International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Blockchain Technology in Healthcare System for Sharing Confidential Information between Departments and Doctors

Mr. Manish Pundlik *[1], Dr. Pramod Pandurang Jadhav [2]

Submitted: 15/11/2023 **Revised**: 27/12/2023 **Accepted**: 07/01/2024

Abstract: In healthcare industry for managing private and confidential information Personal Health Record (PHR) management systems are a popular solution. These systems are mainly offering the solution of managing the access control. The implementation complexity and maintenance cost make it expensive to maintain the PHR system. The employment of Blockchain technology in order to manage access of data, which is needed to be share between multiple users, may improve the cost of implementation and running resources. Additionally, it also helps to maintain privacy, security, audit-ability, and tracking. In this paper, Blockchain-based privacy preserving data sharing system has been proposed. The aim of the proposed system is to maintaining the data access control between different doctors and departments. The system contains two parts first part contains the user definition and the personalized access rules. The second part includes the utilization of definitions and applies during the data access. The prototype of the model has been implemented and the performance of the system has been measured. The results demonstrate the efficiency and low resource consumption of the proposed privacy preserving data sharing system.

Keywords: *Blockchain, tacking, review, Blockchain in healthcare, access control in block chain, data sharing, privacy preserving*.

1. Introduction

The compromised, conventional and outdated technique of supply chain management is the biggest issue of business and technology. In traditional system the tracking and monitoring of the data movement is become complicated. Additionally sharing and managing the data access permission is also an essential requirement. In this situation, the data management and personalized access management provide an effective solution. The utilization of block chain technology to manage access control is the main aim of the solution design. This paper provides a detailed discussion of the block chain based access control management for personalize data sharing.

In this paper, we first conduct a literature review. The aim is to provide an understanding about the block chain based access management system implementation. Additionally, the different other methods of access control has also been explored. Based on the appropriately picked techniques a data sharing system has been proposed in this paper. Therefore, the working process and relevant algorithms has been explained. Next, a simulation scenario has been described to conduct the experiments and highlight the key findings. Finally the conclusion has been provided and future work plan has been discussed.

[1,2]*Department of Computer Science and Engineering*
[1] *Research Scholar, Dr. A. P. J. Abdul Kalam University, Indore*
[2] *Research Supervisor, Dr. A. P. J. Abdul Kalam University, Indore, (M.P.), India.*
E-mail Id: [1]manishpundlik71@gmail.com, [2]ppjadhav21@gmail.com
** Corresponding Author: Manish Pundlik*
Email: manishpundlik71@gmail.com

2. Related Work

This section provides the overview of essential concepts which are used for proposed system design.

2.1 Access Control

Access control is a critical data security procedure that regulates and manages who is allowed to access and use data and resources. It employs secure policies to authenticate users' identities and to confirm that they have the appropriate levels of access. The primary objective is to reduce the risk of unauthorized access, thereby safeguarding sensitive information. As a vital part of security compliance programs, access control enforces security and access rules to maintain the confidentiality of data. In the realm of computational infrastructure, various algorithms and technologies are deployed to restrict access to networks, computers, applications, files, and data. This task becomes increasingly complex and arduous in dynamic and diverse environments, which often include both on-premises systems and cloud services.

2.2 How access control works

Access controls recognize an entity, individual, or application asserting a certain access level and a corresponding set of permissible actions. Tools like Directory services, along with protocols such as Lightweight Directory Access Protocol (LDAP) and Security Assertion Markup Language (SAML), facilitate access controls by authenticating and authorizing users to access various resources like applications and servers. Organizations implement access control models tailored to

their specific needs and desired security standards to ensure protection.

2.3 Types of access control

The main models of access control are:

Mandatory Access Control (MAC): MAC is characterized by its strict and hierarchical approach, where access rights are mandated and enforced by a central authority. Each entity, whether a user or a data resource, is assigned a classification label, and access is permitted based on these labels. This model is well-suited to environments where confidentiality and classification are paramount, such as in military or government settings. The rigid structure of MAC helps prevent data leakage by ensuring that individuals with a lower security clearance cannot access information at a higher classification level. However, its inflexibility and the complexity of managing classifications can make it cumbersome in more dynamic environments. Despite these challenges, MAC's robustness makes it an essential part of national security strategies and other scenarios where data protection is of utmost importance.

Discretionary Access Control (DAC): DAC is a more flexible approach where the owners of resources (like files or data) decide who gets to access them. In this model, users can be granted access based on their identity or their group membership. The rights can be propagated down to different levels, with the resource owners or administrators having the discretion to grant, deny, or pass on permissions. While this model offers more flexibility and ease of use compared to MAC, it also poses higher risks as it relies on the discretion of individual users to manage security, making it more susceptible to accidental or deliberate security breaches.

Role-Based Access Control (RBAC): RBAC restricts system access based on a user's role within an organization. Roles are defined based on authority and responsibility, and access is granted to roles rather than individuals. This means when a user is assigned a role, they inherit all permissions assigned to that role. RBAC simplifies management and administration as roles can be updated without individually changing each user's permissions. It's particularly effective in large organizations with many users and complex access needs, ensuring that users only have access to the information necessary to perform their jobs.

Rule-Based Access Control: Rule-Based Access Control is often considered a subset or an extension of RBAC where access is not only based on user roles but also on rules defined by system administrators. These rules can include conditions like time-of-day restrictions or location-based access controls. For example, a rule might restrict access to a sensitive system outside of business hours or from external networks. This approach allows for more dynamic and flexible access control, adapting to changing circumstances and providing a more granular level of security.

Attribute-Based Access Control (ABAC): ABAC is a more dynamic model compared to the others. It uses policies that evaluate attributes (characteristics) of users, the resource, and the current environment. Attributes can include details like the user's department, the resource classification, and the time of access request. This flexibility allows ABAC to handle a wide range of scenarios and provides a fine-grained access control. It's especially useful in diverse and rapidly changing environments where access needs to be continuously adjusted based on multiple factors. However, the complexity of managing and maintaining the policies and attributes can be challenging.

2.4 Blockchain Application in Access Control

Blockchain technology is recognized for its imperviousness to corruption and its high degree of transparency. Offering comprehensive security and encryption, its decentralized nature significantly diminishes the potential for human errors and offers robust protection against hackers, making it highly relevant for Access Control systems. Traditional Access Control systems often centralize all processed data on a server, which can lead to unauthorized data access and control over client devices by providers. Entrusting security to a third party requires substantial confidence, and the transition to a different Access Control operator raises concerns about data integrity and potential tampering. Additionally, conventional Access Control is susceptible to various attacks.

Blockchain technology addresses and mitigates these concerns. It disperses information across a network rather than centralizing it on a single or few servers. Every end device operates independently, empowering end-users with the choice of what personal data to share within the network. Furthermore, compared to cloud-based systems, running a blockchain is generally more cost-effective, offering a more secure, autonomous, and economical solution for Access Control.

2.5 Recent access control systems

In this section the recent contributions has been discussed which are utilized in different applications for maintaining the security and access control using the block chain technique.

2.6 Abbreviations

The table 1 demonstrate the abbreviations used in the entire paper.

Table 1. Abbreviations used

Abbreviations	Full Form
ABAC	Attribute Based Access Control
AC	Access Contract
AI	Artificial Intelligence
CPSS	Cyber-Physical-Social System
DC	Device Contract
EOS	Enterprise Operation System
GSS	Ground Station Server
HA	Hospital Authority
IoE	Internet of Everything
IoT	Internet of Things
MIRACL	multi-precision integer and rational arithmetic cryptographic library
PC	Policy Contract
PHR	Personal health record
P2P	peer-to-peer
SMs	smart meters
UAVs	Unmanned Aerial Vehicles

2.7 Recent literature

Contemporary access control systems grapple with various issues, including third-party dependencies, inefficiency, and privacy concerns. S. Rouhani and others address these challenges and discuss the potential of blockchain technology as a solution. They provide an insightful overview of access control mechanisms and the current landscape and hurdles of blockchain-based access control systems. [1]

A. Ouaddah and colleagues suggest a blockchain-oriented framework for IoT access control. They begin by outlining a model, architecture, and specifications, followed by the introduction of FairAccess, a decentralized approach aimed at pseudonymous and privacy-centric authorization management. FairAccess introduces innovative transaction types designed to manage permissions such as granting, obtaining, delegating, and revoking access. They conclude by addressing potential limitations and exploring future possibilities. [2]

Addressing the vulnerability of centralized access, C. Yang and their team propose AuthPrivacyChain, a blockchain-enabled access control system. The approach involves using the node's address as the identity marker and redefining encrypted access permissions. The system's design encompasses comprehensive access control, authorization, and revocation processes. Finally, they implement the EOS platform to demonstrate how the system can effectively thwart hackers, prevent unauthorized resource access, and safeguard privacy. [3]

Traditional IoT access control systems, which are typically centralized, often fail to involve all relevant stakeholders in decision-making processes. To address this, M. A. Islam and team propose a permissioned blockchain-based system specifically tailored for IoT. They design and implement an Attribute-Based Access Control (ABAC) system within the Hyperledger Fabric blockchain, utilizing its smart contracts and distributed consensus mechanisms to facilitate a more distributed form of access control. The system's efficacy is validated through performance evaluations. [4]

H. Liu and colleagues introduce fabric-IoT, an access control system designed for large-scale IoT environments, which struggles with centralized control systems. This system is built upon the Hyperledger Fabric blockchain framework and integrates ABAC. It features three types of smart contracts: Data Control (DC) for storing and querying URLs of data from devices, Policy Control (PC) for managing ABAC policies, and Access Control (AC) for implementing the access control itself. This combination of ABAC and blockchain technology enables decentralized, fine-grained, and dynamic access control, proven to maintain high throughput and efficient consensus. [5]

S. Namane and team tackle the challenge of ensuring effective access control in IoT, a task complicated by traditional technologies' inadequacy in large-scale and distributed networks. They propose a taxonomy for blockchain-based access control systems, categorizing them as either partially or fully decentralized. This framework is applied to various IoT applications, analyzing each according to specific criteria. [6]

B. Bera and associates develop a novel access control protocol for IoT-enabled smart grids, named DBACP-IoTSG. This protocol ensures secure data transfer to service providers through a peer-to-peer network, where nodes are tasked with creating and adding blocks to the blockchain. The system is analyzed for its resistance to various attacks, with findings indicating enhanced security features, improved security, and reduced costs. The protocol's computational efficiency was also tested through implementation. [7]

T. T. Thwin and team address the limitations of blockchain and introduce a blockchain-based Personal Health Record (PHR) model. This model utilizes blockchain's inherent tamper resistance, along with proxy re-encryption and other methods, to ensure privacy. It offers detailed and adaptable access control, the ability to revoke access, audit capabilities, and strong resistance to tampering. Their

security assessment confirms the model's robustness, and performance metrics indicate its superior functionality. [8]

Y. E. Oktian and colleagues present Border-Chain, a blockchain-based access control framework designed to enhance the security of IoT networks. This framework ensures two key aspects: first, it confirms that IoT users and services are interacting with authenticated gateways and devices; second, it generates access tokens for querying IoT resources, ensuring that only approved requests are authorized. This protocol is implemented as a smart contract to facilitate collaboration among numerous IoT entities and is operationalized through Node-JS applications linked to Ethereum. The efficacy of Border-Chain in managing authentication and authorization processes is demonstrated. [9]

Y. Chen and team tackle the issue of centralized medical data sharing, traditionally dependent on a trusted intermediary, by proposing a new data sharing scheme. This approach utilizes K-anonymity and searchable encryption within a consortium blockchain environment, specifically Hyperledger Fabric, to secure encrypted data search. The system's chain-code, an attribute-based access control smart contract, ensures that only authorized users can access the data, maintaining privacy. The prototype's implementation attests to the scheme's security, scalability, and practical performance. [10]

CPSS big data typically relies on centralized access control, vulnerable to tampering. To address this, L. Tan and others introduce a blockchain-based access control system named BacCPSS. In this system, the blockchain node's account address serves as the identity marker for data access. Access permissions are redefined, securely stored, and coupled with designed processes for authorization, revocation, and auditing, all secured with lightweight symmetric encryption. The results affirm BacCPSS's viability, effectiveness, and ability to ensure secure access. [11]

S. Saha and team craft a new access control mechanism for hospitals using a private blockchain. This scheme is designed to be resilient against a range of attacks while offering enhanced security and functionality at reduced communication and computational costs. [12]

B. Bera and colleagues propose ACSUD-IoD, an access control scheme specifically for detecting and mitigating unauthorized UAV activities. This system stores transactional data, including both regular and secure drone data as well as anomalous data indicative of unauthorized UAVs. Their analysis confirms the scheme's robustness, supported by cryptographic experiments demonstrating its efficacy and resilience. [13]

In the IoE realm, B. Bera and team discuss the potential of blockchain in mitigating and detecting malicious attacks through access control. They explore various attacks, the evolution of blockchain technology, and propose an AI-enhanced blockchain-based access control system for monitoring and mitigating these threats. The effectiveness of this system is validated through implementation, measuring processing times across different numbers of mined blocks and transactions. [14]

C. Gan and associates focus on the application of blockchain in eHealth systems, emphasizing patient empowerment. Patients assume a supervisory role, allowing institutions to use their medical data while retaining control over it. This approach aims to protect patient rights without hindering medical research and diagnosis. A blockchain-based access control system is proposed to facilitate this, with a detailed case study on Ethereum illustrating its application. [15]

3. Review Summary

In this survey some recently published research articles have been selected. These articles are based on the block chain technology to implement the access control. The implementation of block chain in access control may help in dealing with single-point failure, privacy and access control. In these systems the block chain is being used to store the information to achieve distributed security. Additionally, in order to implement access control it is required to implement access control policies. However, there are a number of approaches available to deal with the authentication and authorization problem. But in distributed scenario ABAC has own importance. Therefore, in this paper an Attribute Based Encryption (ABE) technique has been developed to manage the access control for file sharing in medical scenarios. The next section discusses the proposed method in order to manage the privacy using ABE.

4. Proposed Work

Medical records are often deeply private and sensitive, with their disclosure potentially harming the data owner's reputation. To enhance the security and privacy of medical data sharing, a novel access control method utilizing Attribute-Based Encryption (ABE) has been introduced and is elaborated upon in this section. Recently, there's been a surge in the popularity of medical data management systems, particularly as the limitations of centralized systems have spurred a shift towards more distributed frameworks. These distributed systems adeptly host and share sensitive information, enforcing defined policies. Blockchain technology further fortifies this approach by validating and authenticating data and entities, managing access control, and ensuring secure data storage and computation.

In the realm of medical systems, servers maintain extensive datasets for management and sharing purposes. Access to this data must be strictly limited to authorized users, each with varying roles and permissions. Often, patients desire to

set their own access policies to maintain control over their privacy. To address this need, this paper proposes a secure data sharing and access control mechanism. Attribute-Based Encryption (ABE) is presented as a comprehensive solution for public key encryption, allowing users to encrypt and decrypt messages based on their attributes, thereby safeguarding sensitive information from unauthorized access.

In our work, we introduce Attribute-based Access Control for Secure Sharing (ABAC-SS), a system designed to ensure both the security and privacy of data sharing. This method employs cryptographic security based on the user's attributes. Within a data sharing system, access control is enforced through access policies and user credentials. These policies delineate user roles within groups and dictate the permissible actions for each user. Thus, access control is established by:

$$[\text{User list}, \text{Access policy}]$$

Access control is primarily composed of two elements: the system user list and the corresponding access policies. The user list is dynamic, fluctuating with changes in the user's group membership. The processes of revoking group members or adding new ones can significantly increase the workload for key managers. In situations where user attributes are used directly, adding new members or revoking existing ones directly affects key generation, necessitating frequent key updates. To address these challenges without resorting to a third-party trusted authority, a new solution has been proposed. This solution aims to alleviate the burden on key managers by reducing communication overhead and minimizing the need for frequent key generation and updates.

4.1 Proposed Methodology

The objective of the proposed work is to enhance security while facilitating data sharing and access control. This work is divided into two main modules:

1. **Authentication and Authorization:** This initial phase utilizes user credentials to define a user profile. Through this profile, the system recognizes the user and determines their access capabilities and associated user attributes. Once the user attributes are obtained, cryptographic operations are performed to further secure the process.
2. **Data Encryption and Sharing:** This module outlines the procedures involved in safeguarding data files and delineates the mechanisms for sharing medical documents among various user groups. It focuses on ensuring the confidentiality and integrity of the data as it is transmitted between different parties.

4.1.1 Authentication and authorization

Figure 1 presents an overview of the proposed technique for secure medical document sharing. The diagram illustrates the process of authentication and authorization for secure sharing of medical documents. It also provides a detailed depiction of the system's components as follows:

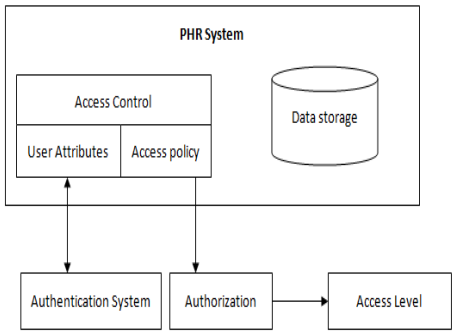

Fig 1. Authentication and authorization process

1. **User Credentials:** Access to the secure data sharing system requires user registration. During this process, users provide private attributes or information, which are used to generate login credentials. These credentials enable user access to the system.
2. **User Database:** This secure data storage has two parts for managing access control. The first part consists of user attributes, which are the initial user information stored in the blockchain and provided during registration. The second part is the user's access policy, with each user assigned an access code that defines their access level based on their role.
3. **Authentication:** This process verifies a user's identity to grant secure access to the system. The user enters their login credentials, which, if verified by the blockchain, grants them access to the system. Upon gaining access, user profiling begins, as explained in the subsequent section.
4. **Authorization:** Once a user is authenticated, they gain access to the system. The system then retrieves the user's access permissions from the access policies. It combines a randomly selected user attribute with an access policy, determining the user's access level to the system.
5. **Attribute:** The combination of a randomly selected user attribute and the access policy flag is organized into a string, serving as the user attribute for further cryptographic security implementation.

Once the user attribute is generated, the user can use the system to upload, download, and share their confidential medical documents with the Personal Health Record (PHR) system. Additionally, users can share common documents among different users with varying access levels.

4.1.2 Data Encryption and Secure Sharing

Figure 2 illustrates the cryptographic process employed for secure document storage and sharing. As depicted in the diagram, when a user intends to store or distribute a document to an individual or a group, a cryptographic method is applied to ensure the document's secure hosting. A key input parameter in this process is the 'Attribute,' which is generated in a previous module and comprises a combination of the user's randomly selected attribute and the access policy flag. Essentially, this attribute acts as a signature of the actual file owner, encompassing both access permissions and private information. Each system user possesses a unique set of these signatures, which are employed when sharing a file with another user or group, providing a secure and authenticated means of document distribution.

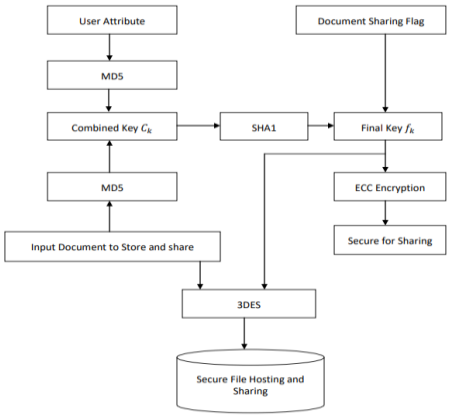

Fig 2. data sharing and cryptography

The third system parameter is sharing flag. That is used to include the sharing permissions. Additionally, this flag has also used to track the data movement. It is a fixed length string of 8 bits. It is used to identify the access level of the user document. In order to understand this practice let the user want to store the data for personal use then the sharing flag becomes 00000001, or for one to one sharing it becomes 00000010 and so on. These bits prepared by the system designer to map the strings to access permission. Next, we utilize the MD5 hash generation algorithm. The MD5 generates any length of string and produce the 128 bit hash as output. The input document which is needed to be secure and share has utilized with the MD5 algorithm to generate 128 bit hash key, which is denoted here has D_k. Additionally the user attribute which is previously generated has also being used with the MD5 algorithm to generate a hash key, which is termed as A_k.

The D_k *and* A_k both the hash key has combined as a string which produces a combined key $C_k = A_k + D_k$. This string has a length 256 bits. Further, we utilized the SHA1 algorithm which is also a hash generation algorithm. That algorithm is able to generate stronger hash than MD5 algorithm. This algorithm generates the 160 bit of hash key. The 256 bit hash C_k is passed on the SHA1 algorithm to generate 160 bit hash code. Next, 160 bits is used for preparing the final encryption key f_k. Therefore, 160 bits and 8 bit sharing flag are combined to generate the complete 168 bits as final encryption key. **The ECC algorithm has used here to secure the final encryption key. Thus,** f_k is the input message to encrypt with the ECC (elliptic curve cryptography). The ECC algorithm is asymmetric key encryption, which generate two keys i.e. private and public key. The encryption algorithm encrypts the data using public key and private key has used to decrypt the document.

In order to understand the ECC working suppose Q= public key, d= private key, P= a point in curve, K= random number, and M= original message. Then, we get the two cipher text blocks which are denoted using $C_1$and C_2.

$$C_1 = K.P$$

$$C_2 = M + KQ$$

The encryption process input file convert into byte array and then set x_1, y_1, x_2, y_2, for curve generation. Now get points on the curve and generate a random no. d from 1 to N. Calculate public key with the help of d and p and generate cipher text C_1 and sequence of C_2. Using the above equations the message can be defined as:

$$M = C_2 - d * C_1$$

$$M = C_2 - KQ$$

At the network scenarios the cipher C_1 and C_2 is sanded on network and the recovery of the original message can be found using the below given expression.

$$M = C_2 - d * C_1$$

$$C_2 - d * C_1 = (M + KQ) - d * (K * p)$$

In next step,

$$C_2 - d = M + KQC_2 = M + KQ$$

$$M = M$$

The 168 bit key is encrypted for secure key exchange. That is provided to any third party for the future data decryption. Finally, the input medical document is secured and shared by using the 168 bit key and triple DES encryption. The outcome of the 3DES is used for sharing or hosting. This section provides understanding about the proposed system for securing the data. In addition, for providing security during the file sharing and exchange among different users a detailed step of process is described. In next section the proposed system is implemented and performance has evaluated.

4.2 The pseudocode provided outlines an ECC algorithm

Step 1: Initialize the System

1. Select an appropriate Elliptic Curve (EC).
2. Choose a Base Point (G) on the curve.
3. Determine the order (n) of the base point.

Step 2: Generate Key Pairs for Users

1. For each user (department or doctor): a. Select a random integer (private key) within the range [1, n-1]. b. Calculate the public key by multiplying the private key with the base point G (publicKey = privateKey * G).

Step 3: Register Users with the Blockchain Network

1. For each user: a. Authenticate the user and ensure integrity checks. b. Add the user's public key to the blockchain network.

Step 4: Encrypt Information for Sharing

1. To encrypt information for a receiver: a. Calculate the shared secret by multiplying the sender's private key with the receiver's public key. b. Encrypt the information using the shared secret.

Step 5: Decrypt Received Information

1. To decrypt received information: a. Calculate the shared secret by multiplying the receiver's private key with the sender's public key. b. Decrypt the information using the shared secret.

Step 6: Share Information Securely

1. When a sender wants to share information: a. Encrypt the information using the receiver's public key (from Step 4). b. Add the encrypted information to the blockchain with appropriate access controls, tagging it with the receiver's public key.

Step 7: Access and Decrypt Information from the Blockchain

1. When a receiver wants to access information: a. Retrieve the encrypted information from the blockchain using their public key. b. Decrypt the information using their private key (from Step 5).

Step 8: Main Execution Flow

1. Initialize the system.
2. Generate key pairs for all participating entities (departments and doctors).
3. Register each entity in the blockchain network.
4. When a department wants to share confidential information with a doctor: a. The department encrypts the information using the doctor's public key. b. The encrypted information is added to the blockchain.
5. When the doctor accesses the information: a. They find the relevant data block in the blockchain using their public key. b. They decrypt the information using their private key.
6. (Optional) Print or log the retrieved information for verification.

Step 9: Start the Process

1. Execute the main function to start the information sharing and retrieval process.

5. Results Analysis

The proposed access control and secure data sharing technique is evaluated in this section. In this context, different parameters are measured by experimental analysis and results are prepared. The performance has measured for computational complexity. Thus, memory usage has been measured and compared with a traditional access control technique. The memory used to process input data using cryptographic algorithm is known as encryption memory. The memory requirements are measured using:

$$Consumed\ Memory = Total\ Memory - Free\ Memory$$

Table 2. Performance of the proposed access control model Encryption and Decryption memory

S. No.	Encryption Memory (KB)		Decryption Memory (KB)	
	SDSA = Proposed Secure Data Sharing Approach, KM = Existing Technique based on key manager			
	SDSA	**KM**	**SDSA**	**KM**
1	11005	12794	12951	14562
2	11061	12671	14891	15521
3	14904	15527	13162	15557
4	18014	20198	13465	14413
5	11301	13829	13784	14928
6	13194	15625	16132	18837
7	12689	14772	13041	15521

Table 3. Performance of the proposed access control model Encryption and Decryption time

S. No.	Encryption Time (MS)		Decryption Time (MS)	
	SDSA = Proposed Secure Data Sharing Approach, KM = Existing Technique based on key manager			
	SDSA	KM	SDSA	Km
1	402	610	225	372
2	498	708	276	396
3	552	742	309	432
4	512	701	385	442
5	601	819	339	478
6	664	847	367	505
7	701	908	441	528

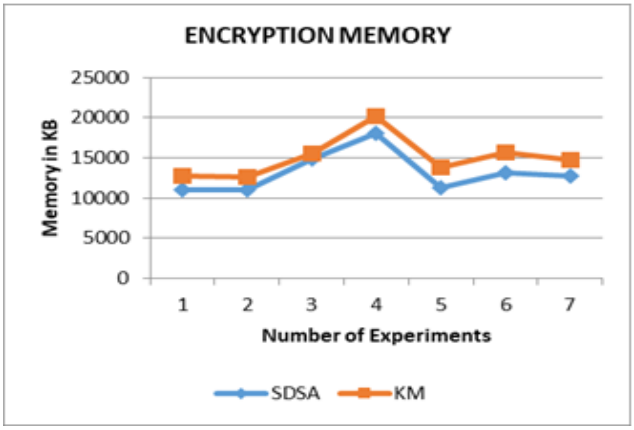

Fig 3. Shows the performance of access control model in terms of Encryption Memory

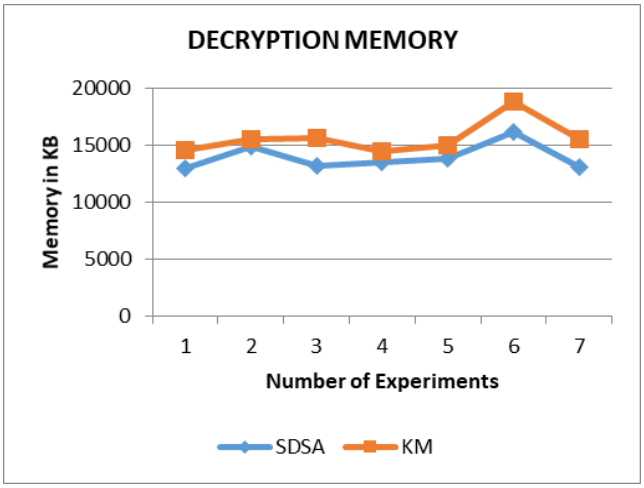

Fig 4. Shows the performance of access control model in terms of Decryption Memory

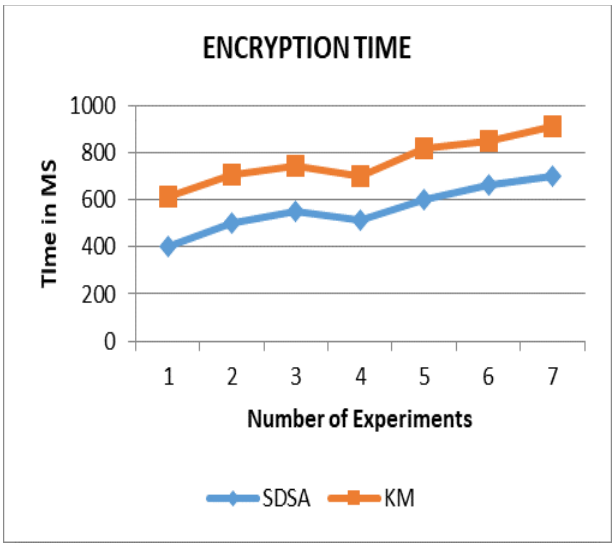

Fig 5. Shows the performance of access control model in terms of Encryption Time

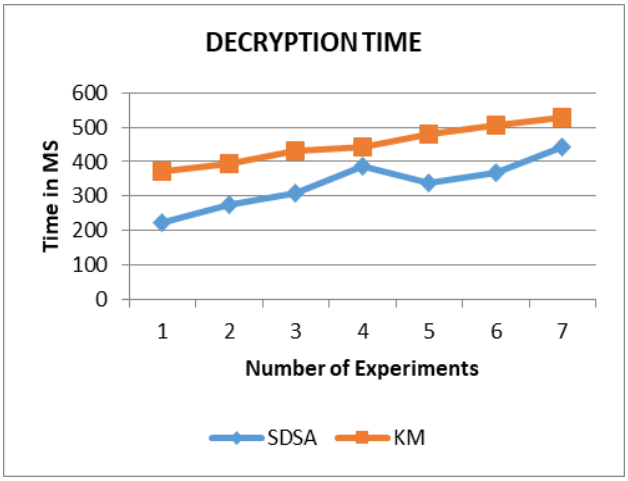

Fig 6. Shows the performance of access control model in terms of Decryption Time

Figure 3 and Table 2 display the memory consumption of the proposed attribute-based encryption technique, which is implemented for access control management. Table 2 provides observed values from experiments, while Figure 3 offers a line graph representation. On the graph, the Y-axis represents the main memory used, and the X-axis denotes the number of experiments, with memory measurements in kilobytes (KB). The blue line indicates the performance of the proposed technique, while the red line depicts the performance of a traditional technique. The results demonstrate that the proposed algorithm is more memory-efficient than the conventional key manager-based approach.

Decryption memory, the memory required to restore original data from encrypted text, is calculated by the difference between total assigned memory and the amount of free memory. Table 2 and Figure 4 detail the main memory usage for both the proposed and traditional

techniques. In these diagrams, the X-axis includes experiments with varying file sizes, and the Y-axis indicates the required memory. The findings reveal that the proposed method uses less memory than the traditional approach. Furthermore, the time taken to perform encryption, known as encryption time, is documented in Figure 5 and Table 3. This metric is also calculated and compared to showcase the efficiency of the proposed system.:

$$\text{Time consumed} = \text{End Time} - \text{Start Time}$$

Figure 6 and Table 3 present a comparative analysis of the time consumption for both the proposed and existing approaches. In the diagram, the X-axis lists various experiments with different file sizes, while the Y-axis represents the time taken for file storage. The results indicate that the proposed system is more time-efficient for file storage compared to the traditional approach. The time consumed is also dependent on the data volume being processed. Furthermore, the proposed model significantly enhances data security compared to conventional data sharing techniques.

The time required to revert encrypted data back to its original form, known as decryption time, is also evaluated. Figure 6 and Table 3 detail the system's performance in terms of decryption time, measured in milliseconds. The X-axis shows the number of experiments conducted, and the Y-axis indicates the time taken for decryption. The findings suggest that although encryption time might be higher, the decryption time remains within an acceptable range. Additionally, the proposed approach improves the efficiency of secure file sharing time usage when compared with traditional methods.

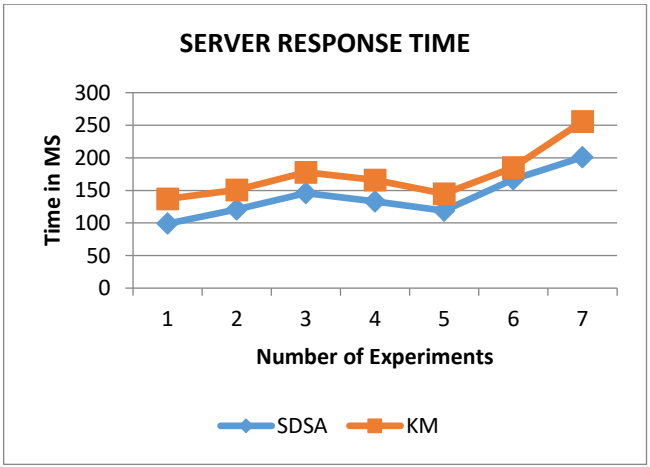

Fig 7. Response Time

The server response time, which refers to the duration the server takes to process and respond to user requests, has been analyzed. The server operates a series of scripts that process user requests and generate results. The time taken for these scripts to execute and produce outcomes is known as the server response time. It's important to note that this response time is exclusive of any encryption or decryption time involved. The performance of the proposed technique regarding server response time is illustrated in Figure 7 and Table 4. A comparative line graph demonstrates that the proposed approach yields a quicker response compared to the traditional method. On this graph, the x-axis represents the number of tests conducted while the y-axis indicates the time required, reflecting the computational overhead. According to the findings, the response time is independent of the document size and is primarily influenced by the server's current workload where the data is hosted.

Table 4. Response Time

Experiments	SDSA	KM
1	99 MS	137 MS
2	121 MS	151 MS
3	146 MS	178 MS
4	133 MS	166 MS
5	119 MS	145 MS
6	167 MS	185 MS
7	201 MS	256 MS

6. Conclusion and Future Work

In recent years, the utilization of medical health record management systems has been increased. Due to large data collection, processing, analysis and integration make it more complex for design and implementation. Moreover, it the security and privacy management is also a concern in traditional medical health record management systems. Therefore, these systems are now being updated by using the smart way of security namely blocks chain technology. In this presented work a demonstration of block chain technology has been discussed. The paper includes a method to perform authentication and authorization of medical health record in shared data storage. The user can apply the custom permissions to share the file to an individual or a group of users.

First the user has been register with the system to generate the login credentials and their signature. Then, the user can utilize the secure data sharing algorithm to add a new file or download file from the secure storage. When a file has been stored into the storage, the signature is also included with the associated file. This signature has used to recognize the identity of the authorized user. In addition, this signature is prepared by using the part of user personal attributes therefore this technique has named here as attribute based encryption. On the other hand, a unique technique for user authorization has been done, in which the private key is being used for recovering the shared document. This key is composed with the user attribute and the document access

level codes. Additionally to secure sharing the ECC algorithm has been used.

The key when utilized to access the file, then the first the encrypted key is deciphered through the ECC algorithm. Then, the components of access level and user identity are identified. Additionally the key is used with 3DES algorithm to retrieve file with the identified access levels. The proposed concept has been implemented using the JAVA technology and their performance has been discussed. Based on the experiments and comparative study we found the proposed technique is efficient and secure technique to prevent the authorized access attack in medical data sharing system.

Author contributions

Mr. Manish Pundlik: Conceptualization, Methodology, Software, Field study, Data curation, Writing-Original draft preparation, Software, Validation., Field study. **Dr. Pramod Pandurang Jadhav:** Visualization, Investigation, Writing-Reviewing and Editing.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] S. Rouhani, R. Deters, "Blockchain based access control systems: State of the art and challenges", Web Intelligence '19, Thessaloniki, Greece, Association for Computing Machinery, October 14–17, 2019,

[2] A. Ouaddah, A. A. Elkalam, A. A. Ouahman, "FairAccess: a new Blockchain-based access control framework for the Internet of Things", Security And Communication Networks, Security Comm. Networks 2017

[3] C. Yang, L. Tan, N. Shi, B. Xu, Y. Cao, K. Yu, "AuthPrivacyChain: A Blockchain-Based Access Control Framework With Privacy Protection in Cloud", Special Section on Blockchain Technology: Principles and Applications, Vol. 8, 2020

[4] M. A. Islam, S. K. Madria, "A Permissioned Blockchain based Access Control System for IOT", 2019 IEEE International Conference on Blockchain (Blockchain)

[5] H. Liu, D. Han, D. Li, "Fabric-iot: A Blockchain-Based Access Control System in IoT", Special Section on Blockchain-Enabled Trustworthy Systems, Vol. 8, 2020

[6] S. Namane, I. B. Dhaou, "Blockchain-Based Access Control Techniques for IoT Applications", Electronics 2022, 11, 2225

[7] B. Bera, S. Saha, A. K. Das, A. V. Vasilakos, "Designing Blockchain-Based Access Control Protocol in IoT-Enabled Smart-Grid System", IEEE Internet of Things Journal, Vol. 8, No. 7, April 1, 2021

[8] T. T. Thwin, S. Vasupongayya, "Blockchain-Based Access Control Model to Preserve Privacy for Personal Health Record Systems", Hindawi Security and Communication Networks Volume 2019, Article ID 8315614, 15 pages

[9] Y. E. Oktian, S. G. Lee, "BorderChain: Blockchain-Based Access Control Framework for the Internet of Things Endpoint", VOLUME 9, 2021

[10] Y. Chen, L. Meng, H. Zhou, G. Xue, "A Blockchain-Based Medical Data Sharing Mechanism with Attribute-Based Access Control and Privacy Protection", Hindawi Wireless Communications and Mobile Computing Volume 2021, Article ID 6685762, 12 pages

[11] L. Tan, N. Shi, C. Yang, K. Yu, "A Blockchain-Based Access Control Framework for Cyber-Physical-Social System Big Data", Special Section on Cloud- Fog-Edge Computing in Cyber-Physical-Social Systems (CPSS), Vol. 8, 2020

[12] S. Saha, A. K. Sutrala, A. K. Das, N. Kumar, J. J. P. C. Rodrigues, "On the Design of Blockchain-Based Access Control Protocol for IoT-Enabled Healthcare Applications", 978-1-7281-5089-5/20/$31.00 ©2020 IEEE

[13] B. Bera, A. K. Das, A. K. Sutrala, "Private blockchain-based access control mechanism for unauthorized UAV detection and mitigation in Internet of Drones environment", Computer Communications 166 (2021) 91–109

[14] B. Bera, A. K. Das, M. S. Obaidat, P. V. kumar, K. F. Hsiao, Y. H. Park, "AI-Enabled Blockchain-Based Access Control for Malicious Attacks Detection and Mitigation in IoE", IEEE Consumer Electronics Magazine, 2162-2248, 2020.

[15] C. Gan, A. Saini, Q. Zhu, Y. Xiang, Z. Zhang, "Blockchain-based access control scheme with incentive mechanism for eHealth systems: patient as supervisor", Multimedia Tools and Applications, Springer Nature 2020