e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 5, Issue 6, June 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.54

International Journal Of Multidisciplinary Research In Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 5, Issue 6, June 2022 |

| DOI:10.15680/IJMRSET.2022.0506091 |

Blockchain-Based Automated Auditing Against Malicious Auditors for Data Integrity and Verification in Cloud Storage

FARDEEN RAEES J, SUJITH P, VIGNESHA CJ, RAJA R

U.G Scholar, Department of CSE, Velammal Institute of Technology, Panchetti, Tamilnadu, India

U.G Scholar, Department of CSE, Velammal Institute of Technology, Panchetti, Tamilnadu, India

U.G Scholar, Department of CSE, Velammal Institute of Technology, Panchetti, Tamilnadu, India

Assistant Professor, Department of CSE, Velammal Institute of Technology, Panchetti, Tamilnadu, India

ABSTRACT: The adoption of cloud storage services can help customers manage their data more effectively. However, it raises a slew of security issues, one of which being data integrity. Existing public verification schemes are vulnerable to procrastinating auditors who may not complete verifications on time, as well as malicious auditors who may not have a good work ethic and misuse the information, whereas public verification techniques allow a user to hire a third-party auditor to verify the data integrity on their behalf. Furthermore, because the majority of public verification methods are built on the public key infrastructure (PKI), they face certificate management issues. In this work, we use blockchain technology to provide a certificateless public verification mechanism against malicious auditors (CPVMA).The main concept is to make auditors record each verification result as a blockchain transaction. Because blockchain transactions are time-sensitive, the verification can be time-stamped once the transaction is registered in the blockchain, allowing users to verify that auditors complete the verifications on time. Furthermore, CPVMA is based on certificateless cryptography, which eliminates the need for certificate management. We give extensive security proofs to validate CPVMA's security, as well as a detailed performance study to illustrate its efficacy.

I. INTRODUCTION

Due to on-demand provisioning and pay-per-use pricing, an increasing number of enterprises are outsourcing their data, apps, and business processes to the cloud, allowing them to obtain financial and technological benefits. However, enterprises are still cautious to utilize cloud services due to concerns about provided cloud services' security, privacy, and reliability, as well as doubts about their cloud service provider's trustworthiness. Cloud service certifications (CSC) are an effective way to solve these problems by generating confidence and boosting the market's openness. Certifications for cloud services aim to ensure a high level of security and compliance. However, because cloud services operate in a constantly changing environment, multi-year validity periods may cast doubt on the legitimacy of such certifications.We claim that continuous auditing (CA) of specified certification criteria is necessary to ensure consistently reliable and secure cloud services and, as a result, boost certification credibility. The CA of cloud services is still in its early stages, and we've discovered that the majority of existing approaches aren't suitable for third-party audits. As a result, we suggest a conceptual CA design, emphasizing key components and procedures that must be executed.

II. LITERATURE SURVEY

Kan Yang, “An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing”, 2012. An efficient and secure dynamic auditing protocol is desired to convince data owners that the data are correctly stored in the cloud. Data loss could happen in any infrastructure, no matter what high degree of reliable measures cloud service providers would take.

Satoshi Nakamoto,“Bitcoin: A peer-to-peer electronic cash system", 2008. Blockchain is a secure, verifiable and tamper-proof distributed ledger for supporting digital asset transactions This Scheme provides a proof of security.The network itself requires minimal structure.The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 5, Issue 6, June 2022 |

| DOI:10.15680/IJMRSET.2022.0506091 |

Florian Tschorsch, Björn Scheuermann, "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies", 2013. We deduce the fundamental structures and insights at the core of the Bitcoin protocol and its applications.Digital money is an exception from this rule. It ignores the propagation delays in distributed systems and leads to temporary inconsistencies.

John Bethencourt, Amit Sahai, "Cipher text-Policy Attribute-Based Encryption", 2008.The cipher text policy attribute-based encryption method allows enforcing such policies to employ a trusted server to store the data and mediate access control.By using these techniques, encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against collusion attacks

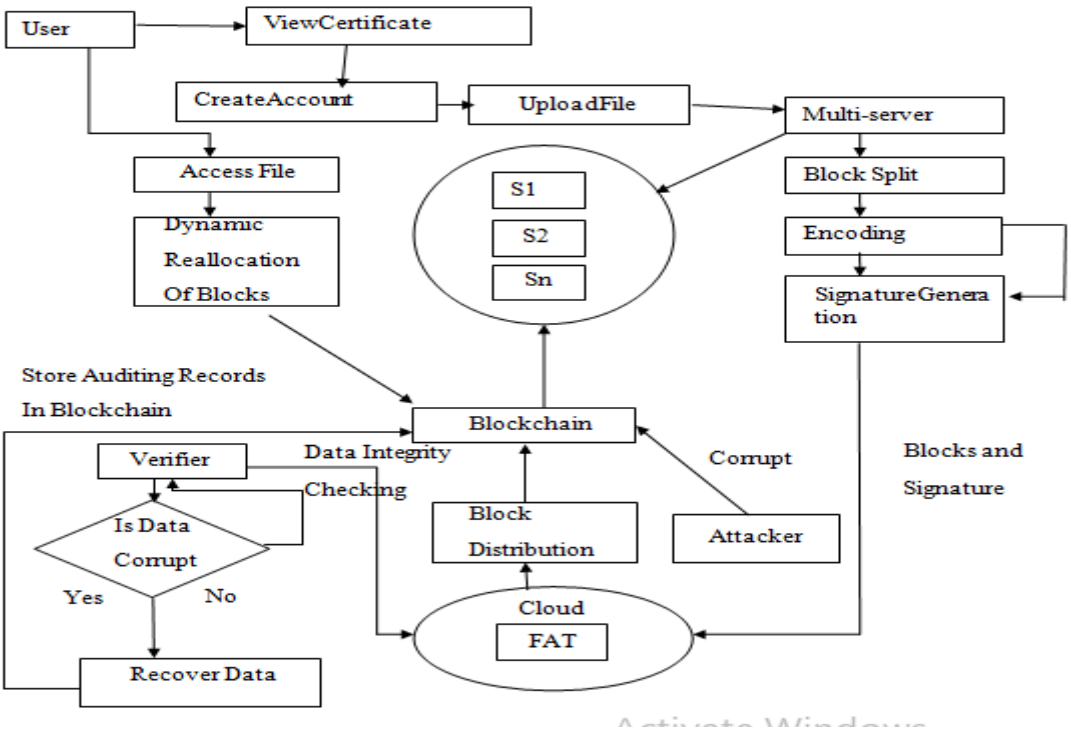
Cong Wang, Sherman S.-M. Chow, Qian Wang, KuiRen, Wenjing Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage", 2016. Users can remotely store their data and enjoy the on-demand high quality applications.It does not immediately offer any guarantee on data integrity and availability.

Jianbing Ni, Kuan Zhang, Yong Yu, Xiaodong Lin, Xuemin (Sherman) Shen, "Providing Task Allocation and Secure Deduplication for Mobile Crowdsensing via Fog Computing", 2017. A fog-assisted secure data deduplication scheme (Fo-SDD) is introduced to improve communication efficiency while guaranteeing data confidentiality.The main challenge is to find proper mobile users for sensing tasks to achieve efficient and scalable data collection

Frederik Armknecht, Jens-Matthias Bohli, Ghassan O. Karame, Zongren Liu, Christian A. Reuter, "Outsourced Proofs of Retrievability", 2014. Minimizes user effort, incurs negligible overhead on the auditor (compared to the SW scheme), and considerably improves over existing publicly verifiable POR.OPOR is technically and economically viable.

Dr. Gavin Wood, "Ethereum: A Secure DecentralisedGeneralised Transaction Ledger EIP-150 Revision", 2013. It aims to provide to the end-developer a tightly integrated end-to-end system for building software on a hitherto unexplored compute paradigm in the mainstream.

III. PROPOSED SYSTEM



| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 5, Issue 6, June 2022 |

| DOI:10.15680/IJMRSET.2022.0506091 |

Server Configuration

Admin configure Multi-Cloud server setup. Server IP Address and Port number is given by the admin for each Cloud. Now a Server Architecture is created for Multi-Cloud Storage. If the admin has to reconfigure the old Multi-Cloud server setup, it can be done. For old server setup, FAT file can be modified or remain same. Audit time will be set by the admin for Data Integrity checking process.

Data Upload and Block Split

User has an initial level Registration Process at the web end. The users provide their own personal information for this process. The server in turn stores the information in its database. After Registration, user can upload files to the server. Uploaded files will be stored in a Server. When the user upload the data to different cloud by the time it is splitted into different blocks using dynamic block generation Algorithm and each block will be appended with Signatures before storing the data in FATFS. Signature generated using MD5 Algorithm. Also, the data gets encoded using for Base64 Algorithm.

Data Integrity Checking and Updating Details in Blockchain

FATFS has proper Indexing and Metadata's for the different Chunks of the Data that is being uploaded by User. Verifier performs Remote Integrity Checking on Cloud Data. Cloud allocates random combination of all the blocks to the Verifier, instead of the whole file is retrieved during integrity checking. This is to protect user privacy from a third party (Verifier). Verifiable Data Integrity Checking Algorithm is done in two steps: Block Checking and File Checking. In Block Checking step: Three signatures are generated for Block level Checking.

- A signature of a block retrieved from a FATFS.
- A new signature is generated for block to be checked.
- A Signature is retrieved from the block appended with the signature which is stored in the Cloud.

The above three signatures are cross checked for Block level Integrity Checking. And the block contents are appended to verify with File level Integrity Checking. And update each and every auditing details in blockchain.

File Recovery and Certificate Generation

Attacker can corrupt data in any one of the cloud servers. On Data Integrity Checking done by the Verifier, Verifier informs Corrupted blocks to the Cloud. Recovery Process will be done by the verifier automatically when data gets corrupted. User can complaint to the Cloud if the user file gets corrupted (Verifier doesn't perform checking on this file).Whenever user access file, Blocks will be reallocated dynamically to provide access confidentiality in cloud and FAT File System will get updated. Auditor will monitor the cloud continuously and they provide the certificate based on the cloud performance,when new user joins in the cloud they will read the certificate and then they can create an account in the cloud.

IV. RESULT

In this paper, we have proposed a certificate-less public verification scheme against the procrastinating and malicious auditor, namely CPVMA. CPVMA utilizes the on-chain 54 currencies, where each verification performed by the auditor is integrated into a transaction on the blockchain of on-chain currencies. Furthermore, CPVMA is free from the certificate management problem. The security analysis demonstrates that CPVMA provides the strongest security guarantee compared with existing schemes. We have also conducted a comprehensive performance analysis, which demonstrates that CPVMA has constant communication overhead and is efficient in terms of computation overhead.

V. CONCLUSION AND FUTURE SCOPE

In this study, we offer CPVMA, a certificateless public verification approach that protects against procrastinating and malevolent auditors. Each verification done by the auditor is integrated into a transaction on the blockchain of on-chain currencies, according to the CPVMA. Furthermore, the certificate management issue is not an issue with CPVMA. In comparison to other schemes, the security study shows that CPVMA provides the strongest security assurance. We've also included a detailed performance analysis, which shows that CPVMA has a low communication overhead and is cost-effective in terms of computing.

For the future work, we will research ways to build CPVMA on different blockchain systems in the future. Because the fundamental disadvantage of proofs of work is their high energy consumption, building CPVMA atop alternative blockchain systems (for example, proofs-of-stake-based blockchain systems) might save energy. However, to obtain

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 5, Issue 6, June 2022 |

| DOI:10.15680/IJMRSET.2022.0506091 |

the same level of protection while maintaining high efficiency, a complex design is required. This is still an open research question that needs to be investigated further. We'll also look into how blockchains can be used to improve the security, performance, and functionality of cloud storage services. We will investigate the integration of blockchain into existing schemes, which should have a significant impact on outsourced data processing, as outsourced data processing (e.g., outsourced computation and searching through encrypted data) has played an essential part in the contemporary information era.

ACKNOWLEDGMENT

The authors would also like to thank the editorial team and all the anonymous reviewers for their valuable suggestions and comments, which helped to improve the quality of the work.

REFERENCES

[1] Yuan Zhang,Chunxiang Xu,Xiaodong Lin,Xuemin Shen, Blockchain-Based Public Integrity Verification for Cloud Storage against Procrastinating AuditorsBlockchain-Based Public Integrity Verification for Cloud Storage against Procrastinating Auditors in IEEE 2021.
[2] Jianting Ning,Zhenfu Cao,Xiaolei Dong,Kaitai Liang,Lifei Wei, Kim-Kwang Raymond Choo, CryptCloud++: Secure and Expressive Data Access Control for Cloud Storage in IEEE 2018.
[3] Taotao Wang,Chonghe Zhao, Qing Yang,Shengli Zhang,Soung Chang Liew, Ethna: Analyzing the Underlying Peer-to-Peer Network of Ethereum Blockchain in IEEE 2021.
[4] Debasis Das, Toward Next Generation of Blockchain Using Improvized Bitcoin-NG in IEEE 2021.
[5] J. Yu, K. Wang, D. Zeng, C. Zhu, and S. Guo, “Privacy-preserving data aggregation computing in cyber-physical social systems,” ACM Trans. Cyber-Phys. Syst., vol. 3, no. 1, 2018, Art. no. 8.
[6] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", White Paper, 2008, [online] Available: https://bitcoin.org/bitcoin.pdf.
[7] C. Prybila, S. Schulte, C. Hochreiner and I. Weber, "Runtime verification for business processes utilizing the Bitcoin blockchain", Future Generation Computer Systems, vol. 107, pp. 816-831, 2020.
[8] L. Gao, T. H. Luan, B. Gu, Y. Qu and Y. Xiang, "Blockchain based decentralized privacy preserving in edge computing" in Privacy-Preserving in Edge Computing, Singapore:Springer, pp. 83-109, 2021.
[9] A. Sahai, and B. Waters, Fuzzy identity-based encryption, in EUROCRYPT, 2005.
[10] M. Ali et al., "SeDaSC: Secure data sharing in clouds", IEEE Syst. J., vol. 11, no. 2, pp. 395-404, Jun. 2017.
[11] N. Attrapadung and H. Imai, "Attribute-based encryption supporting direct/indirect revocation modes", Proc. IMA Int. Conf. Cryptography Coding, pp. 278-300, 2009.
[12] I. Eyal, A. E. Gencer, E. G. Sirer and R. Van Renesse, "Bitcoin-NG: A scalable blockchain protocol", Proc. 13th USENIX Symp. Netw. Syst. Design Implement., pp. 45-59, 2016.
[13] J. Gobel and A. E. Krzesinski, "Increased block size and bitcoin blockchain dynamics", Proc. 27th Int. Telecommun. Netw. Appl. Conf. (ITNAC), pp. 1-6, Nov. 2017.
[14] Z. Zhou, X. Chen, Y. Zhang and S. Mumtaz, "Blockchain-empowered secure spectrum sharing for 5G heterogeneous networks", IEEE Netw., vol. 34, no. 1, pp. 24-31, Jan. 2020.
[15] B. Cao et al., "When Internet of Things meets blockchain: Challenges in distributed consensus", IEEE Netw., vol. 33, no. 6, pp. 133-139, Nov. 2019.
[16] H. Ren, H. Li, Y. Dai, K. Yang and X. Lin, "Querying in Internet of Things with privacy preserving: Challenges solutions and opportunities", IEEE Netw., vol. 32, no. 6, pp. 144-151, Nov./Dec. 2018.
[17] L. Zhong, Q. Wu, J. Xie, J. Li and B. Qin, "A secure versatile light payment system based on blockchain", Future Generation Comput. Syst., vol. 93, pp. 327-337, 2019.
[18] Q. Wang, C. Wang, J. Li, K. Ren and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing", Proc. 14th Eur. Conf. Res. Comput. Secur., pp. 355-370, 2009.
[19] Y. Zhang, C. Xu, X. Liang, H. Li, Y. Mu and X. Zhang, "Efficient public verification of data integrity for cloud storage systems from indistinguishability obfuscation", IEEE Trans. Inf. Forensics Secur., vol. 12, no. 3, pp. 676-688, Mar. 2017.
[20] Y. Zhang, C. Xu, H. Li and X. Liang, "Cryptographic public verification of data integrity for cloud storage systems", IEEE Cloud Comput., vol. 3, no. 5, pp. 44-52, Sep./Oct. 2016.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 5, Issue 6, June 2022 |

| DOI:10.15680/IJMRSET.2022.0506091 |

BIOGRAPHY

Fardeen Raees Jis a B.E. final year student in the department of Computer Science and Engineering from Velammal Institute of Technology, Panchetti. His current research focuses on Blockchain-Based Automated Auditing against Malicious Auditors for Data Integrity and Verification in Cloud Storage.

Sujith P is a B.E. final year student in the department of Computer Science and Engineering from Velammal Institute of Technology, Panchetti. His current research focuses on Blockchain-Based Automated Auditing against Malicious Auditors for Data Integrity and Verification in Cloud Storage.

Vignesha C J is a B.E. final year student in the department of Computer Science and Engineering from Velammal Institute of Technology, Panchetti. His current research focuses on Blockchain-Based Automated Auditing against Malicious Auditors for Data Integrity and Verification in Cloud Storage.

Mr.R.Raja, M.E., is an Assistant Professorof Computer Science and Engineering Department in Velammal Institute of Technology, Panchetti.

Impact Factor
7.54

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com