IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10458

A BLOCK CHAIN-BASED ACCESS CONTROL FRAMEWORK FOR BIG DATA

P. R. Meenakshi Sundaram[1], S. Monika[1], P. Navashree[1], Mr.S.Vivekanandan, M.E.,[2]

Final year B.E, Department of Computer Science and Engineering, Velalar College of Engineering and Technology, Erode, Tamilnadu, India[1]

Assistant Professor, Department of Computer Science and Engineering, Velalar College of Engineering and Technology, Erode, Tamilnadu, India.[2]

ABSTRACT: Cyber-Physical-Social System (CPSS) big data which is usually stored in cloud. The local real-time data which is usually stored in the fog-edge server (FeS) of the mobile terminal devices or sensors. The social data which is usually stored in the social data server (SdS). CPSS big data to be tampered and to be leaked. A light-weighted symmetric encryption algorithm is used to achieve privacy-preserving.

I. INTRODUCTION

Access Control, typically referred to as resource authorization or just authorization, is the confinement of the actions of a particular entity or an individual only to the computing resources and services that it is authorized to use. This is achieved by enforcing predefined access control policies. The underlying policies govern every access of an entity to a particular resource. The policies can be realized in the guise of attributes and the corresponding rules associated with a set of entities and a set of resources. For the access control mechanisms to be sound and ensure integrity, this is achieved by securely establishing the identity of the entities. If this secure enforcement of the establishment of identities is absent, enforcing an access policy is foiled and left useless. While there is an absolute and dire need to enforce access control mechanisms in practice, it comes with issues that need thorough consideration before these mechanisms are put to implementation. Some of the challenges are; it is challenging to achieve access control in resource constrained devices due to their heterogeneous nature and limited computation capabilities.

Also, the dynamic nature of devices makes it hard to implement access control policies. Other important aspects that are challenging are the dynamic topologies, distributive nature, and policy enforcement dynamically. While all of this comes down to whether a solution is viable (or scalable), taking into consideration parameters like time-memory tradeoffs, behavior to different types of traffic, resistance against various attacks, and adaptability to dynamic changes to the network are paramount. However, these issues can be dealt with much ease if a different perspective is put into place. Blockchain technology has seen a tremendous rise, which grew exponentially after the inception of cryptocurrency Bitcoin, which in essence, is backed

2. LITERATURE REVIEW

Current Access Control Systems

A couple of problems in centralized access control systems. As there is a third party, who has access to the data, the risk of privacy leakage exists. Also, a central party is in charge to control the access, so the risk of single point of failure also exists. This study presents an access control mechanism with a temporal dimension to solve these problems and adapts a blockchain-based solution for verifying access permissions. Attribute-based Encryption method also has some problems

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10458

such as privacy leakage from the private key generator (PKG) and single point of failure as mentioned before. Introduce a framework for data sharing and access control to address this problem by implementing decentralized storage.

Access control is a required security part

Current solutions for managing access control in multi administrative domains are not efficient. Based on the static approaches are not scalable and granular and PKI-based systems are difficult to manage. They suggest distributing and recording access policies in a permissioned blockchain. It is also another PKI system based on blockchain to achieve security without trusted third parties. In cloud federation also sharing data between multiple organization is a concern from users privacy perspective. Keeping the personal data related to the users' identities private, while giving them access to the shared data, is the main concern. Alansari et al. propose an attribute-based access control system based on symmetric key encryption. The system checks users attributes with access control policies to grant access permissions to the data belong to the federated organization, while it keeps the users attribute private from the federated organization. This study suggests blockchain and trusted execution environment to preserve the integrity of the policy evaluation process

Access permissions to the personal data

The users of mobile applications always concern about privacy issues as they usually must give access to their private information. Enigma is an access control management system based on Ethereum blockchain which aims to solve this problem. The presented framework addresses three main concerns: data ownership, data transparency & auditability, and fine-grained access control. The system is designed in a way that users are able to control their own personal data and make the process of access to their data transparent. Also, the users can modify or revoke access permissions to their personal data without uninstalling the mobile application.

3. MODULES

A. Transactions to smart contracts

This study uses attribute-based access control mechanism and eXtensible Access Control Markup Language to define policies and store arbitrary data on Bitcoin. They used OP-RETURN script opcode and MULTISIG transactions. In their next study, they considered smart contracts to enforce access control policies instead of simple transactions. Also, in order to evaluate the feasibility and performance of the represented system, they have defined a scenario where smart contracts are considered as resources that need to be protected and access to them is restricted. By employing smart contracts, they were able to add more flexibility, details, and efficiency to their implemented system.

B. Data sharing access control

Using blockchain as an infrastructure for shared data access control management system. A proof of concept has been implemented using Multichain platform and CP-ABE (Ciphertext-Policy Attribute-Based Encryption) access control schema. The analysis result indicates that timely CP-ABE performs better in terms of performance in comparison with timely access control list. As we expected, timely CP-ABE implementation without blockchain is more efficient than blockchain-based solutions, but using blockchain provides security and privacy benefits such as auditing, non-repudiation, as well as no single point of failure

C. Cloud federation

Decentralised Runtime Access Monitoring System (DRAMS) to guarantee the reliability of the access control component in cloud federations dynamically. The represented architecture comprises three components: Logger, Smart contract, and Analyser. Logger component includes "Probing agents" records and forwards data to generate access logs and "Logging interface (LI)". Smart contracts capture logs and carry out monitoring by comparing logs to create dynamic access permissions. Analyzer investigates access permissions based on the system policies

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10458

D. Multiple organizations

It has implemented a smart contract to initialize the roles and the challenge-response protocol to authenticate the ownership of roles and user verification. Challenge-response protocol is utilized for the authentication of the users, who request a service from another organization based on her/his role. This protocol has five steps: declaration, information check, challenge response, and response verification. In summary, a user requests a service corresponding to his/her own roles from another organization. After initial information check, the organization sends an arbitrary data and ask the user to sign it and user responses with the signature. Finally, the authentication confirms after receiving valid signature

4. EXISTING SYSTEM

In this section, we discuss the problems of current access control systems mention a couple of problems in centralized access control systems. As there is a third party, who has access to the data, the risk of privacy leakage exists. Also, a central party is in charge to control the access, so the risk of single point of failure also exists. This study presents an access control mechanism with a temporal dimension to solve these problems and adapts a blockchain-based solution for verifying access permissions. Attribute-based Encryption method also has some problems such as privacy leakage from the private key generator (PKG) and single point of failure as mentioned before. Introduce a framework for data sharing and access control to address this problem by implementing decentralized storage. Current solutions for managing access control in multi administrative domains are not efficient. Static approaches are not scalable and granular and PKI-based systems are difficult to manage. They suggest distributing and recording access policies in a permissioned blockchain. Conifer is also another PKI system based on block chain to achieve security without trusted third parties

5. PROPOSED SYSTEM

The proposed solution is based on a multi-agent system and uses a private blockchain, which provides lightweight and decentralized access control security for an IoT system. The Local Blockchain Manager (LBCM), which includes IoT devices at the bottom of our proposed architecture, a Fog Blockchain Manager (FBCM), which includes fog/edge nodes, a Core Fog Blockchain Manager (CFBCM), which includes core fog nodes and a Cloud Blockchain Manager (CBCM), which represents cloud blockchain storage. Each BCM has a block header, MAC policy header and transactions. Our framework meets the requirements of the CIA (Confidentiality, Integrity and Availability) security triad and is well-suited to the specific requirements of IoT in terms of its scalability, distributed nature, constrained devices and defense against various security issues, such as single points of failure..

6. CONCLUSION

Represented blockchain-based access control architectures and systems have been classified based on domain, access control method, and blockchain platforms. These systems have been tailored based on system requirements. These studies have focused on designing a user-centric system, which owners of the data can define and enforce access control policies directly. Systems have focused on audit ability characteristic and trusted logging provided by block chain to design a reliable access control system. From the transactional perspective, use only transactions to store access control attributes on blockchain, while applied smart contracts to exploit its advantages such as flexibility and automatically enforcing access control policies. Also, the challenges and future directions have been discussed in this paper

REFERENCES

[1] Shorouq Alansari, Federica Paci, Andrea Margheri, and Vladimiro Sassone. 2017. Privacy-preserving access control in cloud federations. In Cloud Computing (CLOUD), 2017 IEEE 10th International Conference on. IEEE, 757–760.

[2] Shorouq Alansari, Federica Paci, and Vladimiro Sassone. 2017. A distributed access control system for cloud federations. In Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on. IEEE, 2131–2136.

[3] Sidney Amani, Myriam Bégel, Maksym Bortin, and Mark Staples. 2018. Towards verifying ethereum smart contract bytecode in Isabelle/HOL. In Proceedings of the 7th ACM SIGPLAN International Conference on Certified Programs and Proofs. ACM, 66–77.

[4] Parwat Singh Anjana, Sweta Kumari, Sathya Peri, Sachin Rathor, and Archit Somani. 2018. An Efficient Framework for Concurrent Execution of Smart Contracts. arXiv preprint arXiv:1809.01326 (2018).

[5] Asaph Azaria, Ariel Ekblaw, Thiago Vieira, and Andrew Lippman. 2016. Medrec: Using blockchain for medical data access and permission management. In Open and Big Data (OBD), International Conference on. IEEE, 25–30.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10458

[6] John Bethencourt, Amit Sahai, and Brent Waters. 2007. Ciphertext-policy attribute-based encryption. In Security and Privacy, 2007. SP'07. IEEE Symposium on. IEEE, 321–334.

[7] Karthikeyan Bhargavan, Antoine Delignat-Lavaud, Cédric Fournet, Anitha Gollamudi, Georges Gonthier, Nadim Kobeissi, Natalia Kulatova, Aseem Rastogi, Thomas Sibut-Pinote, Nikhil Swamy, et al. 2016. Formal verification of smart contracts: Short paper. In Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security. ACM, 91–96. [

8] Thomas Bocek, Bruno B Rodrigues, Tim Strasser, and Burkhard Stiller. 2017. Blockchains everywhere-a use-case of blockchains in the pharma supply-chain. In 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM). IEEE, 772–777.

[9] Santiago Bragagnolo, Henrique Rocha, Marcus Denker, and Stéphane Ducasse. 2018. SmartInspect: solidity smart contract inspector. In 2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE). IEEE, 9–18.

[10] Wei Cai, Zehua Wang, Jason B Ernst, Zhen Hong, Chen Feng, and Victor CM Leung. 2018. Decentralized applications: The blockchain-empowered software system. IEEE Access 6 (2018), 53019–53033.