iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** V **Month of publication:** May 2019

DOI: https://doi.org/10.22214/ijraset.2019.5403

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

Blockchain Enabled Secure Electronic Health Records System Storage with Attribute-Based Signature Scheme

Madhushree N[1], Prof. Kavitha G[2]
[1, 2]*Computer Science and Engineering, UBDTCE*

Abstract: ***Data privacy refers to ensuring that users keep control over access to information, whereas data accessibility refers to ensuring that information access is unconstrained. Conflicts between privacy and accessibility of data are natural to occur, and healthcare is a domain in which they are particularly relevant. In the present article, we discuss how blockchain technology, and smart contracts, could help in some typical scenarios related to data access, data management and data interoperability for the specific healthcare domain. We then propose the implementation of large-scale information architecture to access Electronic Health Records (EHRs) based on Smart Contracts as information mediators. Our main contribution is the framing of data privacy and accessibility issues in healthcare and the proposal of an integrated blockchain based architecture. This technology provides patients with comprehensive, immutable records, and access to EHRs free from service providers and treatment websites. In this paper, to guarantee the validity of EHRs encapsulated in blockchain, we present an attribute-based signature scheme with multiple authorities, in which a patient endorses a message according to the attribute while disclosing no information other than the evidence that he has attested to it. Furthermore, there are multiple authorities without a trusted single or central one to generate and distribute public/private keys of the patient, which avoids the escrow problem and conforms to the mode of distributed data storage in the blockchain. By sharing the secret pseudorandom function seeds among authorities, this protocol resists collusion attack out of N from N −1 corrupted authorities. Under the assumption of the computational bilinear Diffie-Hellman, we also formally demonstrate that, in terms of the unforgeability and perfect privacy of the attribute-signer, this attribute-based signature scheme is secure in the random oracle model. The comparison shows the efficiency and properties between the proposed method and methods proposed in other studies.***
Keywords: Blockchain, Healthcare, EHR, Attribute-based signature (ABS) and Multiple authorities.

I. INTRODUCTION

Electronic Health Records (EHRs) provide a convenient health record storage service, which promotes traditional patient medical records on paper to be electronically accessible on the web. This system was designed to allow patients to possess the control of generating, managing and sharing EHRs with family, friends, healthcare providers and other authorized data consumers. Moreover, provided that the healthcare researcher and providers of such service access these EHRs across-the aboard, the transition program of healthcare solution is expected to be achieved. However, in the current situation, patients scatter their EHRs across the different areas during life events, causing the EHRs to move from one service provider database to another. Therefore, the patient may lose control of the existing healthcare data, while the service provider usually maintains the primary stewardship [1]. Patient access permissions to EHRs are very limited, and patients are typically unable to easily share these data with researchers or providers. Interoperability challenges between different providers, hospitals, research institutions, etc. add extra barriers to high-performance data sharing. Without coordinated data management and exchange, the health records are fragmented instead of cohesive [2]. If the patient has the capability of managing and sharing his EHRs securely and completely, as shown in below figure, regardless of the research purpose or the data sharing among healthcare providers, the healthcare industry will benefit greatly. Drawing support from blockchain technology, the proposed method accomplishes this goal to promote cooperation in the way of deep mutual trust between each organization.

Blockchain technology was formerly developed for the crypto currency Bitcoin and was first presented in the Bitcoin whitepaper by Nakamoto [3] in 2008. Since blockchain technology appeared, it has been celebrated as a new technological revolution just like the invention of the steam engine or the Internet because of its huge impaction on society. In a 2015 World Economic Forum report, 58% of survey respondents expected that 10% of global Gross Domestic Product (GDP) will be relevant to the blockchain technology through 2025 [4]. Blockchain is a decentralized database whose data block is connected chronologically. In the health

care industry, there are many different parties who need to collaboratively manage personal EHRs blockchain (in a model of consortium blockchain), such as medical specialists, hospitals, insurance departments, etc. A variety of parties can lead to resource intensive authentication and the costly information processes for all the stakeholders involved [5]. Based on the Ethereum blockchain technology, the Gem Health Network [6] was constructed to facilitate the access of different healthcare specialists and departments to patient data, reduce health resource waste and treat important illnesses rapidly. In this scenario, the EMRs (in the form of blockchain) of patients should be authenticated based on ownership to avoid misdiagnoses before making accurate diagnoses into block. Furthermore, EMRs stored in block includes name, ID, allergy history and other sensitive data. According to the guidelines of the Health Insurance Portability and Accountability Act (HIPPA) [7], the privacy of patients should be preserved in the process of sharing EHRs. In authentication, for conforming to the characteristics of multiple departments, an attribute-based signature with multiple authorities [8] provides an effective solution to protect the privacy in EHRs systems while attesting that the endorsement derived from the correct patient.

Cloud service providers (CSPs) rely on deduplication techniques to remove duplicate data and thus reduce bandwidth and storage requirements. However, it is equally important for CSPs to ensure the privacy and security of users' data. To address both these issues, secured data deduplication was introduced. Determining duplicate copies in the encrypted image and video data is a substantial challenge. The existing techniques designed for generic data may not be directly suitable for multimedia data. In this paper, a secure block level image deduplication method is presented that eliminates the near identical images in encrypted form, thus protecting the confidentiality of the images. The proposed method adopts the Dual Integrity Convergent Encryption (DICE) protocol. The core idea is to divide the image into blocks and employ the DICE protocol on each block separately. Each block is encrypted using AES with a key that is obtained by hashing the image blocks.

A. Problem Statement

The healthcare researcher and providers of healthcare service access these EHRs across-the aboard, the transition program of healthcare solution is expected to be achieved. However, in the current situation, patients scatter their EHRs across the different areas during life events, causing the EHRs to move from one service provider database to another. Therefore, the patient may lose control of the existing healthcare data, while the service provider usually maintains the primary stewardship. Patient access permissions to EHRs are very limited, and patients are typically unable to easily share these data with researchers or providers.

B. Objectives

1) *More Security:* Once we add the records of a patient into the block we cannot able to change it, suppose if we want to change the records of the same patient, need to create new block for that patient because of more security.
2) *Cost Effective:* By using EHRs system health records of every patient is stored in blocks and make a chain among all the individual blocks and each block has their own private key if we want to get the records of the patient we can use that key so that no need to check up the patient once again, so it's really a cost effective.
3) *Trust:* All the health records of the each patient will be stored in individual block, more over we cannot edit any of the health records once if we feed into the block so that it is very trust worthy.
4) *It Achieves A Perfect Privacy-Preserving For Patient:* Personal health data is a sensible data and must be kept in secret. An EHR system has to implement privacy policies in order to ensure that only the own patient and the healthcare agents, who have explicitly granted permission by the patient, have access to personal health records.

C. Existing System

The healthcare researcher and providers of healthcare service access these EHRs across-the aboard, the transition program of healthcare solution is expected to be achieved. However, in the current situation, patients scatter their EHRs across the different areas during life events, causing the EHRs to move from one service provider database to another. Therefore, the patient may lose control of the existing healthcare data, while the service provider usually maintains the primary stewardship. Patient access permissions to EHRs are very limited, and patients are typically unable to easily share these data with researchers or providers.

D. Disadvantages

1) Less security.
2) No proper Block allocation revised.

E. Proposed System

In this project, to meet the requirement of block chain in distributed EHRs systems, we construct an attribute-based signature (MA-ABS) scheme with multiple authorities. Taking advantage of ABS with the block chain technology, this proposal could preserve the privacy of patients and maintain the immutability of EHRs. The contributions of this work are as follows:

1) First, combing the block chain technology and the construction of an ABS scheme with multiple authorities in a EHRs system for monotone predicates, and the number of the bilinear pairing involving in Signing is linearly increased with the number of authorities.

2) Second, the primary challenge for multiple authorities is collusion attack. To address this risk, a pseudorandom function seed is shared in every two authorities and preserved secretly. Moreover, in KeyGen, the private key of each authority is embedded into the private key of the patient. According to this structure, the protocol resists $N-1$ corrupted authorities collusion attacks.

3) Finally, under the computation bilinear Diffie-Hellman assumption, we prove that, in the random oracle model, the proposal is unforgeable in suffering a selective predicate attack, and it enjoys the perfect privacy for the signer, which prevents the privacy for patient data leakage.

II. LITERATURE SURVEY

A. Survey on "Escrow Free Attribute-Based Signature with Self-Reveal ability"

A major limitation of attribute-based cryptographic primitives is that a curious attribute authority (AA) can simply generate a user's private key to sign or decrypt messages on behalf of this user. With this in mind, different from existing techniques for mitigating the key escrow problem by adopting multiple AAs to generate the attribute-based private key in the attribute-based setting, we make use of a key extraction protocol to replace the key generation algorithm in attributed-based signature (ABS), from which the key generation center (KGC) cannot forge a signature on behalf of a legal user with attributes satisfying the corresponding predicate, despite the the participation in generating the signing key. In addition, considering that the signer anonymous property of ABS makes it difficult for a signer (when necessary) to present evidence to the verifier that a signature is created under his/her signing key, especially in the circumstance where the user uniquely knows his/her private key, we append a signer revelation protocol to our ABS system to enable a user to confirm or deny his/her identity of producing an attribute-based signature. Given these concerns, we define a formal model to capture such a system architecture of ABS called escrow free ABS with self-revealability, and provide a concrete construction [9].

B. Survey on "Multi-authority Attribute-Based Signature"

Attribute-based signature (ABS) is a new cryptographic primitive, in which a signer can sign a message with his attributes, and the verifier can only know whether the signer owns attributes satisfying his policy. Moreover, the signature cannot be forged by any user not having attributes satisfying the policy. ABS has many applications, such as anonymous authentication, and attribute-based messaging systems. But these applications may require a user to obtain attributes from different authorities, which calls for a multi-authority ABS scheme. In addition, multiple authorities can distribute the trust to all authorities, instead of concerning on a single attribute authority. In this paper, we propose a multi-authority ABS scheme, supporting complex policies, expressing AND, OR, and threshold conditions. We use a central authority to assure the usability of attribute keys a user getting from different attribute authorities. To prevent collusion attacks, we adopt a unique global identity (GID) for a user to bind his attribute keys and identity together. And a secret key from the central authority help the verification be independent of the user's identity. So our scheme can fit the requirements of real applications, and also distribute the trust to all authorities in the system [10].

C. Survey on "Blockchain-based System for Secure Data Storage with Private Keyword Search"

Traditional cloud storage has relied almost exclusively on large storage providers, who act as trusted third parties to transfer and store data. This model poses a number of issues including data availability, high operational cost, and data security. In this paper, we introduce a system that leverages blockchain technology to provide a secure distributed data storage with keyword search service. The system allows the client to upload their data in encrypted form, distributes the data content to cloud nodes and ensures data availability using cryptographic techniques. It also provides the data owner a capability to grant permission for others to search on her data. Finally, the system supports private keyword search over the encrypted dataset [11].

D. Survey on "A New Approach to Threshold Attribute Based Signatures"

Inspired by developments in attribute based encryption and signatures, there has recently been a spurt of progress in the direction of threshold attribute based signatures (t-ABS). In this work we propose a novel approach to construct threshold attribute based signatures inspired by ring signatures. Threshold attribute based signatures, defined by a (t, n∗) threshold predicate, ensure that the signer holds atleast t out of a specified set of n ∗ attributes to pass the verification. Another way to look at this would be that, the signer has atleast 1 out of the n ∗t combination of attribute sets. Thus, a new approach to t-ABS would be to let the signer pick some n 0 sets of t attributes each, from the n ∗ t possible sets, and prove that (s)he has atleast one of the n 0 sets in his/her possession. In this work, we provide a flexible threshold-ABS scheme that realizes this approach. We also prove our scheme to be secure with the help of random oracles [12].

E. Survey on "Efficient Attribute-Based Signatures for Non-Monotone Predicates in the Standard Model"

This paper presents a fully secure (adaptive-predicate unforgeable and private) attribute based signature (ABS) scheme in the standard model. The security of the proposed ABS scheme is proven under standard assumptions, the decisional linear (DLIN) assumption and the existence of collision resistant (CR) hash functions. The admissible predicates of the proposed ABS scheme are more general than those of the existing ABS schemes, i.e., the proposed ABS scheme is the first to support general non-monotone predicates, which can be expressed using NOT gates as well as AND, OR, and Threshold gates, while the existing ABS schemes only support monotone predicates. The proposed ABS scheme is comparably as efficient as (several times worse than) one of the most efficient ABS schemes, which is proven to be secure in the generic group model [13].

III.METHODOLOGY

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.

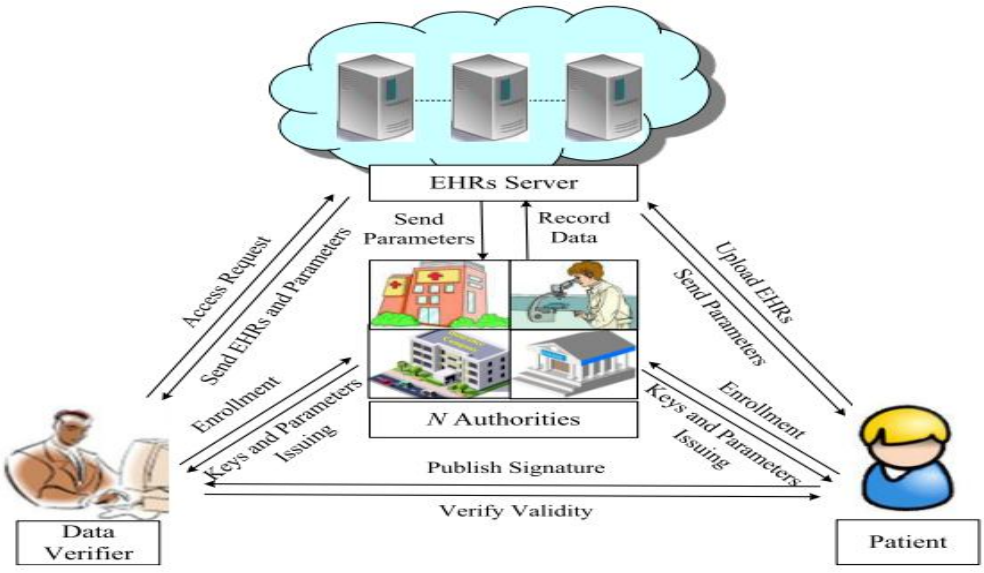


Fig 1: The EHRs system model.

This EHR's system model is shown in Fig 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.

A. Algorithm

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

1) Setup (1^{λ})→ params: It inputs the security parameter 1λ and then outputs the public parameters of this system params.

2) Authority Setup (1^{λ})→ (PK_k, SK_k): This algorithm is executed by the authority. Every authority A_k generates his public and private key (PK_k, SK_k), where k ∈ {1, 2... N}, and N denotes the number of authority in this system.

3) KeyGen (SK_k, GID, S) → (PK_U, SK_U): This algorithm is controlled by each authority A_k and patient U. It inputs the private key SK_k of A_k, the global identifier GID of the patient and an attribute set S; then the algorithm returns the public and private keys (PK_U, SK_U) of the patient.

4) Sign (PK_k, SK_U, M, ϒ) → σ: To sign a message M under the predicate ϒ, it inputs the public key PK_k of A_k, the private key SK_U and the predicate ϒ; then the algorithm outputs the signature σ of M.

5) Verify (PK_U, S, σ, M, ϒ)→ Accept/Reject: To verify a signature σ on a message M with predicate ϒ, it inputs the public key PK_U 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.

IV. EXPERIMENTAL RESULTS

The results of the system are shown below:

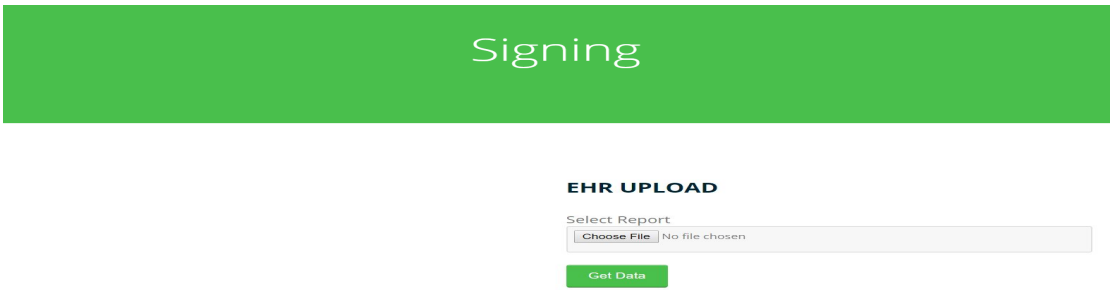


Fig 2: EHR upload page

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

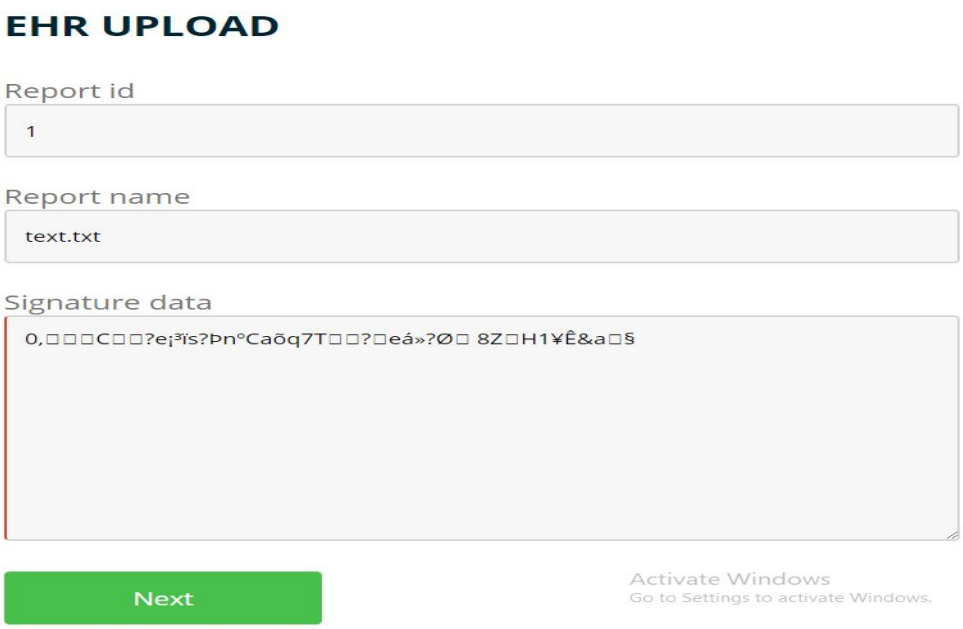


Fig 3: Uploaded data converted into blocks or signature data

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

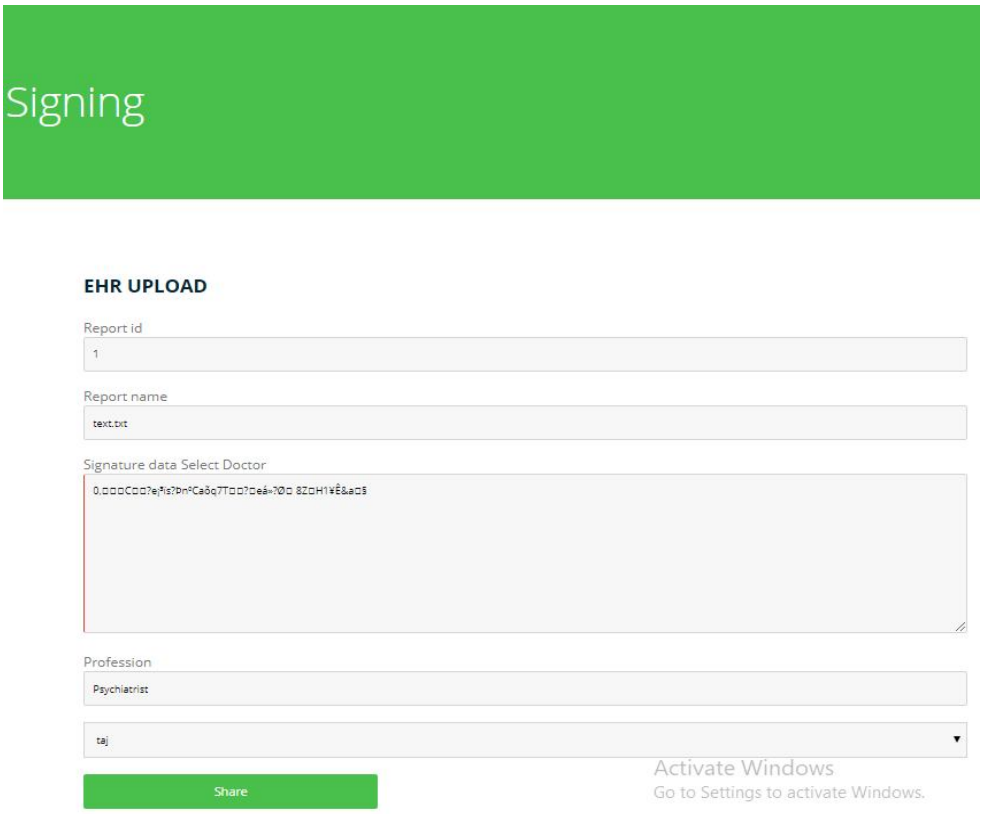


Fig 4: Patient sharing signature data to the doctors with their public keys

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

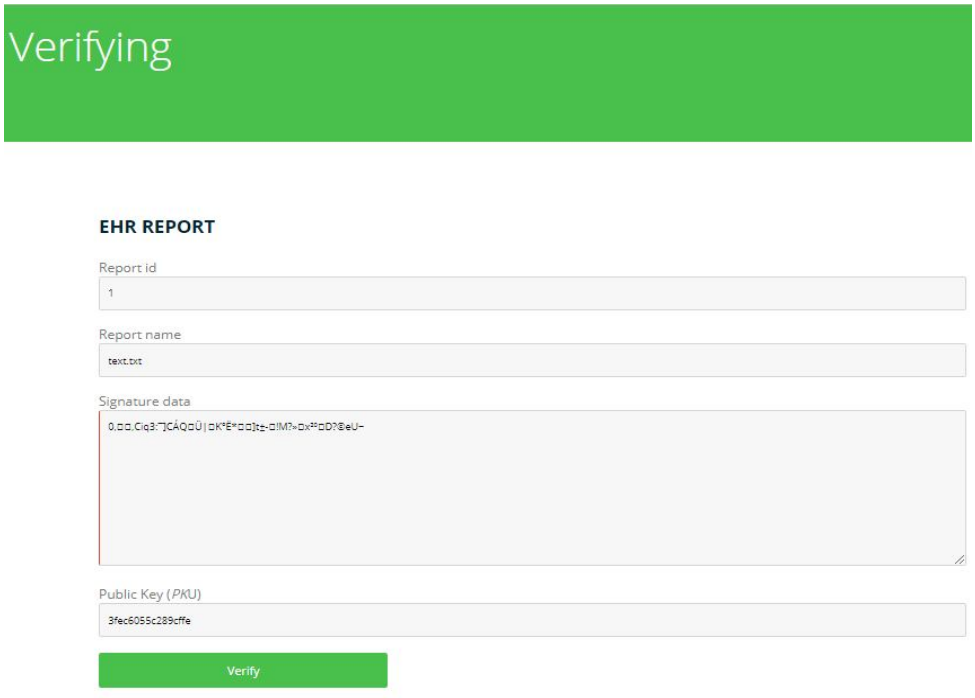


Fig 5: Doctors verifying patient's data with their public key

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

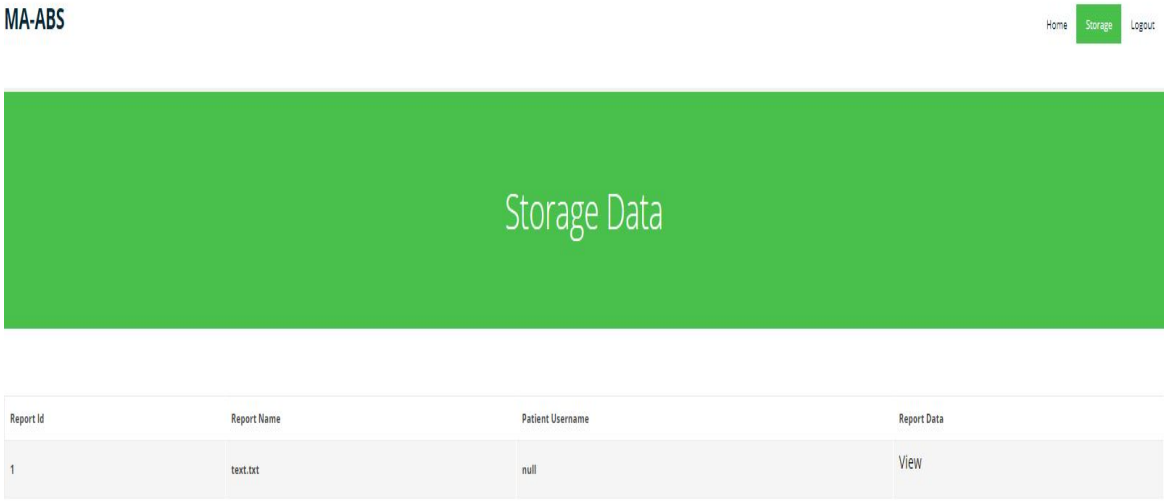


Fig 6: EHR Storage data page

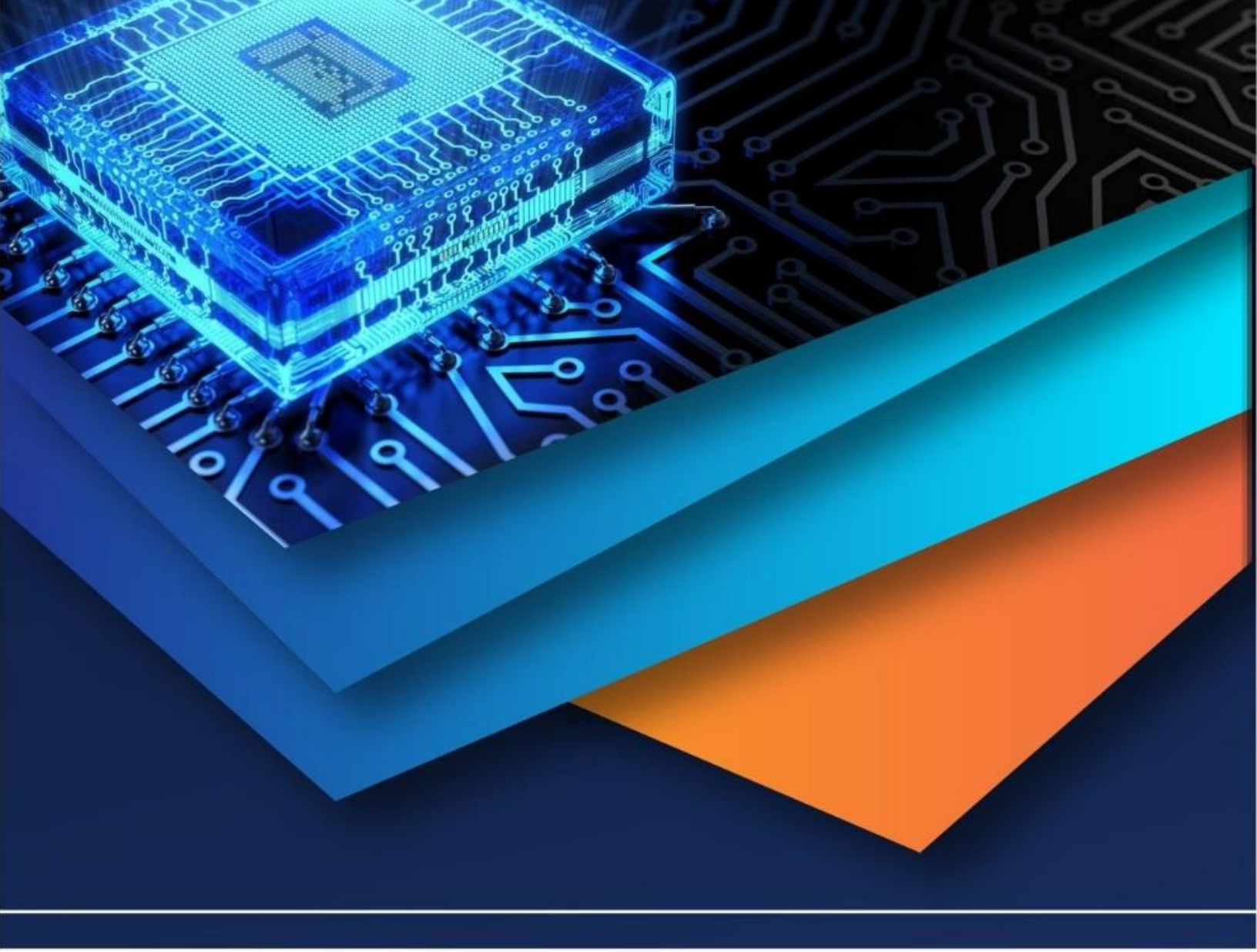
Fig 6 shows that all the signature data is stored in the EHR server.

V. 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] Health Information and the Law. George Washington University Hirsh Health Law and Policy Program. (Aug. 20, 2015). Who Owns Medical Records: 50 State Comparison. [Online]. Available: http://www.healthinfolaw.org/comparative-analysis/who-owns-medical- records-50-state-comparison
[2] K. D. Mandl, P. Szolovits, and I. S. Kohane, ‘‘Public standards and patients’ control: How to keep electronic medical records accessible but private,’’ BMJ, vol. 322, no. 7281, pp. 283–287, Feb. 2001.
[3] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. Accessed: 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[4] World Economic Forum. (Sep. 9, 2015). Deep Shift: Technology Tipping Points and Societal Impact. [Online]. Available: http://www3.weforum. org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf
[5] M. Swan, Blockchain: Blueprint for a New Economy. Sebastopol, CA, USA: O’Reilly Media, 2015, pp. 53–68.
[6] G. Prisco. (Apr. 26, 2016). The Blockchain for Healthcare: Gem Launches Gem Health Network With Philips Blockchain Lab. [Online]. Available: https://bitcoinmagazine.com/articles/the-blockchain-for-heathcare-gem-launches-gem-health-network-with-philips-blockchain-lab-1461674938
[7] U.S. White House. 104th Congress. (Aug. 21, 1996). Public Health Insurance Portability and Accountability Act. [Online]. Available: https://en. wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act
[8] H. K. Maji, M. Prabhakaran, and M. Rosulek, ‘‘Attribute-based signatures: Achieving attribute-privacy and collusion-resistance,’’ in Proc. IACR Cryptol. ePrint Arch., Apr. 2008, pp. 1–23. [Online]. Available: https://eprint.iacr.org/2008/328.pdf
[9] Hui Cui nad Guilin Wang “Escrow Free Attribute-Based Signature with Self-Reveal ability”, july 2013.
[10] Dan Cao and Baokang Zao “Multi-authority Attribute-Based Signature”jan 2012 IEEE.
[11] Hoang Giang Do and Wee Keong Ng “ Blockchain-based System for Secure Data Storage with Private Keyword Search”, 978-1-5386-2002-1/17 $31.00 © 2017 IEEE DOI 10.1109/SERVICES.2017.23
[12] S Sharmila Deva Selvi, Subhashini Venugopalan, C. Pandu Rangan “A New Approach to Threshold Attribute Based Signatures” 2011.
[13] Tatsuaki Okamoto “Efficient Attribute-Based Signatures for Non-Monotone Predicates in the Standard Model” Aug 29, 2014.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY