THINK INDIA JOURNAL

ISSN:0971-1260
Vol-22- Issue-14-December-2019

A Novel Approach for Privacy-Preserving and Fully Decentralized Storage System on Blockchain

Aneela[1],Ashwini K [1], Darshini M[1],Umadevi[1], *Mrs.C.Valarmathi*[2]

[1]Student, Dept. Of Computer Science and Engineering,
[2]Assistant professor, Dept of CSE, SriSairam College of Engineering, Bangalore, Karnataka

ABSTRACT

With the block chain receiving extensive attention in recent years, many storage schemes based on the blockchain havebeenproposed as alternative meansodoudstoragefordata outsourcing. However, the conventional access control methods in the current sharing schemes require either individual permission granting via symmetric keys or a trusted central attribute authority for ciphertext-policy attribute-based encryption (CPABE). In this paper, we propose a fully decentralized data storage and sharing system on a blockchain by using multi-authority CP-ABE and decentralized multi-authority attribute-based signatures (DMA-ABSs). The public ledger of the blockchain provides immutable logs of data address pointers, access policies, attribute public keys and data queries. In addition, data consumers' attributes are publicly verifiable through the DMA-ABS scheme without revealing more private information. Finally, the combination of the multi-authority CPABE with the blockchain guarantees the integrity, confidentiality, and accessibility of the data without the need for trusted third parties, such as a central authority or a data centre.

KEYWORDS:privacy, blockchain, access control, CP-ABE, attribute-based signature.

I. INTRODUCTION:

In recent years, rapidly developing cloud computing has promoted increasingly more organizations and individuals to outsource their data for storage and sharing due to its low cost and high accessibility. However, this datacenter-based strategy heavily depends on trusted third parties who are sometimes compromised, and therefore there are some risks such as the loss of data and failures in service availability. CP-ABE is a well-developed and widely used cryptographic primitive for access control management that allows data owners to encrypt their data and to determine the corresponding access policies for those who can decrypt the data. Therefore, CP-ABE has been applied for blockchain storage to improve the sharing efficiency [4], [5].Multi-authority CP-ABE, which is a decentralized CP-ABE approach in which anyone can create an attribute and authorize different users, can be used to further decentralize blockchain storageauthorityattribute-based signature (DMA-ABS) has been introduced for anonymous authentication before accessing data.In this paper, we combine multi-authority CP-ABE and DMA-ABSs with a blockchain to design a fully decentralized storage and sharing system with auditable access data in which no trusted third parties are required and users' privacy is well preserved. The rest of the paper is organized as follows. Section II provides an overview of the related work.

 Copyright © 2019Authors

ISSN:0971-1260
Vol-22- Issue-14-December-2019

Section III describes the concept and details of the system. Section IV describes the future work in this work and Section V concludes the paper.

II. RELATED WORK:

Typically, a blockchain is managed by a peer-to-peer network, and its data are replicated and stored at individual nodes in the network. Thus, no trust in third parties is required in this decentralized, distributed, and public system, which also eliminates the risks of datacentrebased solutions that we mentioned before. Due to these properties, some storage solutions have been proposed based on the blockchain. Ziskind et al. [1] design a decentralized personal data management system in which the data owner can store and control the access of their data.6942019 IEEE 43rd Annual Computer Software and Applications Conference ©2019 IEEE DOI 10.1109/COMPSAC.2019.10289. Do and Ng [2] introduce a private keyword search into blockchain storage that allows authorizeddataconsumerstosearchforkeywordsoencrypted data. However, individual permission granting is still required. CP-ABE is an advanced access control method that was proposed by Bethencourt et al. [3] for efficient outsourced data sharing. In CP-ABE, the ciphertext determines the access policy structure while the keys are generated according to the attributes (or credentials. To address the efficiency problem of data sharing in the blockchain, Yuan et al. [4] combine CP-ABE with blockchain storage. Even though this scheme enables data sharing depending on attributes, it heavily relies on a central authority for the attribute assignment. Additionally, Jemel and Serhrouchni [5] introduce the valid time to CP-ABE-based blockchain storage where revocation would be unnecessary.

III.METHODLOGY:

In this section, we propose the methodology of this system to show how blockchain technology, multi-authority CP-ABE and DMA-ABS are combined to build a fully decentralized storage system. There are the three following roles for users. 1) Data Owners: users who own data and want to outsource them for storage and sharing. 2) Data Consumers: users who are interested in some data and want to access them. 3) Blockchain Nodes: entities that maintain the blockchain and a discrete hash table for storage. On the basis of these roles, we introduce a new role for attribute distribution: 4) Attribute Authority: users who create attributes and provide authorization. There are three kinds of transactions that are allowed in the scheme: TXATTRIBUTE, which is used for attribute distribution; TXDATA, which is used for data storage and the access policy assignment; and TXACCESS, which is used for retrieval and verification. The cipher is briefly shown as follows. We refer the interested reader to [7] and [9] for more details and the proof. Global Setup(λ) $\rightarrow$ GP. This is the initializing algorithm that takes a security parameter λ as the input and generates global parameters for the scheme.

A correct multi-authority CP-ABE system ensures that if whenever the global parameter GP is initialized by the Global Setup , the ciphertext CT is generated from the message M via the Encryption algorithm with the access structure (A,ρ) , $\{Ki,GID\}$ is a collection of attributes that are issued through the Key Generation algorithm for the same global identities GID, and their associated attributes satisfy the access structure (A,ρ), then the message M can be recovered through the algorithm *decryption(CT,{Ki,GID},GP)=M.* Meanwhile, a correct DMA-ABS scheme ensures that if whenever GP is initialized by the Global Setup, the signature σ

 Copyright © 2019Authors

ISSN:0971-1260
Vol-22- Issue-14-December-2019

on the message M with the predicate (A,ρ) is generated through the ABS.Signing algorithm using {Ki,GID}, which is issued through the Key Generation algorithm for the same global identity GID and for a collection of attributes that satisfies the predicate (A,ρ), the signature is verified to be true. This involves the following algorithms,

Algorithm1Authorization:

1: procedure(λ,i,GID)

2: AAi and UGID form a secure channel

3: AAiexecutes :

4: GP ←Global Setup(λ)

5: (PKi,SK i) ←Authority Setup(GP)

6:Ki,GID←KeyGeneration(GID,i,SKi,GP)

7: AAi sends Ki,GID to UGID 8: to authorize UGID with attribute i 9: end procedure

This is the initializing algorithm that takes a security parameter λ as the input and generates global parameters for the scheme.

Authority Setup(GP) → (PKi,SK i). To create an attribute i, this algorithm uses the commonly agreed parameters GP to produce the pair of public PKi and secret master keys SKi. Encryption(M,(A,ρ),GP,{PKi}) → CT. The algorithm encrypts a message M according to the access structure (A,ρ) and public keys of the relevant attributes to output the ciphertextCT.The private key Ki,GID of an attribute i for a user with the identity GID is issued by taking the user's global identity GID, the global parameter and the authority's secret master key SKi as inputs. Thus, we use the public keys of users as global identities.

*Decryption(CT,{Ki,GID},GP) → M.*If a decryptor holds the private keys of a collection of attributes {Ki, GID} that satisfies the access structure, then message M can be recovered from the ciphertext CT with the global parameters GP. ABS.Signing({Ki,GID},M,(A,ρ),{PKi},GP) → σ. The signature σ of a message M with a predicate (A,ρ) can be generated when the combination of involved attributes satisfies the predicate(A,ρ). ABS.Verification(σ,M,(A,ρ),{PKi},GP) →{ 0,1}.Asignature σ on a message M with the predicate (A,ρ) is verified to be True(1) or False (0) using the public keys of the relevant attributes {PKi}. The {Ki,GID} is a collection of attributes that are issued through the Key Generation algorithm for the same global identities GID, and their associated attributes satisfy the access structure (A,ρ), then the message M can be recovered through the algorithm Decryption(CT,{Ki,GID},GP)=M. Meanwhile, a correct DMA-ABS scheme ensures that if whenever GP is initialized by the Global Setup, the signature σ on the message M with the predicate (A,ρ) is generated through the ABS.

Algorithm 2 Outsourcing Data:

1.PROCESSDATATRANSACTION(TM,σ,PKsig)

2: TXType,CT,AP,TS,(A,ρ) ←Parse(TM) 3: if V erification (TM,σ,PKsig)=Truethen4: if AP = H(CT) then

 Copyright © 2019Authors

ISSN:0971-1260
Vol-22- Issue-14-December-2019

5: TM← TXType||TS||(A,ρ)||AP

6: L[H(TM||σ)] ← TM||σ

7: ds[AP] ← CT

8: end if

9: end if

10: end procedure

Algorithm 3 Access Query:

1:PROCESSACCESSQUERY(TM,σ)

2: TXDATAHash,APQuery,←Parse(TM) 3: if L[TXDATAHash]

= Ø then

4: (A,ρ),AP←Parse(L[TXDATAHash])

5: if AP = APQuery then

6: while L[ρi]

= Ødo

7: {PKi}←Parse(L[ρi])

8: end while

9:ifABS.Verification(TM,{PKi},(A,ρ),σ)= Truethen return ds[AP]

10: end if

11: end if

12: end if

13: end procedure

IV.FUTURE ENHANCEMENT:

The above section describes algorithms to preserve the privacy in the decentralized storage system .Then, as a future work, we would like to address the problems in revocation problems.

V.CONCLUSION:

This paper has presented a novel decentralized storage scheme by using multi-authority CP-ABE, DMA-ABS and blockchain technology. This system provides efficient access control and security of the data storage with the privacy preserved and no central entities required.

REFERENCES:

 Copyright © 2019Authors

ISSN:0971-1260
Vol-22- Issue-14-December-2019

[1] G. Zyskind, O. Nathan et al., "Decentralizing privacy: Using blockchain to protect personal data," in 2015 IEEE Security and Privacy Workshops. IEEE, 2015, pp. 180–184.

[2] H. G. Doand W. K. Ng, "Blockchain-based system forsecuredatastorage with private keyword search," in 2017 IEEE World Congress on Services (SERVICES). IEEE, 2017, pp. 90–93.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in 2007 IEEE symposium on security and privacy (SP'07). IEEE, 2007, pp. 321–334.

[4] C. Yuan, M. Xu, X. Si, and B. Li, "Blockchain with accountable cp-abe: how to effectively protect the electronic documents," in 2017 IEEE 23rd international conference on parallel and distributed systems (ICPADS). IEEE, 2017, pp. 800–803.

[5] M. Jemel and A. Serhrouchni, "Decentralized access control mechanism with temporal dimension based on blockchain," in 2017 IEEE 14th International Conference on e-Business Engineering (ICEBE). IEEE, 2017, pp. 177–182.

[6] H. K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-based signatures," in Cryptographers' track at the RSA conference. Springer, 2011, pp. 376–392. [7] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in Annual international conference on the theory and applications of cryptographic techniques. Springer, 2011, pp. 568–588.

 Copyright © 2019Authors