International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 02 February 2024
Page No: 309 - 320
https://irjaeh.com

# Survey of Secure Data Access Control Models in Cloud Computing for EHR

*Samadhan Shivaji Palkar[1*], Dr. Raghav Mehra[2], Shekhar Dasharath Jalane[3]*

*[1]PhD Scholar, Computer Science & Engineering, Mangalayatan University, Aligarh, Uttar Pradesh, India*

*[2] Professor, Computer Science & Engineering, Mangalayatan University, Aligarh, Uttar Pradesh, India*

*[3] Assistant Professor, AIML, KIT's College of Engineering (Autonomous) Kolhapur, Maharashtra, India*

***Email id:*** *20221417_samadhanshivaji@mangalayatan.edu.in[1], dr.raghavm@gmail.com[2], jalane.shekhar@kitcoek.in[3]*

****Corresponding Author Orcid ID:*** 0009-0001-6323-9006

## Abstract

*Today cloud computing is the first choice of many individuals and different organizations. Computing services offered by different CSP's are available as per need and the requirement. Most of the healthcare organizations are using cloud services for transmitting, storing and processing electronic health records (EHR) of patients. Patient's health record is sensitive and there is possibility of violation of privacy by CSP's. Data access control is one of the best mechanisms to address security issues in cloud computing and ensure the safety, reliability of the system and privacy of the user data. Existing surveys on access control mechanisms in cloud computing focus on all traditional centralized models. However, decentralized access models like block chain with traditional access control model is also used now days for ensuring privacy of EHR. This paper takes the detailed of reviews such existing access control mechanisms in cloud computing, based both types of access control models. Also provides comparisons on each model's advantages and limitations, and discusses the challenges of, and future research direction for access control.*

**Keywords:** *Cloud computing; access control; cloud security; centralized; decentralized; Machine learning; Electronic health record.*

## 1. Introduction

Recently, many companies and organizations have adopted cloud computing as the foundational technology for their information technology (IT) needs, leveraging its advantages such as interoperability, mobility, and cost-effectiveness. Cloud computing involves the virtualization of the entire IT infrastructure, encompassing hardware, software, and [1] networking. This integrated infrastructure is designed to deliver cloud services to end-users through the Internet. Securing electronic health data in a cloud environment poses a significant challenge due to the distinctive characteristics of cloud computing, such as multi-tenancy and resource sharing elasticity. To address this challenge, an access mechanism is essential to ensure the confidentiality, integrity, and availability of cloud data. Access control serves as the traditional and primary line of defense in the system, allowing authorized users to access protected electronic health information and system resources while denying access to unauthorized users. In the realm of cloud computing, access control enables users to access specific applications, safeguard data privacy, and protect the resources of cloud users. Moreover, it assigns the appropriate access permissions for each level of service. Access control in the cloud can be categorized into centralized and decentralized models. The former relies on a central authority to manage access policies and key generation, while the latter depends on multiple authorities to handle keys

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 02 February 2024
Page No: 309 - 320
https://irjaeh.com

and store encrypted resources and access policies.

### 1.1 Motivation

The typical characteristics of proposed access control models are generally twofold [15]. Firstly, they rely on one or more centralized centers to store or oversee various data elements, such as user identities, cryptographic keys, and access rights. Secondly, all three cloud service models necessitate a trustworthy cloud system administrator to oversee access rights and the authorization process for other users. The first vulnerability lies in a potential attack on the centralized center, leading to a single point of failure that could compromise patient data and allow the attacker to manipulate data access and pilfer resources. The second vulnerability arises when an untrusted cloud security administrator exploits their authority to illicitly access resources or tamper with the access rights of legitimate users, resulting in a loss of confidence and trust in the cloud. To mitigate these issues and ensure [8] the confidentiality of patients' health records, researchers are exploring new approaches to decentralize access control in cloud storage. Blockchain technology is one such example. Although managing blockchain techniques is more complex compared to centralized access control, they offer enhanced security in key distribution and file information. However, it's worth noting that blockchain tends to be slower than centralized access control due to its inherent design. This study therefore reviews and analyses the relevant literature on existing access control mechanisms in cloud computing that concern centralized and decentralized access control models, and assesses their advantages and disadvantages. Also techniques used so far for improving effectiveness of data access control techniques is also highlighted. The rest of this paper is organized as follows: Section 2 introduces the background to access control models, blockchain technology, and smart contract techniques. Section 3 presents the existing solutions for access control in centralized and decentralized models in cloud computing, machine learning techniques used for improving overall effectiveness while Section 4 discusses the challenges of, and potential future research direction for access control models in cloud computing. Finally, Section V concludes the paper.

## 2. Background

### 2.1 Access Control

This subsection presents the basic of access control. Basic Element There are three elements involved in the access control model, namely subject, object, and access rights. The subject is the entity (users or applications) that can access an object, while the object is a resource, such as files or directories that requires access. Lastly, access rights include the access policy, such as read or write, from the subject to the object. Traditional access control models in traditional access control, access rights are typically based on predefined rules and roles. DAC (Discretionary Access Control) is a common traditional model where the resource owner has discretion over who is granted access. RBAC (Role-Based Access Control) assigns permissions to roles, and users are assigned to these roles based on their job responsibilities. Encryption based access control Encryption is a technique used to secure data by converting it into a code that can only be deciphered with the appropriate key. In encryption-based access control, access to resources is often determined by possession of the correct encryption key. Access is granted to those who have the necessary decryption keys, providing an additional layer of security beyond traditional access control methods. This approach is particularly effective for protecting data during transmission or storage. In summary, access control models define how permissions are managed, traditional access control relies on predefined rules and roles, while encryption-based access control leverages encryption keys to regulate access. Combining these approaches can enhance the overall security of a system by providing multiple layers of protection.

### 2.2 Block Chain Technology and The Smart Contracts Technique

This subsection presents the basic characteristics of blockchain technology and the smart contracts technique. A blockchain is a distributed database or ledger shared among a computer network's nodes. They are best known for their crucial role in cryptocurrency systems for maintaining a secure and decentralized record of transactions, but they are not limited to cryptocurrency uses. Blockchains can be

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 02 February 2024
Page No: 309 - 320
https://irjaeh.com

used to make data in any industry immutable [12]. It is like a database that holds every transaction as a record. Furthermore, the block chain has multiple properties as listed in [7] such as:

**Decentralization:** No single entity controls the entire block chain. Instead, multiple participants (nodes) contribute to and validate the transactions Transparency: All participants in the network have access to the same information. Transactions are visible and verifiable, enhancing trust. Immutability: Once a block is added to the chain, it is extremely difficult to alter. This ensures the integrity of the recorded transactions. Security: Cryptographic tech niques, consensus algorithms, and decentralization contribute to the security of the block chain network

Smart contracts are self-executing contracts with the terms of the agreement directly written into code. They run on a blockchain and automatically enforce and execute the terms of the contract when predefined conditions are met. Key characteristics of smart contracts include:

- **Automation:** Smart contracts automate the execution of contract terms, reducing the need for intermediaries and minimizing the risk of errors or fraud.
- **Decentralization:** Like other blockchain transactions, smart contracts operate on a decentralized network, ensuring transparency and security.
- **Trust:** The code governing smart contracts is visible and tamper-proof, providing trust among parties involved, as the execution is predetermined and cannot be altered.
- **Efficiency:** Smart contracts streamline processes by automatically executing actions when conditions are met, reducing the time and resources required for traditional contract execution

Smart contracts find applications in various fields, such as legal agreements, financial transactions, insurance, and more. Ethereum is a notable blockchain platform that supports the creation and execution of smart contracts.

## 3. Access Control Models in Cloud Computing

This section presents the current scenario in centralized and decentralized access control solutions in cloud computing.

### 3.1 Centralized Access Control

Liu, Yi et. al. [22] suggests a mobile cloud computing online/offline CP-ABE approach to reduce the computational overheads of electronic health records (EHR). Major processing is enabled by offline encryption, which also guarantees a reduction in the com putational burden of online encryption. The data encryption in the suggested approach is divided into two stages: online and offline encryption. The Internet of Things (IoT) device that owns the EHR encrypts the data during the offline encryption process to create intermediate ciphertext, which is then utilized during the online encryption. When the data is prepared for online en cryption, the owner specifies the access policy and sends the final ciphertext to the cloud. In terms of the expenses associated with online encryption and decryption, the suggested system is better than others. But the compromise between the computation time and storage space should be addressed. Lin, Li et. al. [20] proposes the use of PriGuarder. The cloud data privacy protection technique known as PriGuarder. Three steps make up the suggested approach: DU registration, data production, and DU access. There are two ways to access each stage: direct and anonymous. The operation takes place between the DU and the CS in the direct access mode. When employing the anonymous access mode, the transaction takes place between the DU and a trusted third party (TTP). The TTP uses an attribute fuzzy grouping (AFG) to transform the DU data, identity, or access policy, and then delivers the resultant result to the CS. The DU selects the access mode to create the DU identity during DU registration. The DO then provides their data, a statement of policy rights, and the selected access method during the data generation stage. Ultimately, depending on the chosen access method, the DU is verified during the data access step. The AFG approach, which safeguarded user privacy, is PriGuarder's primary strength. The study, however, ignores the possibility that a malevolent TTP could violate users' privacy. The linked attributes are often categorized into distinct attribute trees using the hierarchy CP-ABE. Li, Jiguo et. al. [17] offer an effective extended file hierarchy CP-ABE technique (EFH-CP-ABE) that solves the

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 02 February 2024
Page No: 309 - 320
https://irjaeh.com

problem of encrypting several files with the same level of access. The DO, CA, CS, and DU are the four entities that make up the EFH- CP-ABE scheme. Three keys are generated by the CA: a public key, a private key for each user, and a secret master key. The study's findings show that users of cloud storage can benefit from security and flexibility provided by the access control mechanism. However, the system has to be improved in terms of the calculation time needed for encryption and decryption. Jamal, Fara et. al. [13] proposes a workaround that offers an effective way to access data and a backup authority node in case of failure. There are seven entities in this agent-based ABE access control technique, which uses the encrypted policy ABE mechanism. The certifying authority initially performs the role of a certificate issuing agency. Second, there are several attribute authorities, and it is the duty of each to provide the approved DUs and the DO with the encryption and decryption keys. Third, in order for the server site agent to retrieve the user's requested data from the cloud storage, the client [21] site agent transmits the desired data to them. Fourth, the server-site handles the server site agent queries. Fifth, the DU and DO receive computing resources and storage services from the client storage server. Sixth, in the event of a certificate authority failure, the author- it's back node is activated upon request. This is accomplished by the authorized agent monitoring the neighboring nodes. Ultimately, the request handler employs shared cache memory scheduling to [26] process data access. The suggested method is safe from threats such as collusion, malware insertion, identity theft, and certifying authority failure. Furthermore, there is an improvement in the reading response times while gaining access to cloud data. Still, there was a requirement for a secure procedure when choosing the backup authority node. Anilkumar, Chunduru et. al. [5] suggest the PB-FGAC method, which combines fine-grained access control (FGAC) with predicate- based access control (PBAC) for Swift object storage on the Open- Stack cloud platform. In addition to helping to prevent access to the entire object, PBFGAC offers fine-grained access control to a predicate, which is a component of the object. The user made a request to the OpenStack cloud, which was handled by the NOVA component (which handles compute instances). The request was then sent to the policy engine service and the object attribute storage services, in that order. Both object-level and user-level access are included in every policy. The PBAC service then assists the user in gaining access to the necessary specified data or predicate. [28] The study's findings show that compared to alternative settings with a default access control policy, such the cloud platforms from Microsoft Azure, Amazon Web Services (AWS), and Open Stack, the model offers more restricted access control. Nevertheless, the suggested paradigm is limited to the JavaScript Object Notation (JSON) document, and handling its confidentiality is also necessary. Ghaffar, Zaidi et.al. [11] Talk about the security risks related to data management activities in centralized cloud storage, including the absence of a shared data configuration, insider attacks, and a data access verification model. They suggest a modified paradigm that makes use of a proxy key mechanism for data access and sharing in cloud storage. This paradigm comprises three phases: data access, data storage, and a data sharing system, in addition to three entities: the DO, DU, and CS. The user and cloud server's authentication mechanisms are involved in the data access, and they subsequently exchange session keys in order to communicate with one another. [30] Users can share encrypted files or data with other users they like by using the storage services provided by the data storage. Once the user has been authorized, the data sharing system looks for the encrypted file using keywords entered by the user. The suggested approach is safe from a variety of threats, including breaches of data confidentiality and man-in-the-middle attacks, as well as impersonation of users or cloud systems. On the other hand, the DU might use relevant terms to search for a certain file, which could return several files or take a lengthy time.

### 3.2 Decentralized Access Control

Tao, Jiyu et. al. [33] created an effective and safe data sharing system using blockchain technology with the Interplanetary File System (IPFS) and attribute-based encryption (ABE). Specifically, we demonstrate that the proposed large-universe ABE without sourced

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 02 February 2024
Page No: 309 - 320
https://irjaeh.com

decryption (LU-ABE-OD) approach is susceptible to key escrow attacks, making it insufficiently secure for data sharing scenarios. In order to encrypt personal data stored in the IPFS system, they build an upgraded multi authority LU-ABE-OD scheme [31] based on their fundamental proposal. Blockchain is then used to store the hash value supplied by IPFS and handle the outsourcing of decryption. In order to focus on increasing overall efficiency in such Blockchain-based access control and data sharing systems, more important features like attribute revocation, user revocation, and policy concealing are not covered in detail in this work. Xu, Jie et.al. [39] created Health chain, a comprehensive blockchain- based program for protecting the privacy of health data. Health data is encrypted to provide granular access management. In particular, users can add or remove authorized doctors with effectiveness by using user transactions for key management. In order to prevent medical conflicts, Health chain also ensures that doctor diagnoses and IoT data cannot be altered or removed. The data owner did not instantly transfer access to a new data requester in case of emergency. Yue, Xiao et. al. [42] created an app known as the Healthcare Data Gateway (HGD) with a blockchain-based architecture that allows patients to easily and securely own, control, and share their own data without compromising privacy. This opens up a new avenue for enhancing the intelligence of healthcare systems while maintaining patient privacy. Here, a purpose-centric access architecture guarantees that patients own and control their health information, and a clearly understood, uniform Indicator Centric Schema (ICS) facilitates the practical organization of various types of personal health information. We also note that one promising method to allow computing on patient data by an untrusted third party without compromising privacy is Secure Multi-Party Computing, or MPC for short. In this case, the Blockchain network is used for the computations, which take a long time. It causes the model to become inefficient. Zhang, Xiaoshuai et.al. [44] they created the Block-based Access Control Scheme (BBACS), which consists of an access model and an access scheme, as an access control solution for sharing Blockchain-based Electronic Medical Records (EMRs). In contrast to current Blockchain-based access strategies for EMRs, our access model may permit user access with block level granularity without requiring the agent layer (gateway) and yet be compatible with the underlying Blockchain data structure. Moreover, the BBACS authentication, encryption, and decryption algorithms eliminate the requirement for a public key infrastructure (PKI), which lowers network development costs and boosts computing efficiency. A blockchain-based EMR server can reply to data requests without the need for an agent or agents, or for disclosing sensitive medical records without authorization. This is particularly useful for devices with limited resources, such those found in eHealth IoT systems. There is no investigation into verifying the algorithms' applicability on other low-resource IoT devices or assessing how scalable they are for use on multiple-user EMRs. Kumar, Randhir et. al. [16] tackles the issue of scalability. They created an improved version of the Bell LaPadula model and assigned distinct clearance and security levels to the peers and transactions. The clearance level means that the peers are spared from maintaining the whole transaction history. [38] Using smart contracts, we created dynamic access control policies to ensure data security throughout the network. It is impossible to verify the accuracy of smart contracts, and any flaws in the model persist. Transaction histories are not kept up to date since they can be utilized to anticipate potential access restriction tactics. Milojkovic, Matea [25] created a Blockchain-based architecture that protects patients' sensitive information while enabling safe, standardized, and effective access to medical data for patients, providers, and other parties. Their approach uses advanced cryptographic algorithms for additional security and leverages smart contracts in an Ethereum-based Blockchain for enhanced access control and data obfuscation. The consensus methods em ployed by Ethereum-based blockchains, such as proof-of-work and proof-of-stake, can be resource-intensive and slow. Vora, Jayneel et. al. [34] research that show patients' access to data is often restricted by the state-of-the-art security protocols now in place for EHRs. This study develops a blockchain-based architecture for

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 02 February 2024
Page No: 309 - 320
https://irjaeh.com

effective EHR maintenance and storage. This further ensures that patients' private information is protected and that patients, providers, and other parties can access medical data quickly and securely. Differential privacy strategies are important to take into account because they enhance privacy. Madine, Mohammad Moussa et. al. [23] created smart contracts based on the Ethereum Blockchain to allow patients to have decentralized, unchangeable, transparent, traceable, trust- worthy, and secure ownership over their data. Medical data about patients is safely fetched, stored, and shared by the system using trustworthy reputation-based re-encryption oracles and decentralized storage of interplanetary file systems (IPFS). They employ algorithms and provide comprehensive implementation details for them. The patient won't have access to their medical records anywhere in the world thanks to Ethereum Blockchain's lack of connectivity across various deployments. In the event that patients forget their wallet credentials, the key management design does not offer any leniency or user-friendly features. Egala, Bhaskara S et.al. [10] created a revolutionary architecture based on blockchain technology that offers a decentralized electronic health record and smart contract-based service automation without [43] sacrificing system security or privacy. In order to address the shortcomings of the Blockchain-based cloud-centric IoMT healthcare system, including high latency, high storage costs, and single point of failure, they have combined the hybrid computing paradigm with the Blockchain-based distributed data storage system in this architecture. To strengthen the security capabilities of the proposed system, a decentralized selective ring-based access control mechanism is added along with device authentication and patient record anonymity algorithms. Rajput, Ahmed Raza et. al. [27] created an emergency access control management system (EACMS) using Hyper ledger com- poser and permissioned blockchain technology. Patients can establish constraints to govern PHR permissions. The system uses smart contracts to define rules for emergency conditions and the time limit for emergency access to PHR data items. By using the Hyperledger composer to create our suggested frame- work, they evaluated its performance in terms of accessibility, privacy, security, and reaction time. The results of the experiments demonstrate that our framework is more efficient than the conventional emergency access approach. Data moving through various healthcare facilities needs to be screened for access violations and privacy violations from various attack vectors. Saidi, Hafida et. al. [29] created a novel Decentralized Self- Management of data Access Control (DSMAC) system for medical data privacy preservation that uses a blockchain-based Self-Sovereign Identity (SSI) model. This system gives patients the tools they need to maintain control over their personal data and permits them to self-grant access rights to their medical records. In order to carry out Role-based Access Control regulations, DSMAC uses smart contracts. It also implements the use of decentralized IDs and verifiable credentials to explain sophisticated access control methods in an emergency. Although the data owner can restrict access to the data in an emergency, there is still room to improve efficiency and integrate machine learning for a dynamic feedback mechanism based on past data access control records. Al-Dahhan, Ruqayah R et. al. [3] suggests a CP-ABE with distributed multi-authority. There are three phases and six enti- ties in the proposed system. In order to retrieve the IDs of each approved DU and AA, the CA has to register them during the startup step. For the DU, the DO drafts an encrypted access control policy. The encrypted access policy is then made available to the CS via the DO. The keys needed by the DU to decode the access policy are then generated by one of the system's distributed AAs. If the DU is approved and matches the attribute granted to them, they can then access and decrypt the resource. The proxy server in charge of keeping up with and updating the DU authorization list is notified by the CA whenever the user withdraws his authorization. The suggested system guards against collusion attacks and maintains data confidentiality. To get the secret key from one of the dispersed AA, the DU has do a lot of computation. Wei, Jianghong et. al. [37] suggests using a multiauthority CP- ABE to safeguard cloud-based outsourced data. Each of the five entities that make

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 02 February 2024
Page No: 309 - 320
https://irjaeh.com

up the suggested strategy had a specific role. Initially, a global parameter for the suggested approach is created by the third party. Second, each AA is in charge of overseeing the authenticity of each user's attribute that pertains to its region as well as creating a public parameter and secret master key. Third, the encrypted data is sent to the cloud by the DO, which bases its access policy on the DU attribute. Fourth, every DU has a distinct secret key, set of attributes, and global identification. Lastly, the data storage and updating of any information sought from any institution falls under the purview of the CS. The suggested method is safe from collusion assaults. Nonetheless, the algorithmic effectiveness of the system is impacted by the quantity of features. Wang, Shangping et. al. [35] suggests a unified method that combines CP-ABE, smart contracts, and blockchain. The four en- tities in the proposed model are the DO, DU, CS, and blockchain. It involves four stages: file encryption, system initialization, key generation, and file decryption. The DO is in charge of establishing the smart contract with the DU's valid access periods, choosing the attribute sets, and defining the access control policies. To decode the encrypted smart contract, the DU must first fulfill its attribute set requirements. After that, it must acquire the content key to unlock the encrypted files that have been stored and gain access to them on the cloud. Blockchain is in charge of deploying and storing smart con- tracts, whereas the CS is in charge of storing encrypted resources or files. Both the performance and the cost of data access are reasonable. The integrity of the file that the DO uploaded is not taken into account in this study, though. In another study Yang, Caixia et. al. [19] suggests a method called Authprivacychain that combines smart contracts and the blockchain technology. The DO, DU, CS, and blockchain are the four entities that make up the suggested model. Initialization, access control, authorization, and authorization revocation are its four stages. The DO publishes the authorization to the DU after first uploading the necessary resources to the cloud and registering the transaction in the blockchain. The CS then queries the blockchain to determine whether or not the resource the DU has sought is permitted after receiving a request for a particular resource from the DU. Lastly, the stored access is provided in response to the request by the CS. To protect the privacy of your data, these processes are encrypted. The suggested method is safe from both internal and external threats, and the Authprivacychain safeguards the resources' availability, authenticity, secrecy, and integrity. However, the setup of the blockchain node affects how well the suggested technique performs in terms of time. This is due to the fact that blockchains come in numerous varieties with varying setup options. When creating a block time, for instance, one block takes two minutes and another takes ten. Alhaqbani, Bandar et. al. [4] provide a framework for connecting electronic health records that allows patients to decide what information is made public about them. The usage of in- direct pseudonym identifiers is how this is accomplished. Its architecture is compatible with currently available technology. We demonstrate how our architecture meets patients' privacy needs and data accuracy standards with a case study. problems with using pseudonyms, especially when writing, where there is a greater chance of participant identification. Marupally, Pavan Roy et. al. [24] based on the Privacy Preserving Portable Health Record (P3HR), a gadget that embeds a smart card inside a USB flash drive and offers encrypted flash memory for safe mobile data storage, a novel design has been suggested to close the gap. Once keys are compromised, several security attacks are feasible.

Steele, Robert et.al. [32] suggested a mobile architecture for personal electronic health records that uses an enhanced digital certificate-based technique to naturally provide a higher level of privacy. Additional security issues related to a strategy based on portable devices are also taken into account. lack precise access control for the EHR, despite the fact that it is kept on mobile devices. Barnickel, Johannes et. al. [6] The Health Net mobile electronic health monitoring and data collecting system is being implemented, along with a suggested security and privacy architecture. A body sensor network integrated into garments that connects wirelessly to the wearer's smartphone makes up Health Net. Data is managed, stored, and transferred

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 02 February 2024
Page No: 309 - 320
https://irjaeh.com

securely via a mobile phone. Information may be shared with other parties, including emergency services, physicians, and private individuals that the user personally trusts, including his family. Who can access the patient's data is within his control? Vital information can only be accessed by emergency physicians in the patient's vicinity with- out the patient's express permission. Li, Zhuo-Rong et.al. [18] seeks to enhance the patient-to- electronic medical record unlink ability method. In the past, cross- reference tables and mathematical conversions have been used to hide the private information included in electronic medical records. Nevertheless, applying these techniques to the unlink ability and unobservability mechanisms is more difficult. Cloud computing is renowned for its vast storage capacity and quick calculation speed. Cloud computing can be used to integrate a hospital's electronic medical record system, make it easier for documents to be shared and exchanged, and give smaller hospitals and clinics with limited resources the room to store electronic medical records. Privacy is jeopardized and CSP can gain knowledge from EHRs kept on cloud servers. Aiswarya. Or et.al. [2] provided a unique method for effectively protecting HER pictures while maintaining patient data privacy. More care needs to be taken to secure the photos be-because they include the patients' most sensitive information. This is accomplished by first dividing the images into pixels, which are subsequently encrypted using the Paillier Cryptosystem. It is kept on cloud storage after encryption. Using the private key, the original data may be unlocked from the cloud. The hospital may require the doctors and other professionals to have access to the key. Cloud-stored EHRs allow CSP to learn, but privacy is jeopardized.

## 4. Challenges and Future Research Direction for Access Control Models in Cloud Computing

Section 3 discussed the different solutions currently proposed for access control models in cloud computing. However, certain issues and limitations remain that must be addressed by future studies. This section presents the challenges and suggested future research direction for both centralized and decentralized access control models in cloud computing.

### 4.1 Centralized Access Control

Section 3.1 outlined the existing centralized access control options; however, the research under discussion depended either on encryption-based models or on standard access policy models, neither of which is adequate for system security. To maintain secrecy and integrity, more hybrid works combining encryption and access policy approaches are needed. Crucially, research on centralized access control makes the assumption that an AA or CA can be trusted. However, there are times when the CA or AA cannot be trusted, which leads to a variety of problems like the loss of private information and keys. It results in the exposing of users' privacy. Furthermore, the CA might fail for any number of reasons, including assaults, but the current procedure Jamal, Fara et. al. [14] for choosing the suitable backup authority node needed to be secured.

Furthermore, the existing research on centralized cloud systems included a variety of approaches and methods, including hash algorithms, symmetric encryption, and public key encryption. These studies save the resources in the cloud storage in an encrypted manner; however, searching for a certain resource or file using relevant keywords may result in the retrieval of many files, lead to incorrect results, or take longer to search. When encrypting numerous files at the same access level, it is also important to improve the computation time for encryption and decryption. However, mobile cloud computing necessitated ad- dressing a trade-off between the computations time for encryption and decryption and storage space. Finally, when more people utilize the cloud system every day, scalability needs to receive greater attention in order to maintain the dependability of the system.

### 4.2 Decentralized Access Control

As evidenced by the work of [9, 35, 41], the idea of using distributed authority to address the problem of centralized authority is still being explored today. Still, there are issues that need to be resolved, such data restoration from a compromised AA or CA. The decentralized blockchain creates a unique identifier for every resource using a hash function, which is then stored in a smart contract. This allows for a private, fast search with the unique identifier

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 02 February 2024
Page No: 309 - 320
https://irjaeh.com

returning the right answer [36]. As a result, de-centralized cloud models handle reading requests more quickly than centralized cloud models. To get over current obstacles such blockchain node configuration, sluggish writing access rights performance, blockchain node registration, and computing resources, more attention must be paid to the application and development of blockchain technology and smart contracts. Moreover, various justifications are needed for the permission revocation covered in Section III-B, such as a user's request. It's possible that the resource has been compromised, in which case the cloud server might choose to disable it. Therefore, greater care must be taken to guarantee that the revocation procedure is quick and safe Yang, Caixia et. al. [40]. Lastly, all of the interactions between the entities in the system are documented in the access log. It is crucial because it can offer a way to identify the interaction that is causing a system assault. In order to find any weaknesses in the system, security analysts can also do post-audit analysis on these records. As a result, access log design must be considered throughout system implementation Yang, Caixia et. al. [41].

## Conclusion

Cloud computing offers various online services that could lead to various security problems, like illegal access to cloud resources. One security measure that regulates access to cloud services is access control. This study analyzed a number of papers that used this taxonomy, comparing the benefits and drawbacks of each, and established a taxonomy for access control models in cloud computing based on centralized and decentralized models. The study found that several approaches, both centralized and decentralized, are required to increase the security of access control models in cloud computing. The system should address the issue of lengthy search times and provide both confidentiality and integrity in centralized access models. Authorization revocation in decentralized access models has to be more secure and quick. In addition, blockchain node setup needs to be improved to boost system performance, and access logs must be used to monitor any system exposure. The report also outlined the present difficulties and suggested a course of action for next investigations into cloud computing access control model research

## References

[1] Md Rayhan Ahmed, AKM Muzahidul Islam, Swakkhar Shatabda, and Salekul Islam. Blockchain-based identity management system and self-sovereign identity ecosystem: A comprehensive survey. IEEE Access, 10:113436–113481, 2022.

[2] R Aiswarya, R Divya, D Sangeetha, and V Vaidehi. Harnessing healthcare data security in cloud. In 2013 International Conference on Recent Trends in Information Technology (ICRTIT), pages 482–488. IEEE, 2013.

[3] Ruqayah R Al-Dahhan, Qi Shi, Gyu Myoung Lee, and Kashif Kifayat. Revoca- ble, decentralized multi-authority access control system. In 2018 IEEE/ACM International Conference on Utility and Cloud Computing Companion (UCC Companion), pages 220–225. IEEE, 2018.

[4] Bandar Alhaqbani and Colin Fidge. Privacy-preserving electronic health record linkage using pseudonym identifiers. In HealthCom 2008-10th Inter- national Conference on e-health Networking, Applications and Services, pages 108–117. IEEE, 2008.

[5] Chunduru Anilkumar and Sumathy Subramanian. A novel predicate based access control scheme for cloud environment using open stack swift storage. Peer-to-Peer Networking and Applications, 14:2372–2384, 2021.

[6] Johannes Barnickel, Hakan Karahan, and Ulrike Meyer. Security and privacy for mobile electronic health monitoring and recording systems. In 2010 IEEE International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM), pages 1–6. IEEE, 2010.

[7] Rafael Belchior, Benedikt Putz, Guenther Pernul, Miguel Correia, André Vas- concelos, and Sérgio Guerreiro. Ssibac: self-sovereign identity based access control. In 2020 IEEE 19th International Conference on Trust, Security and Pri- vacy in Computing and

Communications (TrustCom), pages 1935–1943. IEEE, 2020.

[8] Jason Paul Cruz, Yuichi Kaji, and Naoto Yanai. Rbac-sc: Role-based access control using smart contract. Ieee Access, 6:12240–12251, 2018.

[9] Sourya Joyee De and Sushmita Ruj. Efficient decentralized attribute based ac- cess control for mobile clouds. IEEE transactions on cloud computing, 8(1):124– 137, 2017.

[10] Bhaskara S Egala, Ashok K Pradhan, Venkataramana Badarla, and Saraju P Mohanty. Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control. IEEE Internet of Things Journal, 8(14):11717–11731, 2021.

[11] Zahid Ghaffar, Shafiq Ahmed, Khalid Mahmood, Sk Hafizul Islam, Moham- mad Mehedi Hassan, and Giancarlo Fortino. An improved authentication scheme for remote data access and sharing over cloud storage in cyber- physical-social-systems. IEEE Access, 8:47144–47160, 2020.

[12] Manuel Grana and Konrad Jackwoski. Electronic health record: A review. In 2015 IEEE international conference on bioinformatics and biomedicine (BIBM), pages 1375–1382. IEEE, 2015.

[13] Fara Jamal, Mohd Taufik Abdullah, Zurina Mohd Hanapi, and Azizol Abdullah. Reliable access control for mobile cloud computing (mcc) with cache-aware scheduling. IEEE Access, 7:165155–165165, 2019.

[14] HR Jara and E Schafir. e-health: An introduction to the challenges of pri- vacy and security. In 2014 IEEE Central America and Panama Convention (CONCAPAN XXXIV), pages 1–5. IEEE, 2014.

[15] Galia Kondova and Jörn Erbguth. Self-sovereign identity on public blockchains and the gdpr. In Proceedings of the 35th Annual ACM Symposium on Applied Computing, pages 342–345, 2020.

[16] Randhir Kumar and Rakesh Tripathi. Scalable and secure access control policy for healthcare system using blockchain and enhanced bell–lapadula model. Journal of Ambient Intelligence and Humanized Computing, 12:2321–2338, 2021.

[17] Jiguo Li, Ningyu Chen, and Yichen Zhang. Extended file hierarchy access control scheme with attribute-based encryption in cloud computing. IEEE Transactions on Emerging Topics in Computing, 9(2):983–993, 2019.

[18] Zhuo-Rong Li, En-Chi Chang, Kuo-Hsuan Huang, and Feipei Lai. A secure electronic medical record sharing mechanism in the cloud computing platform. In 2011 IEEE 15th international symposium on consumer electronics (ISCE), pages 98–103. IEEE, 2011.

[19] Shu Yun Lim, Omar Bin Musa, Bander Ali Saleh Al-Rimy, and Abdullah Al- masri. Trust models for blockchain-based self-sovereign identity management: A survey and research directions. Advances in Blockchain Technology for Cyber Physical Systems, pages 277–302, 2022.

[20] Li Lin, Ting-Ting Liu, Shuang Li, Chathura M Sarathchandra Magurawalage, and Shan-Shan Tu. Priguarder: A privacy-aware access control approach based on attribute fuzzy grouping in cloud environments. IEEE Access, 6:1882– 1893, 2017.

[21] Tonglai Liu, Jigang Wu, Jiaxing Li, Jingyi Li, and Yidong Li. Efficient decentral- ized access control for secure data sharing in cloud computing. Concurrency and Computation: Practice and Experience, 35(17):e6383, 2023.

[22] Yi Liu, Yinghui Zhang, Jie Ling, and Zhusong Liu. Secure and fine-grained access control on e-healthcare records in mobile cloud computing. Future Generation Computer Systems, 78:1020–1026, 2018.

[23] Mohammad Moussa Madine, Ammar Ayman Battah, Ibrar Yaqoob, Khaled Salah, Raja Jayaraman, Yousof Al-Hammadi, Sasa Pesic, and Samer Ellahham. Blockchain for giving patients control over their medical records. IEEE Access, 8:193102–193115, 2020.

[24] Pavan Roy Marupally, Vamsi Paruchuri, and Sriram Chellappan. Privacy preserving

portable health record (pˆ 3hr). In 2009 International Conference on Network-Based Information Systems, pages 310–315. IEEE, 2009.

[25] Matea Milojkovic. Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. 2018.

[26] Oznur Esra Par and Ergin Soysal. Security standards for electronic health records. In 2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, pages 815–817. IEEE, 2012.

[27] Ahmed Raza Rajput, Qianmu Li, Milad Taleby Ahvanooey, and Isma Masood. Eacms: Emergency access control management system for personal health record based on blockchain. IEEE Access, 7:84304–84317, 2019.

[28] Pradeep Ray and Jaminda Wimalasiri. The need for technical solutions for maintaining the privacy of ehr. In 2006 International Conference of the IEEE Engineering in Medicine and Biology Society, pages 4686–4689. IEEE, 2006.

[29] Hafida Saidi, Nabila Labraoui, Ado Adamou Abba Ari, Leandros A Maglaras, and Joel Herve Mboussam Emati. Dsmac: Privacy-aware decentralized self- management of data access control based on blockchain for health data. IEEE Access, 10:101011–101028, 2022.

[30] Kamran Sartipi, Mohammad H Yarmand, and Douglas G Down. Mined- knowledge and decision support services in electronic health. In International Workshop on Systems Development in SOA Environments (SDSOA'07: ICSE Workshops 2007), pages 10–10. IEEE, 2007.

[31] Lihua Song, Mengchen Li, Zongke Zhu, Peng Yuan, and Yunhua He. Attribute- based access control using smart contracts for the internet of things. Procedia computer science, 174:231–242, 2020.

[32] Robert Steele and Kyongho Min. Role-based access to portable personal health records. In 2009 International Conference on Management and Service Science, pages 1–4. IEEE, 2009.

[33] Jiyu Tao and Li Ling. Practical medical files sharing scheme based on blockchain and decentralized attribute-based encryption. IEEE Access, 9:118771–118781, 2021.

[34] Jayneel Vora, Anand Nayyar, Sudeep Tanwar, Sudhanshu Tyagi, Neeraj Kumar, Mohammad S Obaidat, and Joel JPC Rodrigues. Bheem: A blockchain-based framework for securing electronic health records. In 2018 IEEE Globecom Workshops (GC Wkshps), pages 1–6. IEEE, 2018.

[35] Shangping Wang, Xu Wang, and Yaling Zhang. A secure cloud storage framework with access control based on blockchain. IEEE access, 7:112713– 112725, 2019.

[36] Shangping Wang, Yinglong Zhang, and Yaling Zhang. A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. Ieee Access, 6:38437–38450, 2018.

[37] Jianghong Wei, Wenfen Liu, and Xuexian Hu. Secure and efficient attribute- based access control for multiauthority cloud storage. IEEE Systems Journal, 12(2):1731–1742, 2016.

[38] QI Xia, Emmanuel Boateng Sifah, Kwame Omono Asamoah, Jianbin Gao, Xiaojiang Du, and Mohsen Guizani. Medshare: Trust-less medical data sharing among cloud service providers via blockchain. IEEE access, 5:14757–14767, 2017.

[39] Qi Xia, Emmanuel Boateng Sifah, Abla Smahi, Sandro Amofa, and Xiaosong Zhang. Bbds: Blockchain-based data sharing for electronic medical records in cloud environments. Information, 8(2):44, 2017.

[40] Jie Xu, Kaiping Xue, Shaohua Li, Hangyu Tian, Jianan Hong, Peilin Hong, and Nenghai Yu. Healthchain: A blockchain-based privacy preserving scheme for large-scale health data. IEEE Internet of Things Journal, 6(5):8770–8781, 2019.

[41] Caixia Yang, Liang Tan, Na Shi, Bolei Xu, Yang Cao, and Keping Yu. Auth-privacychain: A blockchain-based access

control framework with privacy protection in cloud. IEEE Access, 8:70604–70615, 2020.

[42] Xiao Yue, Huiju Wang, Dawei Jin, Mingqiang Li, and Wei Jiang. Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. Journal of medical systems, 40:1–8, 2016.

[43] Peng Zhang, Douglas C Schmidt, Jules White, and Gunther Lenz. Blockchain technology use cases in healthcare. In Advances in computers, volume 111, pages 1–41. Elsevier, 2018.

[44] Xiaoshuai Zhang, Stefan Poslad, and Zixiang Ma. Block-based access control for blockchain-based electronic medical records (emrs) query in ehealth. In 2018 IEEE Global Communications Conference (GLOBECOM), pages 1–7. IEEE, 2018