Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

Block chain based Secure Data Sharing in Cloud-Based IOT System

Umar M Mulani
Research Scholar,
Dr. A. P. J. Abdul Kalam University Indore-India
Assistant Professor, Department of Computer Science and Engineering,
Padmabhooshan Vasantraodada Patil Institute of Technology, Sangli-India.
umarmulani22@gmail.com

Dr. Manoj Patil
Associate Professor, Department of Computer Science and Engineering
Dr. A. P. J. Abdul Kalam University Indore-India.
mepatil@gmail.com

Article Info
Page Number: 9834 - 9851
Publication Issue:
Vol 71 No. 4 (2022)

Article History
Article Received: *15 September 2022*
Revised: *25 October 2022*
Accepted: *14 November 2022*
Publication: *21 December 2022*

Abstract
Numerous security and privacy issues with IoT systems must be properly considered. There are benefits and drawbacks to both centralized and decentralized methods. Delays, computing expenses, and energy concerns constrain decentralized systems, whereas scalability constrain centralized solutions. We proposed a multi-agent architecture to enable straightforward, decentralized IoT access control security solutions. The responsibility for providing the necessary security for cloud computing, local IoT device connectivity, fog node security, core fog node security, and access control falls on blockchain management. The proposed architecture is a versatile strategy that may be applied to various IoT applications. Additionally, because they tend to focus on access control issues in specific IoT applications, such as smart homes, earlier research has not effectively addressed IoT obstacles. The authors are aware that the application and effectiveness of the solution in comparison to similar studies must be assessed during the implementation and testing phases.

Keywords: IoT, Cloud, Blockchain, Security, throughput.

1. Introduction

The IoT is an expansion of the Internet's capabilities that links various digital devices together for the purpose of exchanging data with one another. The Internet of Things, or IoT, is a network of interconnected electronic gadgets. Having devices that are both individually identifiable and capable of exchanging data with one another paves the way for improved human and commercial interaction and the development of more informed policy choices.

IoT will bring about revolutionary advances that improve human life, but it will also bring up various security concerns relating to privacy, system configuration, information

storage/management, and access control, therefore this scenario warrants serious examination. [1]. One of the biggest obstacles of the internet of things is resolving security and privacy concerns. One of the main components of the Internet of Things that can cause security problems is its heterogeneity [2].

Authentication and authorization solutions design is a crucial part of solving security and privacy problems in low-resource IoT devices [3]. To handle the distribution of lightweight and decentralized IoT safe access control, we present an architecture based on a multi-agent system and employ a private distributed blockchain. The proposed solution's primary focus is on protecting the integrity of data transmitted across IoT gadgets, fog nodes, and the cloud.

Background of Access Control System in IoT

Utilizing blockchain technology in IoT, the recent work of [4] eliminates the need for a centralized server. Blockchain technology enables IoT devices and users to keep a distributed database where sensor data may be maintained by individuals in a manner analogous to that of crypto currency [4]. Only a small number of recent papers [5, 6] have proposed analogous methods for other contexts. However, the confidentiality of transactional data is not safeguarded by these methods. The reason for this is that every method employs symmetric key encryption for protecting sensitive information. Here are a few common entry points into the information contained within the Internet of Things.

Access Control in IoT

Authentication and authorization of communication rights and resource access in accordance with predetermined security standards and regulations is what Access Control (AC) is all about [4]. The term "access control" (AC) is used to describe the process by which authorized entities are granted permission to use a system's resources according to a set of rules.

The issue of applying an appropriate access control model to billions of IoT devices is not an easy one. Despite the significant research done on authentication and authorization concerns in the literature, these problems have only just begun to surface in the Internet of Things (IoT) setting. While widely used in IT infrastructure, access control mechanisms such as access control list (ACL), role-based access control (RBAC), and attribute-based access control (ABAC) aren't optimal for providing scalable, efficient, and easily manageable applicability in an Internet of Things (IoT) setting [1].

While ACL's centralized architecture allows for improved management and tracking of actions, it still places limitations on where access control measures can be deployed. Confusion in duty problems arises as the number of IoT devices increases because of the corresponding rise in the complexity of access restrictions. Because of its centralized architecture, ACL has poor granularity and scalability and is very vulnerable to a single point of failure [5].

By leveraging the Internet of Things (IoT) strategy, the RBAC model provides a resource access authorization mechanism to users based on roles and stated principles such as priority, the separation of duties, and administrative function partitioning [6]. In a highly decentralized network,

these methods fall short of completely satisfying the demands of access control mechanisms and inter-device communication. For an IoT setting, you need a Capability-Based Access Control (CapAC) solution because of the problems with traditional access control methods. The ABAC model directly correlates qualities with subjects, hence mitigating the role explosion issue in RBAC. Attribute certificates of users are used to determine who gets what [5]. The complexity of the ABAC model and the importance of policy management both rise in tandem with the number of IoT devices [2].

For extremely extensive IoT-based infrastructures, a capability model is put into action. Each topic in this model has its own capability list that specifies which target objects it can interact with [7]. CapAC has been successfully implemented on a broad scale, although it presents a number of difficulties in the areas of access right propagation, and revocation.

1.1 Access Control Challenges in IoT

The main challenges of applying existing access control mechanisms in the IoT environment are as follows:

1. **Reusability of existing solutions.**

Although access control techniques have been the subject of substantial research and have been successfully implemented in the real world, they cannot be retrofitted onto an existing IoT infrastructure as-is due to their complexity and non-compliance with IoT standards. It takes time to implement, deploy, and accept a system built from the ground up [1].

2. **Centralized vs. distributed access control mechanisms**

Accessible control rules are provided by centralized solutions, yet there is only one potential failure point. Scalability problems [8] prevent centralized, state-of-the-art security frameworks from being implemented in an IoT setting. Users in a centralized end-to-end mechanism do not have control over who can see their information. This decentralized approach to the problem ensures confidentiality with minimal expense and no need for trust in a central authority. These decentralized systems are challenging to administer and call for constant tweaks to the access control policies on individual devices.

3. **Scalability**

The number of devices that can communicate with one another is growing at an unprecedented rate, which is making the task of managing these connections more difficult than ever. Scalability is a key feature of any decentralized and distributed access control method for the Internet of Things [9], as the number of connected devices is expected to explode.

4. **Heterogeneity**

The infrastructure supporting the Internet of Things is decentralized and made up of a wide variety of heterogeneous, networked devices running on a wide variety of underlying technologies.

Providing a scalable, robust, and secure IoT environment is greatly hampered by the fact that the underlying authentication and authorization policies of these technologies vary across domains.

5. Resource constraints

Low-power, loss-prone networks connect IoT devices, which are limited in their ability to compute and store data. The access control system should make it simple to deal with the aforementioned problems, given the available means [10].

As a result, the access control mechanism needed to take into account new criteria, such as those related to the IoT ecosystem, including dispersion, scalability, heterogeneity, and a lightweight design.

The following is a brief overview of the work's contributions:

The main contribution of this work is a novel blockchain-based architecture for the Internet of Things (IoT) security. The method makes use of a multi-agent system using SABE that is based on decentralised access control. The solution makes use of a private hierarchical blockchain to increase the IoT system's security and meet the requirements of low-power IoT devices.

The usage of mobile agent software, which can significantly contribute to the reduction of traffic overheads, serves as further evidence that we developed a generic, lightweight, and scalable solution that can be utilized by a variety of IoT applications.

Ours stresses the efficient and effective security of each layer of an IoT architecture using a private hierarchical blockchain structure, in contrast to competing solutions, and allows a, incorporating of mobility and intelligence, and application Mandatory Access Control (MAC), which is based on a hierarchical security level.

The remainder of the paper is organized as follows: Section 2 discusses the present IoT access control scheme. We quickly examine blockchain in Section 3 and how it relates to the Internet of Things. In Section 4, presents the findings, their analysis, and a discussion of them. The project is finished, and Section 5 discusses the project's future.

2. Literature Review

The relevant work in this paper can be divided into three primary categories with some overlap: multi-agent systems for access control, existing security control solutions in IoT, and blockchain-based access control for IoT.

2.1 Survey on Encryption Methods for security

Data encryption is an effective method to minimize data privacy and preserve data confidentiality. Unidentified privacy-preserving with authentication scheme was proposed in (Z. Guan et al.,2019) which is used to control smart devices and fog nodes nearby. The Paillier encryption algorithm was used to protect data privacy during data aggregation. A lightweight data-conserving compression scheme was introduced for computation in (R. Lu et al. 2017). This approach distinguished by the use of homomorphic Paillier encryption, Chinese Remainder

Theorem, and one-way hash chain techniques not only to combine data of hybrid IoT systems into one but also to insert fake data at the edge of the network at an early stage.

A novel security service has been proposed in (N. Abbas et. al. 2019) to offer start to finish security for IoT gadgets at the fog layer access the character-based encryption and mark cryptographic plans. This scheme provides security features like authentication, anonymity and non-repudiation. In (Yousefi et al.,2017), the author proposed a hybrid encryption algorithm which implemented to minimize safety risks and increase the speed and less computational difficulty of the encryption. The intent of this hybrid algorithm is knowledge privacy, secrecy, non-repudiation in information exchange for IoT.

An Identity-Based Encryption method presented in (N. Farjana et al.,2019) which guarantee secure information transmission to authorized users. Four-tiered hierarchical identity-based architecture for fog computing to offer data security

Table 1 shows encryption methods.

Author & citation	**Technique**	**Method**
(Sheshrao et al. 2016)	Homomorphic Encryption	Multilevel security is used to protect data. Additionally, personal data is safeguarded.
(Vishwanath et al. 2016)	Advanced Encryption Standard (AES)	Encryption and decoding are accomplished using a single standard key. Three datasets were used to assess security at the fog level.
(Farjana et al.,2019)	Identity-Based Encryption (IBE)	Suggested a four-tiered hierarchical design and employed the IBE approach to secure the fog. Efficiencies increased by 30%
(Wang et al. ,2017)	Data Aggregation Technique with Homomorphic Encryption	Securely upload data to public cloud services while protecting user identities. Preserve fog node bandwidth
(Xu et al. 2018)	Attribute-based Encryption and Attribute-based Decryption	Combination of encryption, signatures, and form encryption. Attained confidentiality and authenticity of critical information

2.2 Access control mechanism with smart contract for data sharing

It is plainly inconvenient and inefficient to transmit paper medical record between multiple hospitals by client themselves. Sharing healthcare data is regarded as a critical strategy for improving healthcare quality and lowering medical expenses. Though current E-IOT systems provide a lot of ease, there are still a lot of roadblocks in the way of secure and scalable data exchange across many companies, which limits the advancement of medical decision-making and research. In a centralized system, there is a risk of a single-point attack and data leakage. Furthermore, client are unable to retain control of their personal information in order to share it with someone they trust. It could lead to the unauthorized use of personal information by inquiring groups. Furthermore, different competitive organizations that lack trust partnerships are unable to share data, which will hamper data sharing progress. In this case, it is necessary to ensure security and privacy protection and return the control right of data back to users in order to encourage data sharing. It is relatively simply to deal with security and privacy issues when data resides in a single organization, but it will be challenging in the case of secure health information exchange across different domains. Meanwhile, it should think about ways to stimulate more efficient collaboration in the medical field. One typical solution is to use a secure access control system that allows only authorized entities to access shared data. This approach involves an access policy, which is typically made up of an access control list (ACL) linked to the data owner. An access control list (ACL) is a list of requestors who have authorization to access data, as well as the permissions (read, write, update) they have on that data. Authorization is the process of allowing authenticated users permission to access protected resources in accordance with preset access policies. Authentication is always done first, followed by permission. This mechanism's access policies are primarily concerned with who is executing which actions on which data objects for which goals.. Traditional access control approaches for E-IOTs sharing are deployed, managed and run by third parties. Users always assume that third parties (e.g. cloud servers) perform authentication and access requests on data usage honestly. However, in fact, the server is honest but curious. It is promising that combining blockchain with access control mechanism is to build a trustworthy system. Users can realize secure self-management of their own data and keep shared data private.

Peterson et al. (2016) proposed that client would only be able to authorize access to their records under specified circumstances, according to the proposal (research of a certain type, and for a given time range). Data requestors must meet these conditions to access the given data, according to a smart contract posted directly on the blockchain. The system will terminate the session if the requestor does not have the necessary access rights.

Similarly, smart contracts in Dan et al., (2016) can be used to grant and revoke access rights, as well as alert providers of updated information as they move in and out of networks.

Azaria et al. (2016) MedRec is a decentralized record management system built on the blockchain. Client-Provider Relationship Contracts are used in this system to connect any two nodes where client manage and share medical records with healthcare providers. Providers can add or modify this record in the case of client's permissions. When malevolent entities violate data access rights, a record is kept in the block to trace them down. They also created a user-friendly

graphical interface that enables client to communicate off-chain data while maintaining fine-grained access control.

Nguyen et al. (2019) When mobile users send requests, the admin component built an access protocol based on smart contracts. To prevent malicious attacks and guarantee trustworthy E-IOT sharing, smart contracts will check any transaction using preset access protocol policies. However, due to processing transactions such as Area ID, mobile gateway ID, and client ID, interested miners may infer personal information during the mining process.

Liang et al. (2017) Hyperledger Fabric's channel concept, which isolates different types of activities for users in different channels to share different grained data, was creatively used. chaincode (smart contract) with various access types, permissioned operations, and selected shared data indicated in the certificate by data owners can be launched in the channel. A channel system like this makes effective use of Fabric to promote data privacy in addition to data exchange.

The majority of the access control policies listed above specify who is allowed to do which approved activities on which parts of the data. Policies of various types are employed in many contexts, such as those based on roles, purposes, qualities, and so on. The majority of the systems mentioned above are part of RBAC (role-based access control) schemes.

Yue et al. (2016) designed Healthcare Data Gateway is a blockchain-based app architecture for smartphones and computers (HDG). They presented a purpose-centric access control paradigm with two sorts of data based on access purposes: raw data (healthcare service) and statistics data (medical research). Throughout the workflow, each transaction is processed using various sharing mechanisms for various goals. This system enables client to simply manage and monitor their healthcare data sharing. In most systems, smart contracts have predetermined access regulations based on requestors' roles/purposes and privileges based on role/purpose. However, it is inflexible when dealing with unforeseen or dynamic situations, which could provide a security risk.

(Fernández-Alemán et al., 2013). Another technique, Attribute-Based Access Control (ABAC), has been implemented in secure systems to address remaining difficulties with RBAC extensions and to improve security in specific situations. The ABAC-based system extends role-based features to attributes and establishes various policies for different groups of attributes in access requests. These traits are used to characterize the characteristics of subjects, resources, and the environment, among other things. Access to sharing data is granted only if the requestor's characteristics set complies with preset access policies (Dias et al., 2018).

Maesa et al., (2018) proposed a blockchain-based attribute based access control scheme according to the XACML standard for the compatibility of smart contracts. They go into great depth about how to design and translate access policies. Their method ensures that valid requestors are properly assessed, while malicious or malfunctioning entities are denied access to any resource.

Pussewalage and Oleshchuk, (2018) proposed a delegable attribute-based access control system based on blockchain for managing authorization operations and reducing key management overhead through attribute revocation. They devised a maximum permitted length chain of

delegations, consisting of the delegate and his subsequent delegations, in order to give flexible relegatable access with lower revocation computational overhead.

2.3 Survey on e-IoT data management

Based on Objectives, Models, Architecture, and Mechanisms, Ouaddah et al. [1] gave a thorough analysis of the current access control methods in the Internet of Things (OM-AM). The study also included a taxonomy that was based on an exhaustive review by the authors. In relation to the IoT environment, the article examined the benefits and drawbacks of access control models and protocols. Additionally, they provided a blockchain-based decentralised access control system for the Internet of Things called FairAccess [10]. To protect users' privacy, the framework employed the pseudonymous technique. To grant, get, delegate, and revoke access based on access tokens, they developed a new form of transaction. The Attribute-Based Access Control concept is the foundation for this. The FairAccess authorization system is based on authorization tokens, which grant access rights to a certain resource to the requester or receiver. This resource is defined by its address and a smart contract that expresses its access control regulations. However, this framework might result in a delay as a result of owner communication, solely using tokenization for permission, and ending a token or asking for new access from the owner.

For Internet of Things (IoT) devices, Novo [8] proposes scalable decentralised access management based on blockchain technology. In order to reduce network overheads, the architecture excluded IoT devices from the blockchain network. Regarding IoT access control, the system has a number of benefits, including mobility, accessibility, parallelism, lightweight architecture, scalability, and transparency. This framework provides managers that make it possible to register and verify IoT devices. The distribution of query rights via management hubs increases the scalability of this method, but if the manager is unscrupulous, it could pose security risks.

Liu et al[13] .'s developed an authentication and access control mechanism for an IoT infrastructure that uses an RBAC authorization approach based on the user's role and an ECC (Elliptic Curve Cryptosystem)-based security key. Due to the high user count and RBAC's inability to pre-assign permission, the suggested approach is not scaleable in an IoT setting. The security assessment of the proposed protocol is weak, and frequent message exchanges are required.

By combining secure session key formation, preserving user anonymity, and mutual authentication, Ndibanje et al. [14] increased the efficiency at a low communication cost. This method falls short in protecting the authenticity of sent messages, though.

By concentrating on user and system preferences to grant or deny access, Touati et al. [16] suggested an activity control method (a broader version of context-aware access control). For dynamic access policy adaption, they used a finite state machine and ciphertext-policy attribute-based encryption (CP-ABE).

The key/attribute revocation issue was also the focus of Touati et al. [17]'s batch-based CP-ABE solution. The suggested approach decreases overall complexity and overheads and does not call for additional nodes for processing. For access service management, the Cap-BAC approach is

based on the least privileged concept. To grant access to the necessary resources, the service provider requires an authorization certificate from the user.

3. Proposed approach:

The developed permissioned blockchain-based secured cloud store data introduces for choosing the optimal key for the encryption of medical text data to make highly secured cloud records. GOA [26] is used in the developed model owing to its improved efficiency in determining the optimal solution and does not undergo the local optimum problem. The developed Approach is enclosed with the deviation-based concept for updating the final position of candidates to obtain the optimal solution. First, the GOA deviation is estimated with "the solution in GOA without any computations in it that is represented by dv_1". Similarly, the DHOA deviation is computed and it is expressed dv_2 without any computation in the DHOA. The final position upgrade is taken place as shown in Eq. (2).

$$Pos = Pos + dv_1 + dv_2 \tag{2}$$

The pseudo-code of the proposed GHO is given in Algorithm 1. Here, the successor position of the hunter is depicted as Xt^{sp}. Then, determine the fitness value for every search agent and update both the leader and successor position until the stopping condition to be satisfied. Finally, the best solution is attained.

Algorithm 1: Proposed HGHO
Generate the initial population and its parameters
Calculate the fitness function of every solutions
While (stopping condition)
  For each
    Position update based on the GOA
      Determine the deviation dv_1 of GOA
    Update the position of solution using DHOA
      Upgrade the position when $(hi < 1)$
      Upgrade the position when $(hi \geq 1)$
      Compute the deviation dv_2 of DHOA
    End
    Update the final solution
  End for
Update the parameters
End while
Obtain a best optimal solution

Steps and algorithm definitions for permissioned blockchain-based EHR security

Permissioned Blockchain Steps

The Cloud data sharing scheme is involved on the permissioned blockchain enclosed with different steps and six different algorithms as given below.

System Initialization:

$\text{Setup}(\lambda) \rightarrow (Pu, Sk)$: Here, the setup algorithm is processed with the help of system manager. The input is obtained as security parameter λ and the output is given as the master secret key Sk and public parameters Pu.

Key Generation:

$\text{KeyGen}(Sk, Pu, Su) \rightarrow TK$: Here, the secret key generation algorithm is involved and controlled by the system manager. The input is acquired as the attribute set Su of a user, public parameters Pu and master secret key Sk. Similarly, the output is regarded as the secret key TK.

Data Storage:

$Enc(Pu, S, U, N) \rightarrow (J, D)$ Here, the encryption algorithm is used, which the admin handles. The EHRs N, keywords set U of shared cloud records, access control structure S of client Pt and public parameters Pu are used as the input for the algorithm. The output is accomplished to be a ciphertext D and keywords index J.

Data Query:

$\text{Trapdoor}(Pu, U', TK) \rightarrow S_{U'}$ The user is employed for handling the trapdoor generation algorithm, where the input is acquired as the secret key TK, search keywords set U' and public parameters Pu, and the algorithm's output is attained as search trapdoor $S_{U'}$.

$\text{Search}(J, S_{U'}) \rightarrow D$: Here, the search algorithm is processed with the support of participants, who are presented in the permissioned blockchain. Here, the input is acquired as the search trapdoor $S_{U'}$ and keywords index J and the output is received as the ciphertext D.

Data Decryption:

$\text{Decrypt}(Pu, Sk, D) \rightarrow N$: The user is accessed with the decryption algorithm with the input as ciphertext D, secret key Sk and public parameters Pu. Finally, the decryption algorithm provides the message N as the output.

Steps and algorithm definitions for permissioned blockchain-based E-IOT security

I. Permissioned Blockchain Steps

The E-IOT sharing scheme is involved on the permissioned blockchain enclosed with different steps and six different algorithms as given below.

System Initialization:

$\text{Setup}(\lambda) \rightarrow (Pu, Sk)$: Here, the setup algorithm is processed with the help of system manager. The input is obtained as a security parameter λ and the output is given as the master secret key Sk and public parameters Pu.

Key Generation:

$\text{KeyGen}(Sk, Pu, Su) \rightarrow TK$: Here, the secret key generation algorithm is involved and controlled by the system manager. The input is acquired as the attribute set Su of a user, public parameters, Pu and master secret key Sk. Similarly, the output is regarded as the secret key TK.

Data Storage:

$Enc(Pu, S, U, N) \rightarrow (J, D)$ Here, the encryption algorithm is used, which the admin handles. The E-IOTs N, keywords set U of shared E-IOTs, access control structure S of client Pt and public parameters Pu are used as the input for the algorithm. The output is accomplished to be a ciphertext D and keywords index J.

Data Query:

$\text{Trapdoor}(Pu, U', TK) \rightarrow S_{U'}$ The user is employed for handling the trapdoor generation algorithm, where the input is acquired as the secret key TK, search keywords set U' and public parameters Pu, and the algorithm's output is attained as search trapdoor $S_{U'}$.

$\text{Search}(J, S_{U'}) \rightarrow D$: Here, the search algorithm is processed with the support of participants, who are presented in the permissioned blockchain. Here, the input is acquired as the search trapdoor $S_{U'}$ and keywords index J and the output is received as the ciphertext D.

Data Decryption:

$\text{Decrypt}(Pu, Sk, D) \rightarrow N$: The user is accessed with the decryption algorithm with the input as ciphertext D, secret key Sk and public parameters Pu. Finally, the decryption algorithm provides the message N as the output.

II. Process Carried out for Retrieval of E-IOT using Permissioned Blockchain

The developed method is enclosed with three stages: "system setup, data generation and storage, and data search and access".

Stage 1-System setup:

- $\text{Setup}(\lambda)$: The input is given as the security parameter λ and considered the two different multiplicative cyclic groups such as H_1 and H_2 along with the generator q and the two generators of H_1 be denoted as h_1 and h_2. Assume $f : H_1 \times H_1 \rightarrow H_2$ to be an admissible bilinear map. The system has chosen the variables $\alpha, \beta \in A_q^*$ and has computed $h_2^{\alpha}, h_2^{\beta}, h_2^{\frac{\beta}{\alpha}}$. Then, the four different has functions are chosen as $I_1 : \{0,1\}^* \rightarrow A_q^*$, $I_2 : H_1 \rightarrow A_q^*$, $I_3 : A_q^* \rightarrow H_2$ and $I_4 : H_2 \rightarrow \{0,1\}^*$. The system parameters are described as $Pu = \left(q, f, h_1, h_2, h_2^{\alpha}, h_2^{\beta}, h_2^{\frac{\beta}{\alpha}}, H_1, H_2, H_3, H_4 \right)$ is used and the master secret key Sk is generated with secret as in Eq. (13).

$$Sk = (\alpha, \beta) \tag{13}$$

- $\text{KeyGen}(\lambda)$: Here, the system manager takes the responsibility of choosing $s \in A_q^*$ and the computation of $S = h_1^{\frac{\alpha - s}{\beta}}$, $S' = h_1^{\frac{\alpha}{\beta}} h_2^{\frac{\alpha}{\beta} s}$ are done. The selection of $u_b \in A_q^*$ is done for all attributes $b \in T$ and further, determine $Y_b = h_1^{u_b}$ and $Z_b = h_1^{s} h_1^{u_b I_1(b)}$. Finally, the attribute authority passes the secret key TK towards the users as in Eq. (14).

$$TK = \left(S, S', \{Y_b, Z_b\} \forall b \in T\right) \tag{14}$$

Stage 2: "Data generation and storage"

The client Pt visits the hospital for treating their illness, where the hospital server has randomly chosen $i \in A_q^*$ and has computed $\mu = I_3(i)$ and the server has reserved μ. Here, the term i is used as the secret key between the admin E and client at the time of consultation. The admin E s responsible for handling the encryption algorithm as given below.

- $Enc(n, v)$: In the first step, the admin E has produced the health records $N \in \{0,1\}^*$ related to the client Pt and also has utilized the assess structure (Γ, i) for computing $D_0 = h_1^{\frac{\beta i}{\alpha}}$ and $D_1 = N \cdot I_4\left(f(h_1, h_1)^i\right)$. In the second step, the admin is involved in extracting the keywords sets $b, c \in A_q^*$ for designing the polynomial equations according to the keyword $U = \{u_1, u_2, \ldots, u_n\}$ s given in Eq. (15).

$$\begin{aligned} h(y) &= b(y - I_1(u_1))(y - I_1(u_2)) \ldots (y - I_1(u_n)) + c \\ &= b_n y^n + b_{n-1} y^{n-1} + \ldots + b_1 y + b_0 \end{aligned} \tag{15}$$

Here, for every b_k, $k \in \{1,2,\ldots,n\}$ is used for computing $M_k = h_2^{\alpha b_k}$, $G_0 = h_2^i h_2^c$ and $G_1 = h_2^{\beta i}$. The output of the encryption algorithm is shown in Eq. (16) and Eq. (17).

$$D_N = (\Gamma, D_0, D_1) \tag{16}$$

$$J_u = \left(M_k, G_0, G_1, (B_w, C_w)_{w \in \Gamma}\right) \tag{17}$$

The admin E ha uploaded the ciphertext D_N and J_u into the database server of the E-IOT system present in the hospital. After uploading the data, the cloud server needs to be verifying the authentication of a admin. The admin E has arbitrarily selected $s_1, s_2 \in A_q^*$ for every attribute $b \in T$ and has selected $u_b^{'} \in A_q^*$ and has computed $\eta_1 = h_2^{s_1, s_2} h_2^{u_b^{'} I_1(b)}$ and $\eta_2 = h_2^{s_2 u_b'} h'$. Then, the admin transmits (η_1, η_2, i') towards the E-IOT server that is used for $i^* = I_2\left(\frac{\eta_1}{I_1(b)}\right) \oplus i'$ and also has determined $I_3(i^*)$ to be true or not. Then, the correctness is given in Eq. (18).

$$I_3(i^*) = I_3\left(I_2\left(\frac{\eta_1}{I_1(b)}\right) \oplus i'\right)$$
$$= I_3\left(I_2\left(\frac{h_2^{s_1,s_2} h_2^{u_b' I_1(b)}}{h_2^{u_b' I_1(b)}}\right) \oplus i'\right)$$
$$= I_3\left(I_2\left(h_2^{s_1,s_2}\right) \oplus i'\right)$$
$$= I_3(i) = \mu \quad (18)$$

The manager present in the E-IOT system is involved for extracting the block JE_c, which is the identification of the hospital and the client identity is indicated by JE_{Pt} and the secure keyword is expressed by J_u. The server in the EH system is used to broadcast the new transactions towards the blockchain denoted by $UY_{J_u} = (JE_c, JE_{Pt}, J_u)$.

Stage 3: "Data search and access"

- Trapdoor : The trapdoor $S_{U'}$ belongs to the keyword set is indicated as in Eq. (19).

$$S_{U'} = \left(L_0, L_1, F_j, (Y_b', Z_b') \middle| b \in T\right) \quad (19)$$

- Search : The searcher is performed with the attributes on the permissioned blockchain belongs to trapdoor and has computed the secret value of the leaf node as in Eq. (20).

$$F_w = f(h_1, h_2)^{ss_3 i_w(0)} \quad (20)$$

- Decrypt The data user has obtained the ciphertext $\mathrm{D} = (\mathrm{U}, \mathrm{D}_0, \mathrm{D}_1)$ through the hospital server, and the ciphertext's decryptions are performed with the ciphertext.

$$F_w' = \frac{f(Z_b, B_W)}{f(Y_b, C_W)} = f(h_1, h_2)^{si} \quad (21)$$

$$N = \frac{D_1}{I_4\left(\frac{f(S', D_0)}{F_w'}\right)} \quad (22)$$

The above two equations shows the decryption of medical records for regaining the data related to the client.

In contrast to previous studies, this one is meant to offer a lightweight, scalable, and secure solution. We propose a protocol for capability-based Internet of Things (IoT) access control architecture design based on the use of a blockchain-based decentralised identity, and we analyse the system interactions that arise from this design. All aspects of the suggested method, including its practicability, safety, and efficiency, are assessed [19].

Our method ensures the confidentiality and security of our customers' data. In the proposed method, the client comes first so that the security policy can retrieve the client's medical records. The policy

trades can be obtained using the publicly accessible blockchain. As a result of the public blockchain only storing a transient client ID, it is not possible to record the client's access history to data. In addition, our system reviews clients based on who is responsible for data analysis. This means they have full access to it, albeit being housed on a server.

4. Result Analysis

The permissioned blockchain-based secured cloud storage model is developed in Python and further analysis was conducted to verify the transactional latency, time taken, and effectiveness of the system. The evaluation was made between the developed and state-of-the-art methods to show improvement in the blockchain-based cloud data transmission model. The population size of 10 and maximum count of iterations as 100 was utilized in the developed model [29]. The proposed CCP-ABE was distinguished with other existing algorithms like " Whale Optimization Algorithm (WOA) [28], Coronavirus Herd Immunity Optimization (CHIO) [29], GOA [26] and DHOA [27] and machine learning algorithms like BIoTHR [3] and EACMS [4]".

Convergence analysis

The convergence rate of the proposed model is evaluated with different existing algorithms at the increasing iterations as depicted in Fig. 3. The proposed CCP-ABE-based EHR transmission model secures less ciphertext size, computation cost and encryption cost by tuning the encrypted keys for encryption and decryption, which is observed by comparing with the conventional optimization techniques. The betterment of the proposed model is observed to be 14.2%, 13.3%, 12.02% and 12.4% enhanced than WOA-CCP-ABE, CHIO-CCP-ABE, GOA-CCP-ABE and DHOA-CCP-ABE, respectively at the 40^{th} iterations. Hence, it is verified that the suggested HGHO-CCP-ABE-based model has secured the cloud store data transmission with superior performance.

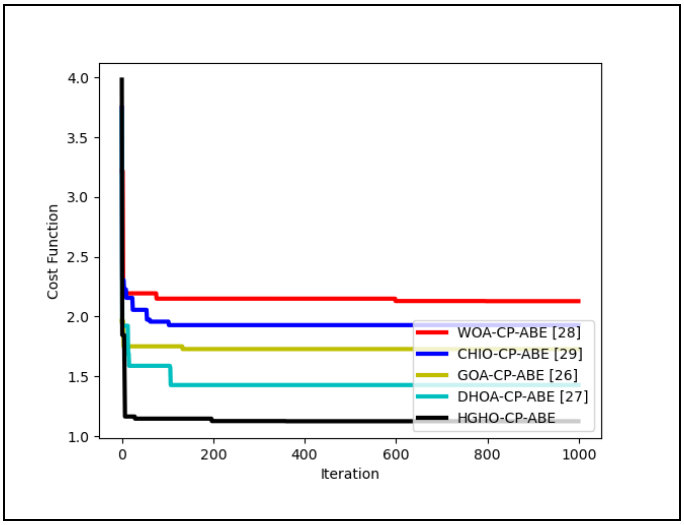

Figure 01: Convergence analysis on proposed permissioned blockchain-based secured Cloud storage data model

Decryption time analysis

The proposed model based on heuristic-based CCP-ABE approach is analyzed to show efficient decryption performance with its time efficiency as in Fig. 2. Here, the analyses are done between both the algorithms and other baseline approaches. The developed method reveals minimum decryption time for retrieving the medical records, where the proposed model is 11.67% and 13.6% superior to BIoTHR and EACMS, respectively.

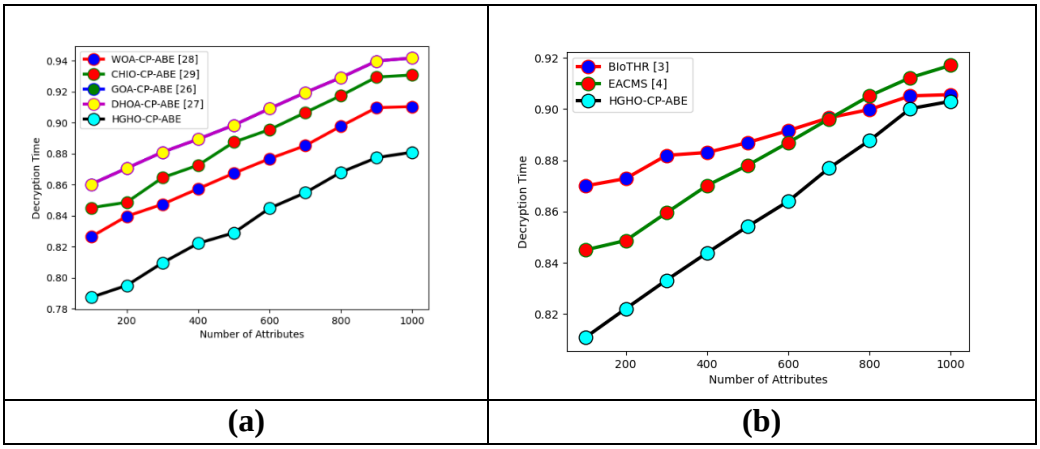

Figure 02: Decryption time analysis on proposed permissioned blockchain-based secured cloud storage model with "(a) different heuristic algorithms and (b) existing models"

Encryption time analysis

The evaluation was made between the proposed and conventional algorithms to check the encryption time of the cloud records as in Fig. 3. The proposed CCP-ABE shows 12.6% and 13.2% improved than BIoTHR and EACMS, which demonstrates the less encryption time is required for the proposed model.

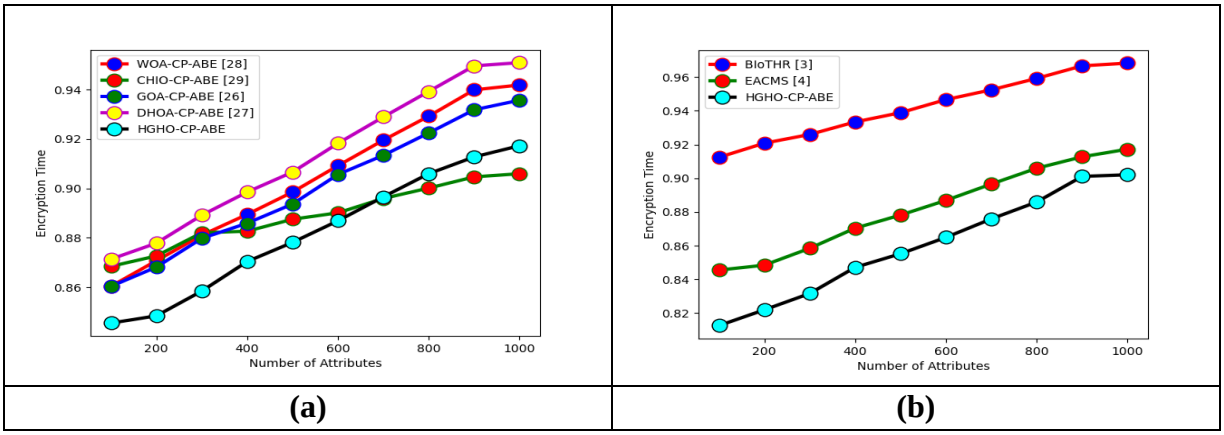

Figure 03: Encryption time analysis on proposed permissioned blockchain-based secured cloud storage model with "(a) different heuristic algorithms and (b) existing models"

5. Conclusion

The use of blockchain in e-IoT systems plays a critical role in present IoT industry, according to the study and the way the blockchain is embraced by different sectors. This may contribute to automated processes for data collection and reviewing, correcting and aggregating data from multiple sources that are permanent, tamper-resistant and provide safe data that have a lower risk of cybercrime. It supports distributed data with redundancy and device fault tolerance. In this research, the IoT industry is addressing current issues. In order to achieve privacy and protection for client information within the E-IOT program, we suggest a system architecture and access control policy algorithm based on blockchain based cryptographic method for participants & accessing the data securely. Implementation of a blockchain network-based E-IOT sharing framework. The research suggested removes the central authority and the system's inherent failure. System protection is accomplished by secure technology, as the ledger cannot be changed by any person as proposed system uses the keys for sharing and accessing the data. The caliper performance evaluations of the proposed system are completed with the configuration of block size, block build time, endorsement policies, and the proposed optimization of assessment methods, such as latency, capacity, and network safety to achieve better results, for various scenarios. This demonstrates the potential and value of blockchains in different fields and demonstrates the possibility to replace existing sanitation systems with next groundbreaking technologies.

References

[1] Manoj E Patil, Tejashri Patil, "Apriori Algorithm against Fp Growth Algorithm: A Comparative Study of Data Mining Algorithms", International Conference in Innovation and Research in Technology and Engineering, (ICIRTE 2022) held on 8th and 9th of April 2022by VPPCOE & VA Mumbai.

[2] NaumanurahemanShakh, Dr. Manoj E Patil, " Sketch to face Conversion using GAN for Forensic Research", IJIRSET, e-ISSN: 2319-8753, Volume 10, Issue 2, February 2021 https://www.ijirset.com/upload/2021/february/69_Sketch_NC.pdf

[3] Narendra, M. Research Reveals the Most Vulnerable IoT Devices. Available online: https://gdpr.report/news/2019/06/12/research-reveals-themost-vulnerable-iot-devices/ (accessed on 11 January 2021).

[4] NaumanurahemanShakh, Dr. Manoj E Patil, " Insect Classification using Custom CNN VS Transfer Learning", IJIRSET, e-ISSN: 2319-8753, Volume 9 Issue 11, November 2020

[5] Dorri, A.; Kanhere, S.S.; Jurdak, R. Blockchain in Internet of Things: Challenges and Solutions. Yingyong Kexue Xuebao/J. Appl. Sci. 2020, 38, 22–33.

[6] Vojković, G.; Milenković, M.; Katulić, T. IoT and Smart Home Data Breach Risks from the Perspective of Data Protection and Information Security Law. Bus. Syst. Res. Int. J. Soc. Adv. Innov. Res. Econ. 2020, 11, 167–185.

[7] Aldowah, H.; Rehman, S.U.; Umar, I. Security in Internet of Things: Issues, Challenges and Solutions. In International Conference of Reliable Information and Communication Technology; Springer: Cham, Switzerland, 2018; pp. 396–405.

[8] Ourad, A.Z.; Belgacem, B.; Salah, K. Using blockchain for IOT access control and authentication management. In International Conference on Internet of Things 2018 June; Springer: Cham, Switzerland, 2018; pp. 150–164.
[9] Ravidas, S.; Lekidis, A.; Paci, F.; Zannone, N. Access control in Internet-of-Things: A survey. J. Netw. Comput. Appl. 2019, 144, 79–101.
[10] Almarhabi, K.; Jambi, K.; Eassa, F.; Batarfi, O. An evaluation of the proposed framework for access control in the cloud and BYOD environment. Int. J. Adv. Comput. Sci. Appl. 2018, 9, 213–221.
[11] Dorri, A., Kanhere, S.S. and Jurdak, R., 2017, April. Towards an Optimized BlockChain for IoT. In Proceedings of the Second International Conference on Internet-of-Things Design and Implementation (pp. 173- 178). ACM.
[12] Stanciu, A., 2017, May. Blockchain Based Distributed Control System for Edge Computing. In Control Systems and Computer Science (CSCS), 2017 21st International Conference on (pp. 667-671). IEEE.
[13] Conoscenti, M., Vetro, A. and De Martin, J.C., 2017, May. Peer to Peer ` for Privacy and Decentralization in the Internet of Things. In Proceedings of the 39th International Conference on Software Engineering Companion (pp. 288-290). IEEE Press.
[14] Boudguiga, A., Bouzerna, N., Granboulan, L., Olivereau, A., Quesnel, F., Roger, A. and Sirdey, R., 2017, April. Towards Better Availability and Accountability for IoT Updates by means of a Blockchain. In IEEE Security & Privacy on the Blockchain (IEEE S&B 2017) an IEEE EuroS&P 2017 and Eurocrypt 2017 affiliated workshop.
[15] Zhao, Z., Zhou, H., Li, C., Tang, J., Zeng, Q.: Deepemlan: deep embedding learning for attributed networks. Inf. Sci. 543, 382–397 (2021)
[16] Pooranian Z, Shojafar M, Garg S, Taheri R, Tafazolli R (2021) LEVER: secure Deduplicated cloud storage with EncryptedTwo-party interactions in cyber-physical systems. IEEE Transact Industrial Informatics. https://doi.org/10.1109/TII.2020.3021013
[17] Narendra, M. Research Reveals the Most Vulnerable IoT Devices. Available online: https://gdpr.report/news/2019/06/12 /research-reveals-themost-vulnerable-iot-devices/ (accessed on 11 January 2021).
[18] NTT Innovation Institute. Mandatory Access Control over IoT Communications. Available online: https://labevent.ecl.ntt.co.jp/ forum2017/elements/pdf_eng/03/C-18_e.pdf (accessed on 16 November 2020).
[19] Dorri, A.; Kanhere, S.S.; Jurdak, R. Blockchain in Internet of Things: Challenges and Solutions. Yingyong Kexue Xuebao/J. Appl. Sci. 2020, 38, 22–33. [CrossRef]
[20] Saad M, et al. (2020) Exploring the Attack Surface of Blockchain: A Comprehensive Survey, IEEE Communications Surveys & Tutorials, 22(3):1977–2008
[21] Chen, C.H., Lu, C.Y., Lin, C.B.: An intelligence approach for group stock portfolio optimization with a trading mechanism. Knowl. Inf. Syst. **62**(1), 287–316 (2020)
[22] Liu Y, Yu F, Li X, Ji H, Leung VM (2020) Blockchain and machine learning for Communications and networking systems. IEEE Commun Survey Tutorials 22(2):1392–1431. https://doi.org/10.1109/COMST.2020.2975911

[23] Zhao, Z., Zhang, X., Zhou, H., Li, C., Gong, M., Wang, Y.: Hetnerec: Heterogeneous network embedding based recommendation. Knowl. Based Syst. 204, 106218 (2020)

[24] Fu X, Yu FR, Wang J, Qi Q, Liao J (2019) Resource Allocation for Blockchain-Enabled Distributed Network Function Virtualization (NFV) with Mobile Edge Cloud (MEC), IEEE INFOCOM 2019. In: IEEE conference on computer Communications workshops (INFOCOM WKSHPS), Paris, France, pp 1–6

[25] Belotti M, Bozic N, Pujolle G et al (2019) A Vademecum on Blockchain Technologies: When, Which and How. IEEE Commun Surveys Tutorials 21(4):3796–3838. https://doi.org/10.1109/COMST.2019.2928178