IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 11, November 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 11, November 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1011041 |

Consortium Blockchain –Based Public Integrity Verification in Cloud Storage for IOT

Tanavi Rajurkar, Sakshi Barge, Krunali Jadhav, Payal Kad, Prof. Dr. Nikita Kulkarni

Student, Dept. of Computer Engineering, K J College of Engineering & Management Research, Pune, India

Student, Dept. of Computer Engineering, K J College of Engineering & Management Research, Pune, India

Student, Dept. of Computer Engineering, K J College of Engineering & Management Research, Pune, India

Student, Dept. of Computer Engineering, K J College of Engineering & Management Research, Pune, India

Head of Department, Dept. of Computer Engineering, K J College of Engineering & Management Research, Pune, India

ABSTRACT: The applications of Internet of Things have emerged in every aspect of people's life. The volume of data gathered can be enormous. Enterprises and personal consumers are increasingly reliant on cloud storage services instead of local storage. While they enjoy the convenience of cloud storage services, they also worry about the integrity of the cloud-stored data since they do not physically own the data. To enable public integrity auditing, third-party auditors as trusted ones verify data integrity on behalf of the data owner. However, the vulnerability of auditors should also be considered. We propose a consortium blockchain based public integrity verification system (CBPIV). In CBPIV, the auditor behaviours are recorded in the consortium blockchain so that authorized parties can audit the auditor to see if the verification results are correct. A smart contract is deployed to check the behaviour of the auditor automatically, which can trigger alerts for unusual behaviours. The evaluation on both security and performance shows that our proposed scheme is secure and alleviates the burden on data owners of limited computation capability. Index Terms—Cloud storage, consortium blockchain, data integrity, Internet of Things (IoT), malicious auditors.

.

KEYWORDS: consortium blockchain based public integrity verification system (CBPIV); Data Integrity; IOT.

I. INTRODUCTION

The Internet of Things (IoT) has developed rapidly over these years and is greatly influencing various aspects of our life, such as communication, work, consumption of information, and entertainment [1]. The incessant data generated by IoT devices grows exponentially. Cloud computing provides resources as services over the Internet, which seems to be a practical choice for IoT data storage. Owing to its convenience and efficiency, cloud storage service is one of the prominent cloud services among personal users and enterprises [2].

However, once the data are outsourced to a cloud, data owners have no actual control of them, which introduces new security challenges, such as integrity [3], confidentiality [4], and privacy issues [5]. Various security incidents by mainstream cloud service providers, such as Google and Amazon, have never ceased in recent years. The data can be deleted or tampered by an untrusted cloud. Data integrity denotes the accuracy and consistency of data, which is essential for analyzing reliable and trustworthy information, especially in the big data era. Thus, it is strongly recommended to check the integrity of the IoT data in the cloud storage environment.

The difference between cloud-stored data integrity auditing and local data integrity auditing is that the integrity of cloudstored data is remotely checked without retrieving users' data and without keeping local copies of them. This is implemented by challenging the cloud to provide cryptographic proofs of the data instead of the original data, and verifying the proofs on the basis of integrity, correctness, and validity to ensure the cloud service providers keep the data intact. Juels and Kaliski, Jr. [6] proposed the concept of proofs of retrievability (POR) where the cryptographic proofs of the data are check blocks embedded randomly during data encryption by data owners. Ateniese et al. [7]

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 11, November 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1011041 |

proposed provable data possession (PDP), where homomorphic verifiable tags are employed as the cryptographic proofs to implement public verification.

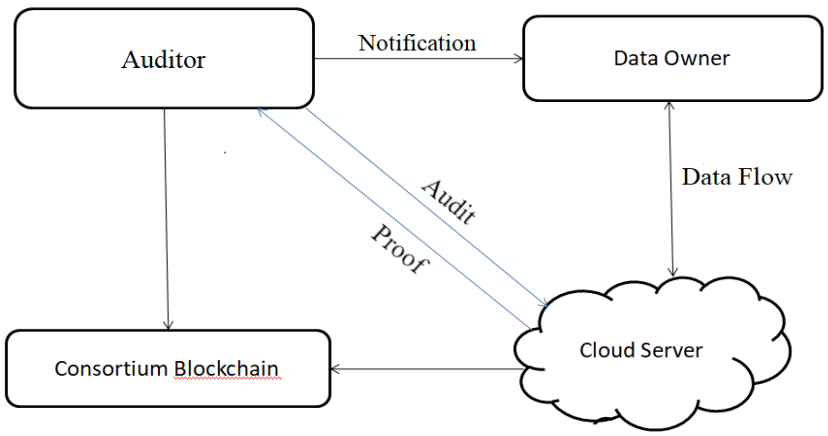
II. RELATED WORK

A.Traditional Remote Data Auditing Remote data auditing (RDA):-enables a data owner to audit data integrity without retrieving them to the local. In the existing protocols, only data owners can audit their data's integrity by themselves, which is called private auditing. While some data owners want to outsource the auditing work to a TPA for periodical auditing, which is called public auditing. Juels and Kaliski, Jr. [6] proposed the concept of POR. The retrievability of cloud data is guaranteed by spot checking and error correction codes. However, it only supports private auditing which leaves a heavy communication and verification burden to data owners during the process of retrieving and using the data. Shacham and Waters [21] improved the POR scheme (SWP for short) by proposing a compact POR against arbitrary adversaries. By utilizing the pseudorandom function and BLS signature, not only the data owner can verify their data in a private way but also anyone who can take the role of the verifier as a TPA can audit the data in a public way. Ateniese et al. [7] proposed PDP, where homomorphic verifiable tags are introduced to implement public verification. To enable public auditing, a TPA is introduced in between the cloud server and the data owner. The TPA takes the heavy computation and communication burden of data owners for sure, but it is hard to say that the auditor is 100% honest and always be loyal to the data owner in the real world. Armknecht et al. [17] proposed an outsourced POR scheme called Fortress for dealing with malicious auditors. In their scheme, the auditor runs two POR: one for the auditor, and the other for the data owner. There is a log which records all the auditing proofs for data owners to verify the auditor's behaviour.

B. Remote Data Auditing With Blockchain Blockchain:- As an emerging technology, has also been applied in improving the efficiency and security of cloud storage services. Filecoin [22] employs blockchain to create a protocol token for storage trading in a decentralized network and offer off-chain storage. Huang et al. [23] used the blockchain data structure to provide a secure data sharing scheme. When the file is uploaded to the cloud, necessary information of the file is also uploaded to the blockchain at the same time. Xia et al. [24] proposed a medical record sharing scheme MeDShare in trustless cloud storage environment with blockchain. Blockchain is employed to record data transitions and sharing in a tamper-proof manner. Besides, they use smart contracts to track the behavior of the data. For data auditing with blockchain, there are also several security issues needed to be addressed. Du et al. [25] tackled the audit information privacy issue of data auditing with blockchain with noninteractive zero-knowledge proof. Zhang et al. [26] proposed a secure certificateless public verification scheme (SCLPV) to prevent from malicious auditors. They introduce a key generation center (KGC) in the scheme to manage system parameters and partial private keys of data owners. Bitcoin is used to generate random challenge indexes which are unforgeable by a malicious auditor. All the auditing proofs are stored into a log file for the data owner to check. Zhang et al. [18] proposed a public verification scheme against procrastinating auditors called CPVPA. An auditor may deviate from the objective of detecting any data corruption as requested to postpone his/her job to verify the data.

III. PROPOSED ALGORITHM

A. System mode:-



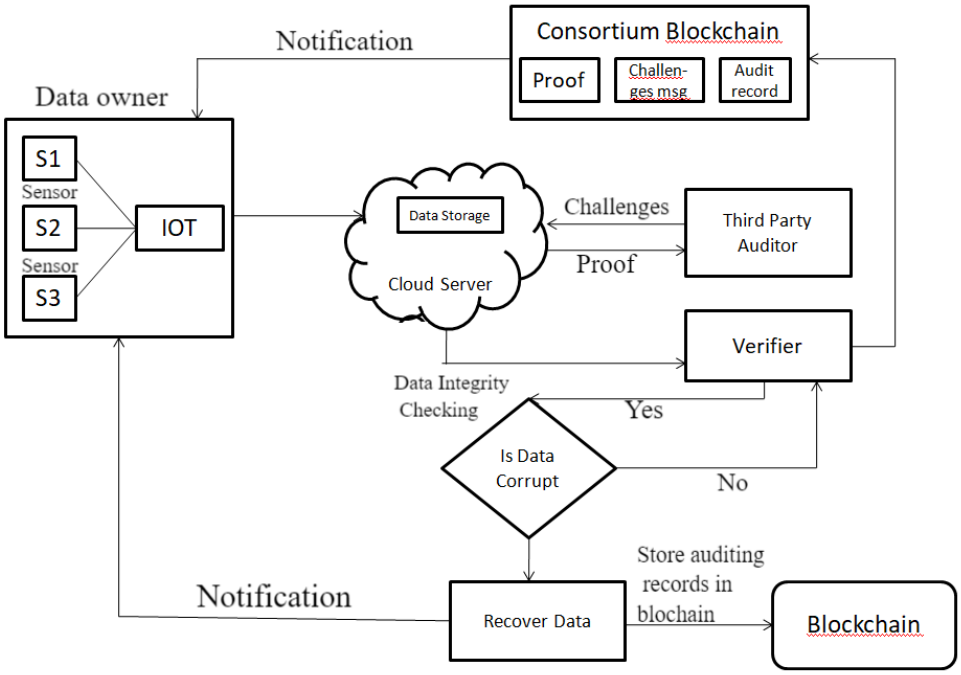
International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 11, November 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1011041 |

B. Architecture:-



IV. DATA IN DIAGRAM

1) Data Owner: The data owner is the IoT device which uploads its data to remote cloud servers. It has limited storage and computation capabilities.

2) Cloud Server: The cloud server refers to the enterprise that provides massive storage space and computing resources for cloud service users.

3) Third Party Auditor: The TPA refers to an independent enterprise which is in charge of auditing the integrity of cloud-stored data on behalf of data owners. When auditing, the TPA sends a challenge message to the cloud server and receives proofs correspondingly. TPA with computation power verifies the correctness of the proofs.

4) Consortium Blockchain: The consortium blockchain stores the auditing records, including challengemessages and proofs from the TPA and triggers a smart contract to verify the correctness of the auditing records. The data owner as the administrator of consortium blockchain authorizes who can join the network. The incentives of authorized nodes are fulfilled by a contractual agreement with the administrator which can be coins or other agreed rewards

V. CONCLUSION AND FUTURE WORK

In this article, we proposed a cloud-stored data integrity auditing scheme for IoT devices based on consortium blockchain, which supports IoT device data owners to examine auditor's behaviors against untrustworthy auditors. In our scheme, with blockchain's advantage of time sensitivity, random challenge messages prevent the collusion between cloud servers and auditors. Besides, auditing records are stored in the consortium blockchain, the task of checking the auditing records is operated by smart contract automatically. Thus, the behavior of auditors is checked by the blockchain. The evaluation on both security and performance shows that our proposal is secure and alleviates the burden on IoT devices.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 11, November 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1011041 |

REFERENCES

[1] R. Goyat et al., "Blockchain-based data storage with privacy and authentication in Internet-of-Things," IEEE Internet Things J., early access, Aug. 24, 2020, doi: 10.1109/JIOT.2020.3019074.
[2] M. N. Khan, A. Rao, and S. Camtepe, "Lightweight cryptographic protocols for IoT-constrained devices: A survey," IEEE Internet Things J., vol. 8, no. 6, pp. 4132–4156, Mar. 2021.
[3] C. B. Tan, M. H. A. Hijazi, Y. Lim, and A. Gani, "A survey on proof of retrievability for cloud data integrity and availability: Cloud storage state-of-the-art, issues, solutions and future trends," J. Netw. Comput. Appl., vol. 110, pp. 75–86, May 2018
[4] N. Baracaldo and J. Glider, "Confidentiality of data in the cloud," in Security, Privacy, and Digital Forensics in the Cloud. Newark, NJ, USA: Wiley, 2019, p. 51.
[5] Y. Yu et al., "Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage," IEEE Trans. Inf. Forensics Security, vol. 12, pp. 767–778, 2017.
[6] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, "Blockchain based data integrity service framework for IoT data," in Proc. IEEE Int. Conf. Web Serv. (ICWS), Honolulu, HI, USA, 2017, pp. 468–475.
[7] D. Francati et al., "Audita: A blockchain-based auditing framework for off-chain storage," 2019. [Online]. Available: http://arxiv.org/abs/1911.08515.
[8] S. Underwood, "Blockchain beyond bitcoin," Commun. ACM, vol. 59, no. 11, pp. 15–17, Nov. 2016. [Online]. Available: https://doi.org/10.1145/2994581
[9] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A survey," IEEE Internet Things J., vol. 6, no. 5, pp. 8076–8094, Oct. 2019.
[10] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in Proc. 3rd Symp. Oper. Syst. Design Implement. (OSDI), vol. 99, 1999, pp. 173–186.
[11] N. Szabo, "Formalizing and securing relationships on public networks," First Monday, vol. 2, no. 9, 1997. [Online]. Available: https://firstmonday.org/article/view/548/469

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.165

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details