Utilizing Block chain in the Internet of Things for an Effective Security Sharing Scheme

Sathish C[1]*, and Yesubai Rubavathi C[2]
[1]Part time research scholar, Assistant Professor, Department of Computer Science and Engineering, Government College of Engineering, Bodinayakanur- 625582, Tamil Nadu, India
[e-mail: csathish9710132@gmail.com]
[2]Professor, Department of Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli- 627003, Tamil Nadu, India
[e-mail: ryesubai123@gmail.com]
*Corresponding author: Mr. Sathish C

Received May 23, 2022; accepted May 6, 2023; published June 30, 2023

Abstract

Organizations and other institutions have recently started using cloud service providers to store and share information in light of the Internet of Things (IoT). The major issues with this storage are preventing unauthorized access and data theft from outside parties. The Block chain based Security Sharing scheme with Data Access Control (BSSDAC) was implemented to improve access control and secure data transaction operations. The goal of this research is to strengthen Data Access Control (DAC) and security in IoT applications. To improve the security of personal data, cypher text-Policy Attribute-Based Encryption (CP-ABE) can be developed. The Aquila Optimization Algorithm (AOA) generates keys in the CP-ABE. DAC based on a block chain can be created to maintain the owner's security. The block chain based CP-ABE was developed to maintain secures data storage to sharing. With block chain technology, the data owner is enhancing data security and access management. Finally, a block chain-based solution can be used to secure data and restrict who has access to it. Performance of the suggested method is evaluated after it has been implemented in MATLAB. To compare the proposed method with current practices, Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC) are both used.

Keywords: cypher text policy attribute-based encryption, block chain, IoT application, DAC, security enhancement and AOA.

1. Introduction

The expansion in the number of gadgets is being driven by the development of the internet. Gadgets are networked as a result of the growth in system management and communication advancements like WiFi, ZigBee and many others. The growth of IoT businesses can be connected to the Association of Gadgets. IoT is one of the most challenging technological advancements in the long term because to the abundance of amazing real-world devices connected to the network that have programming, sensors and applications installed to gather, exchange and give information. IoT encompasses anything pertaining to the Internet in general. The IoT architecture includes a wide range of devices, many of which are available with low power, constrained efficiency, and a restricted handling range. IoT devices can be connected to the Internet using gateways, which also enable them to talk to one another [1]. IoT makes the biosphere more useful, intelligent, and consequently effective. IoT is a clever concept that links the offline world to the online one. A network of Internet-connected items that interact and exchange resources makes up the IoT structure. IoT devices can establish communication without human assistance [2]. One of the main focuses of IoT is information, data and asset sharing across devices. IoT networks are being used more frequently across different industries thanks to the Association of Gadgets. The automobile sector, home automation, medical services, store network boards, vendor partnerships, related armatures, and other industries, as well as security frameworks, are just a few examples of IoT network applications. IoT devices are relevant globally and are becoming more widely available as a result of the aforementioned applications [3, 5].

For businesses, the association of electronics presents several challenges. Unauthorised access, malicious attacks, a lack of connection due to centralization, and other issues are some of the challenges [5]. IoT devices hold sensitive data, making production management for businesses particularly important. Because IoT devices store a lot of data [6, 7], integrated capacity structures, such as the cloud and fog, can be used to store that data. A large amount of information may be handled by the cloud in short bursts. Additionally, it achieves speed, precision, and productivity in terms of managing information. Businesses benefit from efficiency and management benefits, but stagnation, security, and security issues are also brought about by cloud and fog [8, 9].

Unauthorized access to information is a serious problem in any circumstance. The following is how the key contribution is presented:

- In this study, BSSDAC is designed to support secure information transaction operation and access control. The improvement of DAC and security in IoT applications is the primary objective of this research.
- CP-ABE could be created to improve the security of personal data. Keys are produced by the CP-ABE using AOA. The DAC was created to safeguard the owner's security. The block chain-based CP-ABE is designed to maintain secure data storage and exchange.
- Block chain technology is being used by the data owner to improve data security and access control.
- Finally, a block chain-based solution can be used to secure data and manage who has access to it. Performances of the suggested method are assessed after it has been implemented in MATLAB. The RSA and ECC technologies in use right now are contrasted with the suggested approach.

The contribution to the paper can be summed up as follows, with part 2 offering a thorough analysis of pertinent literature. Following a full discussion of the suggested strategy

in Section 3, Section 4 examines the outcomes of the suggested method. Conclusions are presented in Section 5.

2. Related works

An examination of earlier research on blocks chain-based DAC and security is provided in this section.

Using micro-access management, a block chain-based data security sharing stage has been presented by Hong Xu et al. [10]. With a focus on the problem of security leakage during data participation in the IoT, the block chain-based secure data sharing stage with fine-grained access control (BSDS-FA) was created. The first section of this study creates yet another progressive quality-based encryption computation using a stagnant approval community and a progressive characteristic design. The calculation allows for flexible and stylish entry control by dispersing various client credits among several authorized habitats. It then collaborated with the development of fabric block chain at that time to address the issue of excessively high decryption costs aimed at IoT users. The block chain's intelligent deal allows for extremely complex incomplete decoding computations to reduce consumer upward disconnection. Use of verified functions that block chains are capable of recognizing can be used to compensate for the security requirements of information range openness and direct administration.

Block chain-based add-on control with security insurance in the cloud has been described by Caxia Yang et al. [11]. In this case, Auth Privacy Chain was created as an enrollment control method for block chains with a security guarantee. Look at the access control authentication of the data travelling into the cloud, which may also be encrypted and added to the block chain, using the center's registration address as a character from there. Future access control, approval, and denial cycles should be planned in AuthPrivacyChain. The main enterprise operation system (EOS) will see when AuthPrivacyChain is eventually put into use that it not only stops administrators and programmers from gaining assets unlawfully, but also defends guarded security.

A block chain-related combination manage plot that allows for safe communication between robots and robots has been created for the IoT context by Basudeb Bera et al. [12]. Square-based, structured interactions allow for the gathering of secure information. By using distributed cloud server architecture, cloud servers connected to the Ripple Protocol Consensus Algorithm (RPCA) have long been adding squares to the block chain. The exchanges included in a square that is added to a block chain cannot be edited, amended, or erased. In order to make sure that the suggested programme would withstand the numerous anticipated attacks that are most likely in the IoD environment, this section offers a wide range of security inquiries, including appropriate security, normal security, and proper security testing based on breeding under the irregular prophecy model. Also, the sooner the research between the two projects occurs, the more efficient our program's credits are and the less expensive communication and calculation costs when a recommended plot clashes with other explicitly associated projects.

A block chain-based access control method has been proposed by Thein Than Thwin et al. [13] to safeguard the privacy of personal health registration systems. Block chain research was used to add the alternative barrier to the suggested approach. Different cryptographic techniques can be used in conjunction with intermediate encryption to protect security. The recommended design includes components for advanced customizable access control, permission revocation, auditing, and alternative resistance. Inquiry proof that the suggested

paradigm is secure for protection and change resistance is a conclusive security. The display option demonstrates how the projected design might be a written representation of the presentation that is often given by using the current algorithm. So, when used with the PHR framework, the model makes more sense.

Basudeb Bera et al. [14] presented the DBACP-IoTSG, an additional control on the IoT-powered intelligent framework based on block chains. Information from their individual smart metres (SMs) is securely communicated to specialized cooperatives via the anticipated DBACP-IoTSG. Peer-to-peer (P2P) network participation may be established through specialised cooperatives, in which friend centres are in charge of protecting squares from the data they gather from their routine SMS and adding them to the block chain after democratically based approval of the squares Contract calculation. Throughout our work at Block Chain, the data gathered from SMS purchasers is regarded as private and confidential. DBACP-IoTSG has passed arbitrary prophesy security testing as well as routine security testing based on non-mathematical security analysis and programming. Here, the study findings of numerous cryptographic natives are completed using the rational arithmetic cryptographic library (MIRACL) and the widely utilized multi production number.

3. Proposed System Model

The assurance of security for IoT devices and distributed system upgrades are important elements. Regular information sharing arrangements may be built on a foundation of general sequence sharing. The clients can distribute and keep their data on a cloud server in systems that allow for widespread information sharing, but the client may quickly lose ownership of any personal data obtained from the transmission of information. Information security, data access, and the underlying problem are additional concerns. Therefore, it can be claimed that data encryption and access control are crucial precondition for safeguarding data and managing the owner's gateway. In addition to making adequate preparations for security-related concerns, this improves the security of the framework for access control and information security. In order to improve system security in an IoT environment, this study provides DAC and encryption methods. **Fig. 1** presents the suggested design.

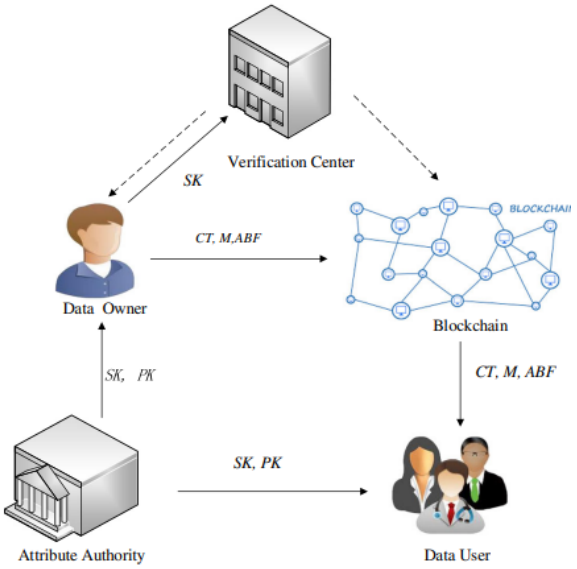

Fig. 1. The Architecture of proposed System

The section below provides a detailed overview of the architecture.

3.1. An overview of the Block chain

Block chains are limited to adding scattered digital records relevant to cryptography. An intermediary is not required for any requests, tasks, or money transfers thanks to the block chain's framework for handling trustworthy transactions. Furthermore taken into consideration while storing in the block chain is the digital signature is used for public validation. With all system users present, the ledger can be generated and maintained. The block chain offers a variety of benefits, some of which are listed below [15], making it a viable technique for decentralized ways in networking.

- It's possible to decentralize a block chain. It is used to establish confidence in the block chain for third-party access by taking into account consensus techniques like proof of work (PoW) and proof of stack (PoS).
- Distributing a block chain is possible. It is more peaceful than conventional centralized systems since it allows more people to access to the network without registering.
- Block chains are unchangeable. Block chain data is displayed as a complete shared copy. Since it is a part of the chain, interference is impossible. Block chain is regarded as the foundational technology in a variety of requests, including block chain asset management, business, IoTs and crypto currencies, due to the aforementioned remarkable characteristics. Block chain has the potential to reshape economies and transform industry.

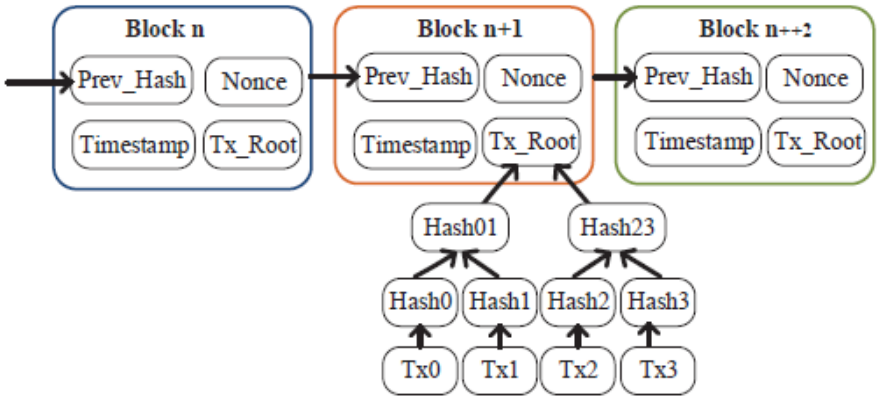

Fig. 2. Technology block diagram for block chains

In **Fig. 2**, you can see the block chain's general structure. With specific public-private key pairs, users are connected to the block chain and the system. This block has a block body and header. The block body is made up of various transactions that were both confirmed and authorized by the user using their public and private keys. The block header consists of the block's initial data, including the number of transactions, block size, timestamp and version number. The Merkle hash tree may be made, which solves the chain's storage issues, by utilizing a hash parameter of every transaction in this block as input. To connect the two blocks constantly, this block also includes the hash parameter from the one before it.

3.2. DAC based on a block chain

The creation of the DAC in the proposed approach considers the block chain to enable efficient DAC. Several operational criteria, such as those pertaining to the starting stage, the registration and application stage, the policy updating, the policy verification, and the tracing with key check, may apply to this suggested DAC. This anticipated data access restriction is shown in **Fig. 3**.

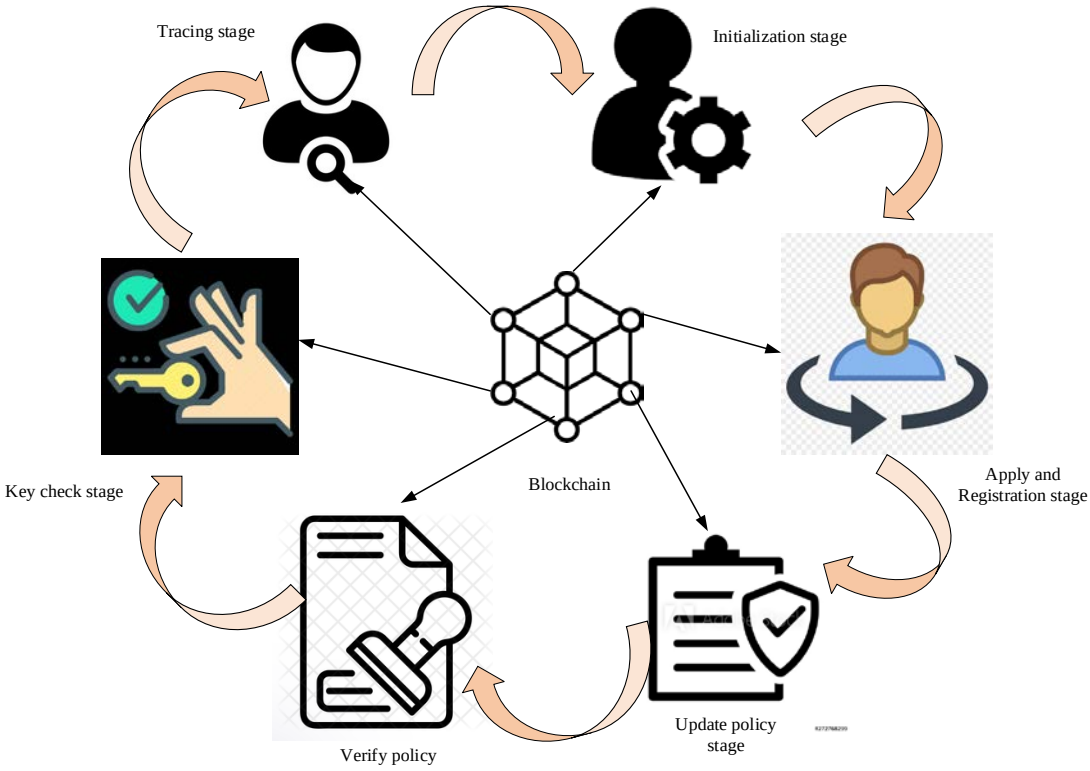

Fig. 3. DAC

Initialization phase:

The startup phase is generated in this phase with the knowledge of the owner, including general parameters, the master key and public variables. With important variables, the main phase of the proposed security technique is launched. Here is how the initialization phase is displayed as,

$$\text{Initialization} \rightarrow (\text{mk}, \text{pk}) \tag{1}$$

In this case, pk stands for the public key and mk for the master key. These keys, which are selected by the data owner, are crucial to this process's data protection. One of these two keys is managed by the owner of the data. Additionally, the block chain structure can be used to store the public key. The process of initialization is effective in enabling the transaction in the system [16].

Apply and register phase:

It can be used to record user registration requests in order to apply in addition to the register phase. In addition to the private key of the data owner, this register phase is regarded as the public key. The particular private key and public key are displayed as follows:

$$\text{KEYGEN}\ (\text{mk}, \text{pk}, \text{uid}, \text{w}) \rightarrow \big(\text{sk}(\text{data}), \text{sk}(\text{search})\big) \quad (2)$$

The general attribute set (w), the unique id, and the master key can all be considered as the algorithm input during this stage. The output of this phase is the search key sk(search) and sk(data). The block chain structure stores the private key. The data owner is effectively gathering private keys during this procedure.

Updating policy

Only the owner of the data is aware of the policy updating process. The policy conditions based on the encrypted data can be verified using this private key. The proposed encryption technique is used to achieve the encryption. Based on the policies and key, the policy is modified.

$$\text{policy updating} \rightarrow (\text{pk}, \text{ct}, \text{Policy}) \quad (3)$$

Here, a policy is defined as one that the data owner has created.

Verification policy

The data owner policy and data user policy can be compared in this phase to grant information access permission. The data user policy is compared to the requirement policy that only the data owner may grant access. The structure of the block chain can be used to examine the policy verification stage. It comes from,

$$\text{policy verification} \rightarrow (\text{pk}, \text{ct}, \text{user Policy}) \quad (4)$$

Tracing with key check

After comparison with the policy are requirements of the data owner. The key is given to the users once this policy has been reviewed and found to be valid. The key check validation is as follows:

$$\text{Key check} \rightarrow (\text{pk}, \text{msk}, \text{sk} - \text{uid}) \quad \text{i.e.}, 0 \text{ or } 1 \quad (5)$$

The values check the key. If the value is 1, it is the right key, and if it is 0, it is the wrong key. Tracing is the final stage of the proposed DAC. This input for the tract approach is regarded as the user's decryption key, master key, and private key. The trace technique's output of 1 indicates that it can successfully identify the user. If not, then the result is 0.

$$\text{Tracing} \rightarrow (\text{pk}, \text{msk}, \text{sk} - \text{uid}) \quad \text{i.e.}, 0 \text{ or } 1 \quad (6)$$

The policy and permission of the data owner are confirmed based on the DAC, and data user security is also improved during transactions. The proposed method strengthens the algorithm for data access and security. Data access begins, and after that, with the help of an encryption mechanism, the data is encrypted.

3.3. CP-ABE

The block chain technique is used to partition the data into blocks. The CP-ABE then makes use of the modified data. The four phases of the CPABR are typically presented as follows.

Initial setup: This step allows for the description of the global attribute set. This stage can be managed with the aid of a professional who takes into account a recognized security variable as well as the system's outputs, inputs and public variables in addition to system master keys.

Encryption phase: This stage can be used while taking into account the data sender, message, public variables, and access design as input. Only headphones with attribute sets that compensate for the access design's capacity for message encryption are used for the input that encrypts the message [17].

Key generation: This step is controlled by an authority that accepts the user's attribute set as input, along with their system master keys as output and the associated secret key as input.

Decryption phase: In addition to accepting input from the cypher text, secret key associated with the specified attribute set, public variable, and data receiver, this stage can also be operated by them. The message is optimally decrypted at this stage if it receive attribute set later compensates for the access structure of the cypher text.

The suggested encryption method is used to protect the user's inputted personal data. In this encryption, the elliptic curve E can be seen as the apex of the prime finite field Z_p with reference parameter b and order p. The point at zero or infinity element of E can also be considered, as well as the cyclic group G_E with order q and generator b. The following are the details of the mathematical model for the suggested technique:

Initial setup:

This method operates while taking the KGC into account and uses the implicit security variable as an input. The universal attribute set used in this method is written as follows:

$$u = \{a_1, a_2, .., a_n\} \tag{7}$$

Every attribute, $a_i \epsilon u$, this technique selects $\alpha_i \in z_q^*$ is a secret key and it a random number. Related with the ECC, each attribute of public key is presented as $pk_i = \alpha_i . b$. Additionally, this technique selects one master key $\alpha_i \in z_q^*$ which is generated randomly. KGC describes one random oracleh: $\{0,1\} \rightarrow z_q^*$. At last, the outputs are $\{u, pk_i, pk, h\}$ and secret key$[\alpha_i, \alpha]$. This secret key is selected with the assistance of the AOA.

Encryption phase

The use of sensors is being considered in this strategy. Resource constraints are taken into account in the final framework. In place of pricey bilinear pairing functions, scalar multiplication operations can be used to encrypt the information generated. Additionally, the symmetric key is used to encrypt the input data, and this key can also be safeguarded. This method is regarded as an encryption method for both public variables and access structures. This message is encrypted using the formulas below:

$$SK + k.PK = (k_x, k_y) \tag{8}$$

Here, $SK \neq 0$. The message M is the integrity and encryption keys. additionally, INT_M and C_M is formulated as $C_M = Enc(M, k_x)$ and $INT_M = HMAC(M, k_y)$. After that, this technique is computes$C_i = q_x(0).PK_I$, Here, $I - Attr\ (X)$ and $I \in \Omega$. Finally, the ciphertext produced by this method is provided as follows:

$$CT = (T, C_M, INT_M, C_i) \tag{9}$$

Key generation:

This method makes use of the KGC and considers the user's collection of system master keys and characteristics. In conjunction with asking the recipient of the data for the secret key for certain attribute sets and KGC certifying the accuracy of these characteristics. In addition, the KGC employs this technique to manage the essential elements associated to each characteristic of the data receiver in addition to managing a distinct individuality related to this attribute set. The following is a presentation of the mathematical function for this key generation:

$$d = \left(d_i = h(u_{id}).\alpha.\alpha_I^{-1}\right), \forall_I \epsilon \gamma \tag{10}$$

Whereas α_I can be thought of as the secret key generated based on an attribute, in this proposed technique, the best secret key generated is chosen using AOA. It is possible to think of $h(.)$as the random oracle. The user attribute set is managed by KGC in a list that is connected to the u_{id}. Finally, this method securely communicates $\{d, u_{id}\}$ to the user while also generating the secret key d which can be made up of d_i.

Decryption phase:

This method may be used in conjunction with a data receiver or with data that has been encrypted using a secret key. As input, the produced key and cypher text are used. This method uses a single recursive function called $\text{decryptkey}(CT, d, x)$, the input is treated as d, CT, x the. If $I = \text{Attr}(x)$, and x is thought of as the leaf node, then the decryption function parameter is provided as follows,

$$\text{decryptkey}(CT, d, x) = \begin{cases} \dfrac{d_I, C_I}{h(u_{id})} & \forall_I \epsilon \gamma \\ \text{Null} & \text{otherwise} \end{cases} \tag{11}$$

In this case, the parameter in the elliptic curve group or null should represent the output of the decryption phase $\text{decrypt key}\,(CT, d, x)$. The leaf node x is doing the following operation,

$$\frac{d_I, C_I}{h(u_{id})} = \frac{h(u_{id}).\alpha.\alpha_I^{-1}.q_x(0).PK_I}{h(u_{id})} \tag{12}$$

$$= \alpha.\alpha_I^{-1}.q_x(0).\alpha_I^{-1}.b \tag{13}$$

$$= q_x(0).\alpha.b \tag{14}$$

This decryption key parameter in the non-leaf node X can be computed continuously for each child node while taking Lagrange interpolation into account. Following that, the decryption key parameter can be stated as follows, if Cx denoted as the child nodes pair of X.

$$\text{decryptkey}(CT, d, x) = \sum_{y \epsilon Cx} \Delta_{I,J}(0).\text{decryptkey}(CT, d, y) \tag{15}$$

In this case, $\Delta_{I,J}(0)$ is known as the Lagrange coefficient for the equations $I = \text{Index}(Y), J = \{\text{Index}\,(Y), I \neq J \text{ and} y \epsilon Cx$. The message is decrypted based on the integrity and decryption key using the following formula:

$$M` = \text{Dec}\left(M, k_x`\right) \tag{16}$$

$$\text{INT}_M = \text{HMAC}\left(M`, k_y`\right) \tag{17}$$

Following that, it optimally and independently encrypts the message M for transmission. With the help of the AOA, the secret key is optimally created in this encryption method. The AOA is described in considerable detail in the section that follows.

3.4. Process of AOA Technique

By using the AOA technique, the best key is generated in the proposed process. The Aquila is the bird species with the greatest effectiveness and skill. Here are a few illustrations of the proposed technique's mathematical design.

Initialization:

The optimization recommendations in the population-related AOA approach begin with a candidate population solution. Key parameters are chosen at random to create the first population. Using the upper and lower limits of the primary generation issue, the initial population can be formed. The original population is used to calculate the best response, and its results are shown in the table below [18].

$$X = \begin{bmatrix} X_{1,1} & \cdots & X_{1,J} & X_{1,Dim-1} & X_{1,Dim} \\ X_{2,1} & \cdots & X_{2,J} & \cdots & X_{2,Dim} \\ \cdots & \cdots & X_{I,J} & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ X_{N-1,J} & \cdots & X_{N-1,J} & \cdots & X_{N-1,Dim} \\ X_{N,I} & \cdots & X_{N,J} & X_{N,Dim-1} & X_{N,Dim} \end{bmatrix} \tag{18}$$

Here, N is referred to as the total number of potential solutions, X_i as the i^{th} solution's decision values, and X as the set of currently available candidate solutions that were generated at random. The issue's dimension size Dim is represented mathematically as follows:

$$X_{I,J} = \text{RAND} \times \left(ub_J - lb_J\right) + lb_J, i = 1,2, \ldots, N, J = 1,2, \ldots, \text{Dim} \tag{19}$$

Here, the j^{th} upper bound is denoted by ub_J, the j^{th} lower bound is denoted by lb_J and the random variable is denoted by RAND.

AOA Mathematical design

While hunting, the Aquila characteristics are managed with the anticipated AOA method. To pursue the target, these traits are applied. Four more strategies are included in the optimization procedure for this strategy: moving inside a deviate search region, moving inside a meet search area and choosing search area with the biggest soar while taking vertical stoop into account. This Aquila is altered by steps of exploitation and exploration with various qualities connected to the circumstances.

Phase 1: Using a vertical stoop and a high soar, the Aquila locates the prey and selects the best hunting location in the first strategy. To find the search space, the Aquila also engages in a significant amount of soar exploration. This character can be described using the equation:

$$X_1(T+1) = X_{best}(T) \times \left(1 - \frac{T}{t}\right) + \left(X_m(T) - X_{Best}(T) * \text{RAND}\right) \tag{20}$$

Here, T and t can be defined as the current and maximum number of iterations, while $X_m(T)$ can be described as the mean parameter of the location with a specific solution correlated with each iteration. The best solution pinpoints the position of the prey as $X_{best}(T)$ and $X_1(T+1)$ as the first search method produced solution. Depending on the amount of iterations, the $\left(\frac{1-T}{t}\right)$ can be used to control the exploratory search. The following equation is used to calculate the mean parameter:

$$X_m(T) = \frac{1}{N}\sum_{I=1}^{N} X_I(T), \forall J = 1,2, \ldots, Dim \quad (21)$$

Here, N can be interpreted as the potential solutions number and the size of the problem's dimensions are denoted as Dim.

Phase 2: The position of the prey can be known in the different techniques after a big soar in which the Aquila rounds the last prey that emerges from the land after those attacks. The short glide attacks outline flight and the name of the technique. In addition, the AO barely makes it to the ultimate prey's designated place before the attack. These qualities are expressed as follows:

$$X_2(T+1) = X_{best}(T) \times LEVY(D) + (X_R(T) - (Y - Z) * RAND) \quad (22)$$

Here, the dimension space as D and the following iteration that is created with the second search technique can be described as $X_2(T+1)$. The random solution $X_R(T)$ is considered in the period of [1 N] in the ith iteration.

$$LEVY(D) = S \times \frac{U \times \sigma}{|V|^{\frac{1}{\beta}}} \quad (23)$$

Here, U and V can be thought of as random variables between 0 and 1 and σ can be calculated using the equation below.

$$\sigma = \left(\frac{\Gamma\left(1+\beta) \times \sin\left(\frac{\pi\beta}{2}\right)\right)}{\Gamma\left(\frac{1+\beta}{2}\right) \times \beta \times 2^{\left(\frac{\beta-1}{2}\right)}} \right) \quad (24)$$

In this case, Y, Z can be viewed as the search spiral shape, and β can be thought of as the constant parameter that is set to 1.5. The spiral shape is displayed as follows:

$$Y = R \times Cos(\theta) \quad (25)$$

$$X = R \times Sin(\theta) \quad (26)$$

Here,

$$R = R_1 + U \times d_1 \quad (27)$$

$$\theta = -\omega \times d_1 + \theta_1 \quad (28)$$

$$\theta_1 = \frac{3 \times \pi}{2} \quad (29)$$

Here, the small number can be described as U which is fixed as 0.00565 and the parameter at fixed amount of search cycles R_1 between 1 and 20 [19], the small variable ω which is fixed as 0.005, d is described as the integer variables of the search space from 1 towards distance.

Phase 3: The third way allows for the precise location of the prey, the Aquila's readiness for an attack and landing, and the use of a steep initial combat to gauge the prey's response. This tactic is known as a gradual fall attack or low flight. In order to carry out the attack and choose the prey, AO also takes advantage of the final's chosen location. These Aquila qualities are presented as follows:

$$X_3(T+1) = X_{best}(T) - X_m(T)) \times \alpha - RAND + (ub - lb) \times RAND + lb) \times \delta \quad (30)$$

Here, the lower bound as lb, the upper bound as ub, the exploitation management variables δ, α are fixed as a constant to a small parameter (0, 1), the present solution mean variable is presented as $X_m(T)$, the approximate prey's position is described as$X_{best}(T)$ and

the next iteration solution is denoted as $X_3(T+1)$ and it is created with the consideration of expanded exploitation.

Phase 4: In this mechanism, the Aquila approaches the prey and engages it in the area where the stochastic variables are present. Grab and walk is the name of this tactic. In the finishing position, the AO also engages the quarry. The following is how this quality is presented:

$$X_4(T+1) = QF \times X_{best}(T) - (G_1 \times X(T) \times RAND) - G_2 \times LEVY(d) + RAND \times G_1 \quad (31)$$

Here, $X_4(T+1)$ is the explanation of the following iteration that may be produced using the quarter approach, and QF is the quality function that is utilised to balance the search strategy. G_1 may be defined as the various gestures of the AO that are used to manage the prey throughout the slope and G_2 can be defined as the decreasing parameter from 2 to 0 that defines the flight slop of the AO that can be used to follow the prey during the decamp from the beginning point.

$$QF(T) = T^{\frac{2\times RAND-1}{(1-T)^2}} \quad (32)$$

$$G_1 = 2 \times RAND - 1 \quad (33)$$

$$G_2 = 2 \times \left(1 - \frac{T}{t}\right) \quad (34)$$

Here, RAND is between 0 and 1 for the random parameter, $LEVY(d)$ is the distribution function for levy flights and $QF(T)$ is the parameter of the quality function.

Phase 5: The overall complexity of computation is examined in this section. The initiation, compute fitness operation, and solution update are three ideas that highlight the computational difficulty of the AOA. N can be thought of as the overall number of solutions found during evaluation, and O(N) can be thought of as the computing difficulty of the solutions found during the loading phase. The computation-complexity solution, also known as the informing process, can be written as O(t*n)+o(t*n*dim), which entails searching for the best places for the answer as well as updating it. In this case, tin and Dim stand for the overall number of iterations and the problem's dimension size, respectively. Additionally, the Aquila's total computational complexity is given as O(n*(t*d+1)).

4. Performance Evaluation

This section evaluates and justifies the effectiveness of the projected DAC and security measures. Performance metrics are assessed in order to confirm the efficacy of the proposed method, including decryption time, encryption time, downloading time, uploading time, memory use for encryption, and memory use for decryption. This performance statistic is used to verify the proposed method. In MATLAB, the proposed technique is put into practice, and results are assessed. The input data is taken into account and is gathered from [20] in order to justify the projected technique's performance. In table 1, the variables for simulation are displayed.

Table 1. Variables for simulation

S. No	Description	Constraints
1	quantity of devices	100
2	Xm	100
3	Ym	100
4	Range of coverage	20
5	Total population	50
6	Instances of iterations	100
7	Lower bound	100
8	Upper bound	-100

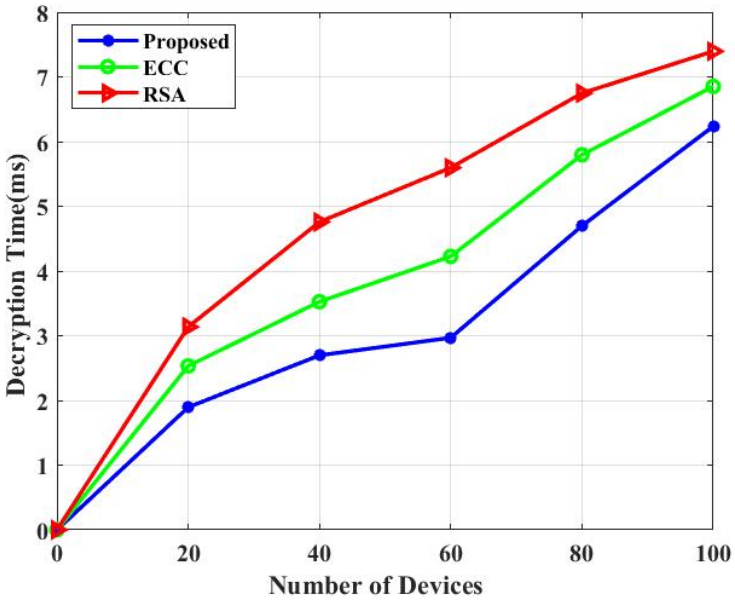

Fig. 4. Decryption Time

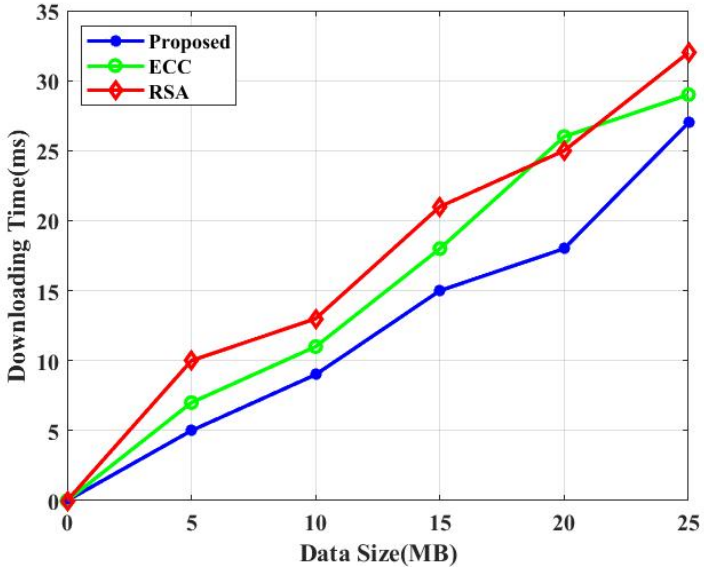

Fig. 5. Downloading Time

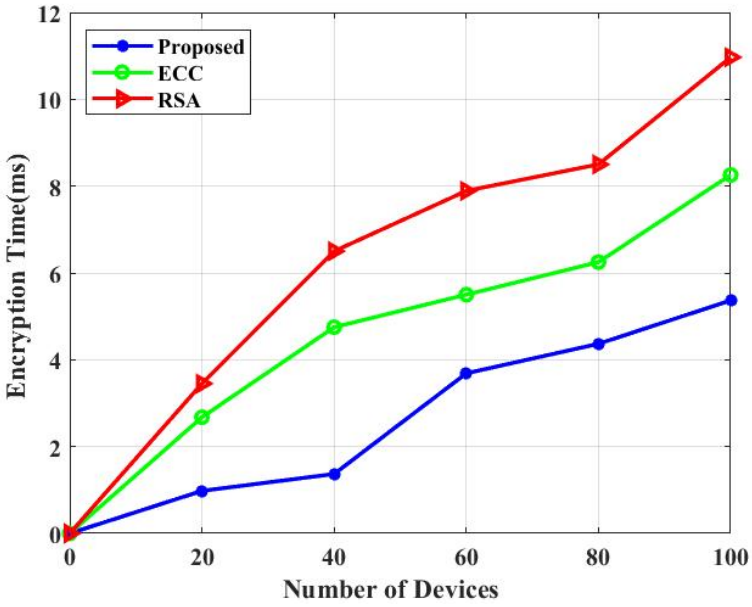

Fig. 6. Encryption Time

The decryption time is examined at and shown in **Fig. 4** and also with comparisons to traditional approaches in order to show the efficacy of the methods offered. The proposed method achieved 1.8ms at epoch 20 according to the Figure. At epoch 20, the RSA is achieved in 3.2 ms and the ECC in 2.8 ms. According to the investigation, the suggested technique yields the best results according to decryption time. To demonstrate the efficiency of suggested technique, **Fig. 5** analyses and shows the downloading time. Additionally, it is put up against more traditional techniques like RSA and ECC. The proposed technique, according to the Figure, can handle 5MB of data in 5ns. At 5MB of data, the RSA key exchange takes 10ms, but the ECC key exchange takes 6.8ms. According to the analysis, the suggested method produced the best outcomes in terms of download speed. The encryption time is analyzed and illustrated in **Fig. 6** to demonstrate the viability of the suggested approach. The traditional methods like RSA and ECC are also contrasted with it. According to the Figure, the suggested technique is achieved in 1 second at 20 devices. At 20 devices, the RSA algorithm runs in 3.8 ms and the ECC algorithm takes 2.8 ms. In line with the analysis, the suggested method yields the best results in terms of encryption instance.

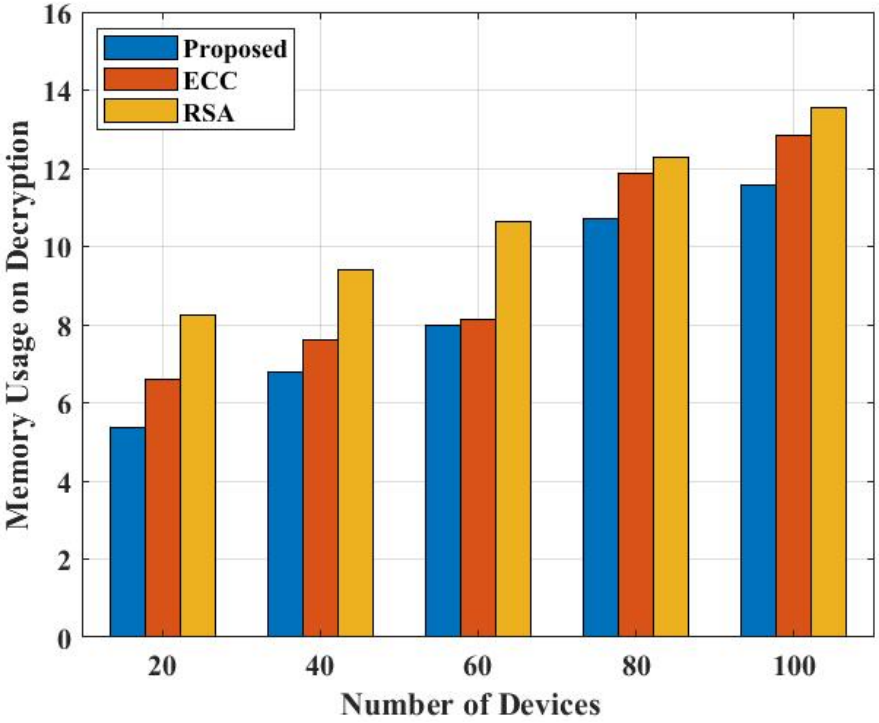

Fig. 7. The performance analysis of decryption Memory usage

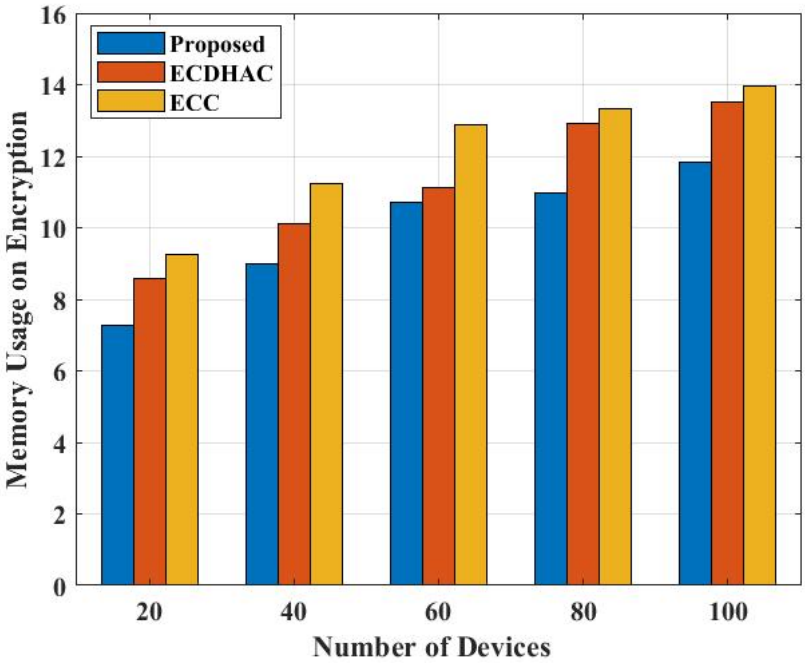

Fig. 8. The comparison analysis of encryption on memory usage

The memory consumption during decryption is examined and demonstrated in **Fig. 7** to demonstrate the efficacy of the suggested methodology. Moreover, it is put up against more traditional techniques like RSA and ECC. The figure shows that the suggested method produces 5 at 20 devices. At 20 devices, the RSA key size is 8.1 and the ECC key size is 6.5. Regarding memory use during decryption, the analysis shows that the suggested technique produces the best results. **Fig. 8**'s analysis and illustration of memory use during encryption serve to support the efficacy of the suggested methodology. It is also contrasted with traditional techniques. The suggested technique achieves 7 at 20 devices. At 20 devices, the ECC and RSA both reach 8.2 and 9. According to the investigation, the suggested technique yields the best results for encryption memory utilization.

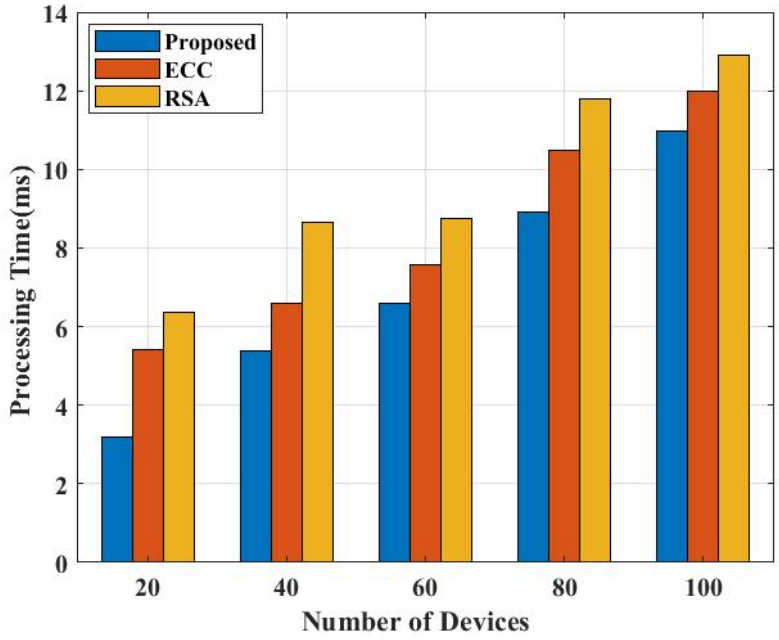

Fig. 9. Processing time

To demonstrate the effectiveness of the provided technique, the processing time is investigated and represented in **Fig. 9**. Additionally, it is put up against established methods like RSA and ECC. According to the Figure, the proposed method achieves 3 ms at 20 devices. The RSA takes 6.2 ms and the ECC 5.8 ms at 20 devices, respectively. The analysis shows that the suggested technique yields the best results in terms of processing time.

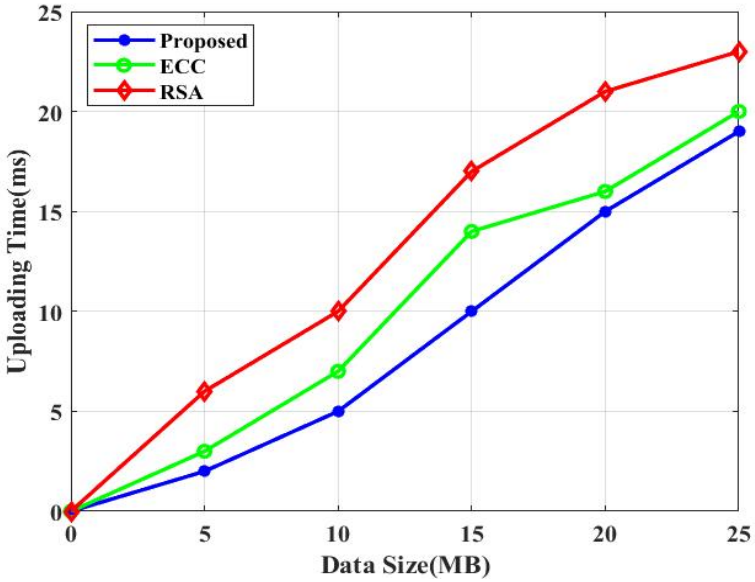

Fig. 10. Uploading time

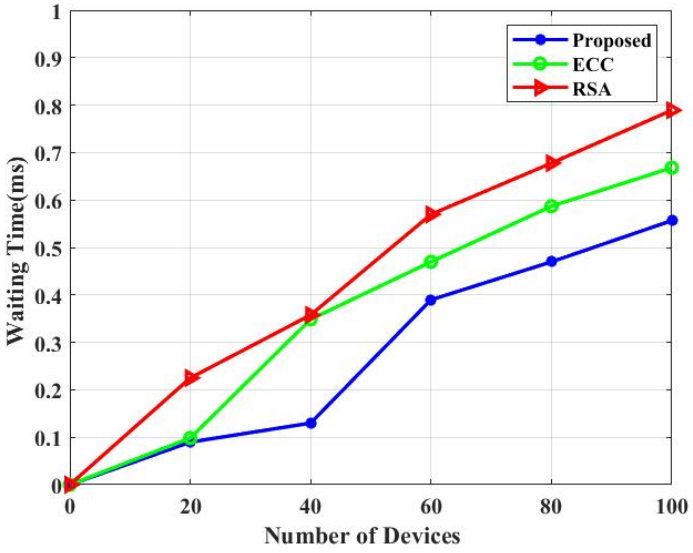

Fig. 11. Waiting time

The uploading time is looked into and depicted in **Fig. 10** to show how well the suggested process works. It is also contrasted with popular methods like RSA and ECC. The proposed method can handle 5MB of data in 3ms, as shown in the Figure. The RSA takes 5.2ms and the ECC 4ms at 5MB data size, respectively. The investigation shows that the suggested technique produces the best results according to uploading time. The waiting time is looked into and depicted in **Fig. 11** to show how well the recommended technique works. The anticipated method achieves 0.02 ms at 20 devices, as shown in the Figure. The ECC is finished at 20 devices in 0.1 milliseconds, while the RSA is acquired in 0.28 milliseconds. The data show that the suggested method produces the best waiting time outcomes.

5. Conclusion

In this study, BSSDAC was developed to support secure data transaction operation and access control. One of the main objectives of this study is to enhance data access management and security in IoT applications. The purpose of CP-development ABE's was to improve data security. AOA has finished the primary generation of the CP-ABE. The development of the block chain-based DAC was done to secure the owner's security. The block chain based CP-ABE was developed to provide secure data storage and exchange. The adoption of block chain technology by the data owner enhances data security and access control. In the end, the block chain-based technique gives the data owner access control and data protection. Performance of the suggested method is evaluated after it has been implemented in MATLAB. Recent technologies like RSA and ECC are contrasted with the proposed technique. According to the analysis, the suggested technique has successfully reduced the amount of time needed for uploading, downloading, encryption, and decryption as well as the amount of memory used for each.

Acknowledgement

I would like to acknowledge and give my warmest thanks to my supervisor Dr. Yesubai Rubavathi.C who made this work possible. His guidance and advice carried me through all the stages of writing my project. I would also like to thank you my committee members for letting my defense be an enjoyable moment, and for your brilliant comments and suggestions, thanks to you.

I would also like to give special thanks to my whole family for their continuous support and understanding when overtaking my research and writing my project. Your prayer for me was what sustained me this far.

Finally, I would like to thank god, for letting me through all the difficulties. I have experienced your guidance day by day. You are the one who let me finish my degree. I will keep on trusting you for my future.

References

[1] Gauhar Ali, Naveed Ahmad, Yue Cao, Muhammad Asif, Haitham Cruickshank, and Qazi Ejaz Ali, “Block chain based permission delegation and access control in Internet of Things (BACI),” *Computers & Security*, Vol.86, pp. 318-334, Sep. 2019. Artical (CrossRef Link)

[2] Shuang Sun, Rong Du, Shudong Chen, and Weiwei Li, “Block chain-based IoT access control system: towards security, lightweight, and cross-domain,” *IEEE Access*, vol. 9, pp. 36868-36878, Feb. 2021. Artical(CrossRef Link)

[3] Egala, Bhaskara S., Ashok K. Pradhan, Venkataramana Badarla, and Saraju P. Mohanty, “Fortified-chain: a block chain-based framework for security and privacy-assured internet of medical things with effective access control,” *IEEE Internet of Things Journal*, vol. 8, no. 14, pp. 11717-11731, Jul. 2021. Artical(CrossRef Link)

[4] Liu, Han, Dezhi Han, and Dun Li, “Fabric-IoT: A block chain-based access control system in IoT,” *IEEE Access*, vol. 8, pp. 18207-18218, Jan. 2020. Artical(CrossRef Link)

[5] Tan, Liang, Na Shi, Caixia Yang, and Keping Yu, “A block chain-based access control framework for cyber-physical-social system big data,” *IEEE Access*, vol. 8, pp.77215-77226, Apr. 2020. Artical(CrossRef Link)

[6] Qin, Xuanmei, Yongfeng Huang, Zhen Yang, and Xing Li, “A Block chain-based access control scheme with multiple attribute authorities for secure cloud data sharing,” *Journal of Systems Architecture*, vol.112, pp.101854, Jan. 2021. Artical(CrossRef Link)

[7] Laurent, Maryline, Nesrine Kaaniche, Christian Le, and Mathieu Vander Plaetse, "A block chain-based access control scheme," in *Proc. of SECRYPT 2018: 15th International Conference on Security and Cryptography*, vol. 2, pp. 168-176, jul. 2018. Artical(CrossRef Link)

[8] Gao, Hongmin, Zhaofeng Ma, Shoushan Luo, Yanping Xu, and Zheng Wu, "BSSPD: a block chain-based security sharing scheme for personal data with fine-grained access control," *Wireless Communications and Mobile Computing*, vol. 2021, no. 6658920, feb. 2021. Artical(CrossRef Link)

[9] Xia, Qi, Emmanuel Boateng Sifah, Abla Smahi, Sandro Amofa, and Xiaosong Zhang, "BBDS: Block chain-based data sharing for electronic medical records in cloud environments," *Information*, vol. 8, no. 2, pp. 44, Apr. 2017. Artical(CrossRef Link)

[10] Xu, Hong, Qian He, Xuecong Li, Bingcheng Jiang, and Kuangyu Qin, "BDSS-FA: a block chain-based data security sharing platform with fine-grained access control," *IEEE Access*, vol. 8, pp. 87552-87561, May. 2020. Artical(CrossRef Link)

[11] Yang, Caixia, Liang Tan, Na Shi, Bolei Xu, Yang Cao, and Keping Yu, "AuthPrivacyChain: A block chain-based access control framework with privacy protection in cloud," *IEEE Access*, vol. 8, pp. 70604-70615, Apr. 2020. Artical(CrossRef Link)

[12] Bera, Basudeb, Durbadal Chattaraj, and Ashok Kumar Das, "Designing secure block chain-based access control scheme in IoT-enabled Internet of Drones deployment," *Computer Communications*, vol. 153, pp. 229-249, Mar. 2020. Artical(CrossRef Linik)

[13] Thwin, Thein Than, and Sangsuree Vasupongayya, "Block chain-based access control model to preserve privacy for personal health record systems," *Security and Communication Networks*, vol. 2019, jun. 2019. Artical(CrossRef Linik)

[14] Bera, Basudeb, Sourav Saha, Ashok Kumar Das, and Athanasios V. Vasilakos, "Designing block chain-based access control protocol in iot-enabled smart-grid system," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5744-5761, Oct. 2020. Artical(CrosRref Link)

[15] Yu, Yong, Yannan Li, Junfeng Tian, and Jianwei Liu, "Block chain-based solutions to security and privacy issues in the internet of things," *IEEE Wireless Communications*, vol. 25, no. 6, pp. 12-18. Dec. 2018. Artical(CrossRef Link)

[16] Shangping Wang, Yinglong Zhang, and Yaling Zhang, "A block chain-based framework for data sharing with fine-grained access control in decentralized storage systems," *IEEE Access*, vol. 6, pp. 38437-38450, jun. 2018. Artical(CrossRef Link)

[17] Sowjanya, K., and Mou Dasgupta, "A ciphertext-policy Attribute based encryption scheme for wireless body area networks based on ECC," *Journal of Information Security and Applications*, vol. 54, p. 102559, Oct. 2020. Artical(CrossRef Link)

[18] Mahajan, Shubham, Laith Abualigah, Amit Kant Pandit, and Maryam Altalhi, "Hybrid Aquila optimizer with arithmetic optimization algorithm for global optimization tasks," *Soft Computing*, vol. 26, no. 10, pp. 4863-4881, feb. 2022. Artical(CrossRef Link)

[19] Wang, Shuang, Heming Jia, Laith Abualigah, Qingxin Liu, and Rong Zheng, "An improved hybrid aquila optimizer and harris hawks algorithm for solving industrial engineering optimization problems," *Processes*, vol. 9, no. 9, p. 1551, Aug. 2021. Artical(CrossRef Link)

[20] https://archive.ics.uci.edu/ml/datasets/Adult

C. Sathish was born in tamilnadu, india. He received B.E in computer science and engineering from Sun college of engineering and technology and M.E degree in computer science and engineering from government college of technology comibatore. He is working as assistant professor in government college of engineering, bodinayakanur, theni,tamil nadu. His main research area is internet of things and wireless communication. Email: csathish9710132@gmail.com

Dr. C. Yesubai Rubavathy was born in tamilnadu, india. She received B.E in computer science and engineering from Kamaraj College of Engineering and Technology and M.E degree in computer science and engineering from Mepco Schlenk Engineering College. She is working as Professor in Francis Xavier Engineering College, tirunelveli, Tamil nadu. Her main research area is internet of things, image processing and pattern recongnition. Email: ryesubai123@gmail.com