DESIGN A SECURE AUTHENTICATION PROTOCOL FOR BLOCKCHAIN BASED SHARING OF ELECTRONIC HEALTH RECORDS

[1]Etikala Aruna, [2]Dr. Arun Sahayadhas
[1]Research Scholar of Computer Science and Engineering, VELS Institute of Science, Technology & Advanced Studies, Pallavaram, Chennai.
[2]Professor of Computer Science and Engineering, VELS Institute of Science, Technology & Advanced Studies, Pallavaram, Chennai.
arunae.phd@velsuniv.ac.in, arun.se@velsuniv.ac.in

ABSTRACT: The Internet has become increasingly important to our daily lives during the past decade. Modern communication technology has improved the efficiency of online services including e-banking, e-rail, and e-health. Not only the Electronic Health Record (EHR) possess immense value, but also implies a lot of privacy. One important strategy for raising the standard of medical care and lowering costs is the sharing of health data. The only way to maintain the privacy of health information is to keep it encrypted, but this compromises search usefulness and flexibility. This paper presents a Secure Authentication Protocol for BlockChain Based Sharing of Electronic Health Records. The described method provides two key advantages with the use of blockchain technology. It is truly decentralized and independent from a single point of failure since it was first free from a reliable authority. Second, as a result of the workload being split among the blockchain network's consensus nodes, it is also computationally efficient. A constant key generation execution time and a linearly increasing file size-dependent encryption time were both obtained by the described approach.

KEYWORDS: Blockchain, Electronic Health Record (EHR), personal privacy, health data, Cloud computing.

I. INTRODUCTION

The healthcare business has undergone a paradigm shift as a result of the development of information technology, moving from remote access to medical records towards the real-time exchange of information from several patients internal sensors [1].

EHRs are a directory of data about medical procedures, treatments, and patient data as well as information on diseases, medications and medical images (like name, race, age, identification number, background information, medical prescription, physical examination, or laboratory test) [2]. It is accessible to authorized medical professionals, facilitating their evaluation of the patient's state and clinical diagnosis. As a result, sharing of EHR data has significant research implications for nations, EHR organizations and people [3]. EHR data sharing among institutions, doctors, and patients can help them accurately diagnose patients and assess their conditions, and having complete EHR data at the individual level can help to enhance the quality of EHR services. EHR data is a great index of the population's general health at the national level. As a result, the question of how to implement secure data exchange based on the confidentiality of patient information and the security of EHR data storage has become increasingly important [4].

Being a centralized system, the cloud server's database could be a prime target for an attacker [5]. Patients may have major problems if an attacker intrudes the cloud server's database and alters, falsifies, or deletes recorded data. The centralized issue with cloud servers can be addressed by

eISSN 1303-5150

blockchain technology, which functions as a distributed ledger. Every transaction is tracked by this technology in a ledger, which is then chained together to create a blockchain using hash values [6]. An attacker cannot alter the transactions on the blockchain as each user of the network maintains the ledgers.

They use blockchain and cloud storage technologies to effectively store EHR data, ensuring that it is stored in both of these formats. Blockchain innovation has been extensively employed in elections, supply chains, healthcare, the Internet of Things, and other applications because of its appealing qualities of accessibility, autonomy, and tamper proof resistance. It keeps the encrypted EHR data in the cloud as well as the EHR data key words in context on the blockchain due to the restricted storage capability of the blockchain. This considerably reduces the storage space required by the blockchain and guaranteeing data integrity and confidentiality.

The blockchain prevents arbitrary data modification by requiring all transactions to be confirmed by a consensus procedure in an untrusted environment. A distributed topology of computing nodes is used to build blockchain, making it resistant to errors and attacks. The interoperability of medical information can also be improved by blockchain technology and smarter contracts. Blockchain therefore has a lot of prospective for usage in the medical industry. They use the consortium blockchain, which is run by a number of carefully chosen healthcare clinics, to provide a secured framework for exchanging EHRs in view of data security and patient confidentiality concerns in the healthcare industry. Compared to the public blockchain, the consortium blockchain allows us to control which user nodes enter and exit the network, providing better privacy protection.

Although encryption guarantees security, it significantly hinders data accessibility. Even the simplest action, like searching, becomes extremely difficult as a result. This issue is resolved by the Searchable Encryption (SE) method. With SE, the cloud server can seek for sensitive information without revealing any specifics about the content being looked for [7]. Additionally, users from different domains interact in a cloud environment; as a result, access control should be implemented to support fine-grained searching features. The request for cloud-assisted blockchain-based Cyber-Physical System (CPS) for healthcare is consistent by all the characteristics listed in encryption algorithm like access control and search functionality. Following is how the rest of this analysis is structured: Associated works are covered in Section II, Section III elaborates the described methodology based on Blockchain, result analysis is described in Section IV. The conclusion is described in section V.

II. LITERATURE SURVEY

Ramani V, Kumar T, Bracken A, Liyanage M, Ylianttila M et al. [8] presented a blockchain-based solution for safe and effective access to medical data. Smart contracts are used by the system to control how medical data is used by doctors, and blockchain technology ensures that consumers may access EHR in a secure and reliable manner.

Liu J, Li X, Ye L et al. [9] BPDS, a (Blockchain-based Privacy preserving Data Sharing) system for protecting the privacy of electronic medical data, was presented. To guarantee that a consensus is achieved for each transaction, the system utilizes Delegated Proof Of Stake (DPoS) resulting in suitable and adequate transaction verification. Only a small number of patients

eISSN 1303-5150

medical data are taken into account by this technique, and it is difficult to tell whether information has been altered using BPDS.

Zuobin Ying, Lu Wei, Qi Li, Ximeng Liu, Jie Cui, et. al. [10] on the basis of CP-ABE, a policy-preserving EHR system was presented. A reliable cryptography prototype called Ciphertext-Policy Attribute-Based Encryption (CP-ABE) can do both one-to-many encryption and fine-grained access control. Although the access policy is associated with the ciphertext in CP-ABE, it is not secured, which will also result in certain privacy leakage. This created an algorithm that can both hide the whole access policy and retrieve the hidden properties from the access matrix. The suggested technique only introduces minimal overhead costs, according to the assessment of element insert, lookup, and recovery that follows.

Jianhong Zhang, Hao Xiao, et. al. [11] suggests a unique public auditing mechanism for the exchange of dynamic information. It can make it such that the designated data users can edit a particular section of the shared information file. As far as it is aware, it is the initial strategy to accomplish this purpose. The auditor's constant contact and computing costs are another remarkable feature of the method. The results of a detailed simulation and comparisons with the most recent scheme demonstrate that the described method has a number of benefits in regards to user revocation, data block updating as well as integrity verification time. Lastly, it explicitly establishes the described scheme's security and assesses the effectiveness of the auditing process.

Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., and Du, X. et al. [12] developed a plan for exchanging medical data to supply data sources, audit and monitor confidential information in clinical data. The issue of sharing medical data between sizable clinical databases without trust can be resolved by this plan. The system is built on the blockchain, tracks data efficiently using smart contracts and access control mechanisms and can identify when data is permitted improperly. However, sharing data is a complicated task.

X. Liang, J. Zhao, S. Shetty, J. Liu and D. Li, et al. [13] presented a decentralized and permissioned blockchain-based system for user-centric health data exchange. In this investigation, smartphone application is used to gather clinical information from individual wearable technology. Healthcare providers as well as health insurance firms received the data after it had been synchronized to the cloud.

G. Zyskind, O. Nathan, et. al. [14] utilizes blockchain to safeguard the confidentiality of personal data. The authors put into practice a technique that transforms a blockchain into an automatic access-control manager without the need for third-party trust, guaranteeing customers own and regulate their information.

Teresa C. Piliouras, Robert J. Suss, Pui Lam Yu, et. al. [15] presents methods for integrating digital imaging technology with clinical workflows and EHR systems. A case analysis using the open source EHR program, OpenEMR (Electronic Medical Record), is provided as an illustration of the difficulties in combining imaging and the EHR innovation within and among medical practices. Vendors of Radiology Information Systems (RIS), Picture Archiving and Communication Systems (PACS), and EHR systems must improve the system interoperability and image sharing features of their product offerings. To make this possible, it needs standards that are better and more comprehensive. This would lessen the pressures placed on medical personnel and Information Technology personnel who should utilize and build device architecture

eISSN 1303-5150

while maintaining adherence to the Health Insurance Portability and Accountability Act (HIPAA) and Meaningful Use (MU).

III. BLOCK CHAIN BASED SHARING OF ELECTRONIC HEALTH RECORDS

The architecture of Secure Authentication Protocol for Block Chain Based Sharing of EHR is represented in below Fig. 1.

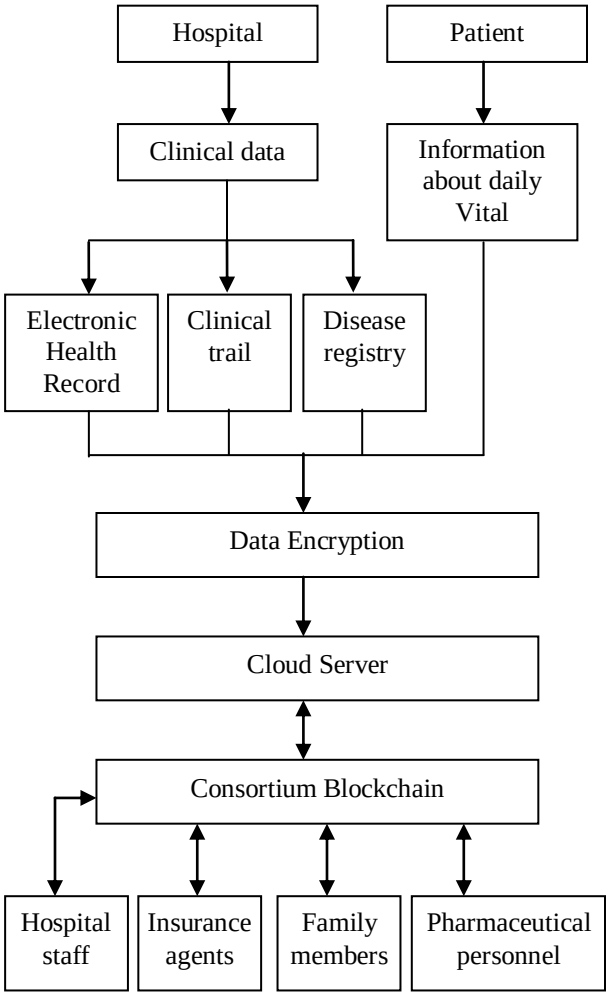

Fig. 1: ARCHITECTURE OF THE SECURE AUTHENTICATION PROTOCOL FOR BLOCK CHAIN BASED SHARING OF EHR

The architecture that supplies the overall algorithm for the described system is described in this section. Additionally, it provides the described scheme's security definition and game-based security model. Hospital, patient, clinical data, EHR, clinical trial and disease registry belong to the Data Owner (DO) entity. As implied by the name, The owner of some data is the DO (in this case, health data) who chooses to share such information with a third-party cloud server. The data owners produce the encrypted text using the GenIndex algorithm, which is subsequently uploaded to the cloud server for secure sharing. Prior to actually outsourcing the clinical data file and related data, the keywords are first encrypted. A patient who encrypts their health information using any popular encryption algorithm, most likely the symmetric key (fast computation) scheme, is the system's data owner. The described technique employs the GenIndex algorithm to encrypt both the related symmetric key employed for the data encryption and keywords included in that information.

Described searchable encryption technique was built using the monotonic access architecture, which is described as: Let μ be the representation of the attribute world. Monotonic access framework, on μ contains non-empty subsets of μ like that if a subset belongs to $\mathbb{A}$ then its superset should be there in $\mathbb{A}$, i.e., $\forall B, C \in \mathbb{A}, if\ B \epsilon\ \mathbb{A}$ if and $B \subseteq C$, then $C \in \mathbb{A}$. They utilize Linear Secret Sharing Scheme (LSSS), π, over Z_P to distribute secret across the access architecture which is described as follows:
1) The vector over Z_P is made up of secret shares $S \in Z_P$.
2) Every access structure based on attribute universe has a share generating matrix, $\times n$, an order whose components come from Z_P.

Cloud Server (CS): CS is the entity in charge of storing encrypted health data, acting as the data user's agent when conducting a keyword search and returning the results. In the case under consideration, a healthcare provider often handles it.

Consortium Blockchain (CB): This entity will create global parameters and initialize

eISSN 1303-5150

the system. Additionally, it registers the user's public key associated with their particular Global ID (GID). The CB will produce a partial search token for customer when the user contacts it with the attributes that describe the search that they want to conduct. In CB, the group of consensus nodes will verify the user's characteristics, and using those characteristics, create a partial search token for user, which is then sent to the client who submitted it.

Role of CB in the suggested scheme:

1) System Setup: Employing Shamir's secret sharing method, the consensus nodes start the system and establish the global public parameters.

2) Registration of Users and Creation of a Partial Search Token: By saving the public key that corresponds to their particular global identity, every user might register themselves with CB. When a user wishes to recover encrypted data from cloud, he or she can get in connection with the CB to have a partial search token created that reflects the user's characteristics. It is also in charge of maintaining and producing the search token.

3) No longer obligated to keep the Master Secret: described CB-assisted plan does not have a single organization in charge of system management.

Data User (DU): The data that is kept on the cloud server is what DU wishes to access. He or she will create a comprehensive search token, this is subsequently sent to the cloud server in order to acquire the file containing the search phrase. Researchers, doctors, hospital personnel, insurance agents, family members, and other individuals may use data in a healthcare system. CS executes the search algorithm using the user's complete search token and the search outcome is then sent back to DU. A system is made more reliable and secure when the number of consensus nodes is increased. As reaching consensus now requires the agreement of more nodes. The system also becomes highly flexible in regards to the volume of transactions it can handle. Because the only nodes in consortium blockchain that may add new blocks to the blockchain are consensus nodes, Given that the consensus nodes are selected by associations which are having extreme level of confidence, the consensus procedure also uses less computational power.

IV. RESULT ANALYSIS

The described strategy is implemented in Java using the Netbeans 8.1 integrated development environment (IDE) and the Java Pairing-Based Cryptography (JPBC) Library on a 64-bit Windows 10 device having an Intel Core i3 processor running at 2.00 GHz and 4 GB of RAM. The baseline field is configured to be 512 bits in size, providing security identical to 1024 bits, while the origin group and destination group orders are configured to be 160 bits each. It primarily focuses on the routine tasks carried out by end users and also how the blockchain innovation helped to lessen the load of those end users and cloud, compares it to current multi-authority searchable encryption systems. The size and number of the group components are used to calculate the storage cost. The computational cost, in contrast, is calculated based on the quantity and variety of operations used to produce the results of each approach. The consensus technique and computing power of such consensus nodes, that are not primary subject of the analysis, determine how well blockchain operations perform. In order to demonstrate performance, it changed the collection's access policy from 8 to 40 with a step duration of 8. In the attribute universe, it has altered the number of attributes.

Fig. 2 shows how long the key generation technique for Attribute-Based Searchable encryption (ABSE) and comparable systems techniques Multiauthority Attribute-Based Keyword Search (MAAKS), Decentralized

eISSN 1303-5150

Attribute-Based Conjunctive Keyword Search (DACKS). In contrast to MAAKS and DACKS, where a linear graph may be seen, the described scheme's key generation time is persistent and does not change with the number of attributes.

Table 1: AVERAGE EXECUTION TIME FOR KEY GENERATION

No. of Attributes	ABSE	MAAKS	DACKS
8	0.0046	0.1	0.12
16	0.0046	0.2	0.23
24	0.0049	0.25	0.29
32	0.0046	0.29	0.35
40	0.0047	0.36	0.4

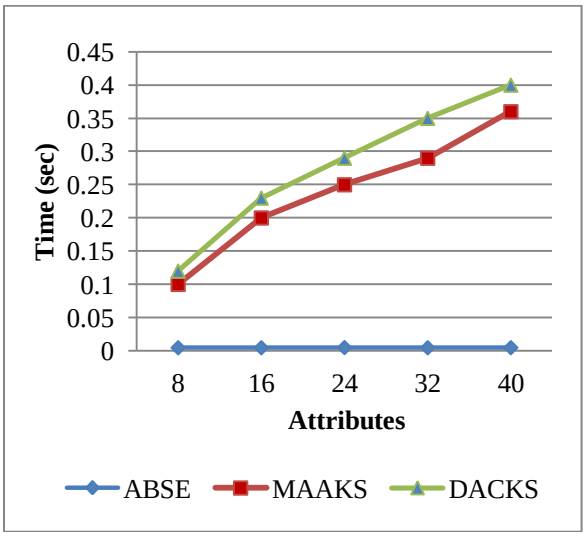

Fig. 2: AVERAGE EXECUTION TIME FOR KEY GENERATION

The properties are not contained in the secret key that is generated for the user in the described approach. The consensus nodes perform it directly at the same moment, during the production of the search token. In this case, to register themselves on the blockchain network, the user will generate a public and private key pair for themselves that corresponds to their unique worldwide identity. As a result, the described approach does away with the requirement for a central authority to control user attributes. When a user requests the generation of a search token, the consensus nodes carry it out.

The smart contracts are responsible for enforcing Access Control regulations. It constructed a large number of arbitrary access policy rules for this test to see how the number of access control rules affected the speed at which transactions were processed. In order for the smart contract to be deployed, a minimum of three administrative privilege rules are necessary. The transactions per second (tps) is the unit used to measure the throughput of a system. Fig. 3 demonstrates that when records are submitted to the blockchain, the proportion of access control regulations has very little of an impact just on latency and throughput of blockchain network. A blockchain network's performance is comparable to a network with fewer limitations, while having 300 access control rules. They may not have accurately reflected the complicated access control rules that must be implemented in real-world situations because it has only constructed arbitrary rules of relatively modest complexity.

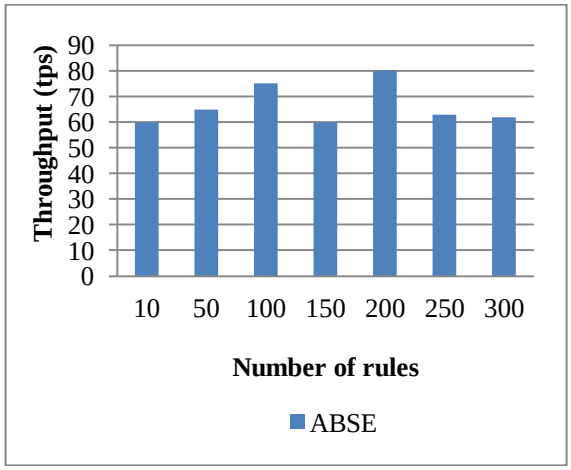

Fig. 3: THROUGHPUT

When taking into account that healthcare providers must have quick access to medical information at the point of care, the time it takes to encrypt documents is crucial. The time required for ABSE encryption (per

eISSN 1303-5150

record) is enhanced linearly with file size, as seen in Fig. 4.

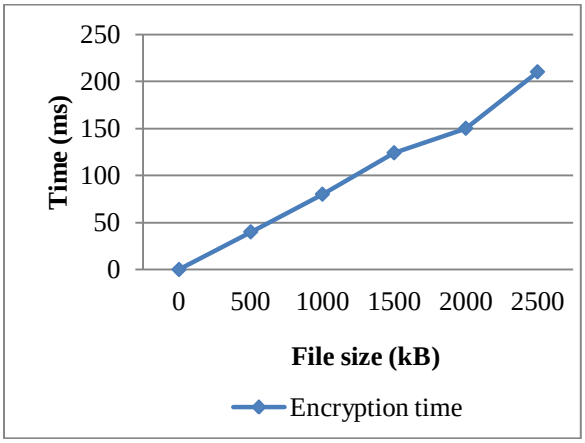

Fig. 4: ENCRYPTION TIME

Therefore from results it is clear that, described model or scheme for sharing of EHRs through cloud by using blockchain is very efficient and secured in terms of average execution of key generation, throughput and Encryption time.

V. CONCLUSION

In this paper, Secure Authentication Protocol for Block Chain Based Sharing of Electronic Health Records is described. By a dedicated client service, the sharing EHR system enables healthcare professionals and patients to easily access and share medical records. Users partial search tokens are created by the consensus nodes, who are also in charge of initializing the system. This lessens the requirement for a global central authority to set up system and lessens the computational strain on data users. Additionally, in contrast to similar ABSE schemes that require a central trusted authority, consensus nodes in the blockchain manage user attributes. The described scheme's key generation time is fixed and does not change when more qualities are added. Performance analysis shows that the encryption time is dependent on file size (kB). The blockchain allows healthcare practitioners to contribute records that are encrypted and securely kept while also requesting approval.

VI. REFERENCES

[1] Jeong Hyeon Han, Joo Yeoun Lee, "Digital Healthcare Industry and Technology Trends", 2021 IEEE International Conference on Big Data and Smart Computing (BigComp), Year: 2021

[2] Tejashwa Kumar Tiwari, Apoorva Tyagi, Gunseerat Kaur, Sumit Badotra, "Design of cloud-based interoperable electronic health record with advanced security for Indian healthcare industry", 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC), Year: 2021

[3] Shelly Sachdeva, Disha Batra, Shivani Batra, "Storage Efficient Implementation of Standardized Electronic Health Records Data", 2020 IEEE International Conference on Bioinformatics and Biomedicine (BIBM), Year: 2020

[4] Nan Liu, Chuan Wang, Xinyu Miao, Hua Bai, Yunan Wang, Limin Yang, Yiming Lei, Wei Zhang, Hong Wang, "A New Data Visualization and Digitization Method for Building Electronic Health Record", 2020 IEEE International Conference on Bioinformatics and Biomedicine (BIBM), Year: 2020

[5] Yong Wang, Aiqing Zhang, Peiyun Zhang, Huaqun Wang, "Cloud-Assisted EHR Sharing With Security and Privacy Preservation via Consortium Blockchain", IEEE Access, Volume: 7, Year: 2019,

[6] Xiaodong YANG, Ting LI, Rui LIU, Meiding WANG, "Blockchain-Based Secure and Searchable EHR Sharing Scheme", 2019 4th International Conference on Mechanical, Control and Computer Engineering (ICMCCE), Year: 2019

[7] Deepthi Rao, D.V.N. Siva Kumar, P. Santhi Thilagam, "An Efficient Multi-User Searchable Encryption Scheme without Query Transformation over Outsourced Encrypted Data", 2018 9th IFIP International Conference on New

Technologies, Mobility and Security (NTMS), Year: 2018
[8] Ramani V, Kumar T, Bracken A, Liyanage M, Ylianttila M, "Secure and efficient data accessibility in blockchain based healthcare systems" in Proc. GLOBECOM, Dec. 2018, pp:206-212.
[9] Liu J, Li X, Ye L, "BPDS: A blockchain based privacy-preserving data sharing for electronic medical records", Proceedings of the 2018 IEEE Global Communications Conference (GLOBECOM), IEEE, 2018, pp:1- 6
[10] Zuobin Ying, Lu Wei, Qi Li, Ximeng Liu, Jie Cui, "A Lightweight Policy Preserving EHR Sharing Scheme in the Cloud", IEEE Access, Volume: 6, Year: 2018
[11] Jianhong Zhang, Hao Xiao, "Public Auditing Scheme of Dynamic Data Sharing Suiting for Cloud-Based EHR System", 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), Year: 2017
[12] Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., and Du, X., "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain", IEEE Access, 2017
[13] X. Liang, J. Zhao, S. Shetty, J. Liu and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, 2017, pp. 1-5.
[14] G. Zyskind, O. Nathan, "Decentralizing privacy: Using blockchain to protect personal data," in Security and Privacy Workshops (SPW), 2015 IEEE. IEEE, 2015, pp. 180–184
[15] Teresa C. Piliouras, Robert J. Suss, Pui Lam Yu, "Digital imaging & electronic health record systems: Implementation and regulatory challenges faced by healthcare providers",2015 Long Island Systems, Applications and Technology, Year: 2015