International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2022/214501 Volume 9, Issue 4, July – August (2022)

RESEARCH ARTICLE

A Novel Distributed Token-Based Access Control Algorithm Using A Secret Sharing Scheme for Secure Data Access Control

Jansi Rani Amalraj
Department of Computer Science, Government Arts College, Coimbatore, Tamil Nadu, India
jansiramalraj@gmail.com

Robert Lourdusamy
Department of Computer Science, Government Arts College, Coimbatore, Tamil Nadu, India
robertatgac@gmail.com

Received: 23 May 2022 / Revised: 27 June 2022 / Accepted: 08 July 2022 / Published: 30 August 2022

Abstract – Electronic health (e-Health) services present a proficient exchange of the patient's records among various entities; they contain physicians, receptionists, nurses, insurance businesses, and lab technologists. The data owner signifies content providers who could record and distribute health reports at the Medical History Database Server (MHDS) surroundings for distribution in e-Health. The MHDS model presents huge chances to sustain supple and prohibited data swap. However, access control provides the MHDS pretense with a severe challenge which hinders the broad acceptance of MHDS-based e-Health services. One major issue needs to be resolved to carry out protected data exchange: 1) how can these communications entities manage access? Many attempts have been made in the past to offer safe and trustworthy access control to e-Health services. However, due to a shortage of trust and the dynamic nature of e-Health services, the model would be vulnerable to many threats and attacks. This work proposed Distributed Token-based Access Control (DTAC) algorithm to deal with this problem. This algorithm allows patients and doctors to put their information on the MHDS and execute protected data swaps with a healthcare provider. The experimental results show that DTAC algorithms provide secure and flexible access control with less computation time and less network latency in the healthcare environment in heterogeneous networks.

Index Terms – Heterogeneous Network, Data Exchange, Security, Unauthorized Access, Access Control, Token, Electronic Health.

1. INTRODUCTION

A heterogeneous network links computers where the protocols and operating systems have important differences [1]. For instance, the local area networks (LANs) that link Apple Macintosh computers to computers running Linux and Microsoft Windows are diverse. In wireless networks that use a range of access technologies, the term "heterogeneous network" is used. A heterogeneous wireless network, for instance, offers coverage over a wireless LAN and maintains that service while shifting to a cellular network.

The main security necessity for heterogeneous networks is non-repudiation, access control, availability, integrity, authentication, encryption, and decryption. Security in a multidisciplinary network is not easy because heterogeneous networks have newer sensitivities than other traditional networks. Figure 1 shows the key security requirements for heterogeneous networks.

- **Access control:** Access control is used to prevent the illegal use of network assets [2]. It is bundled with authentication features. In general, access control is a service commonly required on both personal computers and network connections [3].
- **Cryptography:** Cryptography is used to secure transmitted data when malicious devices are present [4]. Heterogeneous networks use open media; thus, usually, entire devices in the direct broadcast range can receive data. One method for maintaining data confidentiality is to encrypt the data [5]. When there is communication between one sensor device and another or access points (AP) and the Medical History Database Server (MHDS) across heterogeneous networks, cryptography protects data from exposure. If the keys are not encrypted and registered on the device, malicious devices may pose a security risk.
- **Authentication:** Authentication is used to detect a device and avoid impersonation. Message authentication code can be used to achieve authentication.
- **Integrity:** Integrity is used to securely store transmitted data without being altered or damaged during transmission. When broadcast, malicious devices may

RESEARCH ARTICLE

drop or change data. The attackers send it back; this process is recognized as a replay attack. It can be achieved through the hash function.

- **Non-repudiation:** Non-repudiation is related to the fact that if a device sends data, that device cannot refuse to send data. By providing a sign for the data, the device containing the sent data cannot be denied later. In public-key cryptography Device A signs the data based on its private key. All other devices can verify the signed data using A's public key, and there is no denying that A is linked to its signed data.
- **Availability:** Availability is used to maintain network assets available to real devices. This guarantees the survival of the network despite adverse events. In a heterogeneous network, the risk factors for failure to access may be sensor device blocking and DoS attacks. The key outcome is to provide custom paths in the protocol used by the heterogeneous network to mitigate downtime.

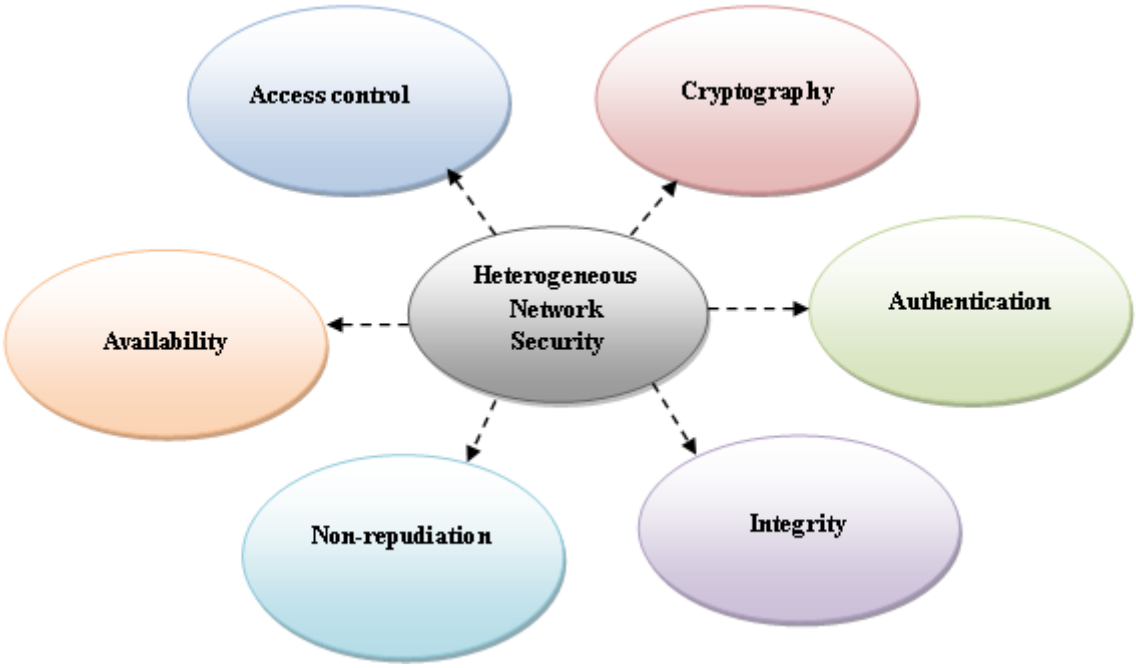

Figure 1 Key Security Requirements for Heterogeneous Networks

Among the key security issues in a heterogeneous environment, access control is important in data security [6]. In information technology (IT), traditional access control techniques such as role-based access control (RBAC), access control list (ACL), and attribute-based access control (ABAC) are widely used. However, due to the following features, they have not been able to come up with a flexible and efficient way to meet the increased demand across multiple networks:

The transmission method for e-Health management over a heterogeneous network strong needs to be improved. Medical services, public health organizations, medical business individuals, and other healthcare experts are just a few of the institutions that make up e-Health services. With the use of the Internet and other e-Health services technology, they may all efficiently access the data. It includes a variety of stakeholders, including patients, nurses, doctors, insurance providers, public health agencies, etc. It has many benefits, including simple patient data access, medical data availability, better and quicker treatment, increased patient safety, and a strong decision support system. However, as more people utilize e-Health services, there are a mounting number of security concerns, including illegal way in to e-Health services, abuse of medical data, bypassing of sensitive data, loss of control over medical data, etc. Access Control prevents illegal access to medical data. It restricts the user's to access resources and prevents unauthorized access by users.

E-Health Heterogeneous networks require a new access control system that provides a secure and robust access control service. Therefore, this paper proposes the Distributed Token-Based Access Control (DTAC) Algorithm for Secure Data Access. With the DTAC algorithm, patients and clinicians can securely exchange data with healthcare providers by putting their data on the MHDS. The foremost purpose of this research is to minimize the security risk of unauthorized access in heterogeneous networks.

RESEARCH ARTICLE

2. RELATED WORK

In this section, the related works on secure data access control are reviewed.

To maintain vehicle network security, Wang et al [2] suggested a dynamic, fine-grained access control approach that is based on attribute-based encryption (ABE). The message sender can choose which vehicles understand the message based on their characteristics, and they can freely revoke the authorization for some vehicles to decrypt data without having to upgrade all non-revoked keys. The authors concluded that this approach is more effective than existing methods in terms of processing complexity and communication overhead.

Tan et al [3] a good data service restriction was suggested mechanism with ciphertext update and compute outsourcing for a fog computing for IoT safe. Time-release encryption was incorporated into ABE by Gajghate et al [4]. To address the shortcomings of CP-ABE & KP-ABE, the authors developed new advanced ABE approaches. To prevent system attacks, utilize two-factor authentication, with the first factor being the standard user ID and password authentication and the second being a mobile-based authentication system. Additionally, the authors create a practical method for providing granular access control for time-sensitive data.

The access policy attribute would be saved in a secret key in the current system using the CP-ABE approach. Additionally, the user must destroy the old document or decrypt it before re-encrypting it if they want to add or remove attributes. The authors will separately save the access policy attributes in a meta-data file to get around this issue. The original document file secret key and the meta-data file secret key are interdependent. In their suggested method, properties can be changed or updated whenever necessary without document decryption. When a user changes or deletes an attribute. The Text size will be fixed when utilizing their system encryption.

Vidhya et al. [5] presented a method deduplicating encrypted content recorded in cloud-using access control, thus evading redundant records. It incorporates deduplication and access control. The outcome of their system demonstrates better competence and is possible for sensible exploitation in the case of enormous storage.

Liu et al. [6] presented a new and realistic IoT information outsourcing system using Corrigan-Gibbs calculation of collective data with the ciphertext-policy attribute-based encryption (CP-ABE). It assists in fine-grained access control and safe aggregation of outsourced IoT information. The user has to allow a little number of calculations in the procedure of information upload and revival. Safety study shows that their system secures the privacy of IoT information. A detailed effectiveness comparison demonstrates that their system provides superior effectiveness on the fog server-side and the client-side.

In cloud computing appliances, A Dual access Control and Data integrity Verifiable system was proposed by Zhang et al. [7]. A hierarchical time tree initiated at the attribute-based encryption skill through utilizing of hierarchical identity-based encryption technique putting an effectual access period also the particular decrypt able era for the users attributes key and encrypted information individually. At last, the safety evidence and competence investigation demonstrate that their method is safe and realistic.

Huang et al. [8] proposed a safe and fine-grained data access control system with ciphertext update and calculation outsourcing in fog computing for IoT. The responsive information of the data owner is initially encrypted utilizing attribute-based encryption by numerous rules also uploaded to the cloud. Thus, user features assure the access policy could decrypt the ciphertext. Using the attribute-based signature method, the features of the authorized user incorporated into the signature satisfy the updated rule and could renovate the ciphertext.

Ding et al. [9] presented a safe access control technique, ARBACV1 utilizing RBACV1 merged with the ABAC method that is more flexible than RBACV1 and could execute fine-grained access control. The clearness of information on the blockchain has affected the populace's huge awareness of data confidentiality defense problems. A total access control method has not been presented on the Ethereum blockchain. Along with the blockchain architecture, the presented access control method ARBACV1 is used to the blockchain by smart contracts, the usage of the blockchain users controlled safely, and the code written in Ethereum.

Xu et al. [10] proposed PMDAC-ABSC, a new confidentiality-protection information access control system using Ciphertext-Policy ABSC, to present a fine-grained control calculate and attribute confidentiality defense concurrently at a multi-authority cloud storage scheme. The presented system is verified to be safe in the normal method and could present privacy, unforgeability, and anonymous authentication.

Li et al. [11] presented a privacy-preserving cloud-assisted mobile multimedia (PPCMM) information distribution system, where all features are explained through the value and name of the attribute. The attribute's values are embedded in the ciphertext and merely the names of the attribute exposed at the access rule. By utilizing the decryption outsource method, many calculation overheads of identical examination and decryption are offloaded to the cloud.

An access control system using blockchain known as BacCPSS for CPSS big data was presented by Tan et al. [12]. At last, a realistic test method on EOS constructed. Outcomes

RESEARCH ARTICLE

demonstrate that BacCPSS is possible and effective and could attain safe access in CPSS while defending confidentiality. Riad et al. [13] outcomes demonstrate outstanding compatibility and effectiveness with various systems and patterns.

Hu et al. [14] proposed the safe access control system using the NTRU cryptosystem for cloud big data storage. Fitri et al. [15] propose access control and safe attribute-based encryption for medical report information. Their scheme was constructed utilizing four access policies at a hospital.

Dixit et al. [16] developed a structure that allows policy-based multi-authority access authorization to EHR schemes used through numerous care providers from various locations. This structure resides on edge and has been constructed utilizing the Semantic Web technologies and the Multi-Authority Attribute-Based Encryption (MA-ABE).

Zheng et al. [17] first construct a new cryptographic primitive (i.e., TFPRE-OT). A novel data sharing strategy is presented to attain differential access control and prevent privacy exposure in generic cloud computing scenarios utilizing TFPRE-OT as the foundation. The authors' in-depth security research demonstrates that the suggested solution can satisfy all necessary safety needs. Eventually, the authors used comprehensive experiments and case studies to confirm the viability of their approach.

Yang et al. [18] presented a lightweight break-glass access control (LiBAC) scheme. It was properly verified safe at the typical method, and widespread experiments were performed to show its competence. Edemacu et al. [19] proposed how to utilize the features technique to attain the attribute revocation in their task. Efficiency and safety investigation demonstrates that their system is safe, expressive, and proficient. Roy et al. [20] presented a fine-grained access control above cloud-based multiserver data. The presented system is the initial to follow fine-grained access control above numerous clouds in MCC surroundings. Their system has been validated broadly in various heterogeneous surroundings, where its effectiveness was discovered well in contrast to other previous systems.

This section reviewed some existing secure data access control in different types of networks. The objective of this literature review is to gain an understanding of current research and discussions relevant to secure data access control and to identify areas of controversy. The next section provided Distributed Token-based Access Control (DTAC) algorithm. By using this algorithm, patients, physicians, and others can securely exchange medical data.

3. SECURE DATA ACCESS CONTROL

Technologies for the authorization of access and authentication to particular services or resources are among the most important elements in defending the safety and confidentiality of heterogeneous devices. Like a basic method to allow safety in the computer system, access control is the procedure that chooses who is approved to have what contact rights on which things concerning a few security policies. A proficient access control scheme was developed to assure the major protection necessities, for example, confidentiality, integrity, and availability. Access control systems, however, have recently been forced into the heterogeneous era to reach a advanced customary with more plan consideration, such as elevated scalability, elasticity, lightweight, and causality. It is because of increased security and privacy issues. Various access control techniques and results with various goals are presented to tackle complex security problems.

Because of disadvantages in conventional access control methods, such as RBAC and ABAC, the necessities forced through heterogeneous situations could not be satisfied. On the other hand, given the numerous huge benefits from a heterogeneous viewpoint, for example, scalability, suppleness, and capability to be disseminated and user-driven, heterogeneous schemes could sustain location and revocation. However, BlendCAC is only supported in fixed sensors. Due to the motion sensors attached to the human body in the heterogeneous network, BlendCAC is not enough. To deal with this problem, this paper focused on token-based secure data access control for the heterogeneous network in the medical environment. Figure 2 shows token-based secure data access control architecture.

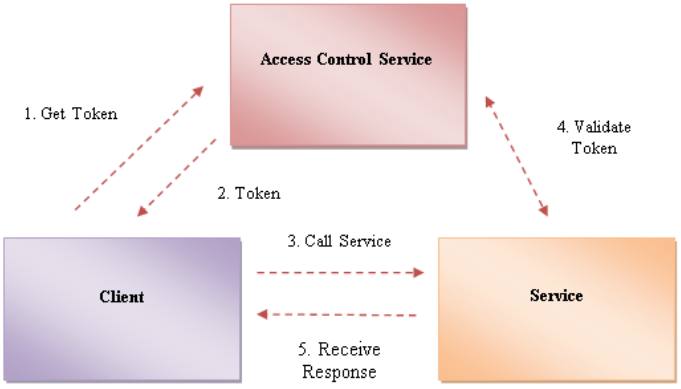

Figure 2 Token-Based Secure Data Access Control Architecture

The steps are:

- The client requests the ACS to get a Token.
- The client requests the service using this token (by adding this token in the header of the message).
- When it receives the request, the service calls the ACS to validate the token (using the same type of credentials or using some of the rules defined on the ACS Portal).

RESEARCH ARTICLE

- If the token is valid, the service sends a response to the client.

4. DISTRIBUTED TOKEN-BASED ACCESS CONTROL

The data owner signifies a content provider who could record and issue health reports at the MHDS surroundings for distribution in e-Health. The MHDS model presents huge chances to sustain supple and restricted data swap. Access control problems at the MHDS pose a severe challenge that hinders the broad adoption of MHDS-based e-Health services. For example, information swap among communicating entities over the MHDS worsens the safety problems. Present access control methods are not compatible with the MHDS surroundings.

Numerous techniques have been presented to tackle the problems associated with MHDS safety and outsourced information. Previous cryptographic techniques are enough if data owners desire just to record their responsive information on the MHDS. However, e-Health services need data swaps between patients and their healthcare providers. To execute a secure data swap, we should tackle one main concern: 1) how could we manage access by these communicating entities? Conventional access control mechanisms could not be used in these surroundings because they presume servers at a similar domain are completely trusted. They could implement access control policies to address the concern. In MHDS surroundings, servers are exterior of the user's reliance domain and, therefore, sensitive information should protect from unauthorized usage. This safety concern becomes more difficult in real-time healthcare services.

This work presented a novel Distributed Token-based Access Control (DTAC) algorithm to deal with this problem. The presented technique allows patients and doctors to put their information on the MHDS and execute secure data exchange with healthcare providers. This paper proposed DTAC, a novel and safe system that sustains both safe cryptography and scalable distributed token-based data access control simultaneously; in terms of that, permitted user has the usage right to which kinds of healthiness reports. The method assigns supple usage rights to individual users using their rights and the aim of utilizing the data. This technique presents data confidentiality by encryption methods. This approach shares a token and secret key based on the secret sharing scheme to set unsafe communication between interacting entities. Figure 3 shows the Distributed Token-based Access Control architecture.

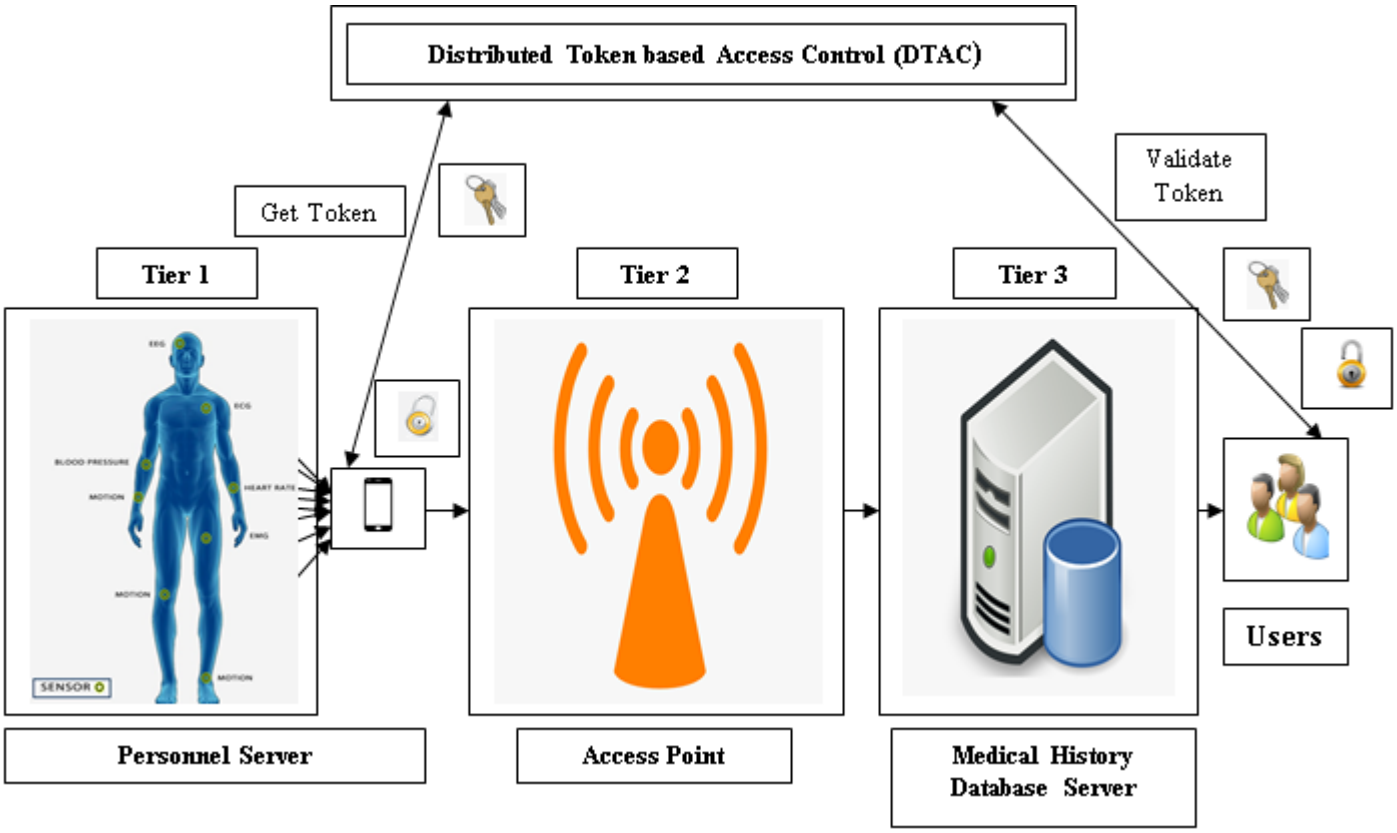

Figure 3 Shows the Distributed Token-Based Access Control Architecture

RESEARCH ARTICLE

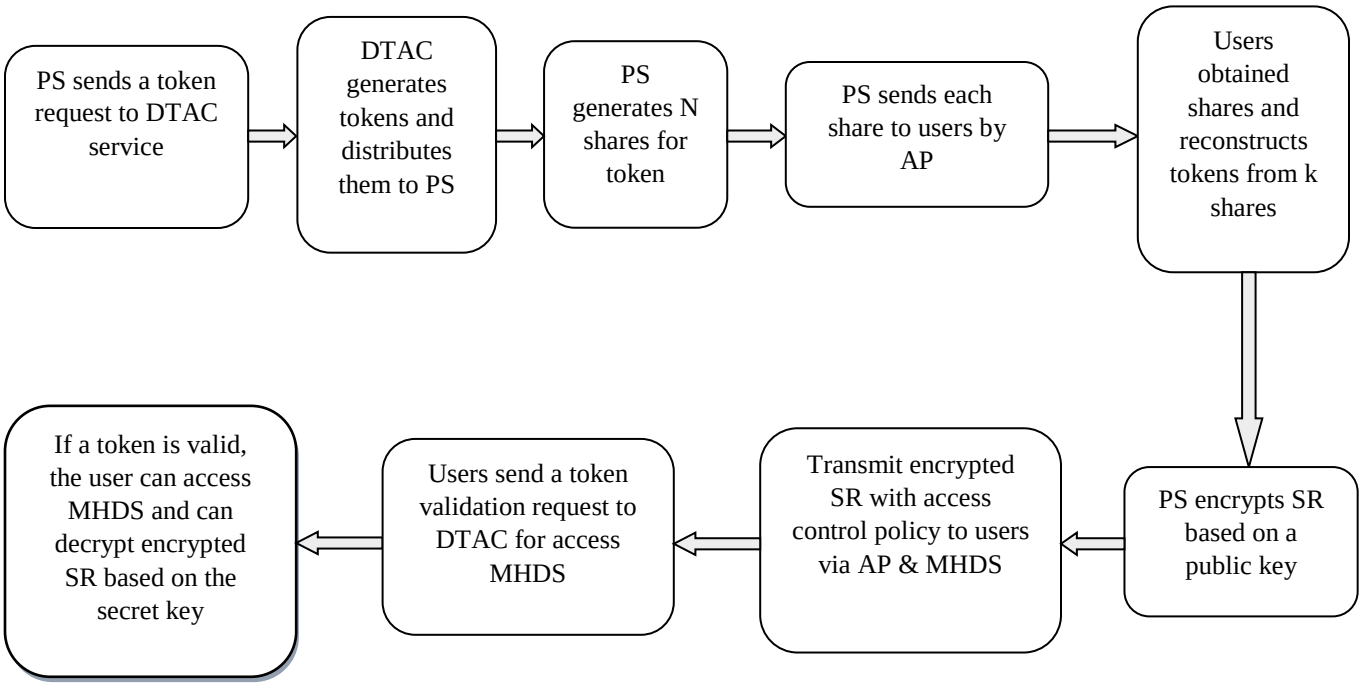

Figure 4 Block Diagram of the DTAC Algorithm

In Heterogeneous Network with a healthcare environment, the DTAC algorithm presented that elucidated in Algorithm 1 to improve existing security techniques. A Personnel Server (PS) plans to transmit a packet to the Medical History Database Server (MHDS). For security, it generates Public Key and Secret Key for cryptography. A public key is used for encryption, and a Secret key is used for decryption. Thus secret key sharing with the user is essential for decryption. For safe secret sharing, the personnel server used the S4C algorithm.

For access control, PS sends a token request to Distributed Token-based Access Control Service (Step 1). Then, DTAC Service generates tokens using Algorithm 2 (Step 2). After token generation, DTAC distributes the token to the requested PS (Step 3). Following this, PS received a token from DTAC (Step 4). For safe token distribution, the PS creates shares for Token (Step 6) discussed in Algorithm 3. Afterward, it sends each token distribution to the user by Access Point (AP) & MHDS (Step 7-9). After receiving each token share, the user can reconstruct the Token (Step 11-13), discussed in Algorithm 4. After token distribution, the personnel server takes Sensor Readings (SR) from the human body and encrypts SR using the public key.

It transmits encrypted SR to MHDS via AP (Step 10). If the user wants to access MHDS, he should send the token validation request to DTAC (Step 15-16). If the token is legitimate, the user could use MHDS (Step 17). Otherwise, the user cannot access MHDS (Step 21). After encrypted SR is received from MHDS, the user can decrypt it based on the secret key, and they can access the original SR (Step 18-19). Figure 4 shows the DTAC algorithm block diagram.

Personnel Server (PS), User (U), Access Point (AP), Medical History Database Server (MHDS), Sensor Readings (SR), and Distributed Token-based Access Control Service (DTAC) are the Inputs

Distributed Token-based Access Control was the expected outcome

Personnel Server Side

1. PS send a token request to DTAC
2. Token = Generate_Token() // Algorithm 2
3. DTAC distributes Token to PS
4. Token = PS received token from DTAC
5. Let N, k // N is the number of token shares to be created, and k is the number of token shares that should reconstruct
6. TSH[] = Generate_Token_Shares(Token, N, k) // Algorithm 3
7. For each share TSHi in TSH, do
8. Forward TSHi with k to U
9. End For

RESEARCH ARTICLE

10. Take SR, encrypt, and upload encrypted SR to MHDS via AP
11. U received Token Shares with k
12. Take k Token shares to reconstruct
13. Token = Reconstruct_Token(k shares) // Algorithm 4
14. To access MHDS, U sends the Token validation request to DTAC
15. DTAC checks Token is valid or not
16. IF token is valid
17. U can access MHDS
18. U received encrypted SR from MHDS
19. U can decrypt and access SR
20. Else
21. U cannot access MHDS
22. End IF

Algorithm 1 Distributed Token-Based Access Control Algorithm (DTAC)

4.1. Token Creation

HMAC-SHA-1 algorithm is used for token creation. Message authentication with HMAC is based on cryptographic hash algorithms. HMAC can be combined through any iterative cryptographic hash algorithm, such as SHA-1 and MD5, using a private shared key. The hash function's characteristics are what give HMAC its cryptographic strength.

One of the most important requirements in the field of open information and communication technologies is the presentation of a technique to verify the authenticity of the users in an unreliable medium. Such integrity checks are achieved using techniques that employ a secret key referred to as "message authentication codes" (MAC). Normally, MAC is utilized among two parties, distributing a secret key to confirm data broadcasted among these parties. In this section, provide such a MAC method using cryptographic hash functions (HMAC) for generating tokens.

HMAC can use in a mixture with any iterated cryptographic hash function. SHA-1 and MD5 are instances of hash functions. HMAC utilizes a secret key to verify and calculate the message authentication values. The foremost aims of this structure are

- To utilize, devoid of changes, obtainable hash functions. Particularly hash functions execute fine in software and for which code is widely and freely obtainable.
- To protect the unique effectiveness of the hash function devoid of acquiring an important degradation.
- To utilize and manage keys simply.
- To contain a fine understood cryptographic study of the power of the authentication method using sensible suppositions in the essential hash function.
- Let for simple changeability of the essential hash function in the case earlier, or very safe hash functions are discovered or needed.

This section states HMAC via a general cryptographic hash function (indicated by H). Particular instantiation of HMAC requires defining a specific hash function. Followed by present candidates for such hash functions containing RIPEMD-128/160, SHA-1, and MD5. Furthermore, these various comprehensions of HMAC would denote through HMAC-RIPEMD, HMAC-MD5, HMAC-SHA1, and so on.

A secret key K and a cryptographic hash function, denoted by H, are required for the definition of HMAC. Assume that H is a cryptographic algorithm that hashes data by repeatedly applying a key compression function to data blocks. Indicate by L the hash output byte-length (for MD5, L=16, and SHA-1, L=20) and by B the byte-length of such blocks (B=64). The hash function block length B is the maximum length that the authentication key K can be. Appliances that use keys longer than B bytes first hash the key using H, and then they use the ensuing L byte string as that of the real key to the HMAC algorithm. Regardless, the minimum recommended length for K is L bytes (as the output length of the hash). Algorithm 2 explains token generation.

To compute the HMAC-SHA-1 token above the data `Personnel Server Id' and 'DTAC Id,' perform,

(1) The class SecretKeySpec declares a private key in a carrier way (Step 1). Without needing to go through a SecretKeyFactory (based on providers), it might be used to create a SecretKey from a byte array. This class is only used for raw private keys, such as DES keys, which might be represented as byte arrays and have no associated key parameters.

(2) Mac class - This class presents the working of a "Message Authentication Code" (MAC) algorithm (Step 2). A MAC presents a method to ensure the integration of data sent over or recorded at an untrustworthy medium using a secret key. A MAC method is based on a cryptographic hash function called HMAC. HMAC could use with any cryptographic hash function, for example, SHA256, in a mixture with a secret shared key. HMAC stated at RFC 2104Mac.getInstance(HMAC_SHA1_ALGORITHM) method provides a Mac object which implements the specified MAC algorithm.

(3) m.init(sK) method initializes this Mac object with the given key (Step 3).

RESEARCH ARTICLE

(4) m.doFinal(data.getBytes()) method executes the specified bytes array (rH) and finishes the MAC function (Step 4).

(5) Finally, encode this rH to Token utilizing the encoding method (Step 6-Step 17).

```
1   PS_Id, DTAC_Id, HmacSHA1 are the Inputs
2   Token was the expected outcome
3   SecretKeySpecsK = new SecretKeySpec(DTAC_Id.getBytes(), HmacSHA1)
4   Mac m = Mac.getInstance(HmacSHA1)
5   m.init(sK)
6   byte[] rH = m.doFinal(data.getBytes())
7   Token = new String(encode(rH))
    // encode function
8   char[] encode(byte[] bt)
9   {
10      char[] H = {'a', 'b', 'c', 'd', 'e', 'f', '0', '1', '2', '3', '4', '5', '6', '7', '8', '9', }
11      am = bt.length;
12      char[] r = new char[2 * am]
13      p = 0
14      For (l = 0; l<am; l++)
15      r [p++] = H[(0xF0 &bt[l]) >>> 4]
16      r [p++] = H[(0x0F &bt[l])]
17      End For
18      return r
19  }
```

Algorithm 2 Generate_Token()

4.2. Generate Token Shares

After token creation, the PS must transmit the Token to U for access. However, token sharing in a heterogeneous network is insecure and incompatible because of its dynamic nature. The secret-sharing method is essential to address this issue. This method divides the token into numerous token shares, transmuting all token shares to the user by AP & MHDS. Token shares creation is discussed in Algorithm 3. This algorithm gets token, k (Number of shares necessity for reconstruction) and N (Number of shares to be created) for input (Step 1).

This algorithm assigns a token to p0 at the beginning (Step 3). Then it generates k-1 random numbers. This algorithm sets k to be 3 for convenience of use. As a result, p1 and p2 are two arbitrary numbers (k-1 = 2). (Step 4). This method estimates N shares following the generation of random integers (Step 5-8). A PS then transmits every part to you through AP and MHDS.

```
1   Token, N, k is given as an Input
2   Token_Shares (TSH) was the expected output
3   Let p0 = SecKey, TSH = {}
4   Create Random (k-1) numbers (p1 and p2)
5   Let f(y) = p0 + (p1 * y) + (p2 * y^2)
6   For y=1; y<=N; y++
7       TSH[y-1] = (y,f(y))
8   End For
```

Algorithm 3 Generate_Token_Shares

Figure 5 shows the token shares generation and reconstruction architecture. In this figure, Token S is split into n shares and distributed these shares to the user. Followed by the user reconstructing k shares and getting the original token S.

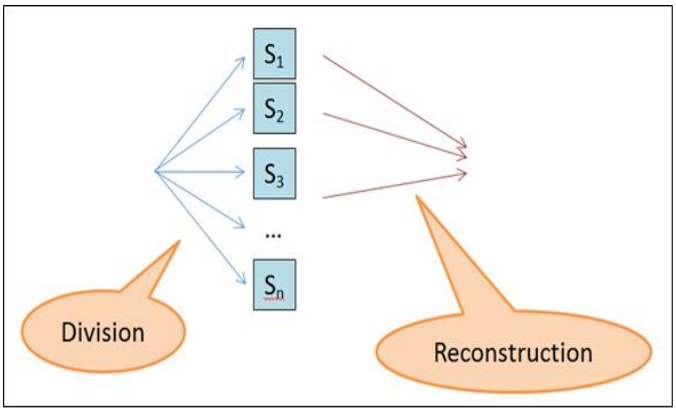

Figure 5 Token Shares Generation and Reconstruction Architecture

4.3. Token Reconstruction

A user receives k token shares to rebuild the token after obtaining all N token shares. The advantage of the DTAC technique is this. An AP may be fabricating any token shares if its behaviour changes to be malicious. As a result, the k token shares obtained by this approach are sufficient for reconstruction. The reconstructing method was mentioned in Algorithm 4.

This approach applies a Lagrange polynomial equation on k token shares (Step 1). It displays p0, p1, p2, and so on. For simplicity, k values are set to 3 (it gives during the generation of token shares); as a result, this algorithm only delivers p0, p1, and p2 (Step 2). Here, p0 is a token (Step 3).

RESEARCH ARTICLE

1. k shares (y0,s0), (y1,s1), ... , (yk,sk) is given as an Input
2. Token was the expected output

   The following steps are as follows
3. $f(y) = \sum_{j=0}^{k}(sj * lj(y))$ // Lagrange polynomial
4. f(y) = p0 + (p1 * y) + (p2 * y^2)
5. Token = p0

Algorithm 4 Reconstruct_Token

5. RESULTS AND DISCUSSIONS

This section presents the experimental outcomes and investigation of the DTAC algorithm in a heterogeneous network. For experimental analysis, randomly created sensor readings were utilized. In this simulation, eight sensors are assumed to be placed randomly and uniformly throughout a human body [22]. This sensor measures human EEG, ECG, blood pressure, heart rate, EMG, and motion level. Followed by these sensor readings are transmitted to PS. To evaluate the DTAC algorithm, java was used. During DTAC algorithm implementation, Personnel Server sends a token request to DTAC Service. Then the DTAC service generates a token based on Algorithm 2; furthermore, the token shares generation and distribution to the user based on Algorithm 3. Furthermore, a token reconstruction is based on an algorithm. After token reconstruction, the user wants to access a medical history database, so it sends the token validation request to the DTAC service; DTAC checks and informs the token is valid, user can access the medical history database server due to the reason of token is valid.

To assess the access control algorithm, evaluate the DTAC algorithm with further well-known access control algorithms. These are BlendCAC[21], RBAC [21] and ABAC [21].

5.1. Computation Time Comparison

Along with the outcomes demonstrated in image 6, the standard entire delay instance needed through the DTAC function of token generation, token shares generation, and token reconstruction is 206.43 ms, which is approximately similar to BlendCAC RBAC, and ABAC. The total delay contains the round trip time (RTT), time for the token request, token distribution to PS, token shares distributed to the user via AP and MHDS, and time for access right validation.

Token processing takes 206.43 ms to complete, or 98 per cent of the entire execution time, making it the phase that requires the most computation. The computation time difference for each stage is shown in Table 1.

The whole validation procedure is separated into two phases—token processing and token validation—where the average time of the validation procedure is 206.51 ms (206.43 ms + 0.08 ms). However, the DTAC performs better than the BlendCAC, RBAC, and ABAC in token processing and validation. It takes time to examine the rules in the database since BlendCAC, RBAC, and ABAC also need one to manage user-role-permission association or maintain attribute-permission rules. The BlendCAC (0.12 ms), RBAC (0.1 ms), and ABAC (0.1 ms) exhibited faster token validation speeds than DTAC in their analysis (0.08 ms). Execution time comparison for each phase is shown in Figure 6.

Table 1 Computation Time Comparison for Each Stage

Algorithm	Token Processing (Token Generation + Token Shares Generation + Token Reconstruction)	Token Validation	Total Delay
BlendCAC	210.27	0.12	210.39
RBAC	207.68	0.1	207.78
ABAC	210.57	0.1	210.67
DTAC	206.43	0.08	206.51

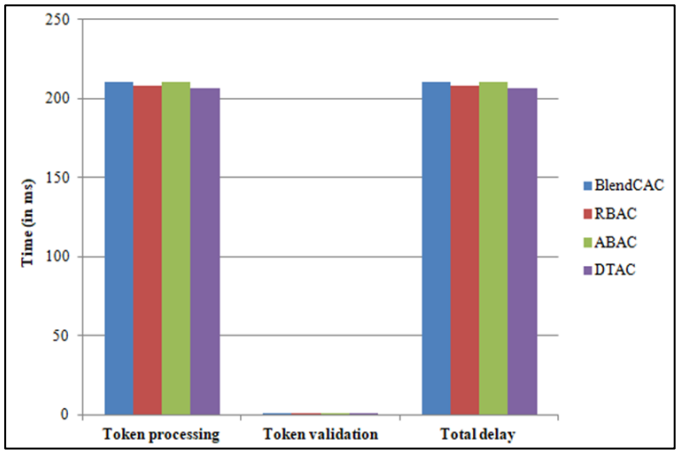

Figure 6 Execution Time Comparison for Each Phase

5.2. Network Latency

Table 2 shows the whole network delay measured and contrasts the DTAC implementation time with BlendCAC, RBAC, ABAC, and a criterion exclusive of enforcing access control. The staff server engaged with the user and stored the token information during the primary service demand situation, where a lengthy delay was seen. As a result, the network latency was drastically lowered, and the level of security was raised by meeting the locally cached indication information intended for token justification. The criterion devoid of access control takes thirty-one ms to get demanded information, while the DTAC exhausted 34 ms. So DTAC

RESEARCH ARTICLE

algorithm merely initiates regarding 3 ms additional latency. Therefore, overhead is trivial in provisions of delay. Figure 7 showed the DTAC had less latency than BlendCAC, RBAC, and ABAC.

Table 2 Network Latency Comparison

Algorithm	10	20	30	40	50
No Access Control	31.7	31.3	31.8	31.2	31.5
BlendCAC	36.9	36.2	36.8	36.3	36.4
RBAC	39.2	39.9	39.3	39.8	39.6
ABAC	42.3	42.8	42.4	42.7	42.5
DTAC	34	39	35	37	36

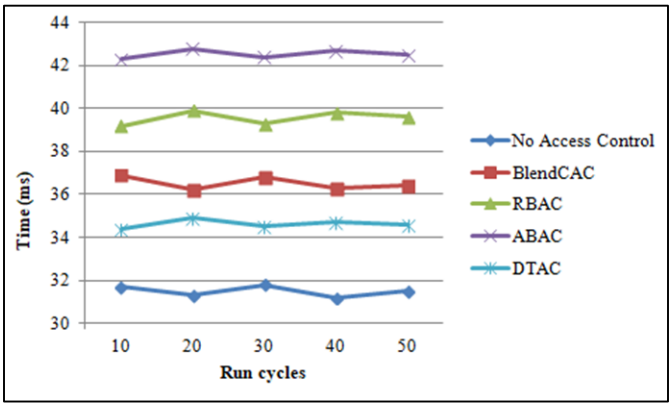

Figure 7 Network Latency Comparison

6. CONCLUSION

This paper provided a distributed and Token-based Access Control framework that leverages heterogeneous network security to manage the problems in access control plans in heterogeneous medical devices. The proposed method allows patients and doctors to put their information on the MHDS and execute protected data exchange with healthcare providers. DTAC supports both secure cryptography and scalable access control simultaneously, in terms of which genuine user has the usage right to which kinds of health reports. The method assigns supple usage rights to individual users using their rights and the aim of utilizing the information. The experimental results proved that DTAC algorithms provide secure and flexible access control with less computation time and less network latency in the healthcare environment in heterogeneous networks.

REFERENCES

[1] C. Sun, Q. Li, L. Cui, H. Li, Y. Shi, "Heterogeneous network-based chronic disease progression mining", 2019 IEEE Big Data Mining and Analytics, Volume 2, Issue 1, pp. 25 - 34, Oct 2018.

[2] Wang, T., Kang, L., & Duan, J. (2021). Dynamic fine-grained access control scheme for vehicular ad hoc networks. Computer Networks, 188, 107872.

[3] S.Y. Tan, "Secure Data Access Control With Ciphertext Update and Computation Outsourcing in Fog Computing for Internet of Things", 2018 IEEE Access, Volume 6, pp. 22464 - 22465, Apr 2018.

[4] K. S. Gajghate, R.V. Mante, "Secure Document Sharing and Access Control on Cloud for Corporate User", 2018 IEEE Second International Conference on Inventive Communication and Computational Technologies, ISBN: 978-1-5386-1974-2, Apr 2018.

[5] R. Vidhya, P. G. Rajan, T. A. Lawrance, "Elimination of Redundant Data in Cloud with Secured Access Control", 2017 IEEE International Conference on Technical Advancements in Computers and Communications, ISBN: 978-1-5090-4797-0, April 2017.

[6] L. Liu, H. Wang, Y. Zhang, "Secure IoT Data Outsourcing With Aggregate Statistics and Fine-Grained Access Control", 2020 IEEE Access, Volume 8, pp. 95057 - 95067, Dec 2019.

[7] Q. Zhang, S. Wang, Duo Zhang, "Time and Attribute Based Dual Access Control and Data Integrity Verifiable Scheme in Cloud Computing Applications", 2019 IEEE Access, Volume 7, pp. 137594 - 137607, Sep 2019.

[8] Q. Huang, Y. Yang, L. Wang, "Secure Data Access Control With Ciphertext Update and Computation Outsourcing in Fog Computing for Internet of Things", 2017 IEEE Access, Volume 5, pp. 12941 - 12950, Jul 2017.

[9] X. Ding, J. Yang, "An Access Control Model and Its Application in Blockchain", 2019 IEEE International Conference on Communications, Information System and Computer Engineering, ISBN: 978-1-7281-3681-3, July 2019.

[10] Q. Xu, C. Tan, Z. Fan, W. Zhu, Y. Xiao, F. Cheng, "Secure Multi-Authority Data Access Control Scheme in Cloud Storage System Based on Attribute-Based Signcryption", 2018 IEEE Access, Volume 6, pp. 34051 - 34074, Jun 2018.

[11] Q. Li, Y. Tian, Y. Zhang, L. Shen, J. Guo, "Efficient Privacy-Preserving Access Control of Mobile Multimedia Data in Cloud Computing", 2019 IEEE Access, Volume 7, pp. 131534 - 131542, Sep 2019.

[12] L. Tan, N. Shi, C. Yang, K. Yu, "A Blockchain-Based Access Control Framework for Cyber-Physical-Social System Big Data", 2020 IEEE Access, Volume 8, pp. 77215 - 77226, Apr 2020.

[13] K. Riad, R. Hamza, H. Yan, "Sensitive and Energetic IoT Access Control for Managing Cloud Electronic Health Records", 2019 IEEE Access, Volume 7, pp. 86384 - 86393, Jul 2019.

[14] C. Hu, W. Li, X. Cheng, J. Yu, "A Secure and Verifiable Access Control Scheme for Big Data Storage in Clouds", 2018 IEEE Transactions on Big Data, Volume 4, Issue 3, pp. 341 - 355, Sep 2018.

[15] N. A. Fitri, M. U. H. A. Rasyid, A. Sudarsono, "Secure Attribute-Based Encryption with Access Control to Data Medical Records", 2018 International Electronics Symposium on Knowledge Creation and Intelligent Computing, ISBN: 978-1-5386-8079-7, Oct 2018.

[16] S. Dixit, K. P. Joshi, S. G. Choi, "Multi Authority Access Control in a Cloud EHR System with MA-ABE", 2019 IEEE International Conference on Edge Computing, ISBN: 978-1-7281-2708-8, Jul 2019.

[17] Zheng, T., Luo, Y., Zhou, T., & Cai, Z. (2022). Towards differential access control and privacy-preserving for secure media data sharing in the cloud. Computers & Security, 113, 102553.

[18] Y. Yang, X. Liu, R. H. Deng, "Lightweight Break-Glass Access Control System for Healthcare Internet-of-Things", 2018 IEEE Transactions on Industrial Informatics, Volume 14, Issue 8, pp. 3610 - 3617, Sep 2017.

[19] K. Edemacu, B. Jang, J. W. Kim, "Efficient and Expressive Access Control With Revocation for Privacy of PHR Based on OBDD Access Structure", 2020 IEEE Access, Volume 8, pp. 18546 - 18557, Jan 2020.

[20] S. Roy, A. K. Das, S. Chatterjee, "Provably Secure Fine-Grained Data Access Control Over Multiple Cloud Servers in Mobile Cloud Computing Based Healthcare Applications", 2019 IEEE Transactions on Industrial Informatics, Volume 15, Issue 1, pp. 457 - 468, Apr 2018.

RESEARCH ARTICLE

[21] R. Xu, Y. Chen, E. Blasch, G. Chen, "BlendCAC: A Smart Contract Enabled Decentralized Capability-Based Access Control Mechanism for the IoT", 2018 computers journal, Volume 7, Issue 39, July 2018.
[22] Vadlamudi, M. N., & Hussain, A. (2022). Design and implementation of energy-aware cross-layer routing protocol for wearable body area network. International Journal of Pervasive Computing and Communications.

Authors

Mrs. Jansi Rani Amalraj, Research Scholar (Ph.D-Part-time), Department of Computer Science, Government Arts College (Autonomous), Coimbatore, India. She is currently working as an Assistant Professor in Nirmala College for Women (Autonomous), Coimbatore, India. She has 15 years of teaching experience. She has presented papers in International and National Conferences, and has also published articles in peer reviewed journals. Her broad field of interest includes Data Mining, Data Security and Network Security.

Dr. Robert Lourdusamy, completed his Ph.D from PSG College of Technology, India and has cleared SET and NET. He was working as a member of faculty of the Computer science and Information System Department, King Saudi University, Riyadh, KSA. Currently working as an Associate Professor and Head, Department of Computer Science, Government Arts College (Autonomous), Coimbatore, India. His broad field of research and teaching interests includes Data Compression and Data Management. He has successfully guided four Ph.D. Scholars. He has authored more than 20 papers in national and international peer reviewed journals, and more than 30 papers in national and international conference.

How to cite this article:

Jansi Rani Amalraj, Robert Lourdusamy, "A Novel Distributed Token-Based Access Control Algorithm Using A Secret Sharing Scheme for Secure Data Access Control", International Journal of Computer Networks and Applications (IJCNA), 9(4), PP: 374-384, 2022, DOI: 10.22247/ijcna/2022/214501.