Secure Systematic Blockchain Based Access Control Scheme With Multiple Attribute Authority

Dhanya P[1], Shiny S[2]
[1, 2] Dept of Computer Science and Engineering
[1, 2] Ponjesly College of Engineering

Abstract- *Ciphertext-policy attribute-based encryption (CP-ABE) used for secure data sharing. In existing system all user attributes are managed by a single central authority, it is easy to occur a single point of failure. In this work propose a Blockchain-based Multi-authority Access Control scheme called BMAC for sharing data securely. In addition,to establish a trust among multiple authorities and make a smart contract to compute tokens for attributes managed across multiple management domains, it reduces communication and computation overhead on the user side. The blockchain helps to record the access control process in a secure manner.*

Keywords- Access control, Blockchain, Attribute Authority, cipher-text

I. INTRODUCTION

The introduction of Bitcoin did the introduction of Blockchain technology. Bitcoin is a form of digital currency introduced by a pseudo name called ‘‘Satoshi Nakamoto’’ in 2008. He represented that direct online payment from one party to another without using a third party. This electronic cash system mainly overcomes the problem of double-spending the money, primarily the digital currency nature that allows being easily duplicated and spent more than once. This problem is solved by linking each transaction with one another in a tamper-resistant manner.

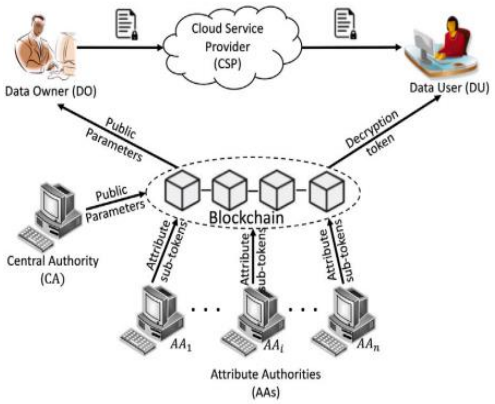
The blockchain is an indestructible digital ledger for keeping track of economic maintain not only financial transactions but virtually everything that has a value.When implement blockchain technology, no government interference is needed, and zero percent of fraud due to consensus validation.

II. PROPOSED SYSTEM

In this work propose a blockchain-based multi-authority access control scheme, named BMAC, for secure cloud data sharing to address the issues mentioned above such as multi-authority cross domain collaboration, single point of failure and high computational and communicational overhead. A trustable access logs is recorded on blockchain, the data owner can easily monitor user behaviour. The main contributions are:

A decentralized access control scheme based on blockchain and multi-authority attribute-based encryption, it can solve the problems of a single point of failure high computation and communication overhead on the data user side. The data access logs are recorded on the blockchain and realize auditable access control management.

III. SYSTEM DESIGN



Central Authority(CA)

The CA has a responsible for the format of system by setting up system parameters and utilize smart contracts.

Attribute Authorities(AA)

The AA is responsible for managing attributes to data users through blockchain. There is a many-to-many mapping relationship between attributes.

Cloud service provider(CSP)

The CS is essential for data management and for allowing legitimate users access to data

Data Owner(DO)

The DO performs data access control based on cryptography. DOs set access policies, perform encryption on data file before uploading it to the CSP, and uploads hash value of data ciphertext and key ciphertext to blockchain.

Data User(DU)

When a user wants to access data, they need to request a decryption token from the blockchain, and the decryption token is associated with a series of attributes. Users have different decryption permissions with different attributes. If the user's attributes satisfy the access policy can decrypt successfully.

Blockchain

The blockchain stores public parameters and access metadata. It also has entities to perform partial trusted computing, and enable multiple AA to manage user attributes. As each entity has a unique address in the blockchain network, which used as a global identity of entity.

IV. ALGORITHM DESCRIPTION

Diffie Hellman Key Generation Algorithm

Private key of sender = Xa
Public key of sender = Ya
Private key of receiver = Xb
Public key of receiver = Yb
'a' is the primitive root of prime number 'n'

Step-02:

Sender calculates its public key as

$$Ya = a^{X_a} \, mod \, n$$

Receiver calculate its public key as

$$Yb = a^{Xb} \, mod \, n$$

Step-03:

Sender calculates secret key as

$$Secret \; key \; = (Yb)^{Xa} mod \; n$$

Receiver calculates secret key as

$$Secret \; key \; = (Ya)^{Xb} mod \; n$$

V. CONCLUSION

In this work propose a multi-authority attribute-based access control scheme based on blockchain, named BMAC, for data sharing. This scheme achieves each attribute is managed across different domains and eliminates a single-point bottleneck of the existing multi-authority system. Besides, with the blockchain-based scheme, trustable and immutable access logs are recorded on blockchain, such that data owner can easily monitor users' access behaviour.

REFERENCES

[1] V. Goyal, O. Pandey, A. Sahai, B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data" Proceedings of the ACM Conference on Computer and Communications Security, Vol. 89–98, 2006, pp. 89–98.

[2] Y. Xue, K. Xue, N. Gai, J. Hong, D.S.L. Wei, P. Hong, "An attribute-based controlled collaborative access control scheme for public cloud storage", IEEE Trans. Inf. Forensics Secur. 14 (11) (2019) 2927–2942.

[3] J. Hao, C. Huang, J. Ni, H. Rong, M. Xian, X.S. Shen, "Fine-grained data access control with attribute-hiding policy for cloud-based iot", Comput. Netw. 153 (2019) 1–10.

[4] J. Li, N. Chen, Y. Zhang, "Extended file hierarchy access control scheme with attribute-based encryption in cloud computing", IEEE Trans. Emerg. Top. Comput. (2019) 1.

[5] M. Chase, "Multi-authority attribute-based encryption", in: Theory of Cryptography. LNCS, Vol. 4392, 2007, pp. 515–534.

[6] A. Lewko, B. Waters, "Decentralizing attribute-based encryption", in: Advances in Cryptology – EUROCRYPT 2011. LNCS, Vol. 6632, 2011, pp. 568–588.

[7] K. Yang, X. Jia, K. Ren, B. Zhang,"Dac-macs: Effective data access control for multi-authority cloud storage systems", in: 2013 Proceedings IEEE INFOCOM, 2013, pp. 2895–2903.