Journal of Computer Engineering & Information Technology

Research Article

A SCITECHNOL JOURNAL

The Use of Attribute-Based Signature in a Blockchain for Health Records System Storage

Ravikumar Ch*

Abstract

Healthcare Blockchain technology, as a necessity for an effective patient-centered solution to healthcare applications, has immense potential and improves the quality value of electronic healthcare data (EHRs). In order to generate a solid outcome with a patient-centered strategy, we must address many issues and criteria in terms of privacy and also protection, the use of technology, and regulating processes. To maintain the integrity of EHRs embedded in Blockchains, we offer to multiple authorities an attribute-based signature technique in which a patient accepts a message based on the attribute, providing no specifics other than how he attested to it.

Keywords

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

Introduction

Electronic health records (EHRs) provide a service that is very efficient for health record preservation and it will sort out the current medical data on a paper into something that can be quickly accessed on the internet. Furthermore, under the current situation, patients submit their EHRs to numerous locations during their lives, causing the EHRs to move from one service provider to another. As a result, when the patient controls the initial stewardship, the patient risks losing information about current health care data. Patients with EHR permissions are in short supply, and patients rarely have access to their data. As a result, we present Attribute-based signature (ABS), which allows a party to sign a message by identifying the contents. In ABS, a signer who requires a set of authority attributes can sign a message that contains a predicate that is satisfied by his attributes. The signature denotes that a message has been attached by a single user with a small number of properties that satisfy the criteria. Furthermore, we provide a structure for developing ABS mechanisms, after which we will demonstrate a few practical things based on the operations. Finally, we provide a model that is very secure when dealing with a malicious attribute authority, but the protection for this mechanism is proven as the generic group model.

Multiple authorities were introduced into the ABS and MAABS schemes to aim for the protection of patients' confidential data in an EHR system using Blockchain. This satisfies the need for block chain architecture while also ensuring the immutability of the information and the development of patients' private keys. Finally, the protocol's security is demonstrated by the CBDH assumption in terms of unforgettability and privacy. It also describes the expense of work and protocol, which increases as the number of authorities and patients, as well as qualities, increases.

Related Work

This study is built on providing security and privacy to cloud data with cryptography-based access control and attribute encryption. PKE-based approaches commonly employ high-key management systems or allow for the encryption of a file using several user keys from separate sets in order to implement fine-grained access controls.

They look at the use of Blockchain technology to facilitate this change across five stages: (1) digital access rules, (2) information aggregation, (3) knowledge accessibility, (4) patient identification, and (5) immutability of knowledge. We usually look into the problems of block chain-enabled patient-driven capacity, including the number of clinical data transactions, privacy and security, patient involvement, and incentive. We continue by stating that, while patient-driving capacity is linked to a potential treatment trend, given these challenges, it is critical to check how the block chain works [1].

In this paper, The Electronic Health Record (EHR) has a special relationship with doctors (EHR). Doctors, on the other hand, recognise that they are unable to give its effective therapy, despite the fact that they are not. Modern EHR systems, on the other hand, are slow and clunky, making doctors sluggish. Sure, there are many advantages and disadvantages to today's EHRs, as well as a breakdown of how they address the issues they confront. One possible approach is to use the Blockchain, which is the infrastructure that now powers the bit coin cryptocurrency [2].

Modern cloud storage has relied nearly exclusively on storage providers, who act as trusted third parties to move and store data. Data availability, high operational expenses, and data security are among issues that such a setup faces. This article demonstrates how to use blockchain technology to create a secure distributed data space for a keyword search system. The technology will allow users to upload data in encrypted form, distribute data content to cloud nodes, and ensure data availability using cryptographic methods. It gives the data owner the ability to grant permission for others to search their data [3].

EMRs are highly crucial non-public data for support identification and care, and they are typically circulated and shared with peers such as assistance providers, insurance firms, hospitals, scientists, and patient families. This is a huge barrier to keeping track of a patient's medical history. The preservation of the privilege to utilise management by multiple consents, as well as the storage and exchange of knowledge across different entities, only illuminates a patient's technique of care. A patient with a serious medical condition, such as cancer or HIV, must keep a detailed record of their care and treatment, as well as their compliance with post-treatment procedures [4].

This paper [5,6] offers a perfectly secure attribute-based signature (ABS) approach to the conventional model. The protection of the

***Corresponding author:** Ravikumar Ch, Department of Computer Science and Engineering, Lovely Professional University, Punjab, India, E-mail: chrk5814@gmail.com

Received: September 26, 2021 **Accepted:** October 04, 2021 **Published:** October 11, 2021

proposed ABS framework is proven using regular statements, the decision linear (DLIN) assumption, and the presence of collision resistant hash functions. The provable predicates of a new ABS system are much more specific than those of existing ABS schemes, in that the new ABS scheme is the first to accept generic non-monotonic predicates, which will be represented using NOT gates and AND, OR, and Threshold gates, whereas existing ABS schemes only support monotonous predicates. The proposed ABS technique is nearly as effective as the existing one.

Problem Statement

Healthcare researchers must have access to these EHRs on board, and the healthcare solution transformation programme must be completed. To establish the most effective information exchange among healthcare professionals, including patients, standardisation of issue lists is essential across the sector. Certain types of trouble list planning, such as lists auto populated, face severe enforcement and patient security issues in electronic contexts and paper-based solutions may not work. The patient may lose entire control over current healthcare information, whilst the service provider usually retains main control. Patients' access to EHRs is limited, and they are often unable to share such information with researchers or physicians. Interoperability challenges among multiple providers, hospitals, research institutions, and other organisations add to the challenges of high-performance data sharing. Without structured data management and sharing, medical records are distributed rather than integrated [7].

Research Objectives

1) High Security: We can't change a patient's records once they've been inserted into the block; for example, if we need to change the data of the same patient, we'll have to construct a new block for that patient because of the high security.

2) Cost-Effective: When using EHR's method, each patient's health records are kept in blocks that form a chain between all of the individual blocks, and each block has its own private key that we can use to get patient records without having to search the patient again, making it a very cost-effective solution.

3) Trust: All of the patient's health records will be stored in individual blocks; however, we won't be able to modify any of the health records once we've inserted them into the block, so it's pretty trustworthy.

4) It achieves Perfect Privacy-Preserving for Patients: Personal health information is delicate and should be kept private. An EHR programme must have security measures in place to ensure that personal health records can only be accessed by patients and healthcare staff who have given the patient specific consent.

Proposed Model

In this research, we develop a multiple-authority attribute-based signature (MAABS) technique to meet the requirements of block chain in distributed EHR systems. This approach will secure patient privacy and maintain EHRs immutable by combining ABS with block chain technologies [8].

1) First, the use of block chain technology in conjunction with the establishment of an ABS system with numerous authorities in an EHRs system for monotonous predicates, with the number of bilinear pairs involved in Signing increasing linearly as the number of authorities increases.

2) The main issue, according to various authorities, is corruption. Seeds of a pseudorandom characteristic are exchanged and discreetly stored in each and every two authority to mitigate this risk. In fact, each authority's private key is included in the patient's private key in KeyGen. The protocol prohibits conspiracy attacks by N 1 compromised officials under this configuration [9].

3) Finally, we show that, in the random oracle model, the plan is unforgiving in suffering a selective predicate attack, and it retains the signer's entire privacy, which protects patient data from leakage, using Diffie-bilinear Hellman's computation principle.

Modules

1) EHRs Server: The EHRs server functions similarly to a cloud storage server, storing and delivering EHRs.

2) Authorities: N authorities are various institutions, such as hospitals, medical insurance companies, medical research institutes, and so on, that are in charge of accepting enrolment and exchanging patient data.

3) Patient and Data Verifier: Patients have the ability to develop, manage, control, and sign their own EHRs, as well as set the predicate, while the data verifier has access to this signature and may check its accuracy.

The four parties in this EHR system model are presented in Figure 1: an EHRs server, N authorities, patients, and data verifiers. The EHRs server, as illustrated in the diagram, functions similarly to a cloud storage server, storing and transferring EHRs. N authorities are numerous institutions, like as hospitals, medical insurance companies, medical research institutes, and so on, that are in charge of accepting enrolment and exchanging patient data. Patients can develop, manage, control, and sign their own EHRs, as well as set the predicate, with the data verifier having access to this signature and verifying its accuracy.

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.

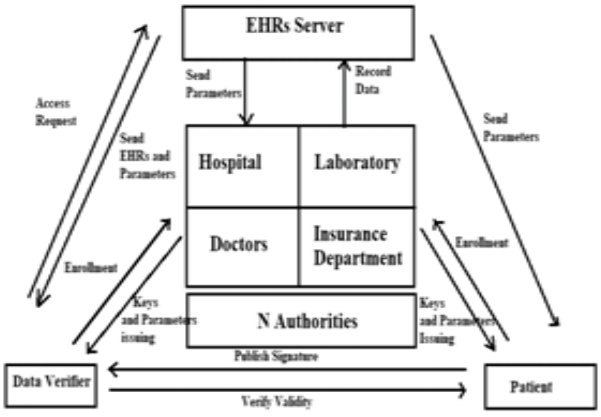

Figure 1: Proposed model.

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 [10].

Experimental results

The results of the system are shown below:

Signing Figure 2 is the EHR uploading page where the patient can upload their EHR file. Figure 3 shows uploaded patient's health record is converted into signature data. Figure 4 shows patients can share signature data to the doctors with their public keys. Figure 5 shows that the doctors can get the signature data of uploaded EHR record of the patient with their public key. Figure 6 shows that all the signature data is stored in the EHR server.

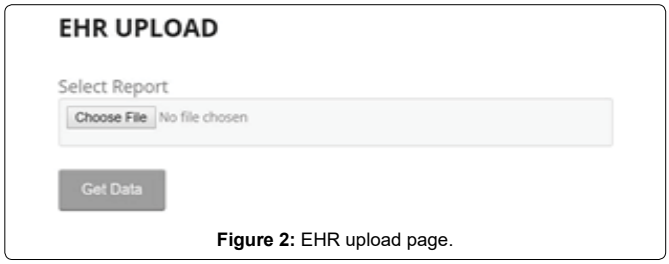

Figure 2: EHR upload page.

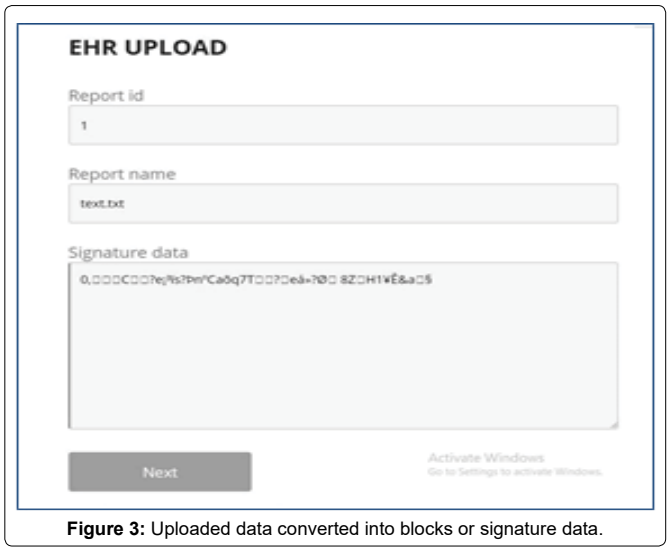

Figure 3: Uploaded data converted into blocks or signature data.

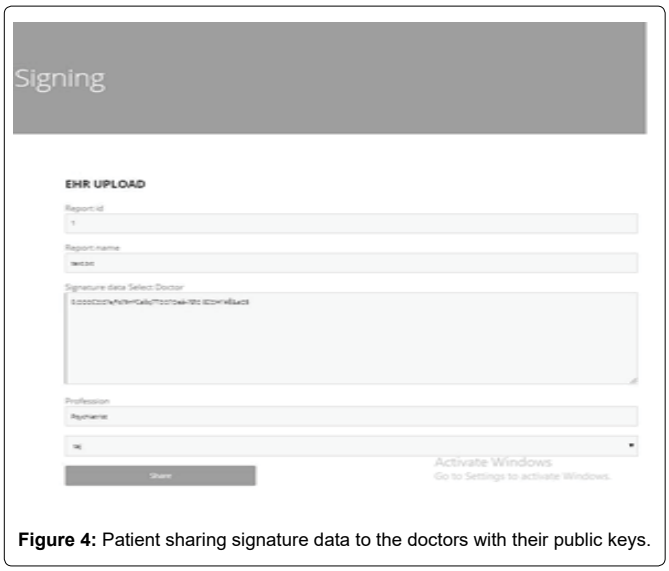

Figure 4: Patient sharing signature data to the doctors with their public keys.

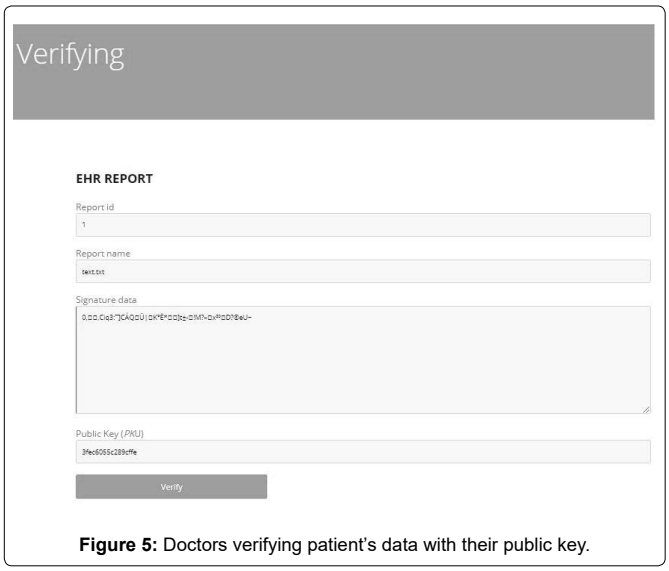

Figure 5: Doctors verifying patient's data with their public key.

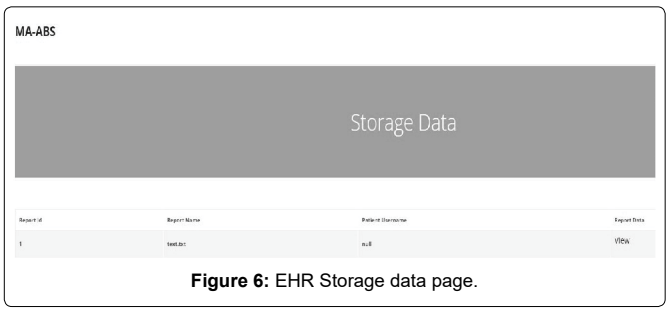

Figure 6: EHR Storage data page.

Conclusion

Multiple authorities are brought into ABS and put forward an MAABS scheme, which fits the requirements of the blockchain structure while also assuring the anonymity and immutability of the information, with the goal of safeguarding patient privacy in an EHRs system on blockchain. N – 1 corrupted authorities cannot succeed in collusion assaults since PRF seeds are required among authorities and the patient private keys must be created. Finally, the

protocol's security is demonstrated in terms of enforceability and perfect privacy using the CBDH assumption. The performance and cost of this procedure grow linearly with the number of authorities and patient features, according to the comparison analysis. A non-monotone predicate can be employed in a variety of distributed system applications, enhancing the predicate's representation. The path of future work in Blockchain technology will be to support general non-monotone predicates.

References

1. Ming Li, Shucheng Yu, Wenjing Lou (2012) Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute based Encryption, IEEE Transactions on Parallel and Distributed Systems, 24(1): 131-143.
2. IEEE (2012) Improving the interoperability of healthcare information system through HL7 CDA and CCD standards.
3. Yao Zheng (2011) Privacy-preserving personal health record system using attributebased encryption. Master's thesis, Worcester Polytechnic Institute.
4. Li M, Yu S, Cao N, Lou W (2011) Authorized private keyword search over encrypted personal health records in cloud computing in ICDCS.
5. Okamoto T, Takashima K (2014) Efficient Attribute-Based Signaturesfor Non-Monotone Predicates in the Standard Model. Ieee Cloud Computing 2.
6. Li M, Yu S, Ren K, Lou W (2010) Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings. SecureComm 10: 89-106.
7. Yu S, Wang C, Ren K, Lou W (2010) Achieving secure, scalable, and fine-grained data access control in cloud computing, in ieee infocom 10.
8. André Henrique Mayer (2019) Cristiano André da Costa6, Rodrigo da Rosa Righi, Electronic health records in a Blockchain: A systematic review. Health Informatics J 1-16.
9. Agarwal N, Tapaswi S (2018) A Trustworthy Agent-Based Encrypted Access Control Method For Mobile Cloud Computing Environment. Journal Pervasive And Mobile Computing.
10. Narayan S, Gagne M, Safavi-Naini R (2010) Privacy preserving phr system using attribute-based infrastructure. Ser CCSW 10: 47-52.

Author Affiliation Top

Department of Computer Science and Engineering, Lovely Professional University, Punjab, India