ARIV
International Journal of Technology
Paper ID: AIJT12042020 Vol1 Issue 2 2020

Authentication or Multiple Authorities proceeding verifies signature to the Assertion of Blockchain in Medical Records

M. Arutkani Achilles & A. Hemlathadhevi
Meenakshi College of Engineering, India

Abstract

The rapid development of Blockchain technology promotes population healthcare, including medical records also as patient-related data. Medical records are entirely controlled by hospitals rather than patients, which complicates seeking medical advice from different hospitals. Patients face a critical need to focus on the details of their own healthcare and restore the management of their own medical data. The rapid development of Blockchain technology promotes population healthcare, including medical records also as patient-related data. This technology provides patients with comprehensive, immutable records, and access to Medical records free from service providers and treatment websites. In this paper, to ensure the validity of Medical records encapsulated in Blockchain, we present a Verifies Signature scheme with multiple authorities, during which a patient endorses a message according to the attribute while disclosing no information aside from the evidence that he has attested thereto. Furthermore, there are multiple authorities without a trusted single or central one to get and distribute public/private keys of the patient, which avoids the escrow problem and conforms to the model 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 authority. Under the idea of the computational bilinear Diffie-Hellman, formally demonstrate that, in terms of the enforceability and excellent privacy of the attribute-signer, this Verifies Signature scheme is secure in the random oracle model.

Index Terms: Verifies Signature (VS), Blockchain, electronic, Medical records, multiple authorities, preserve privacy.

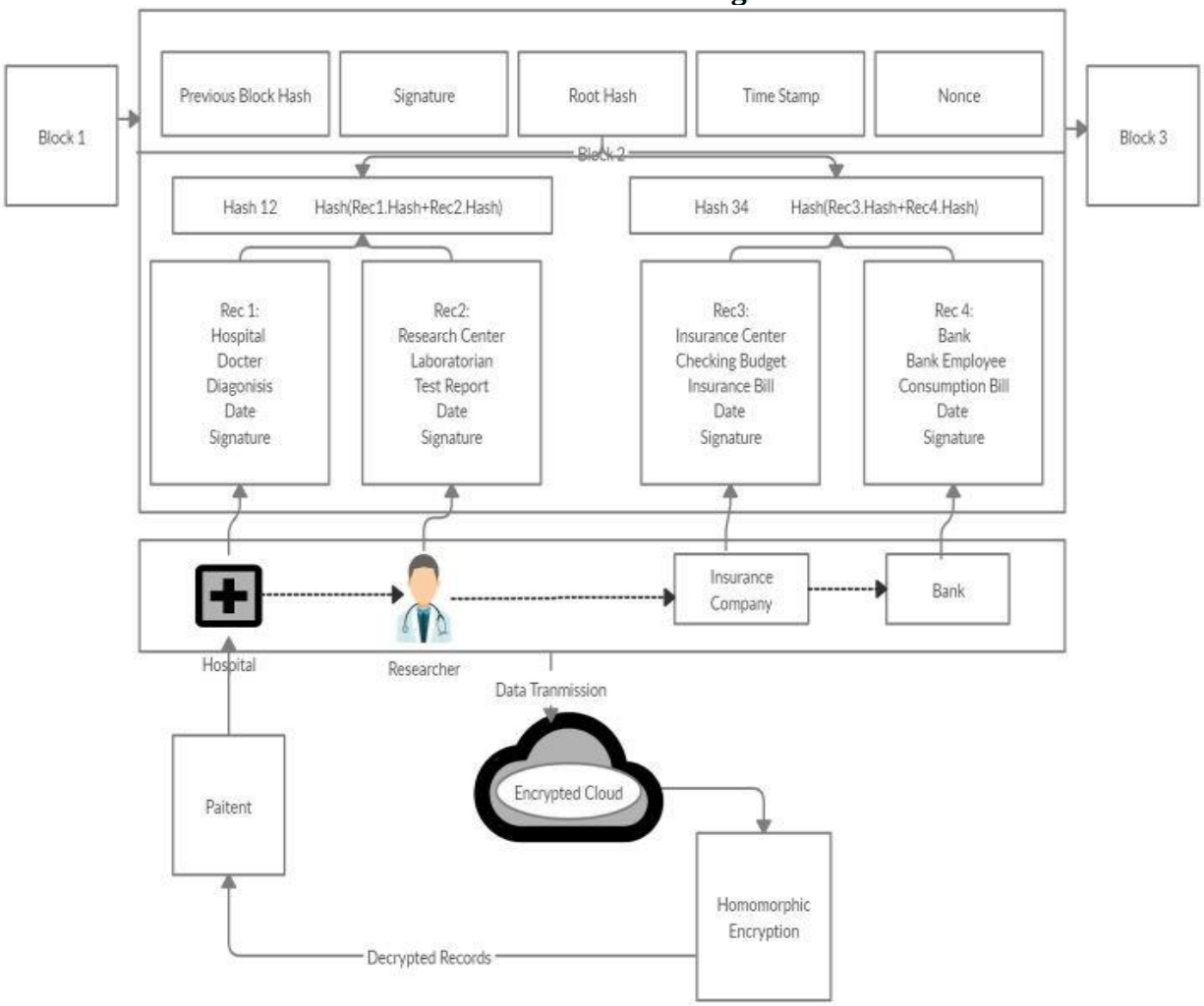
Introduction

Electronic Health Records (Medical records) 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 Medical records with family, friends, healthcare providers and other authorized data consumers. Moreover, provided that the healthcare researcher and providers of such service access these Medical records across-the aboard, the transition program of healthcare solution is expected to be achieved. However, in the current situation, patients scatter their Medical records across the different areas during life events, causing the Medical records 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 (Tang, et al, 2019). Patient access permissions to Medical records 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 (Guo, et al., 2019). If the patient has the capability of managing and sharing his Medical records securely and completely secure 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. Follows the matter that the medical records that need most popular may denied the process. Simple way that the predicate follows the same way of participation on one roll with the same species of data contain on across the fellowship of one roll across the other may varies from one data to another among the centralized server.

Blockchain could be a decentralized database whose data block is connected chronologically. In the healthcare industry, there are many different parties who need to collaboratively manage personal Medical records Blockchain (in a model of consortium Blockchain), such as medical

specialists, hospitals, insurance departments, etc. A variety of parties can result in resource-intensive authentication and therefore the costly information processes for all the stakeholders involved (Li, et al., 2012). Based on the Ethereum Blockchain technology, the Gem Health Network was constructed to facilitate the access of various 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 the block. Furthermore, EMRs stored in the block include name, ID, allergy history and other sensitive data. According to the guidelines of the Health Insurance Portability and Accountability Act (HIPPA), the privacy of patients should be preserved in the process of sharing Medical records.

FIG 1 Architecture Diagram



Our Contributions

In this paper, to meet the requirement of Blockchain in distributed Medical records systems, we construct a Verifies Signature scheme with multiple authorities. Taking advantage of Verifies Signature with the Blockchain technology, this proposal could preserve the privacy of patients and maintain the immutability of Medical records. The contributions of this work are follows:

- First, combing the Blockchain technology and the construction of Proof-of-work this work proposed a scheme with multiple authorities in a Medical records system for monotone predicates, and the number of the bilinear pairing involving in Signing is linearly increased with the quantity of authorities. Taking advantage of this technique it achieves perfect privacy-preserving for a patient.
- The explicit claim of the signature reveals nothing about the identity or attributes of the patient. From another point of view, it guarantees the verifier in enforceability as well. The signature of a patient whose attributes satisfy the claim cannot be generated by collusion of parties who integrate their attributes together. Hence it constructs a secure and controllable mechanism.

1. ***On-Chain and Off-Chain Storage Model:*** For the problem of limited storage capacity and computational resources of the Blockchain, we adopt a combination of Blockchain and off-chain storage to implement data storage. That is, only the addresses of data stored on the Blockchain, and the medical record is encrypted and stored in each node. This makes easier to sharing medical record cross different CDOs while avoiding cumbersome data migration. Specifically, as shown in Fig. 2, once a doctor has created a medical record, he signs the medical record with his private keys related to his attributes and stores the signed medical record in his database. Then the doctor can share the medical record by signing the address of the stored data with his attributes and publishing it on the Blockchain. When users want to access the medical record, they first verify the publisher's signature of the stored address on the Blockchain, and then retrieve the medical record from the node and verify the medical record.

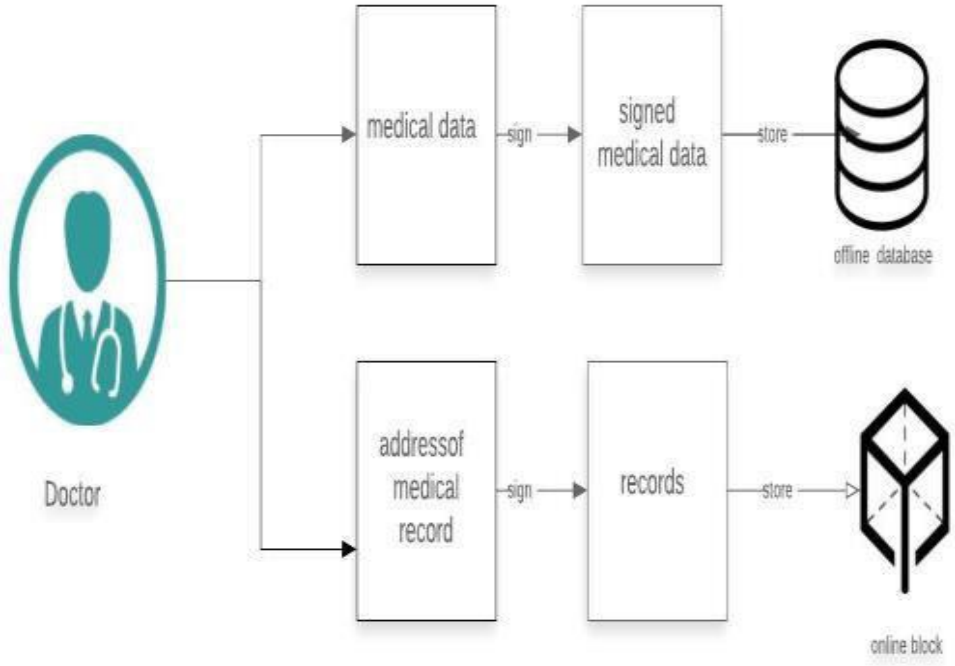


FIG 2 off-chain and on-chain storage

2. ***Roles: there are three major roles***

   User: in our protocol, users include doctors, patient and other users such as researchers. Doctors are responsible for creating a medical record and signing the data with their attributes. Doctors also can share the medical record with other users by broadcast its address in the Blockchain. Patients and other users can retrieve and access the medical record whose stored address are published on the Blockchain by verifying the signatures of both medical records and its address.

   Authority Agency: The different attributes of the user are issued by one or more authority agencies. Authority agencies are responsible for issuing the signature keys related to the attributes to the users.

   Administrator: the administrator generates a global public parameter GP when the system is initialized, and it assigns a global identity GID to each user entering the system. The administrator also manages medical records.

3. ***Nodes:*** The nodes are divided into primary and Backup node.

   Primary node: they collect the group of traction broadcasted d on the network into one block, creating a new block

Backup Node: They can create new transactions and publish them to the network. If they satisfy the access policy, they can verify the signature of the transaction. In our scheme, in addition to having its unique identifier, a node has a series of attributes. Every transaction that the user publishes to the block will carry his signature. This signature does not reveal the identity of the signer but is based on a series of attributes of the signer. When a user accesses data in a block, he needs to verify this signature first. Verification can pass only if the signature matches a specific attribute. Conversely, if the signer's attributes do not meet the verifier's requirements, the verification fails, indicating that this is not a medical record created by a doctor who meets these specific requirements. Attribute-based signatures can not only achieve the anonymity of signers but also can effectively verify the authenticity of medical record data.

Performance Analysis

Sign-Verify, the cost of the proposed protocol increases with the number to the authority and attribute of the user linearly. In the process of Sign, this protocol needs the cost of (6-t) Ts NTp. In the process of Verify, the cost of Ts Te (2tN 1) Tp is consumed. For the communication overhead, the signature size in the proposed construction is only related to the entity attribute number, i.e., the size of signature is (6 t) G. Considering the other properties, this protocol with multiple authorities supporting monotone predicate, and its security is proven in the random oracle model with the secure manner into which

1. ***Global Setup:*** The global setup phase is to install the Health- care scheme. The input of this phase is a security parameter λ, and the global setup algorithmic will generate a bilinear group output the global public parameter GP = (N, g). In addition, G with the generator g, and its order is N. The algorithm will choose a hash function that will be used for the system. This hash function H can map the global identities GID to an element of G.

Algorithm 1 Global Setup Phase

Input: a security parameters g, the global public parameter GP = (N, g), and a hash
Output: a bilinear group G of order N, which generator is function H which map the global identities GID to an element of G.

Under the intractability of CBDH problem. Furthermore, the proposed protocol achieves perfect privacy and resists collusion attacks. In addition, the protocol developed by Okamoto and Takashima has a unique feature of supporting the Non- monotone predicate, which can be described by the NOT gates as well as the AND, OR and threshold gates. System Setup, this algorithm produces the system public parameters interactively execute the Authority Setup algorithm to generate their master secret keys. In this phase, we require that authorities can reach a consensus on the authenticity of all master secret keys, although there has no trusted center. Next, Level users can obtain their signing key from users who distributed execute the Key Generation algorithm.

Algorithm 2 Authority Setup Phase

Input: global public parameter GP. Output: the signature key SIK and the verification key V K for each attribute i.

Then, users will produce some medical-related information, e.g., diagnosis. To ensure the non-repudiation of such information, we require that users run the User-Sign algorithm to sign it. Finally, an authority collects the medical-related information users run **User-Sign** algorithm to sign it. Finally, an authority collects the medical-related information and signatures from Level 2 users to form a block. To ensure the authenticity of block, we require the authority signs it by running **Authority-Sign** algorithm. The message M taken as input to this signing algorithm consists of previous block hash, time stamp, Merkle root of medical records, and identity of the authority.

2. ***User Setup:*** Every doctor and patient entering the sys- tem needs to run this algorithm. The user needs to submit an application to the authority, and the authority will then issue the signature key corresponding to the user's attribute and parameter $GP = (N, g)$, user's global identities GID, a set of the user's attributes i and the signature key $SIK = \alpha_i, y_i$ as some system parameters to be used. It takes the global public input and generate the signature key set for each attribute. In this phase, it calculates the user's signature key. $SIK_{i,GID} = \{g^{\alpha i}, H(GID)^{y i}\}$ for each attribute i.

Algorithm 3 User setup Phase

Input: the global public parameter *GP*, the global identities of the user *GID*, a set of the user's attribute *i* and the signature key *SIK*.

Output: the signature key set $SIK_{i,GID}$ for each attribute *i* corresponding to each *GID*

Verification: In our system, doctors and patients put the EHR on healthcare Blockchain to allow the doctors in different hospitals to view the data. When viewing data, the user needs to verify that the data was issued by a doctor with specific attributes. First the user needs to verify the EHR address stored in the transaction in the Blockchain, , then the medical records stored in the database is found by address and the medical records is verified,

Algorithm 4 Transaction Verification

Input: the global public parameter *GP* , the EHR address *Addr* and the signature σ in *ProposalRecord*, a series of attributes that need to be verified and the corresponding verification key $\{VK\}$.

Output: if the verification is successful, output 1, otherwise output 0

2: use the hash function *H* to get the hash of the address *H* (*Addr*);

3: calculate the verification formula with the verification key*V K* ;

4: check whether the equation holds? 5: **return** {0, 1};

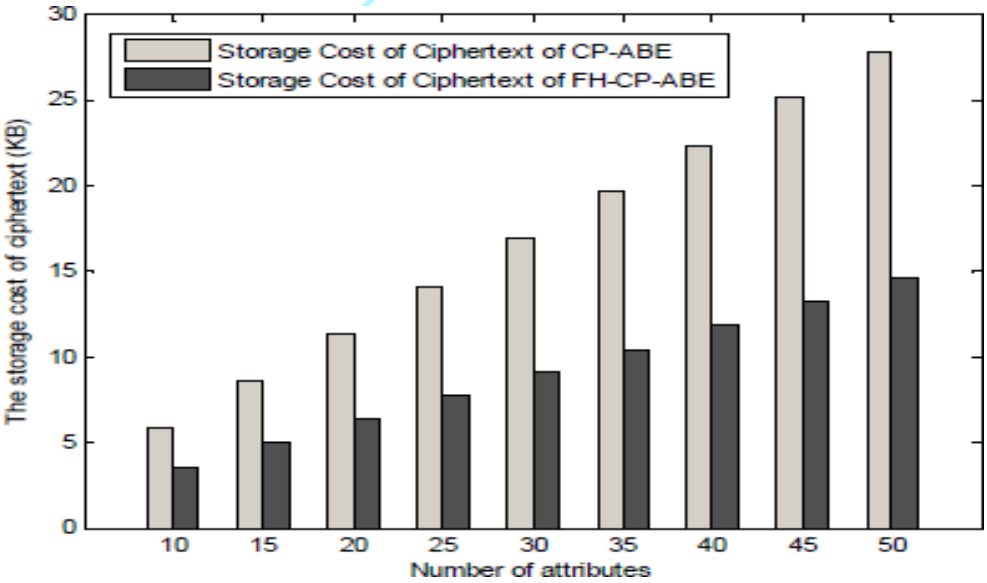


FIG 3 Attribute meets the predicate

Table 1 Comparison among signing, verification and collusion attack.

Properties	4	3	2	1	Ours
Cost of Signing	(lt+t+3)Te	(7l+15)Te	(6+2l+lt)Te	(l+t+16)Te+ 3Tp	(6+t)Ts+NTp
Cost of Verification	(2lt+1)Te+ (l+2+((t-1)(l+1)) Tp	(l+1)Te+ (l+2)Tp	(l+2)Te+ (l+4)Tp	(2lt+12)Te+ (l+7+(t-1)(l+1))Tp	Ts+Te(tN+1)Tp
Size of Signature	(l+t+2)|G|	(7l+11) |G |	(l+t+2) |G |	(l+t+11) |G|	(2+t) |G|
Multi- Authority	Extensible	Extensible	No	Extensible	Extensible
Security Model	Generic Group	Standared	Generic Group	Standared	Random
Privacy	Perfect	Perfect	Perfect	Im Perfect	Perfect
Resist collusion attack	No	No	No	No	Yes

l denotes the number of attributes involved in the predicates.

t denotes the number of user attribute that meets the predicates.

Conclusion and Future Work

Aiming at preserving patient privacy in a Medical records system on Blockchain; multiple authorities are introduced into ABS and put forward a Verifies Signature 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 authority cannot succeed in collusion attacks. Finally,

the security of the protocol is proven under the CBDH assumption in terms of enforceability 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

Gordon, W.J. and Catalini, C., 2018. Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. *Computational and structural biotechnology journal*, *16*, pp.224-230.

Guo, R., Shi, H., Zhao, Q. and Zheng, D., 2018. Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems. *IEEE access*, *6*, pp.11676-11686.

Li, M., Yu, S., Zheng, Y., Ren, K. and Lou, W., 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), pp.131-143.

Sun, Y., Zhang, R., Wang, X., Gao, K. and Liu, L., 2018, July. A decentralizing attribute-based signature for healthcare blockchain. In *2018 27th International conference on computer communication and networks (ICCCN)* (pp. 1-9). IEEE.

Tang, F., Ma, S., Xiang, Y. and Lin, C., 2019. An efficient authentication scheme for blockchain-based electronic health records. *IEEE access*, *7*, pp.41678-41689.

Wang, H. and Song, Y., 2018. Secure cloud-based EHR system using attribute-based cryptosystem and blockchain. *Journal of medical systems*, *42*(8), p.152.

Xu, W., Wu, L. and Yan, Y., 2018. Privacy-preserving scheme of electronic health records based on blockchain and homomorphic encryption. *J. Comput. Res. Develop.*, *55*(10), pp.2233-2243.

Zhang, P., White, J., Schmidt, D.C., Lenz, G. and Rosenbloom, S.T., 2018. FHIRChain: applying blockchain to securely and scalably share clinical data. *Computational and structural biotechnology journal*, *16*, pp.267-278.