ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
pp. 75-79

Locating Faults in A Multi-Storage Cloud Based On Blockchain Base Auditing

N. Dhiviya[1], T. Escaline Freetha[2]

[1,2]Department of Computer Science and Engineering, Udaya School of Engineering, Udaya Nagar, Kanyakumari, Velloamodi, Tamil Nadu, India. divisridivya@gmail.com

ABSTRACT

Cloud computing has attracted wide attention because it can provide data storage and computation to us. However, when the users outsource the data to the cloud server, the users lose control over the data, so the data auditing is very important to protect users' data. To reduce computation and communication costs of the users, the existing schemes utilized a trusted third party (TPA) to conduct verification on behalf of users. However, TPA is a centralized party, which is vulnerable to external attacks and internal faults. In this paper, we present a decentralized public auditing scheme for cloud storage based on blockchain, which improves the reliability and stability of auditing results. In the proposed scheme, the cloud service providers work together to perform data verification without TPA. Finally, the security analysis shows that the scheme can resist a variety of attacks, and the experimental results demonstrate that the proposed scheme has enhanced security and reliability.

Keywords: Multicloud Storage, Block Chain, Data Auditing

1 Introduction

Blockchain is a new and emergent technology that is expected to change the way current markets work. It is a distributed digital ledger and is decentralized. With the current working capacity of blockchain, it has the potential to be the operating system of smart cities. Blockchain is technology that is open source and distributed and is used to record transactions between parties. It provides a way to develop a system that is both verifiable and secured. Blockchain is open source, so different versions of blockchain are available on the market. Each version is developed depending upon the different needs of the various industries. Blockchain is neither owned nor singly controlled by any one authority.

Blockchain technology is evolving at a swift pace. It started with Bitcoin, and now there are many types of blockchain. Organizations are developing different versions of blockchain depending upon their need and benefits. The critical development in blockchain innovation is that it permits its members to transfer resources across the Internet without the requirement of an incorporated outsider.

The blockchain concept was created as the fundamental innovation behind the cryptocurrency called Bitcoin. Blockchain technology is currently being tested in many different asset management and procurement services for opportunities and has already led to many applications. Similar to today's sophisticated flow of goods, there is a lack of transparency and

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
pp. 75-79

trust. There are many intermediate people associated with high documentation requirements, which leads to time-consuming processes.

2 Related Works

Provable Data Possession (PDP) is a technique for ensuring the integrity of data instorage outsourcing. PDP (CPDP) scheme based on homomorphic verifiable response andhash index hierarchy. The security of this scheme is based on a multi-prover zero-knowledge proof system. The experiments show that the solution introduces lower computation and communication overheads in comparison with non-cooperative approaches

3 Proposed Methodology

Using Blockchain, We propose a secure and accurate data auditing scheme for multi-cloud storage services. We design an accurate dispute arbitration mechanism for theproposed scheme. Our scheme can resist malicious multi-cloud storage service organizers.Can have an eye on the user's data like when the auditing was last made, when the file waslast accessed etc.

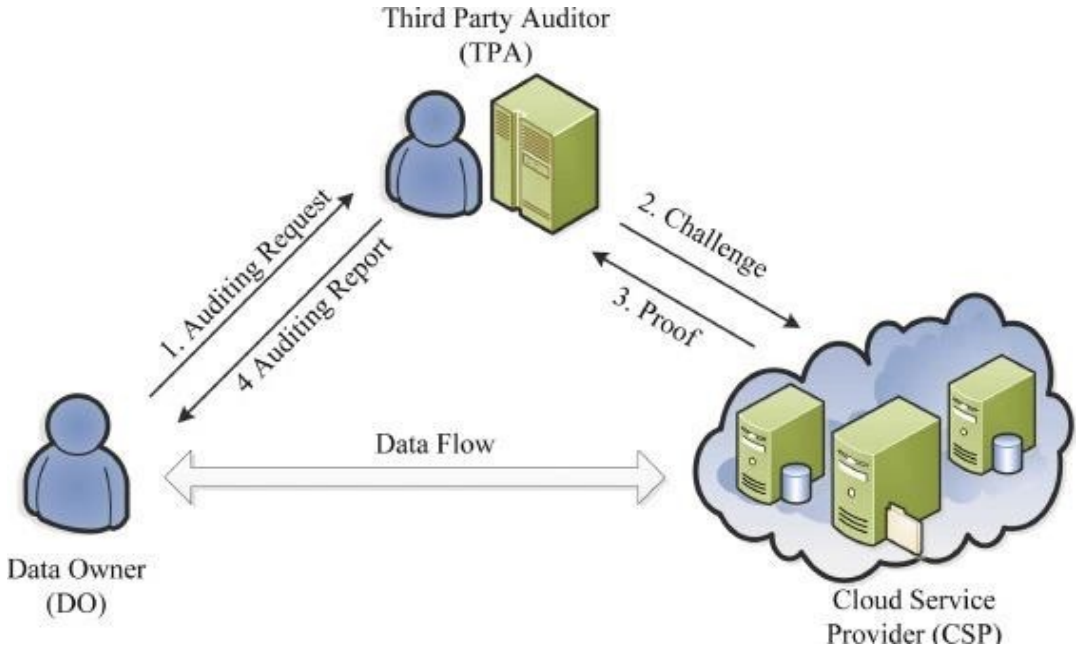

Figure 1: *System model of the auditing scheme based on the trusted third part*

The proposed schemes introduced above have the same problem: the client needs toaccess the complete data back-up; however, it is not suitable in practice obviously as mentioned before. Many scholars have carried out research on this issue later. In 2007, Ateniese et al. proposed the concept of provable data possession (PDP) firstly based on RSA homomorphic linear authenticator and random sampling technology. The user can check the data stored in there mote server without downloading all the data to the local machine thus solving the defect existed in the early proposed schemes; however, their scheme only supports the static data. In 2008, Shacham and Waters proposed two improved schemes based on BLS short signature the

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
pp. 75-79

first scheme based on BLS signature supports infinite time public verifications on the data; the second scheme calculates the authenticators using pseudorandom function but does not support public verification.

System Module

There are five entities in the system model of our scheme: users (data owner), key generation center (KGC), cloud server providers (CSP), third party auditor (TPA) and blockchain system.

User: The user is responsible for generating data tags, transmitting data to the cloud service provider and dynamically updating the cloud data. Meanwhile, authorize TPA to periodically verify the integrity of cloud data.

Third Party Auditor (TPA): It is responsible for verifying the integrity of cloud data, and writing verification results to log files and broadcasting to the block chain.

Cloud service provider (CSP): It is responsible for providing cloud storage services to users and responding to TPA authentication requests. It not only has a large storage space,but also has a huge computing power. In this paper, CSP is composed of cloud server organizer (CO) and cloud servers (CS). The CO is responsible for transferring replicas to the CS, and sending the challenge information to the CS when receiving the challenge information sent by the TPA. After obtaining the evidence returned by the CS, the CO aggregates the data and sends it to the TPA. The CS is responsible for storing data.

Key generation center (KGC): It is responsible for generating part of the private key forthe user and sending it to the user through a secure channel.

Block chain system: It is responsible for helping TPA generate unpredictable challenge information and records the audit results of TPA. In addition, it also helps users verify the behavior of TPA. Here, the relationship between the entities in the system model is briefly introduced. After the user uploads the local data to CO, CO will send different replicas of the user to different CS for storage. In addition, users can access and update outsourcing data anytime. In order to ensure the integrity of the data, the users delegate the TPA to periodically audit the data and verify the audit results of TPA for a long time. Our scheme consists of five algorithms, Setup, Partial Key Generation, Secret Value Generation, Data Upload, Auditors.

Setup: This algorithm is performed by the KGC to generate the master key and public parameters used in the following algorithm.

Partial Key Generation: KGC performs this algorithm to obtain the partial key for users. Itinputs the master key and the identity of the user, outputs the partial key. Secret Value Generation: This algorithm is executed by the user to obtain the secret value and public key. The algorithm randomly selects Suas the secret value and calculates the public key forthe user.

Data Upload: This algorithm enables a user to outsource the data to CSP. The user generates replica files and calculates tags for all data blocks and sends them to the cloud server. Of course, the cloud server should also ensure that the uploaded data is correct.

Audit: This algorithm requires TPA to regularly audit the integrity of cloud data, and usersto verify the behavior of TPA in a longer period. TPA sends challenge information to CSP,CSP generates data integrity proof, and TPA verifies the correctness of the proof. Furthermore, this

algorithm enables TPA to generate a log file, which records the verification information of TPA, and allows the user to audit the behavior of TPA by checking the validity and correctness of the log file.

4 Result and Discussion

Blockchain is famous for its outstanding performance in various cryptocurrency systems. Blockchain is a linear collection of data elements, where each data element is called a block. All blocks are linked in chronological order to form a chain, and the encryption hash function is used for security protection. As shown in Figure 3, each blockcontains the hash value of the current block (BlockHash), the previous block hash value (PreBlockHash), a random number (Nonce), the time stamp of the current block added to the blockchain (Time), the root node value of the Merkel hash tree (MerkleRoot), and multiple transaction records (Tx). In the blockchain, the participants who verify the validityof a transaction are called miners. Before generating new blocks, miners will collect as many transactions as possible, and find solutions to a difficult problem until they become effective nonce. This process is the Proof-of-Work (PoW), also known as "mining".

5 Conculsion

The paper presents case studies discussing Blockchain–Cloud integration that help to enhance the understanding of its readers. A detailed survey is conducted to examine the publishing patterns in the areas of Blockchain technology coupled with Cloud computing,Healthcare, Smart cities, and Finance. Furthermore, we discuss the concept of Blockchain-as-a-Service (BaaS) and explore key cloud service providers (CSP) which are offering blockchain services. The work presents a literature survey of publications concerning the implementation of BaaS along with a comparison between various blockchain services being offered by the CSP. The study performed presents us with a few questions to furtherinvestigate. What are the challenges of Blockchain–Cloud integration? What are the futureapplication areas for BaaS? What kind of pricing and SLA policies can be created for ensuring efficiency and QoS? What type of architecture can be created for rendering BaaS?Through this work, readers can obtain an insight into the existing literature and will be ableto craft their research journeys to answer some of the above questions.

Reference

1. Benil T; Jasper J, Year: 2020, “Cloud based security on outsourcing using blockchain in E-health systems,” *Computer. Netw.* Vol: 178, pp. 107344.

2. Bommadevara Nagendra; Andrea Del Miglio; Steve Jansen, Year: 2018, "Cloud adoption to accelerate IT modernization," *McKinsey* Cloud Adoption to Accelerate ITModernization. McKinsey Digital; Atlanta, GA, USA.

3. Carlin Sean; Kevin Curran, Year: 2011, “Study on cloud computingsecurity,” Journal of Software, Vol: 22, no: 1, pp. 71–83.

4. De Caro Angelo; Vincenzo Iovino, Year: 2011, "jPBC: Java pairing based cryptography," in Proceedings ofthe 16th IEEE Symposium on Computers and Communications, ISCC 2011, Kerkyra, Corfu, Greece,.

5. Shen Wenting; Jing Qin, Jia Yu; Rong Hao; Jiankun Hu, Year: 2018, "Enablingidentity based integrity auditing and data sharing with sensitive information hidingfor secure cloud storage," IEEE Transactions on Information Forensics and Security, Vol: 14, no: 2, pp. 331–346.

6. Song Dawn; Elaine Shi; Ian Fischer; Umesh Shankar, Year: 2012, "Cloud data protection for the masses,"IEEE Computer, Vol: 45, no: 1, pp. 39–45.

7. Juels, Ari; Alina Oprea, Year: 2013, "New approaches to security and availability for cloud data," Communications of the ACM, Vol: 56, no: 2, pp. 64–73.

8. F. Sebe; A. Martinez-Balleste; Y. Deswarte; J. Domingo-Ferrer; J. J. Quisquater, Year: 2004, Time-bounded remote file integrity checking, Technical Report 04429.

9. Huang Haiping; Peng Zhu; Fu Xiao; Xiang Sun; Qinglong Huang, A blockchain-based scheme for privacy-preserving and secure sharing of medical data, *Computer. Secur.*

10. Ren Kui; Cong Wang; Qian Wang, Year: 2012, "Security challenges for the public cloud," IEEE Internet Computing, Vol: 16, no: 1, pp. 69–73.

11. Song Dawn; Elaine Shi; Ian Fischer; Umesh Shankar, Year: 2012, "Cloud data protection for the masses," IEEE Computer, Vol: 45, no: 1, pp. 39–45.

12. Miyachi Ken; Tim K. Mackey, Year: 2021, "hOCBS: A privacy-preserving blockchain framework forhealthcare data leveraging an on-chain and off-chain system design," *Inf. Process. Manag,* Vol: 58, pp. 102535.

13. Armbrust Michael; Armando Fox; Rean Griffith; Anthony D. Joseph; Randy Katz; Andy Konwinski; Gunho Lee et al., Year: 2010, "A view of cloud computing," Communications of the ACM, Vol: 53, no: 4, pp. 50–58.

14. Carlin Sean; Kevin Curran, Year: 2011, "Study on cloud computing security," Journal of Software, Vol: 22, no: 1, pp. 71– 83.

15. Choudhury Tanupriya; Abhirup Khanna; Teoh Teik Toe; Madhu Khurana; Nguyen Gia Nub, Year: 2021, "Blockchain Applications in the IoT Ecosystem," Springer.