the application. For instance, a healthcare environment composed of sensors that collect patients data, which can be either sensitive or non-sensitive. The data type may or may not be privacy-sensitive information. In the heterogeneity of IoT, security is a major

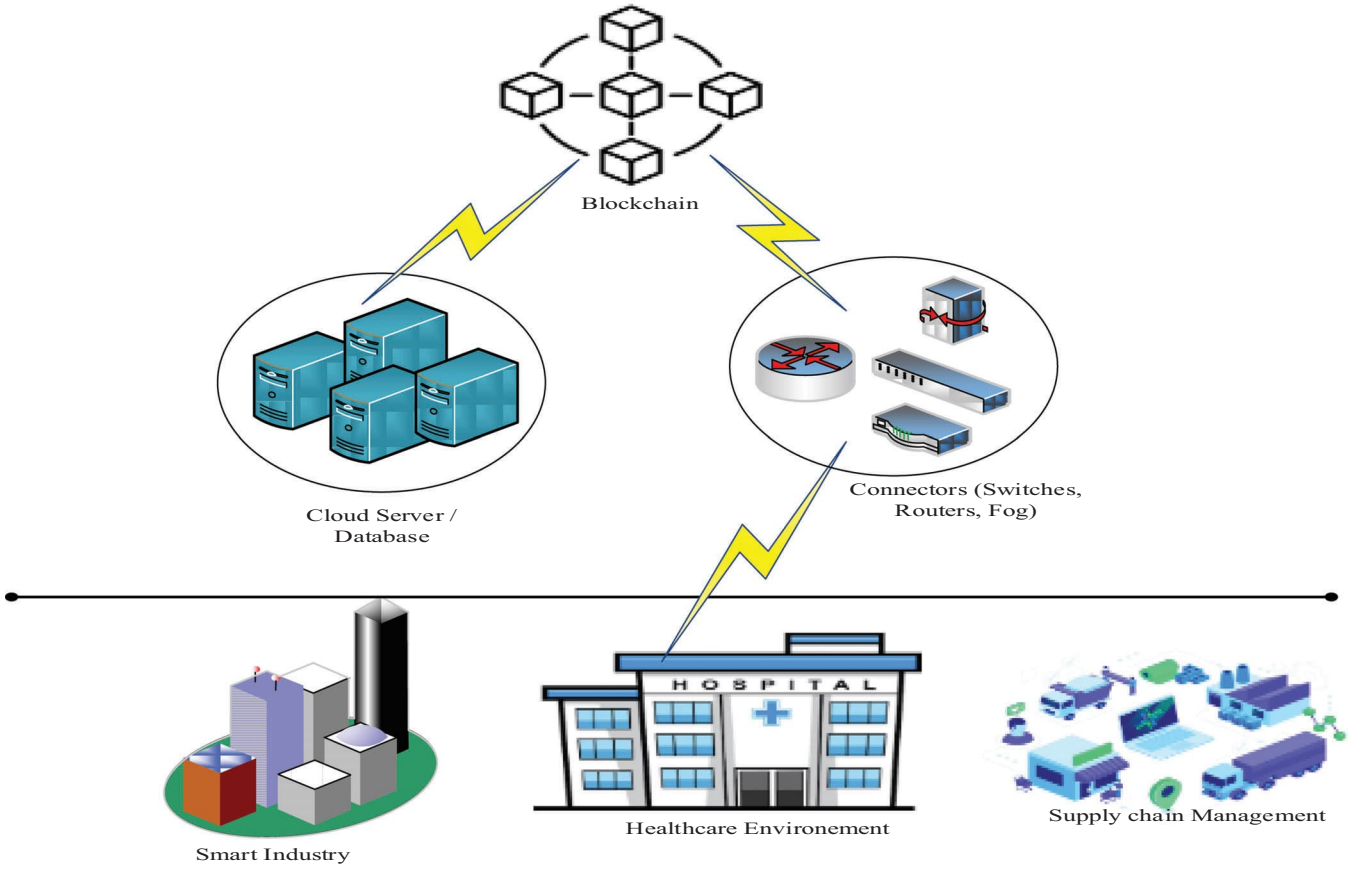

FIGURE 1 | Architecture of integrated heterogeneous cloud-IoT with blockchain technology.

challenge since it involves intruders, attackers, and so on within the system. To overcome all the security challenges, blockchain technology is incorporated [5–10]. It is developed in different types, such as public, private, consortium, and hybrid. The public blockchain is decentralized, which is accessed from anywhere. In simple the blockchain structure is constructed with several blocks composed of hashes. The hashing is performed using the traditional SHA-256 algorithm. A blockchain acts as a tool for security provisioning in which nodes are connected for the verification of hashes and updating them. However, the original information in the blocks is unknown to the verifier. It is operated efficiently for all critical applications due to its strength in security.

The aspect of security is presented for authentication, access control, data security, key exchange, and so on [11–15]. There exist key challenges in security such as validation, use of security credentials, methods/algorithms to be used, etc. On the other hand, it is also challenging in security provisioning for resource-constrained, memory utilization, energy consumption, and processing capabilities of IoT devices. The integration of blockchain with IoT for heterogeneous data is essential to improve scalability, interoperability, availability, etc. The blockchain technology presents multiple benefits such as transparency, complexity, and risks to attackers, and more.

Cloud-based services are integrated with IoT to store collected data [16–19]. The storage of data comprises all types, which is essential in providing security. There are numerous weakness, which majorly occurs among connected devices. The goal is to enhance security aspects by satisfying all the security requirements. Blockchain is one of the popular solutions incorporated in the integration of heterogeneous IoT with cloud. The development of this type of architecture is challenging since it needs to be flexible to support any type of application. The combination of heterogeneous cloud-IoT with blockchain technology architecture is depicted in Figure 1. It assists with the solution in providing security risks as well as multiple real-time applications.

In the blockchain algorithm, the consensus algorithm plays a vital role [20–22]. This algorithm is responsible for deciding whether the arrived requests need to be validated against the credentials. A better design of the consensus algorithm ensures improved reliability of the system. In this paper, the issue of scalability and assistance for heterogeneity is presented. It incorporates a secure, authentication-based consensus algorithm in blockchain technology to secure the data. To solve scalability, lightweight methods are used, and the storage of data is clustered to manage a huge amount of data from a variety of applications.

1.1 | Contribution of this Paper

1. The exchange of security credentials during authentication is secured in a decentralized blockchain with the incorporation of the lightweight QUARK algorithm.

2. In the decentralized blockchain, proof-of-authentication (PoAH) performs node authentication based on the computation of trust values.
3. The collected data is uploaded by the DO, who determines the confidentiality level of the data before it is uploaded. The confidentiality level is computed using a dual fuzzy logic algorithm.
4. From the confidential level prediction, as low and high different methods are used, such as Laplace-based differential privacy and the lightweight TWINE algorithm, respectively.
5. As the proposed system is a heterogeneity IoT the data in the cloud is clustered and stored. A hybrid distance in H-DBSCAN is applied.

1.2 | Organization of this Paper

This paper is organized into the following sections, Section 3 deals with the summary of previous research areas, methods and the limitations that exist in each work, Section 3 highlights the key problems that are stated from prior research work, Section 4 expands the proposed methodologies that are defined to overwhelm the stated problems, Section 5 demonstrates the development of the proposed heterogeneity IoT system in the simulator and evaluates the results to measure the performance efficiency, Section 6 concludes the research work with the extension of future directions.

2 | Related Works

A lightweight blockchain-based security scheme (LBSS) is the application in the healthcare environment [23]. The three main aspects of security as integrity, confidentiality, and availability, were concentrated in this work. The data fragmentation was performed to improve the confidentiality of data, and a hashing scheme is enabled to provisioning integrity. The process of data fragmentation requires combining the data again during retrieval, which needs to be accurate without any mismatch in the data. In this paper, the authors have presented FairShare, which designs a fair, accountable, and secure data sharing scheme for the industrial IoT [24]. The designed system model incorporates fog nodes for reducing the computations that are to be performed. To assure security and privacy, proxy re-encryption is used. For the process of encryption, the AES cryptography algorithm was involved to generate symmetric keys and re-encryption keys. The use of the AES cryptography algorithm is a symmetric key encryption that uses the same key for encryption and decryption. So while sharing the symmetric key, it could be leaked by an intruder.

A blockchain-based access control scheme for multiple domains was designed, which was named BaCS [25]. This design is used for a distributed IoT environment that incorporates a lightweight symmetric encryption algorithm. The DO and consumer information includes the address, along with the signature and keys. In this work, the address was generated using the secret key and the public key of the individual. The access rights of each consumer are determined, and then the access is verified, and then further permission is provided. A ynamic secure access control using blockchain (DSA-Block) technology [26]. The hyperelliptic curve cryptography (HECC) algorithm was used to create private and public keys for device and user attributes. In blockchain SHA-256 algorithm was used for hashing. The cloud was comprised of local domain authority and global domain authority. In this work, trust values were estimated, and it uses the practical Byzantine fault tolerance (PBFT) consensus algorithm for access control.

A secure trust management scheme was proposed in this paper with the use of blockchain technology [27]. In this work, a special entity called a trust manager is deployed to estimate and maintain trust values. The trust value was computed using the user's identity, and it was stored in an array. Then it was validated using the ID3 algorithm based on the threshold value. If the threshold value falls within the threshold, then it is allowed access. The computation of trust value based on the consideration of identity was not efficient. However, the identity was unique; it was commonly generated as a series for devices. A mutual authentication protocol to secure the system from various attacks [28]. It uses a challenge-response model, based on which the session key was established. The process was categorized into five such as: initialization phase, registration phase, authentication phase, communication phase, and revocation phase. It uses octet-based balanced-tree transitions, challenge challenge-response mechanism, and pseudo pseudo-random number generator.

A lightweight hierarchical blockchain-based multi-chaincode access control [29]. There are three main components involved in this design they are edge blockchain manager, aggregated edge blockchain manager, and cloud consortium blockchain manager. These three entities work consequently one after a consecutive manner. The request from IoT is processed in all three elements, and it gives access to the request. It uses a signature and access policies for validation. A BcmECC that presents an elliptic curve cryptography (ECC) based lightweight authentication protocol [30]. In this work, the shared session key was generated to assure security. The device manufacturer was considered to be the TA with which the registration is held. It is connected to blockchain, which enables security. The device was verified using the session key and public key. In this work, mutual authentication was performed, while it does not consider any unique metric for authentication of the device. The blockchain uses a conventional hashing algorithm, which is not a lightweight algorithm that has higher computations.

A physical unclonable function (PUF) based identity management was developed in this paper that uses PUF to solve security issues [31]. The Challenge-Response pair was generated for each device, which is used for authentication. The PUF was unique for each device, and hence it assured secure authentication. Here, the response was hashed before sending to the server for authentication. A novel privacy-preserving scheme was developed for the IoT environment that uses homomorphic encryption [32]. It operates as a privacy set intersection technique, and it also uses blockchain based on smart contracts. The three key processes followed in this work were data initialization, interaction setting, and result distribution. The Bloom filter was included in the blockchain, which was responsible for encrypting the public key.

A blockchain-based high-efficiency access control framework, i.e., BHE-AC, was proposed [33]. The three key processes

performed were registration, the blockchain-based token requesting mechanism, and data retrieval. The registration model involves performing registration of users and resources. In blockchain, smart contracts were generated and validated upon access to the data from the server. The token is generated for the request, and as per the token, it processes and allows access permission. The token is requested by the user with the submission of the address and identity. While all the users are deployed with an address and identity, which is common, and if the address is true, then a token is generated. Hereby, the token was generated for the entire user without any specific security check.

An identity-based authentication scheme for the agriculture environment that uses the HECC algorithm [34]. The proposed authentication scheme operates in three phases such as setup, registration phase, and authentication and key management phase. Initially, a private key was generated based on the hyperelliptic curve, and for registration, the user identity was taken into account. Then, during authentication, it computes the keys after the validation of the identity. The authentication of users was carried out based on the consideration of identity alone, which could be fake for illegitimate users. An attribute-based access control (A-BAC) policy is presented in this paper, which incorporates the Advanced Encryption Standard for encryption and the elliptic curve Diffie-Hellman algorithm for sharing keys [35]. The DO uploads data in encrypted form using AES-128, and the data and attributes are stored in interplanetary file system (IPFS). Then the stored data is accessed by the DU requesting the file location, i.e., content identifier, and the data is retrieved, further decrypted. The DO and DUs are not authenticated in this system, which is a main security risk. Since the illegitimate DO could upload irrelevant data or occupy unnecessary resources. In contrast, the participation of illegitimate users may increase the traffic in the network, which may mitigate access to legitimate DUs. The used AES algorithm was a symmetric cryptography algorithm that uses the same key for encryption and decryption. The DO encrypts the file using the key generated from the AES algorithm, which is not secure, since the key has to be shared with all the requesting DUs.

An attribute access control scheme for IoT (AAC-IoT) that incorporates hyperledger fabric (HLF) Blockchain. According to this work, the DO and DU's were authenticated with multiple factors as identity, certificate, signature, and PUF [36]. The access control policy is defined, and for every user, the number of attributes is selected using a fuzzy logic method. The credentials of the DO are secured using a lightweight PRESENT algorithm. Then, the QUARK algorithm was involved in hashing in the blockchain. For the authentication of the DU, the neural network was used, which enables authentication of multiple users at a time. According to this work, the credentials of the DO are only secured using lightweight cryptography, while the DU's credentials are also significant to be secured. Since there may be participation of illegitimate users in the system. This work fails in providing security for the data that is to be uploaded to the cloud. The storage of raw data is unable to maintain the secrecy of the confidential data.

The major concern from the previous research is the scalability and security, since the environment is heterogeneous. These two major challenges are addressed in the proposed system with appropriate algorithms that solve the scalability issue and enhance the system performance over the previously achieved algorithms' results.

3 | Problem Statement

A secure blockchain-based privacy-preserving access control (BPAC) scheme is presented in this paper [37]. The confidentiality is assured with the fully homomorphic encryption (FHE) algorithm. In this BPAC model, the certificate authority is trusted, and it is responsible for generating private and public keys. According to this work, the subscriber requests access directly to the publisher, while the publisher encrypts and sends it to the blockchain. Then the blockchain authorizes access request, and it again re-encrypts before forwarding to the subscriber. The blockchain is considered to be a private broker in this system, and the key problems of this work are highlighted in the following,

- In this work, the blockchain performs re-encryption, i.e., encryption is processed twice, which needs to be decrypted twice to extract the data that consumes time.
- The credentials that are considered for authentication are not unique, and hence, there are chances to allow illegitimate subscribers.

In this paper, the authors have developed an access control-enabled blockchain (ACE-BC) framework [38]. The attribute-based encryption scheme is used for encryption, and additional homomorphic encryption for user key generation. The blockchain is a TA in this system, while it connects with a proxy server where the DO receives a re-encryption key. The encryption is performed twice by the DO and decrypted twice by the DU.

- In this work, the blockchain performs re-encryption, i.e., encryption is processed twice, which needs to be decrypted twice to extract the data that consumes time.
- The use of a homomorphic encryption algorithm has the traditional problem of being slow, and it requires a larger amount of resources for processing.

This work presents a proxy re-encryption approach for data sharing in the cloud with the incorporation of blockchain [39]. It develops an identity-based encryption and proxy re-encryption to provide security. According to this work, the blockchain is considered to be a TA that gives a secret key based on the user's identities. In blockchain, the traditional SHA-256 hashing algorithm is used. The encryption of data is performed by the DO based on the generated random number. Hence, the defined problems are enlisted below,

- Since the encryption is performed twice, it consumes twice the time for the conversion of the cipher text. Similarly, the decryption is also performed twice, which also consumes twice the time.
- The traditional use of the SHA-256 hashing algorithm in blockchain is not a lightweight algorithm and which is not able to withstand collision attacks.

The authors of this paper have proposed a hybrid centralized and blockchain-based authentication architecture [40]. The devices are registered and authenticated using the security credentials such as an identity and group identity. After successful authentication, the symmetric encryption key is used for encryption. Due to the use of a symmetric key, it is encrypted based on the generated public key. In this work, proof-of-work is presented for validating the blockchain transactions. The critical problems predicted in this work are,

- The proof-of-work consensus algorithm was not able to support the scalability of the system, which fails to operate with the increase in requests.
- The blockchain uses the traditional SHA-256 hashing algorithm, which includes multiple computations than the lightweight hashing algorithm.
- Also, the use of symmetric key cryptography requires secure exchange of keys, since the same key is used for encryption as well as decryption.

From the previous research methods, the key problems are stated in the following,

- Decentralized blockchain enables assurance of security, while the traditional use of the SHA-256 algorithm is vulnerable to collision attacks and also has a larger number of computations when compared with lightweight hashing algorithms. The increase in computation fails to operate for a huge system that is composed of numerous devices.
- The concept of using re to the performance of encryption for data security increases the computation time, due to encryption twice and decryption twice by the DO, as well as the DU, and hence it creates scalability issues.
- The security for uploaded data is provided by the use of a cryptography algorithm that is common for all the data. However, the data needs to be stored securely, it consumes the same computations for all the data that is to be uploaded.
- The absence of security results in scalability issues due to the increase in traffic of illegitimate devices into the system for accessing and storage.

4 | Proposed SCSB Heterogeneous IoT System

The proposed SCSB heterogeneous IoT system is designed to work in a scalable environment, as shown in Figure 2. This is a heterogeneous system that comprises a variety of devices in a system. It submits different types of information for processing and storage. In the current system model, IoT devices transmit their data via DOs to the cloud server, without direct peer-to-peer communication. The deployment of decentralized blockchain into this system ensures secure data storage and the elimination of illegitimate devices.

4.1 | System Model

The proposed solution is developed to improve scalability issues and support heterogeneity in the IoT environment based on the incorporation of a decentralized blockchain. The IoT devices in the proposed SCSB system do not directly communicate with each other. Instead, each device interacts with the DO, who then uploads the collected data to the cloud through a secure process involving a TA and the blockchain. There are five key entities in this system, and they are the data owner, the DU, the TA, the decentralized blockchain, and the cloud server. The work nature of each entity in this system is illustrated below:

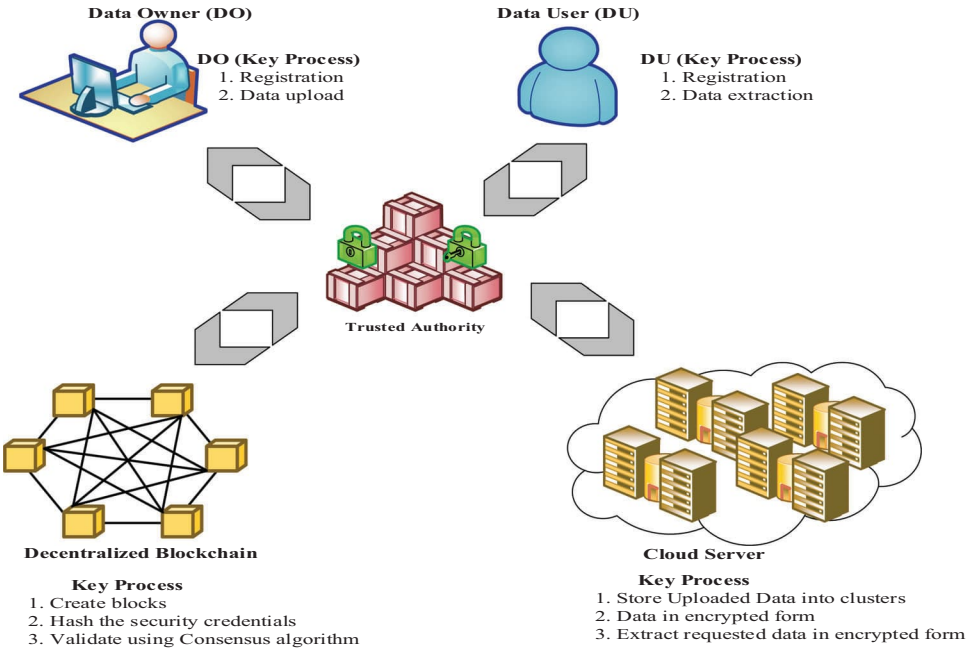

FIGURE 2 | SCSB work process.

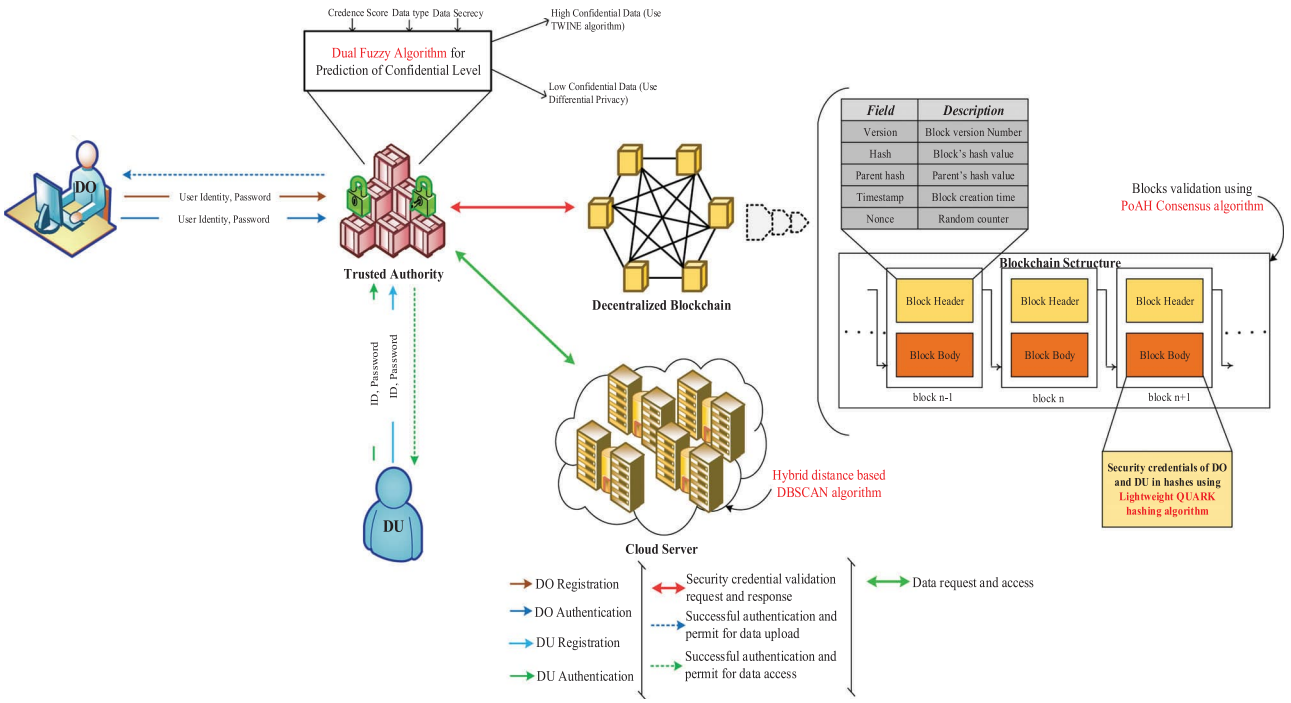

FIGURE 3 | Proposed SCSB architecture model.

i. DO: The DOs collect information from IoT devices and upload the data to the cloud server. There are multiple DOs participating in the system, andeach DO has an individual login.

ii. DU: dual The DU participates in the system to access the cloud and extract uploaded data. Each DU requests the cloud via a TA. The DUs are validated with basic credentials of Identity and password.

iii. TA: This entity in the system is trusted and hence it is responsible for validating credentials for authentication. It maintains the attributes for each data when the DO uploads the data. The TA connects with blockchain to ensure security. The credentials are stored in hashes on the blockchain.

iv. Decentralized blockchain: The blockchain is decentralized, which is able to provide access to all DOs and DUs. The blockchain is composed of blocks that enable to manage of credential secrecy.

v. Cloud server: The cloud server is responsible for storing the encrypted data uploaded by the DO. The data is accessed from the cloud by the DU after the completion of authentication.

The constructed SCSB heterogeneous IoT system model is depicted in Figure 3. As per the developed system model, the processes in blockchain and cloud are executed.

4.2 | DO and DU Authentication and Blockchain Consensus Algorithm

Let the system be composed of L and M number of DOs and DUs that are represented as $\{DO_1, DO_2, DO_3,\ldots DO_L\}$ and $\{DO_1, DO_2, DO_3,\ldots DO_M\}$. The DO and DU have unique identities and passwords, using which the DO and DU are identified in the system. On completion of successful authentication, the DO uploads the data, and the DU accesses the required data. The credentials are stored in a decentralized blockchain. The blockchain stores security credentials in the form of hashes using the lightweight QUARK algorithm. For each authentication, the security credentials are verified, and then it allows access.

The lightweight QUARK algorithm constructs a sponge based on three phases as initialization, absorbing phase, and squeezing phase. Assume the identity and password are denoted as *sc*. The size of the sponge will be of $b = r + c > = n$, where c is the capacity and n is the length of output. Hereby, the process performed in sponge construction is depicted below,

i. Initialization phase: In this step, the *sc* is the security credential which is padded with a '1' bit. This padding is presented with the addition of '0' until it reaches the length of r that is multipliable. The term r is the block length, which is one of the parameters used in the QUARK algorithm.

ii. Absorbing phase: Let the r bits of blocks involve the XOR function with the last r bits of $Y_{b/2\text{-}r},\ldots, Y_{b/2\text{-}1}$ that represents the state. It is inserted along the application of permutation P.

iii. Squeezing phase: Then, in this step, r bits in the state are obtained as output along with the application of permutation P. This is performed until n bits are obtained as output.

Based on this hashing, the DO's and DU's security credentials are hashed by themselves before sending an authentication request.

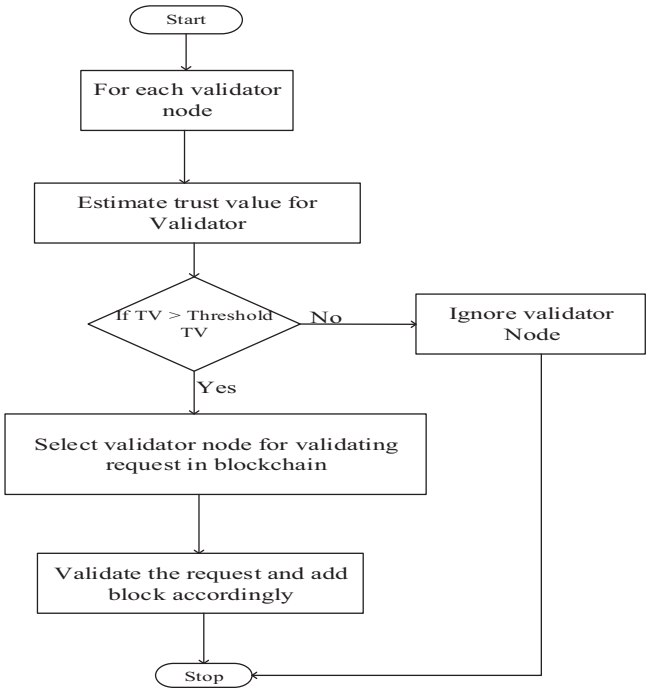

FIGURE 4 | PoAH working flowchart.

In blockchain, the blocks are equipped with hashes in each block, which are used for authentication. This algorithm is able to overwhelm multiple attacks such as collision, differential, etc. It resists the stealing of security credentials of DO and DU, which enables mitigation of illegitimate device participation in the system.

The heterogeneity of IoT comprises numerous devices that submit a huge number of requests for processing; hence, a lightweight Proof-of-Authentication (PoAH) consensus algorithm is presented in the blockchain. Using this consensus algorithm, a trusted validator is selected among the nodes for validation in the blockchain. The incorporated PoAH is suitable for resource-constrained devices, and it can support the scalability of the system. At the time of validation of blocks, the authentication of a node is performed based on the estimation of the trust values of the node. PoAH maintains scalability by using lightweight operations and a dynamic trust score evaluation mechanism, enabling fast validation even with increased IoT nodes. The transactions in the blocks are signed using a traditional digital signature algorithm (Figure 4).

The trust value, represented as TV, is estimated from the summation of the node's behaviour and the number of successful authentications. The node behaviour is defined as participation in the system with the neighbouring nodes. The use of a lightweight hashing algorithm in the blockchain enables to perform faster validation and maintains the same level of security. The presented consensus algorithm works with the validation of the security credentials of DU and DO using the selected trusted node. On receiving the validation request, the node is selected, and then it determines the public key for the verification of the signature of the block. After the validation of the signature, the hash values are computed.

Scalability is influenced by the network topology. Clustered or hierarchical topologies better performance with PoAH, while flat or fully meshed topologies can induce delay due to higher communication overhead.

Pseudocode 1. Proposed lightweight PoAH

Input: Lightweight QUARK hash, private (*PK*), and public (*PuK*) key for each node.

Output: Validated blocks with trusted nodes

1. Begin
2. Blockchain receives a request for validation
3. The validating nodes sign the block using their private key and broadcast the request.
4. Nodes check with the signature and submit trust values.
5. If (TV>Threshold)
   {
   Select as validator node and then add blocks
   Else
   Estimate trust value for next node
   }
   End if
6. End

4.3 | Data Storage in Cloud

On completion of authentication of the DO based on the registered credentials, it is allowed to upload the collected data. The confidentiality level of the data is predicted using a dual fuzzy logic algorithm that takes into account data type, credence score, and data secrecy. The confidentiality level is categorized into high and low. The highly confidential data is encrypted using the lightweight TWINE algorithm [41], while the low confidential data is secured using Laplace-based differential privacy. In this process of data storage, initially, the dual fuzzy logic is applied to determine the confidentiality level.

The dual fuzzy logic algorithm is constructed with two fuzzy logic blocks. Each fuzzy logic block consists of three entities: a fuzzifier, an inference engine, and a defuzzifier (Figure 5).

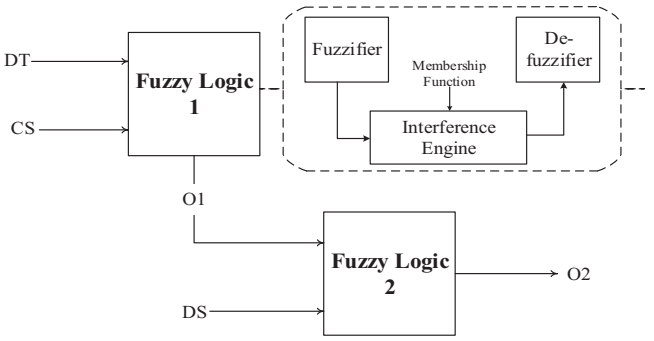

FIGURE 5 | Dual fuzzy logic.

TABLE 1 | Fuzzy logic 1 rules set.

DT	CS	O1
H	H	H
H	L	H
L	H	L
L	L	L

TABLE 2 | Fuzzy logic 2 rules set.

DS	O1	O2
H	H	H
H	L	H
L	H	L
L	L	L

The fuzzy logic method is operated based on the prediction of the degree of truth, which uses Boolean logic to determine the outcome as true or false in 1 or 0. It is operated with a defined set of rules based on the fed input parameters. The work process of each entity is illustrated in the following,

i. Fuzzifier: The fuzzifier is the initial block that performs fuzzification, which receives input values. According to the proposed dual fuzzy logic, the first fuzzy logic considers data type and credence score. Then the second fuzzy system considers data secrecy and outputs 1 as its input. The input is in crisp values, and it is converted to a fuzzy set for further processing.

ii. Interference engine: This engine is fed with knowledge base fuzzy rules, which work on 'IF-THEN' rules defined for the submitted input. For the given two input values, a set of four rules is developed. The inputs are presented in high and low values that are defined as a range of values. From the input values, the degree of membership function is designed.

iii. Defuzzifier: The extracted outcome based on the membership functions is in the form of a fuzzy set. In this block, it is converted into crisp values.

The data type is categorized into two as normal data and emergency data. It is predicted based on the static threshold value for each measurement. Then, the credence score is determined based on the number of successful authentications and the amount of data uploaded. The increase in these two metrics results in a higher credence score. Data secrecy is the importance of data storage in the cloud. For example, it could be more sensitive and hence it requires high data secrecy. It could include specifications in the data such as company agreements, income tax information, transactions, account details, and others. According to these three parameters, the dual fuzzy logic determines the high confidential level and low confidential level of data storage in the cloud. The fuzzy rules for the prediction of the confidential level are illustrated in Tables 1 and 2.

If the dual fuzzy logic method results in high, then the data follows the lightweight TWINE algorithm; else Laplace-based differential privacy is used. The TWINE algorithm of 64-bit, lightweight block cipher. It uses the bitwise exclusive OR operator. The three key processes followed are encryption, key schedule, and decryption. The reverse of encryption is performed in decryption. Let the plain text be in the size of 64-bit, round key *RK*, which is generated from the secret key. Initially, the round function is applied, which is based on the nonlinear layer using 4-bit S-boxes. Along with this, the diffusion layer is used to permute 16 blocks. Then, the S-box mapping is performed for a specified number of bits, and it shuffles the block. The next step is to key schedule the round keys that are produced and processed. Further, the inverse process of encryption is presented for decryption.

If the outcome is low confidential data, then the Laplace-based differential privacy method is used. The differential privacy is enabled to provide security for the data. It is a mechanism that adds noise to secure the data from attackers. Differential privacy is developed using two numeric values as epsilon and delta, which are represented as ε and δ.The value of δ is included as the multiplicative bound. If the value is set low, then the risk is also smaller. In the Laplace mechanism based differential privacy adds Laplacian noise to the function. It computes the function *f*, then it adds noise from the Laplace distribution. The noise to be added is determined as follows,

$$N = [\text{Sensitivityof } f/\varepsilon], \text{where } \delta = 0 \tag{1}$$

The mathematical formulation for the Laplace mechanism is given as,

$$[D] = f[D] + \varepsilon \tag{2}$$

Let D be the data to be stored in the cloud by data owners. Based on the use of differential privacy, the data is secured.

4.4 | Data Clustering

The data are clustered in the cloud to ensure scalability in storage due to the arrival of a huge amount of data that is collected from heterogeneous sources. The clustering of data is presented using H-DBSCAN. This algorithm uses two key parameters, such as minPts and eps, i.e., epsilon. The minPts denotes a minimum number of points that cluster a dense region; on the other hand, theeps defines the distance measurement that is measured using the points that are located. In this work, hybrid distance is used that takes into account the Manhattan distance and the Euclidean distance. The formulation for the Manhattan and Euclidean distance measures is given as:

$$d_1 = \sum_{i=1}^{n} |x_i - y_i| \tag{3}$$

Then the Euclidean distance formula is measured as follows:

$$d_2 = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2} \tag{4}$$

where x_i and y_i are the data points in the cloud based on which the clusters are constructed. In this work, a hybrid distance is used that estimates d_1 and d_2 for the same set of data points, and then it predicts the average for it. The hybrid distance measure is given below:

$$D = \frac{d_1 + d_2}{2} \tag{5}$$

Initially, identify the neighbouring point present within eps; then predict the core points. In case the predicted core point is already in a cluster, ignore it; else, consider it in cluster construction. On identifying the density-connected points concerning the core points, the data are clustered. The data points that are covered within minPts within the radius eps. All the neighbouring points are considered to be in the same cluster. The process of clustering enables the improvement of scalability of data storage.

Pseudocode 2. H-DBSCAN algorithm

Input: Owner's Data, eps, minPts
Output: Clusters (C)
1. Start
2. Let C = 1
3. For each non-visited point *p*
– {
– Assign *p* as a visited point
– Determine neighbours N using D
– if |*N*| ≥ minPts
– *N* = *N*∪ *N*'
– }
4. If (*p*' is not included in any cluster)
– {
– addp'to C
– else
– ignore
– }
6. Stop

As per the above pseudocode, the H-DBSCAN algorithm is developed. Based on the clustering of data in the cloud, the scalability of heterogeneous data is achieved. The use of a hybrid distance measure enables improved the perfect identification of neighbouring data points which enhances clustering.

5 | Experimental Evaluation

In this proposed SCSB IoT heterogeneity system is developed using simulator to obtain results. This section is categorized into simulation setup and comparative analysis.

5.1 | Simulation Setup

In this section, the proposed SCSB IoT heterogeneity system is designed in the iFogSim simulation tool. It presents to develop '*n*' number of DOs and DUs that perform data upload and data access from the cloud. To ensure security, a decentralized blockchain is incorporated for authentication and validation of nodes. On the other hand, scalability is one of the main issues in IoT heterogeneous systems, which is solved with the use of lightweight algorithms and by clustering data in a cloud server. In Figure 6, the sequence diagram of the proposed SCSB is depicted with the entities that are involved in the system. According to this flow, the process in this SCSB is carried out. After completion of authentication, the data are stored based on the confidentiality of the data. The designed SCSB system in iFogSim is depicted in Figure 7, which shows connectivity between fog nodes and DO, DU. The fog nodes in this model act as an intermediate entity that is responsible for creating a link between nodes. The process of fog nodes is to receive the request and forward it to the TA.

Then, the process of registration and data upload is illustrated in Figures 8 and 9. Each DO has the right to upload multiple data at a time, and also the data can be of any type. This simulator software is an open source tool and it works with JDK 12.0.2, NetBeans IDE 8.2, and MySQL-5.7.36 (WAMP SERVER 3.2.6). These software are installed on the Windows 10 operating system. The specifications used in the SCSB system are given in Table 3.

5.2 | Comparative Analysis

The comparative analysis is conducted for the following parameters such as execution time, encryption time, decryption time, storage efficiency, throughput, latency, and hit rate. The proposed SCSB IoT heterogeneity system is compared with previous research works such as ACE-BC, proxy re-encryption, and blockchain authentication. On the other hand, Tables 4 and 5 illustrate the comparison of the proposed research work with previous research methods.

5.2.1 | Execution Time

The execution time is defined as the time taken for the DU to process the request and obtain access from the cloud. An increase in execution time demonstrates poor performance of the system. In Figure 10, the performance of execution time for SCSB, ACE-BC, proxy re-encryption, and blockchain-based authentication is depicted. From this plot, the proposed SCSB system attains a lesser execution time than the prior research works; this result is obtained due to the use of a lightweight consensus algorithm. The involvement of illegitimate devices increases the execution time due to the submission of higher traffic, fake requests, occupied resources, and so on.

The previous research works use blockchain while it is operated using the SHA-256 algorithm, which is equipped with multiple computations and hence increases execution time. Further, the use of re-encryption provides stronger security; however, it is supposed to increase execution time due to the performance of encryption and decryption twice.

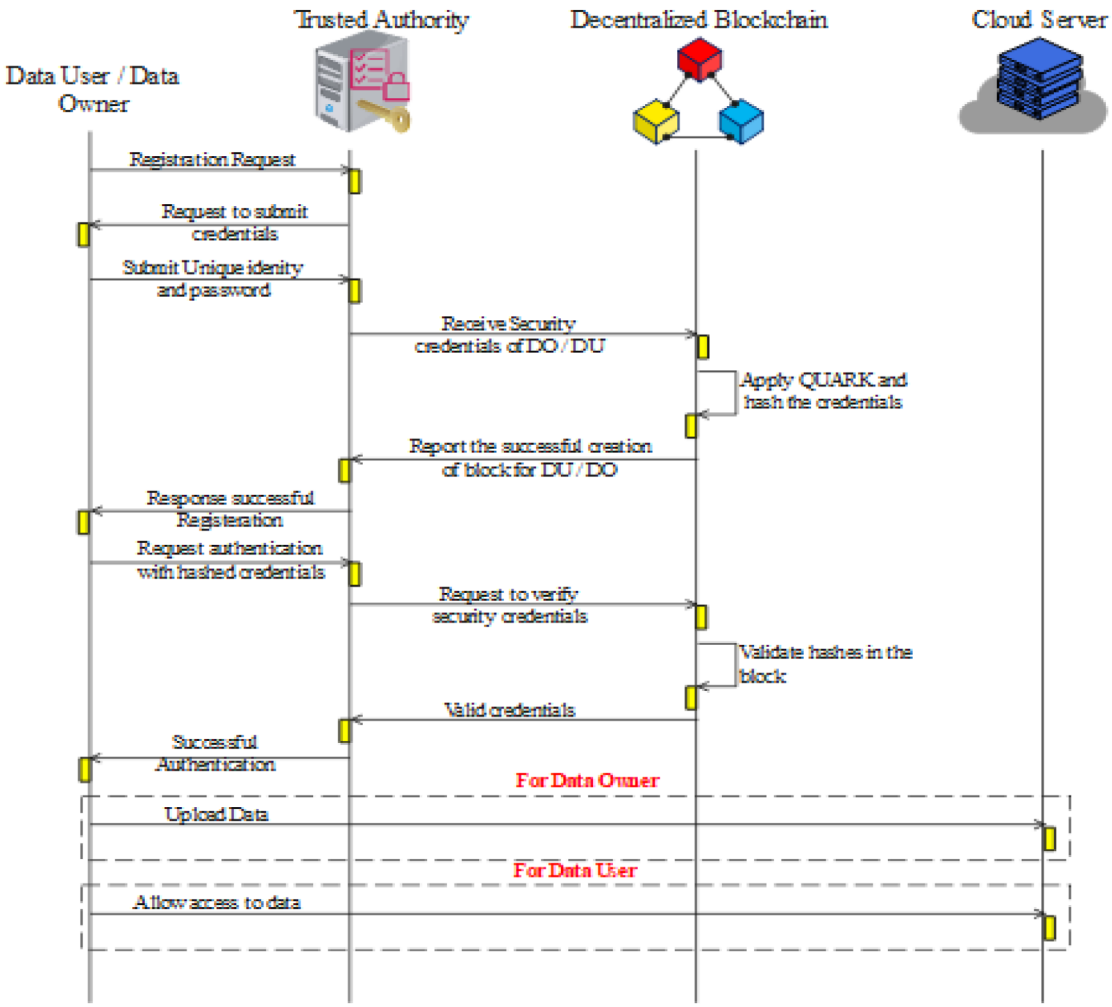

FIGURE 6 | SCSB sequence diagram.

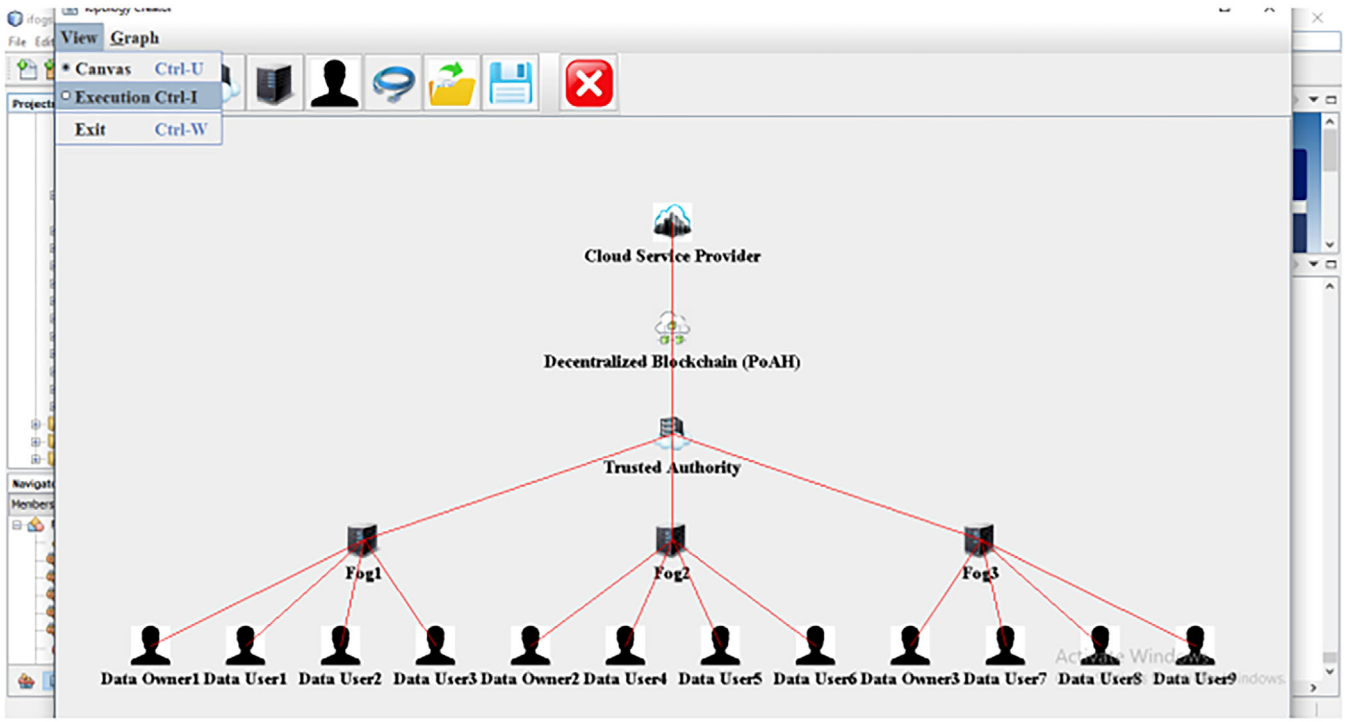

FIGURE 7 | iFogSim SCSB system model.

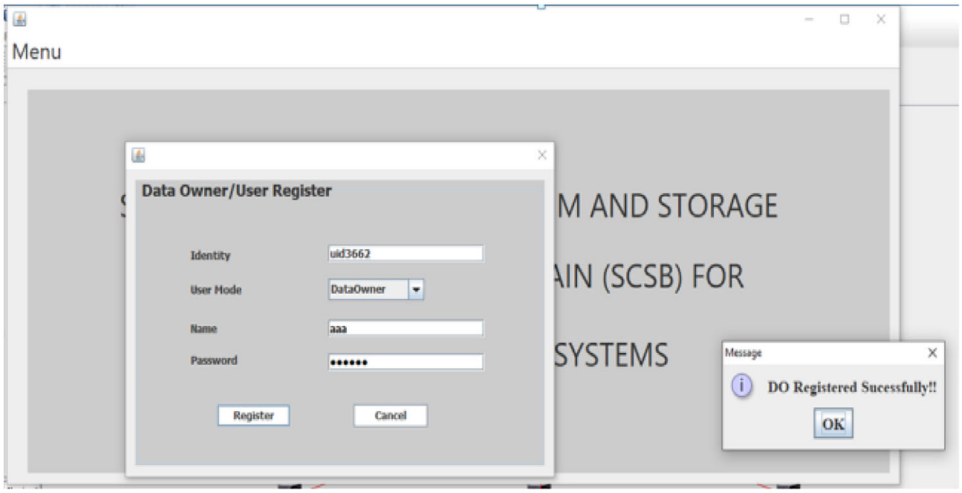

FIGURE 8 | DO and DU registration.

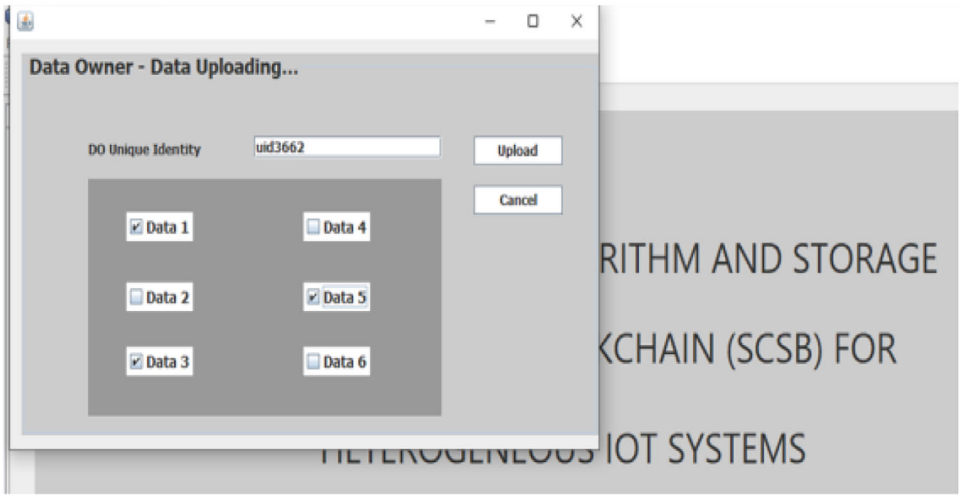

FIGURE 9 | DO data upload.

The average of execution time for the proposed is 5.3 s whereas the highest execution time in previous research work is 23 s. In the SCSB system, the execution time gradually increases with respect to the increase in the number of devices.

5.2.2 | Encryption Time and Decryption Time

The encryption and decryption time is defined as the time taken for the device to encrypt and decrypt the message using private and public keys. The algorithm with minimum computations mitigates the encryption and decryption time of data.

The encryption and decryption time is measured concerning the increase in the number of access attributes. The comparative results for this parameter are depicted in Figure 11, where the proposed SCSB system achieves a lesser time for encryption and decryption than the existing research works.

The incorporation of a lightweight consensus algorithm, and blockchain with lightweight hashing, enables improvement in encryption time and decryption time. It enhances scalability in heterogeneous systems, since the use of algorithms minimizes computations and processing. A comparative Table 6 is demonstrated to identify the time difference between the proposed and existing algorithms.Hence, the development of a lightweight algorithm is an efficient solution for minimizing processing time and achieving scalability.

TABLE 3 | Simulation specifications.

Entity	Specification
Data owner	3
Data user	9
Fog nodes	3
Trusted authority	1
Cloud service provider	1

5.2.3 | Storage Efficiency

The storage efficiency discusses about the ability of the cloud server to store heterogeneous data. The heterogeneous data

TABLE 4 | Comparison of existing and proposed processes.

Reference	DO auth-entication	DU auth-entication	Blockchain	Data storage confidentiality
[30]	✗	✓	✓	✗
[31]	✗	✓	✓	✗
[32]	✗	✓	✓	✗
[34]	✗	✓	✗	✗
[35]	✓	✓	✓	✓
[36]	✓	✓	✓	✓
[38]	✓	✗	✓	✓
[39]	✗	✗	✓	✓
Proposed (SCSB)	✓	✓	✓	✓

TABLE 5 | Comparison of existing methods.

Reference	DO authen-tication	DU authenti-cation	Blockchain technology	Consensus algorithm	Hashing algorithm in blockchain	Data storage security algorithm	Application supported
[30]	–	Mutual authentication (ECC-based authentication protocol)	Smart Contracts	Proof of Stake	SHA-256 algorithm	–	Decentralized application
[31]	–	Majority-based verification	Smart Contracts	–	SHA-256 with ECC algorithm	Data stored without security	Not mentioned
[33]	–	Blockchain-based token requesting mechanism	Smart Contracts	–	SHA-256 algorithm	–	Not mentioned
[34]	–	Identity-based authentication	–	–	–	–	IoT-based-Agriculture
[35]	–	–	Ethereum smart contract	Proof-of-Authority	Collision-resistant hash function	AES-128 encryption	Not mentioned
[36]	Hashing credentials using the QUARK algorithm	Artificial neural network	Hyperledger Fabric blockchain	Not mentioned	QUARK hashing algorithm	PRESENT algorithm	Any Sensitive IoT application
[38]	Identity auth-entication	–	Distributed blockchain	Not mentioned	SHA-256 algorithm	Attribute encryption mechanism	Cybersecurity in IoT
Proposed (SCSB)	Lightweight QUARK algorithm	Lightweight QUARK algorithm	Decentralized blockchain	Proof-of-Authentication	Lightweight QUARK algorithm	TWINE algorithm and differential privacy	Heterogeneous IoT

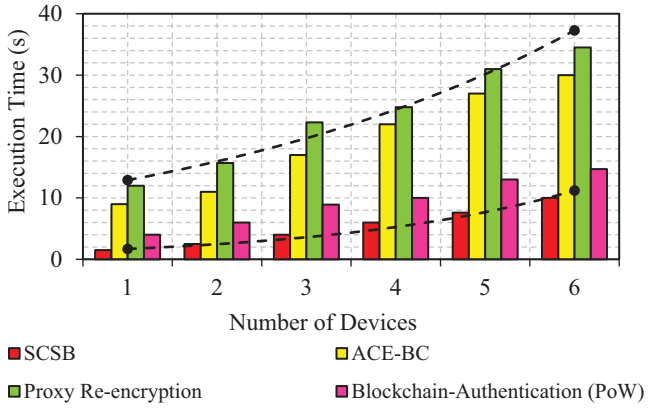

FIGURE 10 | Comparison of execution time.

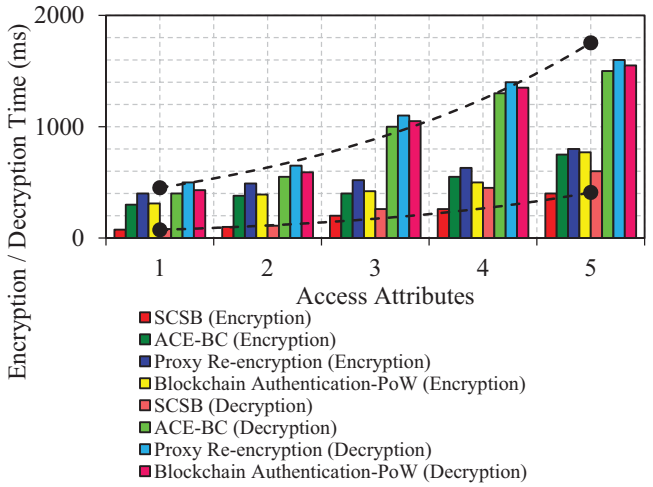

FIGURE 11 | Comparison of encryption and decryption time.

TABLE 6 | Average encryption and decryption time.

Methods used	Encryption time (ms)	Decryption time (ms)
SCSB	207	300
ACE-BC	476	950
Proxy Re-encryption	568	1050
Blockchain-based authentication (PoW)	478	994

storage causes a scalability issue due to the arrival of excessive data from data owners. In the proposed SCSB system, the data is clustered using H-DBSCAN before it is stored in the cloud. The storage of data based on clustering is enabled to support the scalability issue, which in turn improves storage efficiency.

The results obtained for storage efficiency are depicted in Figure 12. The previous research work validates the data and stores all the raw data directly into the storage, which makes the storage clumsy. From the obtained result, the storage efficiency of the proposed system is better than the previous methods. The process of clustering gathers a set of data into particular groups, which categorize the data into classes of data in a cloud server.

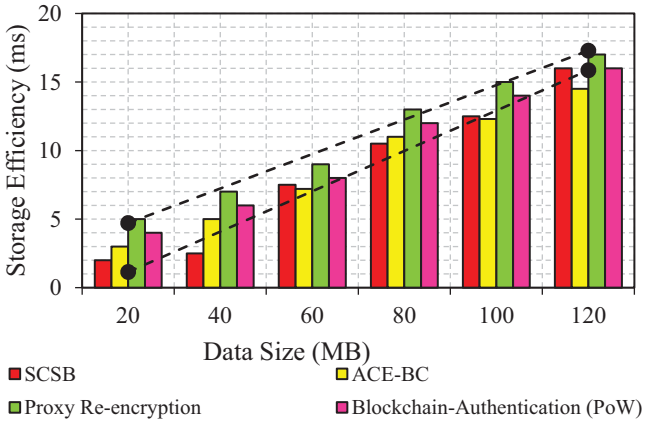

FIGURE 12 | Comparison of Storage Efficiency.

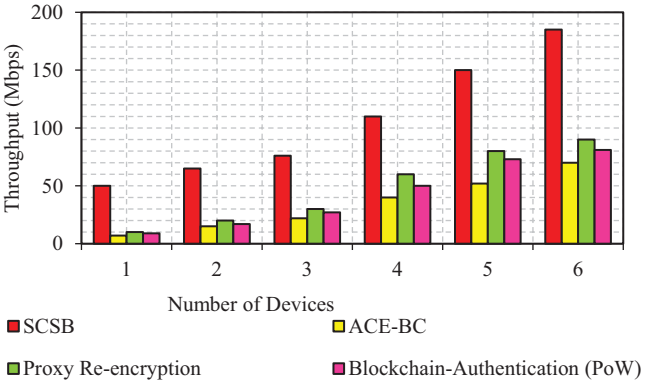

FIGURE 13 | Comparison of Throughput.

5.2.4 | Throughput

Throughput is a significant network parameter that measures the amount of data transferred to the end server within a given amount of time.

The throughput is plotted with the increase in the devices which increases the number of requests for processing. Each device can submit more the one request, and the request can be for uploading the data or accessing the data. Whatever the request, it is essential to authenticate, validate, and then provide the required service for it. The graphical result of throughput is shown in Figure 13, in which the SCSB system achieves higher throughput than the previous research methods.

The average throughput of the proposed system is 106 mbps, and the minimum throughput reached is 34 Mbps. The increase in throughput assures to perform better transmission of messages from devices. The larger gap between throughput for the proposed and existing methods illustrates that the data storage and data access is efficient in the SCSB system.

5.2.5 | Latency

Latency is defined as the delay that occurs in data transmission while transferring data from the source to the destination.The

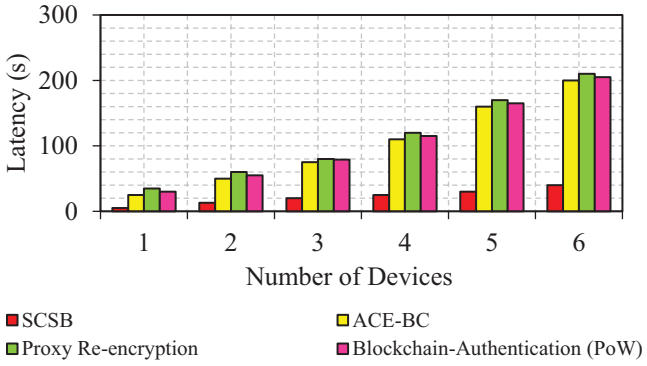

FIGURE 14 | Comparison of Latency.

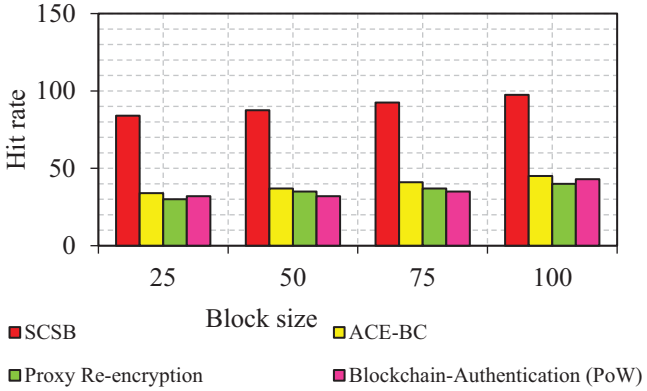

FIGURE 15 | Comparison of the hit rate.

TABLE 7 | Average latency.

Methods used	Latency (s)
SCSB	22.15
ACE-BC	103.4
Proxy re-encryption	112.5
Blockchain-based authentication (PoW)	108.15

increase in latency defines the consumption of excessive time for data transmission. Hence, the increase in latency results in poor performance of the system.

The performance evaluation of latency is depicted in Figure 14 which shows a comparison of the proposed SCSB system and existing methods.From the obtained results, the latency of proposed system is lesser than the existing method that uses proxy re-encryption and blockchain based authentication (Table 7).

The average latency achieved in each method is depicted in Table 5. According to this table, the proxy re-encryption method results in higher latency due to the processing of encryption and decryption twice for each data from the device. On the other hand, the use of lightweight algorithms tends to minimize the number of computations, which reduces the latency. Also, the use of lightweight algorithms is suitable for managing the scalability of the system, and it is simple for resource-constrained IoT devices.

5.2.6 | Hit Rate

The performance of hit rate with the increase in block size is demonstrated in Figure 15. The parameter hit rate defines the successful device requests in the blockchain. In the proposed SCSB system, a lightweight consensus algorithm is incorporated, which increases the hit rate due to the use of trusted nodes for block validation.

The previous research methods are lesser in hit rate due to the absence of the selection of trusted nodes for validation. If the validation is conducted by an illegitimate node, then it results in poor management that minimizes the hit rate.

5.3 | Use Case—Smart Industry

The proposed SCSB heterogeneous IoT system enables the capture of data from multiple devices. Hereby, the industrial application is considered for the use case.

The application of industry is advanced with automation in the production of a product. Hence, the equipment in an industry is monitored due to the absence of human intervention. Figure 16 shows the use case architecture for an industrial application. The presence of different equipment in an industry is monitored using IoT sensors, and the information is collected by the DO and uploaded. Further, the uploaded data is accessed by the DU after performing authentication.The sensor data can be sensitive to representing high temperature or pressure of the motor [42], which requires immediate action. In this way, the data is collected and transferred to the server via the blockchain to ensure security.

5.4 | Security Requirements

- Integrity -
  Integrity is defined as the protection that is provided to the data in the system. In the SCSB system, the data to be uploaded is secured using cryptography and differential privacy based on the importance of the data. The importance of the data is determined by the data owner and corresponding security is applied such as the lightweight TWINE algorithm and differential privacy. Hence, the SCSB system achieves this security requirement of integrity [43].
- Availability -
  The requirement of availability in security means the provisioning of required resources for all authorized users. In the proposed SCSB system decentralized blockchain is used which restricts the involvement of illegitimate DOs and DUs. This blockchain technology incorporates lightweight hashing that stores security credentials in blocks, which cannot be altered.
- Confidentiality -
  Confidentiality is the property that enable security for the private information of all DOs and DUs. The SCSB system incorporates a decentralized blockchain where the security credentials are stored in hash form to assure security.

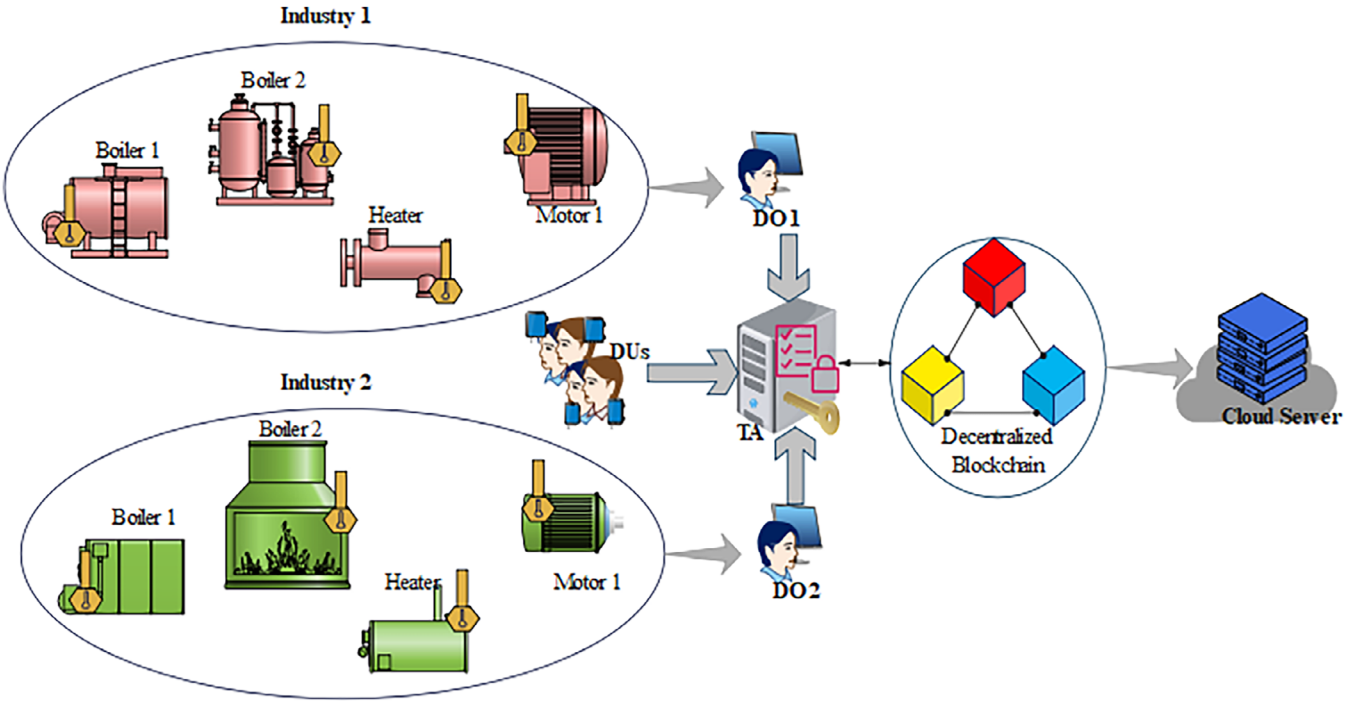

FIGURE 16 | Industrial use case architecture.

TABLE 8 | Table security threat mitigation summary table.

Threat	Potential risk	SCSB countermeasure
Man-in-the-middle	Interception and manipulation of data during transmission.	Use of Trusted Authority (TA) for routing all communication; secure hashing with QUARK for credentials.
Impersonation attack	Illegitimate access by posing as a legitimate user or device.	Dynamic credential hashing with lightweight QUARK; credentials change with each authentication session.
Spoofing attack	Gaining unauthorized access to the system to cause damage or collect intel.	Secure authentication using unique IDs and passwords hashed with QUARK; device legitimacy verification.
Eavesdropping attack	Unauthorized reading or alteration of data in transit.	End-to-end encryption using TWINE and Laplace-based differential privacy; data encrypted before transfer.
Password attack	Guessing or stealing passwords to gain unauthorized access.	Strong password requirements; passwords are never stored in plaintext but hashed and secured in blockchain.
Replay attack	Reuse of captured valid credentials or data packets to gain access.	Non-reusable hashed credentials via QUARK; timestamps and trust validation using PoAH.
Collusion attack	Multiple malicious nodes colluding to gain network control.	Trust-based node validation with Proof-of-Authentication (PoAH); dynamic trust scoring and validator rotation.
Denial of service (DoS)	System overload from illegitimate or excessive requests.	Node validation through PoAH ensures only trusted nodes process requests; clustering improves load handling.
Blockchain tampering	Unauthorized modification of blockchain data.	Immutable blocks with QUARK-hashed credentials; consensus validation using PoAH with trusted nodes.

- Authorization -
  The property of authorization is to assure authentication for the devices that participate in the system. In this proposed SCSB system model, the DOs and DUs are authenticated using unique identities and passwords that enables to allow access only for authenticated devices.

5.5 | Security Threats

- Man-in-the-middle attack -
  The behaviour of this attack is to interrupt a transmission in the middle and make the other end device believe it is a legitimate device. In this proposed SCSB system, the DO and DU connect with the server via a TA, which is a legitimate entity in the system that never performs illegitimate activities. Therefore, the occurrence of a man in the middle attack is restricted to this system.
- Impersonation attack -
  The impersonation attacker is involved in the system to steal private information that is transferred. If the security credentials are stolen then the attacker could get permission to either upload data or access data. In the SCSB system the security credentials are changed during each authentication which enables to overcome impersonation attacks in this system.
- Spoofing attack-
  This type of attack is launched to stream access into the system, so that it could understand the system and damage it. The proposed system incorporates lightweight hashing for authentication and cryptography for secure data upload. Hence it assures the system is protected against spoofing attack.
- Eavesdropping attack-
  The eavesdropping attackers aim to delete or modify the information that is shared from one device to another. If the shared data is raw then this attacker alerts the original information and updates it with fake information into it. This attacker is complex to be launched in the SCSB system due to the use for using and cryptography before transmission of any information.
- Password attack-
  This password attack is an attacker that has an intention to compromise a user for accessing the password information to access the system. The user is requested to set a complex password for higher protection, also, the password is shared in hashed form that is stored in the blockchain, which cannot be compromised or altered. Hence, the password attack fails in this system Table 8.

6 | Conclusion

In this paper, a priority-based lightweight authentication and access control is designed for Cloud-IoT is proposed. It mainly focuses on solving the scalability issue in the IoT heterogeneous environment. Initially, the data owner and the DU are registered and authenticated using the user ID and password. The transmission of these security credentials is based on the lightweight QUARK algorithm. This is also used in decentralized blockchain to improve security and minimize computations. The authenticated data owner uploads data to the cloud after predicting the confidentiality level using a dual fuzzy algorithm. Here, the low confidential data is secured using the lightweight TWINE algorithm and differential privacyfor highly confidential data. The data is secured in the cloud, and it is clustered using the H-DBSCAN algorithm. The arrival of excessive heterogeneous data causes scalability, which is solved by using clustering. In the blockchain, a lightweight PoAH consensus algorithm is presented for validating the request. This consensus algorithm prefers a trusted node for validation, which ignores illegitimate nodes. As a result, the entire proposed SCSB system achieves better performance in terms of security and scalability.

Author Contributions

All authors work equally to accomplish this study.

Conflicts of Interest

The authors declare no conflicts of interest.

Data Availability Statement

Data will be provided upon request to the corresponding author.

References

1. M. Noaman, M. S. Khan, M. F. Abrar, S. Ali, A. Alvi, and M. A. Saleem, "Challenges in Integration of Heterogeneous Internet of Things," *Intelligent Mobile Edge Computing for Smart Internet of Things: Architecture, Algorithm, and Application, Scientific Programming* (Hindawi, 2022).

2. C. Parmar, A. Todankkar, S. Wayal, and J. Gaydhane, "Middleware to Address Heterogeneity Problem in IoT," *International Journal of Advances Research in Science, Communication and Technology* 2, no. 3 (2022).

3. V. Nguyen, J. A. Cabrera, G. T. Nguyen, D. You, F. H. P. Fitzek, "Versatile Network Codes: Energy Consumption in Heterogeneous IoT Devices," *IEEE Access* 8 (2020).

4. S. Chen, P. Gong, B. Wang, A. Anpalagan, M. Guizani, and C. Yang, "Edge AI for Heterogeneous and Massive IoT Networks," in *19th IEEE International Conference on Communication Technology (ICCT)* (2019).

5. S. Zafar, K. M. Bhatti, M. Shabbir, F. Hashmat, and A. H. Akbar, "Integration of Blockchain and Internet of Things: Challenges and Solutions," *Annals of Telecommunications* 77 (2022): 13–32.

6. P. Bagga, A. Kumar Das, V. Chamola, and M. Guizani, "Blockchain-Envisioned Access Control for Internet of Things Applications: A Comprehensive Survey and Future Directions," *Telecommunications Systems* 81 (2022): 125–173.

7. Y. Zhang, L. Zhang, Q. Wu, Y. Mu, "Blockchain-Enabled Efficient Distributed Attribute-Based Access Control Framework With Privacy-Preserving in IoV," *Journal of King Saud University—Computer and Information Science* 34, no. 10 (2022): 9216-9227.

8. L. Hang and D.-H. Kim, "Design and Implementation of an Integrated IoT Blockchain Platform for Sensing Data Integrity," *Sensors* 19, no. 10 (2019): 2228.

9. L H. Al-Farhani, Y. Alqahtani, H. A. Alshehri, R. J Martin, S. Lalar, and R. Jain, "IoT and Blockchain-Based Cloud Model for Secure Data Transmission for Smart City," *Recent Advances in IoT and Blockchain-Based Security/Privacy in Advent Technology* (Hindawi: Security and Communication Networks, 2023).

10. W. Rafique, M. Khan, S. Khan, and J. S. Ally, "SecureMed: A Blockchain-Based Privacy-Preserving Framework for Internet of Medical Things," *Advances of Intelligent Sensory Data Processing and Protection in IoT* (Hindawi: Wireless Communications and Mobile Computing, 2023).

11. M. Tcholakian, K. Gorna, M. Laurent, H. Kaffel, B. Ayed, and M. Naghmouchi, "Self-Sovereign Identity for Consented and Content-Based Access to Medical Records Using Blockchain," *Recent Advances in IoT and Blockchain-Based Security/Privacy in Advent Technology* (Hindawi: Security and Communication Networks, 2023).

12. A. Sekar Rajasekaran, M. Azees, and K. Yahya, "FHAAPS: Efficient Anonymous Authentication With Privacy Preservation Scheme for Farm-to-Home Communication," *Security Hardened and Privacy Preserved Vehicle-to-Everything (V2X) Communication* (Hindawi: Security and Communication Networks, 2023).

13. S. Bhattacharyya, S. Athithan, and S. Pal, et al., "An IoT-Enabled Intelligent and Secure Manufacturing Model Using Blockchain in Hybrid Cloud Communication System," *Blockchain-Assisted Secure Smart Cities Communication* (Hindawi: Security and Communication Networks, 2023).

14. M. T. Al Ahmed, F. Hashim, S. J. Hashim, and A. Abdullah, "Authentication-Chains: Blockchain-Inspired Lightweight Protocol for IoT Networks," *Electronics* 12, no. 4 (2023): 867.

15. S. M. Hosseini, J. Ferreira, and P. C. Bartolomeu, "Blockchain-Based Decentralized Identification in IoT: An Overview of Existing Frameworks and Their Limitations," *Electronics* 12, no. 6 (2023): 1283.

16. C. Nartey, E. T. Tchao, and J. Dzisi Gadze, et al., "Blockchain-IoT Peer Device Storage Optimization Using an Advanced Time-Varient Multi-Objective Particle Swarm Optimization Algorithm," *EURASIP Journal on Wireless Communications and Networking* 2022 (2022): 5.

17. P. Bagga, A. Kumar Das, V. Chamola, and M. Guizani, "Blockchain-Envisioned Access Control for Internet of Things Applications: A Comprehensive Survey and Future Directions," *Telecommunication Systems* 81 (2022): 125–173.

18. Y. Mezquita, B. Podgorelec, A. Belén Gil-González, and J. Manuel Corchado, "Blockchain-Based Supply Chain Systems, Interoperability Model in a Pharmaceutical Case Study," *Sensors* 23, no. 4 (2023): 1962.

19. N. Kumar, V. Goel, R. Ranjan, M. Altuwairiqi, H. Alyami, and S. A. Asakipaam, "A Blockchain-Oriented Framework for Cloud-Assisted System to Countermeasure Phishing for Establishing Secure Smart City," *Blockchain-Assisted Secure Smart Cities Communication* (Hindawi: Security and Communication Networks, 2023).

20. D. Chatziamanetoglou and K. Rantos, "Blockchain-Based Cyber Threat Intelligence Sharing Using Proof-of-Quality Consensus," *Advances in Cyber Threat Intelligence* (Hindawi: Security and Communication Networks, 2022): 3303122.

21. S. Zhou, K. Li, L. Xiao, J. Cai, W. Liang, and A. Castiglione, "A Systematic Review of Consensus Mechanisms in Blockchain," *Mathematics* 11, no. 10 (2023): 2248.

22. A. Guru, B. K. Mohanta, H. Mohapatra, F. Al-Turjman, C. Altrjman, and A. Yadav, "A Survey on Consensus Protocols and Attacks on Blockchain Technology," *Applied Sciences* 13 (2023): 2604.

23. O. Said, "LBSS: A Lightweight Blockchain-Based Security Scheme for IoT-Enabled Healthcare Environment," *Sensors* 22, no. 20 (2022): 7948.

24. J. Sengupta, S. Ruj, and S. D. Bit, "FairShare: Blockchain Enabled Fair, Accountable and Secure Data Sharing for Industrial IoT," *IEEE Transactions on Network and Service Management* 20, no. 3 (2023): 2929–2941.

25. Na Shi, L. Tan, C. Yang, et al., "BacS: A Blockchain-Based Access Control Scheme in Distributed Internet of Things," *Peer-to-Peer Networking and Applications* 14 (2021): 2585–2599.

26. S. Alshehri, O. Bamasaq, D. Alghazzawi, and A. Jamjoom, "Dynamic Secure Access Control and Data Sharing through Trusted Delegation and Revocation in a Blockchain-Enabled Cloud-IOT Environment," *IEEE Internet of Things Journal* 10, no. 5 (2022): 4239–4256.

27. F. Jeribi, R. Amin, M. Alhameed, and A. Tahir, "An Efficient Trust Management Technique Using ID3 Algorithm with Blockchain in Smart Buildings IoT," *IEEE Access* 11 (2022): 8136–8149.

28. R.-K. Sheu, M. Sunil Pardeshi, and L.-C. Chen, "Autonomous Mutual Authentication Protocol in the Edge Networks," *Sensors* 22, no. 19 (2022): 7632.

29. A. I. Abdi, F. E. Eassa, K. Jambi, K. Almarhabi, M. Khemakhem, A. Basuhail, "Hierarchical Blockchain-Based Multi-Chaincode Access Control for Securing IoT Systems," *Electronics* 11, no. 5 (2022): 711.

30. J. Lanaky, A. M. Rahmani, and S. Ali, et al., "BcmECC: A Lightweight Blockchain-Based Authentication and Key Agreement Protocol for Internet of Things," *Mathematics* 9, no. 24 (2021): 3241.

31. P. Gangwani, S. Joshi, H. Upadhyay, and L. Lagos, "IoT Device Identity Management and Blockchain for Security and Data Integrity," *International Journal of Computer Applications* 184, no. 42 (2023): 49–55.

32. Q. Zhou, C. Lai, Q. Guo, H. Ma, and D. Zheng, "A Novel Privacy Protection Scheme for Internet of Things Based on Blockchain and Privacy Set Intersection Technique," *Journal of Cloud Computing* 11 (2022): 93.

33. B. Chai, B. Yan, J. Yu, and G. Wang, "BHE-AC: A Blockchain-Based High-Efficiency Access Control Framework for Internet of Things," *Personal and Ubiquitous Computing* 26 (2022): 971–982.

34. B. Hassan, A. A. Al Sanad, and I. Ullah, et al., "A Cost-Effective Identity-Based Authentication Scheme for Internet of Things-Enabled Agriculture," *Wireless Communications and Mobile Computing* (2022).

35. Z. Ullah, B. Raza, H. Shah, S. Khan, and A. Waheed, "Towards Blockchain-Based Secure Storage and Trusted Data Sharing Scheme for IoT Environment," *IEEE Access* 10: 36978–36994.

36. S. Alshehri and O. Bamasag, "AAC-IoT: Attribute Access Control Scheme for IoT Using Lightweight Cryptography and Hyperledger Fabric Blockchain," *Applied Sciences* 12, no. 16 (2022): 8111.

37. Z. Liu, L. Meng, Q. Zhao, et al., "A Blockchain-Based Privacy-Preserving Publish-Subscribe Model in IoT Multidomain Data Sharing," *Wireless Communication and Mobile Computing* 8, no. 2022 (2022): 1–13.

38. A. Alharbi, "Applying Access Control Enabled Blockchain (ACE-BC) Framework to Manage Data Security in the CIS System," *Sensors* 23, no. 6 (2023): 3020.

39. K. O.-B. ObourAgyekum, Q. Xia, E. B. Sifah, C. N. A. Cobblah, H. Xia, and J. Gao, "A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain," *IEEE Systems Journal* 16, no. 1 (2021): 1685–1696.

40. O. A. Khashan and N. M. Khafajah, "Efficient Hybrid Centralized and Blockchain-Based Authentication Architecture for Heterogeneous IoT Systems," *Journal of King Saud University—Computer and Information Sciences* 35, no. 2 (2023): 726–739.

41. T. Suzaki, K. Minematsu, S. Morioka, and E. Kobayashi, "TWINE: A Lightweight, Versatile Block Cipher," *ECRYPT Workshop on Lightweight Cryptography* (2011).

42. M. W. Ashraf, S. M. Idrus, F. Iqbal, R. A. Butt, & M. Faheem, "Disaster-Resilient Optical Network Survivability: A Comprehensive Survey," *In Photonics* 5, no. 4 (2018): 1–24.

43. M. Faheem, B. Raza, M. S. Bhutta, & S. H. H. Madni, "A Blockchain-Based Resilient and Secure Framework for Events Monitoring and Control in Distributed Renewable Energy Systems," *IET Blockchain* 4, no. 3 (2024): 1–15.