International Journal of Scientific Research in Science and Technology
Available online at : www.ijsrst.com
Print ISSN: 2395-6011 | Online ISSN: 2395-602X
doi : https://doi.org/10.32628/IJSRST52310539

Secure And Efficient Access Control Over Blockchain PHR Cloud Storage System

Sreeja Lekshmi R J[1], R. Sowmiya[2]

[1]PG Scholar, Department of CSE, Ponjesly College of Engineering, Nagercoil, India

[2]Assistant Professor, Department of CSE, Ponjesly College of Engineering, Nagercoil, India

ARTICLEINFO

Article History:

Accepted: 07 Sep 2023
Published: 29 Sep 2023

Publication Issue
Volume 10, Issue 5
September-October-2023
Page Number
312-321

ABSTRACT

A novel architecture of blockchain-based secured electronic health record (EHR) management system is presented in this paper. Electronic health data record-keeping in cloud-based storage systems always pose a threat to information security. Intruders can delete EHR of patients, giving benefits to insurance companies or hiding medical malpractices. A secured EHR management system is required that would essentially solve such issues. The blockchain is an emerging technology that can be adapted to develop a secured and an efficient data management system. Storing and sharing health records through electronic systems pose security risks. However, establishing a new blockchain based system replacing the existing system is expensive. In our proposed architecture, we introduced an integration mechanism, named as the blockchain handshaker, between the existing cloud based EHR management system and public blockchain network to develop a secured health record management system. A blockchain-based protocol that secures health records, addressing all of the main security and complementary properties defined in current regulations. A prototype to provide evidence on the feasibility of the proposed concept is presented in this paper. The performance assessments demonstrate the efficiency of our proposed solution in terms of computation, communication, and storage.

Keywords : Electronic Health Record, Cloud Storage, Blockchain, Secured PHR

I. INTRODUCTION

Electronic Medical Record (EMR) Systems is considered to be a critical role in improving healthcare intelligence, quality, user experience and related costs. EMR system could eventually save more than billions of dollars annually [1]. These medical records serve as a systematic collection of personal health information, including health monitoring data, lab tests, images, diagnoses, prescriptions and medical

histories, and they are appeared to be controlled by users themselves, in which users store their own health records, and share them selectively with physicians for medical care [2].

Nowadays, more and more electronic health records (EHRs) systems are increasingly using cloud storage service (e.g., Google Health) for storing and retrieving the records to enhance interoperability, which can avoid exposing people to additional examination and unnecessary costs. Data sharing in EHRs systems is important for improving the quality of healthcare delivery. However, data sharing has raised some security and privacy concerns by putting the sensitive health data in third party cloud service providers, because healthcare data could be potentially accessible by a variety of users, which could lead to privacy exposure of patients [3]. Traditional encryption schemes cannot support complex and flexible encryption scheme that corresponds to different users on the large number of records in cloud service provider. Therefore, it is essential to enforce efficient data querying and sharing for securing electronic medical records in cloud computing [4].

Cloud computing environments provide an excellent opportunity to accommodate e-Health services in different scenarios in effectively. The cloud-based environment can offer numerous benefits by its scalability and mobility [5], but there are barriers that must be managed. A cloud-based Electronic Health Record (EHR) management system can provide the ability to share patient records with other clinical centres, and the integration of all the EHRs of a group of clinical centres in order to help medical staff. Cloud-based EHR management systems, security are a critical concern. EHR in cloud-based management systems can be exposed to abuse, leakage, loss or theft [6]. EHRs can be deleted or tampered by intruders to tamper treatments giving benefits to insurance companies or hiding medical malpractices. EHRs are closely related to health insurances. Several countermeasures are proposed to provide security of EHRs using cryptographic techniques [7].

Generally, a healthcare blockchain is treated as a distributed ledger to store health records for sharing, exchanging or other purposes among stakeholders [8]. In e-Health systems, data can be generated from different sources such as clinics, hospitals, and pathologies. In a blockchain-based EHR management system, all the data related to patients are stored in the distributed ledger offered by a blockchain network. The process of storing a set of related data is known as a transaction. A key concept of blockchain, smart contract, empowers trustless features among different entities in the EHR management system. Hence, no trusted third party is required to store data in the blockchain [9].

In this paper, we present an efficient and secure fine-grained access control scheme which not only achieves authorized users to access the records in cloud storage, but also supports a small set of physicians to write on the records. In order to improve the efficiency, we put forward a novel technique called match-then-decrypt, which is used to perform the decryption test without decryption. The contribution of this paper can be summarized as follows:

(1) An integrated blockchain network with the traditional cloud-based EHR management system was presented.

(2) A fine-grained access control scheme which not only achieve authorized users to access the records, but also support a small set of physicians to prescribe on the records.

The rest of the paper is organized as follows. Section 2 presents an overview and a summary of related work. Our proposed system architecture is described in Section 3. An implementation of the system prototype is demonstrated in Section 4. Finally, Section 5 concludes the paper with some future directions.

II. RELATED WORKS

Electronic medical records (EMR) are quite important and sensitive data that relates to personal privacy. Patient controlled encryption (PCE) of medical records was introduced to enable a patient to assemble, maintain and manage a secure copy of his or her medical records. Several systems have been proposed or implemented to enable access control on electronic medical records [10], which is strictly an online system that keeps patients' medical data encrypted at rest on backend servers, and only the trusted server which has access to the private keys can decrypt the data before sending it to the users. Hu et al. proposed a hybrid public key infrastructure (HPKI) for mutual authentication and distribution of sensitive EMR [11]. They delegate the trust and security management to the medical service provider, which is not suitable in untrusted cloud provider service. More importantly, when the server is unavailable, access control decisions cannot be made, or records cannot be retrieved.

Benaloh et al. designed a hierarchical-based encryption and access control scheme that does not rely on a trusted online server to mediate access control decisions [12]. In their patient controlled encryption (PCR) system, these techniques do not support fine grained access control required by medical applications. However, the scheme is not scalable with the number of users, and it introduces high complexity in key distribution and management. In order to provide data confidential and preserve patients privacy, storage of these sensitive data over untrusted servers requires more sophisticated cryptography techniques.

Attribute-based encryption (ABE) was proposed by Sahai and Waters [13] in 2005, which is a kind of public key cryptography associated with a set of attributes. It enables one-to-many encryption and is envisioned as a promising cryptographic primitive for realizing access control. There are two kinds of ABE schemes [14], ciphertext-policy attribute-based encryption (CP-ABE) and keypolicy attribute-based encryption (KP-ABE). CP-ABE allows data owners to define access control over attributes and predicates (e.g., and, or) in the process of encryption, then only those users whose attributes satisfy the policy can decrypt the data by decryption.

A number of variants of attributed-based encryption (ABE) schemes have been proposed for fine-grained access control of medical records in different settings. Ibraimi et al. propose a multiauthority CP-ABE scheme for protecting EMRs across different domains (e.g. healthcare providers and family members) and a mediated CP-ABE scheme for EMRs to address revocation of user attributes before an expiration date. A prototype system in [15] implemented using a new key and ciphertext-policy attribute-based encryption which allows for flexible and automated policy generation.

However, almost all of these existing ABE schemes require a large number of exponentiations during encryption and many parings computation in decryption at the user side. There are a few papers introduced cloud computing to different WSN applications such as vehicular ad hoc network [16], industrial supervision [17], patient data collection [18], energy monitoring [19] and environmental monitoring [20]. In a typical medical system, such as personal health records (PHR) [21], we must ensure their information confidentiality while the traditional encryption measures always inefficiency, at the same time we have the flexible sharing demand while the patients always lose physical control to their sensitive data. By this taken, how to achieve data confidentiality, flexible resource sharing and fine-grained access control becomes an important research direction.

Zhang et al. present a blockchain based secure and privacy-preserving PHI sharing (BSPP) scheme for diagnosis improvements in e-Health systems [22]. Two kinds of blockchains, private and consortium, are constructed by devising their data structures, and consensus mechanisms. To achieve data security,

access control, privacy preservation, and secure search, all the data including the PHI, keywords and the patient identity are public key encrypted with a keyword search. Furthermore, the block generators are required to provide proof of conformance for adding new blocks to the blockchains, which guarantees the system availability.

A blockchain-based health data sharing [23] framework that sufficiently addresses the access control challenges associated with sensitive data stored in the cloud. The system is based on a permissioned blockchain which allows access to only invited, and hence verified users. Furthermore, in order to provide data provenance, auditing and secured data trailing on medical data, the authors employ smart contracts and an access control mechanism in their another work [24]. Yue et al. in [25] also propose a three-layered system: data usage layer, data management layer, and data storage layer. The cloud in this work is a storage infrastructure which is different from the aforementioned works. This work proposes that the private blockchain plays the role of the cloud. Transactions are used to carry instructions, such as storing, querying and sharing data.

The existing works provide miscellaneous frameworks for healthcare data sharing in e-Health systems with blockchain. They take a blockchain as an assisted tool for data sharing instead of taking it as the main tool for data storage, data management, and data sharing. Furthermore, the works mentioned above do not discuss integrating blockchain to an existing healthcare system.

III.PROPOSED METHODOLOGY

In this paper, we propose blockchain-based system architecture to develop a tamper-proof EHR management system. There are three types of blockchain platforms exist so far: public blockchain, consortium blockchain and private blockchain. In public blockchain, anyone can join in the consensus process. Hence, a particular organization joining the public blockchain has no control on the consensus tasks, i.e. the control is decentralized. Contrarily, only a group of preselected nodes can perform the consensus tasks in the consortium blockchain. Giving an example of the consortium blockchain, each of a group of organizations building a blockchain network nominates one or multiple nodes as consensus nodes.

In the private blockchain, only authorized nodes of an organization are capable of performing consensus tasks. Thus, all of the nodes that are responsible for consensus can be controlled by the organization. In order to build a tamper-proof EHR system we choose public blockchain network as our blockchain in this paper. Integrating the blockchain network to the traditional cloud-based EHR systems is a design challenge. A suitable design methodology needs to be selected that allows blockchain technology to be integrated and current stakeholders are not affected as well. In our system design, we would like to use bottom-up approach for integrating blockchain to the cloud-based EHR managements systems. We develop a prototype of blockchain based EHR management system using, a public blockchain network, for showing the feasibility of blockchain integration to the traditional cloud-based EHR management systems.

Figure 1 : Patients Electronic Health Record (EHR)

1.1 Attribute-based encryption (ABE)

Attribute-based encryption (ABE) extends identity-based encryption (IBE) by using a public key as an

arbitrary string to identify a user. CP-ABE scheme used by the healthcare providers share a public key for encryption which avoids PKI; however, each healthcare provider has their unique decryption (private) key. Further, CP-ABE supports policies to specify which secret keys decrypt which ciphertexts (encrypted data) and each healthcare provider's key is associated with the set of attributes and ciphertext policies. The secret key of healthcare provider can decrypt the particular ciphertext only if the key is valid and verifed with the access policies associated with the ciphertext.

ABE scheme is divided into five main parts.

1. Setup The setup algorithm takes the implicit security parameter as input. It outputs the public parameters PK and a master key MK.
2. Encrypt(PTDATA, Ai) The encryption algorithm takes the plain text data (PTDATA), and attribute (Ai) as input. The algorithm encrypts Ai and produces a ciphertext (CTDATA) such that only a user who possesses a set of attributes that satisfies the access policies will be able to decrypt.
3. Key Generation(MK, S) The key generation algorithm takes the master key MK and a set of attributes S that describe the key as input. It outputs a private key SK.
4. Decrypt(CTDATA(Ai)) The decryption algorithm takes ciphertext CTDATA as input. If the key matches with the hashed key (HTKEY), then the algorithm will decrypt the ciphertext and return a message M.
5. Delegate(SK, S) The delegate algorithm takes as input a secret key SK for some set of attributes S and a set S⊆S. It outputs a secret key SK for the set of attributes S.

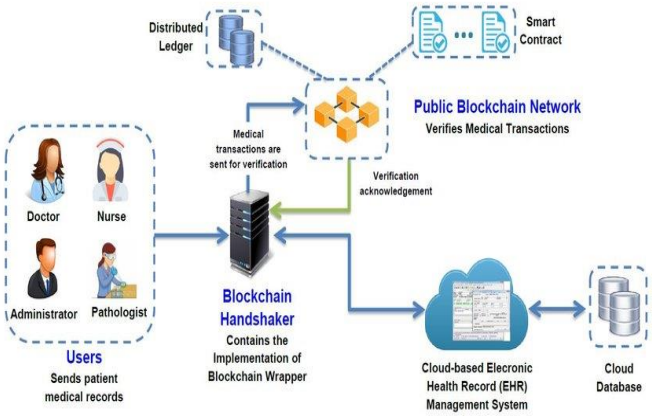

Figure 2: Architecture of an integrated Cloud-based Blockchain Network

1.2 Proposed Methodology

Cloud: The cloud stores the ciphertexts received from the EHR-O and re-encrypts them before distributing them to the requesting EHR-Us. We assume the cloud is honest but curious i.e., it follows the algorithm the way it is but tries to gather secret information as much as possible.

In this section, we discuss our proposed architecture based on blockchain for a tamper-proof cloud-based EHR management system. The architecture is depicted in Figure 2. There are four key components in our proposed architecture: user application, blockchain handshaker, cloud, and public blockchain network. Each component is explained as follows:

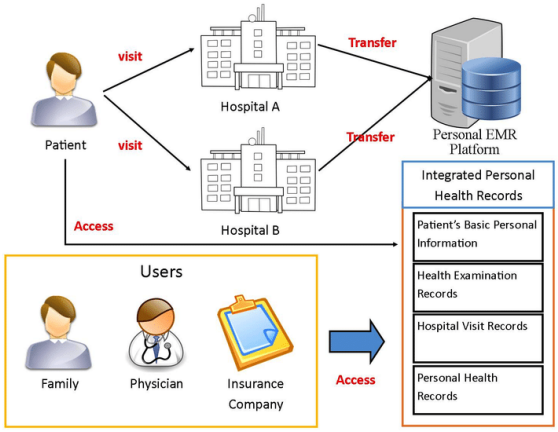

Figure 3 : Flow of Information in Blockchain Handshaker (BH). transaction Integrated Personal Health Records

User Application

User application is a software module that provides two functionalities. Firstly, it provides application interfaces for users. In our system, there are several types of users such as doctors, nurses, system administrators, pathologists, etc. Each type of user has different role. Hence, the user application provides specific user interfaces based on a user role. Secondly, user application builds an initial transaction(TI) based on data inserted by a user (e.g. patient blood pressure) and some system generated data (e.g. timestamp). TI is sent to blockchain handshaker for verification purposes. In summary, user application establishes a link between users and blockchain handshaker.

Blockchain Handshaker

Blockchain handshaker (BH) is the key component of our proposed architecture. This component acts as a wrapper component that connects user application, cloud-based EHR system and public blockchain network in our proposed architecture. BH has three sub-components, namely transaction template manager (TTM), transaction generator (TG), and transaction validator (TV). The internal architecture of BH is illustrated in Figure 3. Description of each component of BH is described below:

Transaction template manager (TTM): contains a set of predefined transaction templates for blockchain network. Transaction templates are generated by the system administrator following specifications of the blockchain network platform and set of attributes in corresponding smart contracts.

Transaction generator (TG): builds a blockchain transaction (TC) from an initial transaction (TI) following one of the templates in TTM. TG does the mapping between TI and a suitable template in TTM.

Transaction validator (TV): is the core component of BH that controls the overall interactions among international blocks of BH and handshaking user applications, blockchain network and cloud. TV receives an initial transaction TI from user application, sends it to TG and waits for receiving a blockchain transaction TC from TG. Upon receiving a TC, TV sends it to blockchain network for validation.The blockchain network returns validated transaction T ' I . If the validation is true, ACK is sent as valid transaction to the cloud for storing in cloud database. Otherwise, ACK is sent as invalid transaction and stored for future audit tasks.

Public Blockchain Network

We use a public blockchain network (e.g. Ethereum) in our proposed architecture. The public blockchain network comprises blockchain nodes, distributed ledger and smart contracts. Blockchain nodes are in fact miners that are responsible for maintaining blockchain according to the consensus mechanism. In other words, blockchain nodes receives transactions and validate based on smart contracts. If a transaction is found as valid, data are converted to blocks and added in the distributed ledger. Public blockchain network sends an acknowledgement as true or false to the transaction validator (TV) of the blockchain handshaker.

Cloud

The cloud provides two services in our proposed architecture that are similar to the traditional cloud-based EHR management system. The first service includes hosting the EHR management system. The second service is the storage service. The cloud provides a database for storing all health records. EHR management system receives transactions T ' I from BH, performs all tasks related to it and stores Figure 3: Internal Architecture of Blockchain Handshaker (BH). transaction data in the cloud database. The cloud responds with appropriate data in response to access requests from users.

Key management

Key management must be cost-effective, and their components must be carefully implemented. In the proposed system, key management is done as follows. It generates the public key and the master private key using the setup algorithm. If a doctor wants to read the patient information, doctor needs to send a request to the patient. If the patient accepts the request, then two keys are generated. From the

generated keys, one of the keys is sent to the doctor's mobile number and other is sent to doctor's e-mail id. Finally, the combination of these two keys decrypts the patient data. Once the entire authentication gets confirmed, then the doctor can access the patient's record and address the patient's problem.

3.3 Security

The security of the proposed framework has been hinted in the explanation of the framework. These security aspects define the credibility of the framework. Some of the important security aspects that the model satisfies have been summarized in this Sect.

1. Collusion resistance The proposed framework is highly collusion resistant. There are very few chances of collusion between the keys generated for the users with the same attributes or with diferent attributes as the algorithm includes randomness in the generation of keys. It is difcult to fnd two input attributes that hash to the identical output; that is, with two inputs a and b, Hash (a)=Hash (b) and a≠b.

2. Data confidentiality The users who are not authorized, that is, those who do not possess the required attributes should be deterred from accessing the data stored in the cloud server. In addition, the unauthorized access to key authority information should also be detained. This data confidentiality is simply guaranteed in the proposed framework. If the attributes belonging to a user cannot satisfy the access policy defined by the owner on the information, the user cannot recover the properly deciphered information. In order to access the information, the user should possess the intended role-based attributes.

3. Backward and forward secrecy In an ABE-based system, the backward secrecy refers to the situation in which any user who prefers to hold an attributes should be prevented from manipulating the old information before he gets hold of the attribute. Forward secrecy dictates that any user who drops an attribute must be prevented from access to the plaintext information of the data exchanged after the attribute is dropped, unless the rest of the attributes belonging to that user satisfy the defined access policy.

4. Reliability Since the entire process of storing and sharing is controlled by the owner, there are very few chances of the loss and leak of information. Since the complete process is cloud depended, it is highly fault tolerant and reliable.

IV. RESULTS AND DISCUSSION

In order to evaluate the performance of our proposed scheme presented which uses key encapsulation mechanism, and adopts a 224-bit MNT elliptic curve from the Stanford Pairing-Based Crypto library [26] to implement our scheme in software. Our experiments are done on three dedicated hardware platforms: a 3.20 GHz Intel Core CPU with 4 GB of RAM running 32-bit Linux Kernel version 3.2.0, a 1536 MHz ARM-based HTC G18 with 768 MB of RAM running Android OS, and a 1.3 Ghz ARM-based Nexus ME370T with 1 GB of RAM running Android OS.

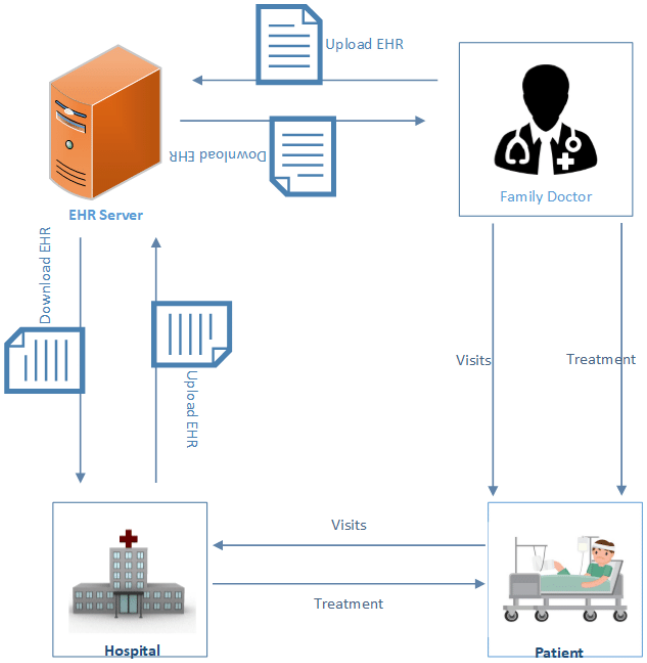

Figure 4 : Flow of Information

In a CP-ABE scheme, both decryption time and ciphertext size depend on the complexity of the ciphertext's policy and they increase linearly with the growing number of attributes in policy. To illustrate

this, we choose 100 of the most complex policies as the form (A 1 AND A 2 AND . . . AND A), of which A ni is an attribute, and the values of n increase from 1 to 100 in our experiments. This approach ensures that all the ciphertext components are involved in the decryption computation. In each case, we construct a corresponding standard decryption key that contains exact n attributes.

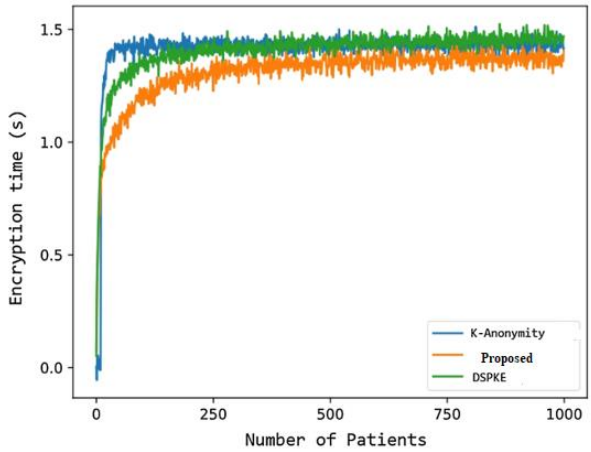

Figure 5 : Encryption Time Analysis

In practice, ABE is a public key encryption mechanism not suitable for encrypting data directly. In our experiment, as employed in related work [27], the message is encrypted separately using a symmetric encryption scheme AES (Advanced Encryption Standard) under a symmetric key k and the ABE ciphertext is the encryption of that symmetric key k. Following this mechanism, we select a random 128-bit symmetric key for each of these 100 different policies, then using the normal (non-outsourced) Decrypt algorithm and outsourced Decrypt algorithm to decrypt the resulting ABE ciphertext. However, in our experiments, we do not consider the effect of symmetric encryption [28]. Thus, all ciphertext size and decryption time depend on the key encapsulation variant of our scheme.

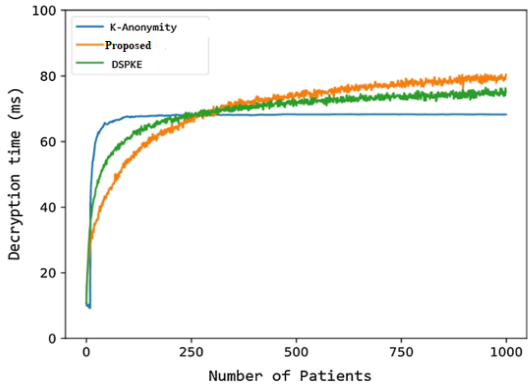

Figure 6 : Decryption Time Analysis

Fig.5 shows the Encryption time analysis. Fig. 6 shows the Decryption time analysis. From the experimental analysis, it is found that the total time required for the proposed method to process the PHR is within the acceptable range and Fig. 5, Fig.6 confirms that the time taken to encrypt and decrypt is better than the state of the art methods.

V. CONCLUSION

In this paper, we consider the ABE applications in heathcare system of PHR records sharing in cloud computing, in which mobile devices are used as information collecting nodes. The blockchain is an emerging technology that can be adapted to develop a secured and an efficient data management system. However, establishing a new blockchain based system replacing the existing system is expensive. In our proposed architecture, we introduced an integration mechanism, named as the blockchain handshaker, between the existing cloud based EHR management system and public blockchain network to develop a secured health record management system. A blockchain-based protocol that secures health records, addressing all of the main security and complementary properties defined in current regulations. In this work, a blockchain-based protocol that secures health records while addressing all of their main properties, namely confidentiality, access control, integrity, access revocation, emergency access, interoperability, and anonymity. Also, affords several decentralized features, preventing one single entity

from compromising the healthcare system. Furthermore, compared to decentralized solutions, our protocol addresses the challenging problem of fulfilling all the main properties of health records, whereas other solutions focus on offering mechanisms for specific properties only. Performance analysis demonstrates that our scheme not only reduces private key overhead but also provides fast decryption for the users.

VI. REFERENCES

1. Shi, Shuyun, et al. "Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey." *Computers & security* 97 (2020): 101966.
2. Neesha Jothi, Wahidah Husain, et al. 2015. Data mining in healthcare–a review. Procedia Computer Science 72 (2015), 306–313.
3. Tanwar, Sudeep, Karan Parekh, and Richard Evans. "Blockchain-based electronic healthcare record system for healthcare 4.0 applications." *Journal of Information Security and Applications* 50 (2020): 102407.
4. Shahnaz, Ayesha, Usman Qamar, and Ayesha Khalid. "Using blockchain for electronic health records." *IEEE access* 7 (2019): 147782-147795.
5. Keshta, Ismail, and Ammar Odeh. "Security and privacy of electronic health records: Concerns and challenges." *Egyptian Informatics Journal* 22.2 (2021): 177-183.
6. de Oliveira, Marcela T., et al. "Towards a blockchain-based secure electronic medical record for healthcare applications." *ICC 2019-2019 IEEE International Conference on Communications (ICC)*. IEEE, 2019.
7. Chen, Yi, et al. "Blockchain-based medical records secure storage and medical service framework." *Journal of medical systems* 43 (2019): 1-9.
8. Chen, Hannah S., et al. "Blockchain in healthcare: a patient-centered model." *Biomedical journal of scientific & technical research* 20.3 (2019): 15017.
9. Chen, Yi, et al. "Blockchain-based medical records secure storage and medical service framework." *Journal of medical systems* 43 (2019): 1-9.
10. K.D. Mandl, W.W. Simons, W.C. Crawford, J.M. Abbett, Indivo: a personally controlled health record for health information exchange and communication, BMC Med. Inform. Decis. Mak. 7 (1) (2007) 1.
11. J. Hu, H.-H. Chen, T.-W. Hou, A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations, Comput. Stand. Interfaces 32 (5) (2010) 274–280.
12. J. Benaloh, M. Chase, E. Horvitz, K. Lauter, Patient controlled encryption: ensuring privacy of electronic medical records, in: Proceedings of the 2009 ACM Workshop on Cloud Computing Security, ACM, 2009, pp. 103–114.
13. A. Sahai, B. Waters, Fuzzy identity-based encryption, in: Proceedings of the Eurocrypto on Advances in Cryptology, 2005, p. 557.
14. V. Goyal, O. Pandey, A. Sahai, B. Waters, Attribute-based encryption for fine– grained access control of encrypted data, in: Proceedings of the 13th ACM Conference on Computer and Communications Security CCS '06, 2006, pp. 89–98.
15. J.A. Akinyele, M.W. Pagano, M.D. Green, C.U. Lehmann, Z.N. Peterson, A.D. Rubin, Securing electronic medical records using attribute-based encryption on mobile devices, in: Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices, ACM, 2011, pp. 75–86.
16. Q. Kang, X. Liu, Y. Yao, Z. Wang, Y. Li, Efficient authentication and access control of message dissemination over vehicular ad hoc network, Neurocomputing 181 (2016) 132–138.
17. V. Rajesh, J. Gnanasekar, R. Ponmagal, P. Anbalagan, Integration of wireless sensor

network with cloud, in: Proceedings of the 2010 International Conference on Recent Trends in Information, Telecommunication and Computing, IEEE, 2010, pp. 321–323.

18. C.O. Rolim, F.L. Koch, C.B. Westphall, J. Werner, A. Fracalossi, G.S. Salvador, A cloud computing solution for patient's data collection in health care institutions, in: Proceedings of the Second International Conference on eHealth, Telemedicine, and Social Medicine, 2010. ETELEMED'10, IEEE, 2010, pp. 95–99.
19. W. Kurschl, W. Beer, Combining cloud computing and wireless sensor networks, in: Proceedings of the 11th International Conference on Information Integration and Web-based Applications & Services, ACM, 2009, pp. 512–518.
20. K. Lee, D. Murray, D. Hughes, W. Joosen, Extending sensor networks into the cloud using amazon web services, in: Proceedings of the 2010 IEEE International Conference on Networked Embedded Systems for Enterprise Applications (NESEA), IEEE, 2010, pp. 1–7.
21. F. Nzanywayingoma, Q. Huang, Securable personal health records using ciphertext policy attribute based encryption, in: Proceedings of the 2012 IEEE 14th International Conference on e-Health Networking, Applications and Services (Healthcom), 2012, pp. 502–505.
22. Zhang, Aiqing, and Xiaodong Lin. "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain." *Journal of medical systems* 42.8 (2018): 140.
23. Wang, Yong, et al. "Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain." *Ieee Access* 7 (2019): 136704-136719.
24. Rahman, Mohammad Saidur, et al. "A novel architecture for tamper proof electronic health record management system using blockchain wrapper." *Proceedings of the 2019 ACM international symposium on blockchain and secure critical infrastructure*. 2019.
25. Yue, Li, et al. "Blockchain Enabled Privacy Security Module for Sharing Electronic Health Records (EHRs)." *International Journal of Computer and Communication Engineering* 8.4 (2019): 155-168.
26. Fan, Kai, et al. "Medblock: Efficient and secure medical data sharing via blockchain." *Journal of medical systems* 42 (2018): 1-11.
27. Abdullah Al Omar, Mohammad Shahriar Rahman, Anirban Basu, and Shinsaku Kiyomoto. 2017. Medibchain: A blockchain based privacy preserving platform for healthcare data. In International conference on security, privacy and anonymity in computation, communication and storage. Springer, 534–543.
28. H. Qian , J. Li , Y. Zhang , J. Han , Privacy-preserving personal health record us- ing multi-authority attribute-based encryption with revocation, Int. J. Inform. Secur. 14 (6) (2015) 4 87–4 97.

Cite this article as :

Sreeja Lekshmi R J, R. Sowmiya, "Secure And Efficient Access Control Over Blockchain PHR Cloud Storage System", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 10 Issue 5, pp. 312-321, September-October 2023. Available at doi : https://doi.org/10.32628/IJSRST52310539

Journal URL : https://ijsrst.com/IJSRST52310539