International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2019): 7.583

Blockchain for Health Records System Storage using Attribute-Based Signature

Nenavath Chander

Assistant Professor, Keshav Memorial Institute of Technology, Hyderabad, Telangana-500029, India
Corresponding author's e-mail: *chander.nenavath[at]gmail.com*

Abstract: ***Block chain technology has increased popularity over the last years and found its use in various areas and addressed several important issues. As the requirement for an effective patient-centered solution to healthcare applications, healthcare block chain technology holds enormous potential and improves the quality value of electronic healthcare records (EHRs). With a patient-centered strategy, we have to face various issues and criteria in terms of privacy and also protection, the use of technology, regulating processes need to be taken into considerationin order to produce a good result. Throughout this paper, to ensure the integrity of EHRs incorporated in block chain, we propose to multiple authorities an attribute-based signature strategy where a patient approves a message as per the attribute thus revealing no details apart from the facts how he has attested to it. in addition, there are several authorities to produce and distribute public or private keys of the patient also confirms the mode of distributed data memory in the block chain.***

Keywords: Electronic Health Record System, Blockchain, Multiple Authorities, Attribute Based Signature

1. Introduction

Electronic health records (EHRs) offers service that is very efficient for the health record storage, and it will sort out the present medical data of a paper to accessible easily on web. Moreover in the present condition, patients send their EHRs among the various places in life period, so the EHR s to migrate from one service provider to other service provider. Hence, the patient has the chance to lose the information of the current health care data, when the patient generally manages the initial stewardship.

Patients who can get permissions to EHR are less and patients are hardly cannot get the data with providers. So, here we introduce Attribute based signature (ABS) will permits a party to sign a messages by identifying the data. In ABS a signer, who needs a group of attributes from authority, can have the access to sign a message with a predicate which is fulfilled by his attributes. The signature describes that an individual user with few number of attributes fulfilling the predicate has attached to a message. And also we offer a structure for developing ABS mechanisms, then we will show few practical things depending on the operations, furthermore, we give a model that is very secure upon a malicious attribute authority, but the protection for this mechanism is proved as the generic group model.

To aim for the protecting the patients confidential data in an EHR system in block chain, multiple authorities were introduced into ABS and MAABS scheme, that satisfies the need of the block chain architecture, and also giving assurance the immutability of the information and also patients private keys are also need to be developed. At last, the protocol security is proved by CBDH assumption in the factors of unforgettability and also privacy. It also describes the work and protocol cost that improves with the number of authorities and also patients as well as attributes.

2. Literature Review

This research is depends up on offering security and privacy via cryptography-based access control to hold cloud data, and attribute encryption.. Common PKE based methods use high key management systems, or allow encryption of a file by using several user keys of various sets to use fine-grained access controls. In this work [1] They look at the application of blockchain technology to promote this transformation across 5 processes: (1) digital access rules, (2) aggregation of information, (3) accessibility of knowledge, (4) identification of patients and (5) immutability of knowledge. We usually check challenges to block chain-enabled patient-driven capacity, explicitly the amount of clinical information transactions, privacy and safety, patient involvement and incentive. We continue to conclude by indicating that, while patient-driving capacity is associated with a promising trend in treatment, considering these difficulties, it is important to verify how the block chain can promote the exchange of knowledge from hospital-centred to patient-centred information.

[2] Doctors have a specific relation to the Electronic Health Record (EHR). On a side, doctors recognize that they are unable to deliver its effective therapy although they are not. And on the contrary modern EHR systems are downward slow, gawky so sluggish doctors. Sure, there is much pros and cons about now days EHRs, within a rundown of the way they deal with the problems they face. One solution may relate to the block chain, the infrastructure currently driving the bit coin crypto currency.

In this paper [3], in order to secure the integrity of EHRs embedded in the block chain, we propose through multiple authorities an attribute-based signature system where a patient approves a message as per the attribute although revealing no details apart from the proof that he has referred to it. In addition, there are numerous authorities without a trustworthy single one to produce and allocate the patient's public / private keys, that ignores the issue of escrow and

correspond to the model of storing data dispersed in the block chain. By exchanging the seeds of the hidden pseudorandom feature between authorities, this method avoids collusion attack from the compromised authorities out of N −1. relies on the premise of the theoretical bilinear Diffie-Hellman, we often formally prove that such a attribute-based signature system is safe in the randomized oracle system, in view of the unforgeability and total confidentiality of the attribute signer. The paper proves the efficiency and properties given in other studies between the proposed method and methods proposed in various researches.

In this paper [4] Modern cloud storage has depended almost entirely on storage providers, which function to migrate and storing data as trustworthy third parties. Such design faces a variety of challenges like availability of data, high operating costs and data security. This article, implements a technique which optimizes blockchain technology to get the keyword search system with such a secure distributed data space. The system will allow the user to upload the data in encrypted form, distribute the data content to cloud nodes, and use cryptographic methods to guarantee the data availability. It allows the data owner the capacity to give other people permission to search on their data. Eventually, the device enables encrypted data set search by private keyword.

Electronic medical records (EMRs) [5] very important non-public data for support identification and care, typically circulated and shared among peers such as aid providers, insurance companies, hospitals, scientists, families of patients. This provides a significant obstacle to keeping up to date the past of a patient's situation.

The storage and sharing of knowledge among different entities, the preservation of the privilege to use management by various consents, only illuminates a patient's method of care. A patient with a major medical scenario such as cancer or HIV must have an extensive record of care and treatment and observance of post-treatment procedures.

In this paper [6] the standard model this article introduces a completely secure attribute-based signature (ABS) scheme. Within regular statements, the decision linear (DLIN) assumption and the presence of collision resistant hash functions, the protection of the suggested ABS framework is proved. The provable predicates of a new ABS system are much more specific compared with the current ABS schemes, i.e. the new ABS scheme is the initial one to accept generic non-monotonic predicates, that will be represented utilizing NOT gates and AND, OR, and Threshold gates, whereas the current ABS schemes endorse only monotonous predicates. The suggested ABS mechanism is relatively as effective as the successful ABS techniques that are known to be safe in the community design.

3. Problem Statement

Healthcare researchers access these EHRs on board, the transformation program of healthcare solution is required to be completed. Standardisation of issue lists throughout the healthcare industry is required to implement most effective information sharing among healthcare providers including particularly patients. Paper-based systems may not function in electronic environments and certain types of trouble list planning, like lists auto population, pose major enforcement and patient security issues. The patient might lose all control of present information on healthcare, whereas the service provider typically keeps primary control. Access approvals for patients to EHRs are restricted, and patients generally cannot share such data with researchers or providers. The complexities of interoperability among various providers, hospitals, research institutions and so on add additional obstacles to strong-performance data sharing. The medical records are dispersed, rather than integrated, without structured data management and sharing.

4. Research Objectives

1) High Security: When we insert a patient's records into the block we can't alter it, for example, if we need to modify the data of the same patient then we have to create a new block to that specific patient due to the high Security
2) Cost Effective: While using EHR's method, every patient health records are maintained in blocks which form a chain between all of the individual blocks and every block has its own private key if we want to get patient records, and we can use that key so that we don't have to search the patient once again, so it's really a cost-effective.
3) Trust: All of the patient's health records will be held in individual blocks, however, when we insert into the block, we can't edit any of the health records once therefore it's quite trustworthy.
4) It gains a Perfect Privacy- Preserving for Patient: Personal health information is sensitive information and should be kept secret. An EHR program must enforce security policies to ensure the personal health records are accessible by the patient’s and healthcare personnel that have explicitly granted the patient's permission.

5. Proposed Model

In this project, we create an attribute-based signature (MAABS) mechanism with multiple authorities to fulfil the requirements of block chain in distributed EHRs systems. Taking benefit of ABS with the block chain technology, this idea will protect patient privacy and keep EHRs immutable.. The contributions of this work are as below

1) Firstly, the application of block chain technology as well as the development of an ABS system with multiple authorities in an EHRs system for monotonous predicates, and the amount of bilinear pairings involved in Signing is increased linearly with the various authorities.
2) Second, to several authorities the main issue is corruption assault. To counter this risk seeds of a pseudorandom feature are exchanged and secretly stored in each and every two authorities. In fact, in KeyGen each authority's private key is integrated in to the patient's private key. As per this arrangement, the protocol prevents conspiracy attacks by N − 1 compromised authorities.

3) Ultimately, within Diffie-Hellman's bilinear computation principle, we prove that, throughout the random oracle model, the plan is unforgivable in suffering a selective predicate attack, and it maintains the signer's complete privacy, that protects patient data from leakage.

A. Modules

1) **EHRs Server***:* The EHRs server is just like a cloud storage server, which is responsible for storing and transmitting the EHRs.
2) **Authorities***:* N authorities are various different organizations, such as hospitals, medical insurance organizations, medical research institutes, etc., which are responsible for accepting the enrolment and exchange of patient information.
3) **Patient and Data Verifier***:* Patients may create, manage, control and sign their own EHRs and define the predicate while the data verifier is allowed to access this signature and verify the correctness.

This EHR's system model is shown in Figure 1, consisted of the following four parties: a EHRs server, N authorities, patients and data verifiers. As shown in above diagram, the EHRs server is just like a cloud storage server, which is responsible for storing and transmitting the EHRs. N authorities are various different organizations, such as hospitals, medical insurance organizations, medical research institutes, etc., which are responsible for accepting the enrolment and exchange of patient information. Patients may create, manage, control and sign their own EHRs and define the predicate while the data verifier is allowed to access this signature and verify the correctness.

B. Algorithm:

The MA-ABS scheme in EHRs system has five algorithms as follows:

1) Setup (1λ)->params: It inputs the security parameter 1λ and then outputs the public parameters of this system params.

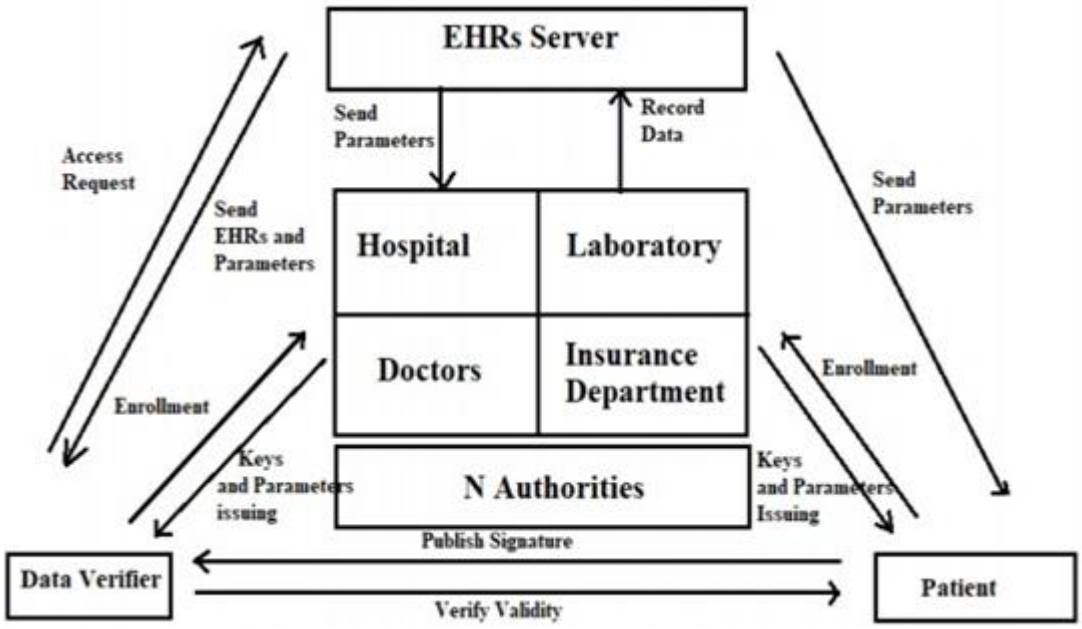

Figure 1: Proposed model

2) Authority Setup (1λ)->(PKk, SKk): This algorithm is executed by the authority. Every authority Ak generates his public and private key (PKk, SKk), where k ∈{1, 2... N}, and N denotes the number of authority in this system.
3) KeyGen (SKk, GID, S) ->(PKU, SKU): This algorithm is controlled by each authority Ak and patient U. It inputs the private key SKk of Ak, the global identifier GID of the patient and an attribute set S; then the algorithm returns the public and private keys (PKU, SKU) of the patient.
4) Sign (PKk, SKU, M, ϒ) ->σ: To sign a message M under the predicate ϒ, it inputs the public key PKk of Ak, the private key. SKU and the predicate ϒ; then the algorithm out puts the signature σ of M.
5) Verify (PKU, S, σ, M, ϒ)->Accept/Reject: To verify a signature σ on a message M with predicate ϒ, it inputs the public key PKU of the patient with attribute set S and the signature with predicate ϒ. First, if the attributes of the data verifier do not satisfy ϒ, it returns null. Otherwise, only if the attribute set S satisfies the predicate, will this algorithm verify the correctness of signature σ and return Accept or Reject.

6. Experimental Results

The results of the system are shown below:

Signing:

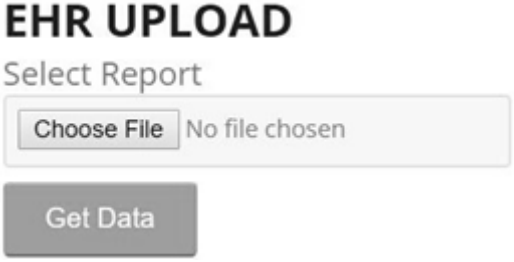

Figure 2: EHR upload page

Figure 2 is the EHR uploading page where the patient can upload their EHR file.

Figure 3: Uploaded data converted into blocks or signature data

Figure 3 shows uploaded patient's health record is converted into signature data.

Figure 4: Patient sharing signature data to the doctors with their public keys

Figure 4 shows patients can share signature data to the doctors with their public keys.

Figure 5 Doctors verifying patient's data with their public key

Figure 5 shows that the doctors can get the signature data of uploaded EHR record of the patient with their public key.

Figure 6: EHR Storage data page

Figure 6 shows that all the signature data is stored in the EHR server

7. Conclusion

Aiming at preserving patient privacy in an EHRs system on blockchain, multiple authorities are introduced into ABS and put forward a MAABS scheme, which meets the requirement of the structure of blockchain, as well as guaranteeing the anonymity and immutability of the information. PRF seeds are needed among authorities and the patient private keys need to be constructed, N – 1 corrupted authorities cannot succeed in collusion attacks. Finally, the security of the protocol is proven under the CBDH assumption in terms of unforgeability and perfect privacy. The comparison analysis demonstrates the performance and the cost of this protocol increases linearly with the number of authorities and patient attributes as well. A non-monotone predicate could be used in many distributed system applications, which enriches the representation of the predicate. Supporting general non-monotone predicates in blockchain technology is the direction of future work.

References

[1] Ming Li, Shucheng Yu, and Wenjing Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute based Encryption", IEEE Transactions on Parallel and Distributed Systems 2012.
[2] IEEE 2012 paper on "Improving the interoperability of healthcare information system through HL7 CDA and CCD standards".
[3] Madhusree N, kavitha G paper on "Blockchain Enabled Secure Electronic Health Records System Storage with Attribute-Based Signature Scheme" Journal in IJRASET Volume 7 Issue V, May 2019
[4]]"Privacy-preserving personal health record system using attribute based encryption, " Master's thesis, worcester polytechnic institute, 2011.
[5] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized private keyword search over encrypted personal health records in cloud computing, " in ICDCS '11, Jun. 2011.
[6] Tatsuaki Okamoto, Katsuyuki Takashima, " Efficient Attribute-Based Signatures for Non-Monotone Predicates in the Standard Model"in IEEE CLOUD COMPUTING, VOL. 2, OCTOBER-DECEMBER 2014
[7] M. Li, S. Yu, K. Ren, and W. Lou, "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings, " in SecureComm'10, Sept. 2010, pp. 89– 106.

[8] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing, " in IEEE INFOCOM'10, 2010
[9] André Henrique Mayer, Cristiano André da Costa, Rodrigo da Rosa Righi, "Electronic health records in a Blockchain: A systematic review"Health Informatics Journal1–16, 2019
[10] Neha Agarwal, Shashikala Tapaswi, "A Trustworthy Agent-Based Encrypted Access Control Method for Mobile Cloud Computing Environment" in Journal Pervasive and mobile computing, 2018.
[11] S. Narayan, M. Gagn´e, and R. Safavi-Naini, "Privacy preserving phr system using attribute-based infrastructure, " ser. CCSW '10, 2010, pp. 47–52.