International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 09 | September - 2022 Impact Factor: 7.185 ISSN: 2582-3930

BLOCKCHAIN-BASED PUBLIC INTEGRITY VERIFICATION FOR CLOUD STORAGE AGAINST PROCRASTINATING AUDITORS

NIKHIL.S, Mr. V. NAGARAJAN., AP

• II MCA, SRI MUTHUKUMARAN INSTITUTE OF TECHNOLOGY, CHENNAI.

• Professor, MCA SRI MUTHUKUMARAN INSTITUTE OF TECHNOLOGY, CHENNAI.

ABSTRACT

The deployment of cloud storage services has significant benefits in managing data for users. However, it also causes many security concerns, and one of them is data integrity. Public verification techniques can enable a user to employ a third-party auditor to verify the data integrity on behalf of her/him, whereas existing public verification schemes are vulnerable to procrastinating auditors who may not perform verifications on time. We present rigorous security proofs to demonstrate the security of CPVPA, and conduct a comprehensive performance evaluation to show that CPVPA is efficient.

1.INTRODUCTION

An increasing number of organizations outsource their data, applications and business processes to the cloud, empowering them to achieve financial and technical benefits due to on-demand provisioning and pay-per-use pricing. However, organizations are still hesitant to adopt cloud services because of security, privacy, and reliability concerns regarding provisioned cloud services as well as doubts about trustworthiness of their cloud service provider. Cloud service certifications (CSC) are good means to address these concerns by establishing trust, and increasing transparency of the cloud market. Cloud service certifications attempt to assure a high level of security and compliance. However, considering that cloud services are part of an ever-changing environment, multiyear validity periods may put in doubt reliability of such certifications. We argue that continuous auditing (CA) of selected certification criteria is required to assure continuously reliable and secure cloud services, and thereby increase trustworthiness of certifications. CA of cloud services is still in its infancy and we reveal that most of existing methodologies are not applicable for third party auditing purposes. Therefore, we propose a conceptual CA architecture, and highlight important components and processes that have to be implemented.

2.OBJECTIVE

With cloud storage services, users outsource their data to cloud servers and access that data remotely over the Internet [1], [2]. These services provide users an efficient and flexible way to manage their data, while users are free from heavy local storage costs [3], [4], [5]. Although users enjoy great benefits from these services, data outsourcing has also incurred critical security issues [6], [7], [8]. One of the most important security concerns is data integrity [9], [10]. Unlike traditional data management paradigm, where users store their data locally, users would not physically own their data once having outsourced the data to cloud servers. Therefore, users are always worried about the data integrity, i.e., whether the outsourced data is well maintained on cloud servers. The integrity of outsourced data is being put at risk in practice [11], [12]. For example, the cloud servers may always conceal incidents of data corruption for good reputation, may delete a part of data that is never accessed to reduce the storage costs [13], [14]. Furthermore, an external adversary may tamper with the outsourced data for financial or political reasons [15]. Therefore, the integrity of outsourced data should be verified periodically. The verification can be performed by the users themselves. However, this lays a heavy communication burden on users to retrieve verify the data.

3.EXITING SYSTEM

In cloud computing, remote data integrity checking is an important security problem. The client's massive data is outside his control. The malicious cloud server may

corrupt the client's data in order to gain more benefits. However, cloud services are part of an ever-changing environment, resulting from fast technology life cycles and inherent cloud computing (CC) characteristics, like on-demand provisioning and entangled supply chains. Hence, such long validity periods may put in doubt reliability of issued certifications. And also cloud service customers do not longer possess their data locally, assuring that their data is being correctly stored and integrity is maintained in cloud environments is of critical importance. Data integrity may be threatened by, for example, malicious insiders, data loss, technical failures, and by external attackers.

4.PROPOSED SYSTEM

In MultiCloud environment, remote data integrity checking is required to secure user's data. User will upload file to Cloud. This file is split into blocks using Dynamic Block generation Algorithm and stored in a MultiCloud environment. File Allocation Table (FAT) File System has proper Indexing and 11 Metadata for the different Chunks of the Cloud Storage. Here the auditor agrees to inspect logs, which are routinely created during monitoring operations by services providers to assess certification adherence. If Attacker corrupts data in MultiCloud, the continuous auditing process helps the verifier to perform Block level and File level checking for remote data Integrity Checking using Verifiable Data Integrity Checking Algorithm. Cloud provides random blocks to Verifier for Integrity Checking which is to protect user privacy from Verifier (Third Party). File recovery is done by the Verifier automatically if the data gets corrupted during checking. Users can complaint cloud for file recovery. And also, we use blockchain for proposed system. We add all the details about auditing record in blockchain for security purpose

FEASIBILITY STUDY

These services provide users an efficient and flexible way to manage their data, while users are free from heavy local storage costs. Although users enjoy great benefits from these services, data outsourcing has also incurred critical security issues. One of the most important security concerns is data integrity.

Java

Java is an object-oriented programming language developed initially by James Gosling and colleagues at Sun Microsystems. The language, initially called Oak (named after the oak trees outside Gosling's office), was intended to replace C++, although the feature set better resembles that of Objective C.

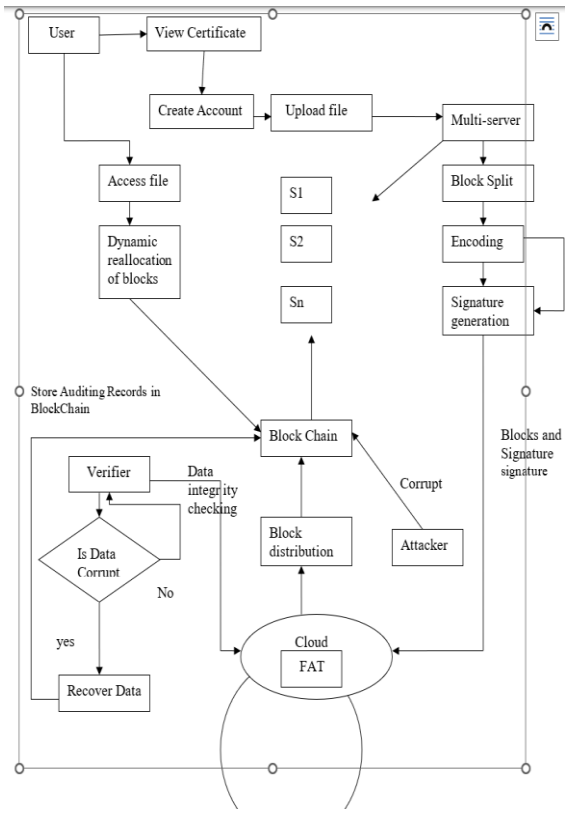
Apache Tomcat Server

Apache Tomcat (formerly under the Apache Jakarta Project; Tomcat is now a top-level project) is a web container developed at the Apache Software Foundation. Tomcat implements the servlet and the Java Server Pages (JSP) specifications from Sun Microsystems, providing an environment for Java code to run in cooperation with a web server. It adds tools for configuration and management but can also be configured by editing configuration files that are normally XML-formatted. Because Tomcat includes its own HTTP server internally, it is also considered a standalone web server.

Blockchain

With the emergence of Digital Currency (aka Crypto currency), several enterprises or financial institutions are experimenting with the Distributed Ledger system as a trusted way to track the ownership of the assets without any central authority. The core system behind the new currency system is Blockchain technology. A walkthrough of the basic building blocks of the Blockchain technology is described below. A Blockchain is basically a chain of Blocks. Blocks are hashed using SHA-256 hashing algorithm to generate the signature of the data associated with it.

Architecture



5.MODULES DESCRIPTION

User: The user is the data owner, who outsources her/his data to the cloud server and accesses the outsourced data as needed. After data outsourcing, the user employs a TPA, agrees a verification period with TPA, and let TPA periodically verify the data integrity.

Cloud server: The cloud server is subject to the cloud service provider, and provides cloud storage services. It has not only significant storage space, but also a massive amount of computing power.

Auditing: Auditing works for the user. It feeds back the verification results to the user and the cloud server, and detects the data corruption as soon as possible. The communication between auditing and other entities is authenticated.

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 39 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 uploads the data to different cloud by the time it is spitted 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 Update details in blockchain

FATFS has proper Indexing and Metadata 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.

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.

6.CONCLUSION

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

7.REFERENCES

1. J. Yu, K. Wang, D. Zeng, C. Zhu, and S. Guo, "Privacy-preserving data aggregation computing in cyber-physical social systems," ACM Transactions on Cyber-Physical Systems, vol. 3, no. 1, p. 8, 2018.
2. H. Ren, H. Li, Y. Dai, K. Yang, and X. Lin, "Querying in internet of things with privacy preserving: Challenges, solutions and opportunities," IEEE Network, vol. 32, no. 6, pp. 144– 151, 2018.
3. J. Li, H. Ye,W.Wang,W. Lou, Y. T. Hou, J. Liu, and R. Lu, "Efficient and secure outsourcing of differentially private data publication," in Proc. ESORICS, 2018, pp. 187–206.
4. L. Zhong, Q. Wu, J. Xie, J. Li, and B. Qin, "A secure versatile light payment system based on blockchain," Future Generation Computer Systems, vol. 93, pp. 327–337, 2019.
5. G. Xu, H. Li, Y. Dai, K. Yang, and X. Lin, "Enabling efficient and geometric range query with access control over encrypted spatial data," IEEE Trans. Information Forensics and Security, vol. 14, no. 4, pp. 870–885, 2019.
6. K. Yang, K. Zhang, X. Jia, M. A. Hasan, and X. Shen, "Privacy preserving attributekeyword-based data publish-subscribe service on cloud platforms," Information Sciences, vol. 387, pp. 116– 131, 2017.
7. H. Yang, X. Wang, C. Yang, X. Cong, and Y. Zhang, "Securing -centric networks with content-based encryption," Journal of Network and Computer Applications, vol. 128, pp. 21–32, 2019.
8. Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data 101 dynamics for storage security in cloud computing," in Proc. of ESORICS, 2009, pp. 355–370.
9. X. Zhang, H. Wang, and C. Xu, "Identity-based key-exposure resilient cloud storage public auditing scheme from lattices," Information Sciences, vol. 472, pp. 223–234, 2018.
10. J. Ni, K. Zhang, Y. Yu, X. Lin, and X. Shen, "Providing task allocation and secure deduplication for mobile crowdsensing via fog computing," IEEE Transactions on Dependable and Secure Computing, to appear, doi. 10.1109/TDSC.2018.2791432.
11. H. Shacham and B. Waters, "Compact proofs of retrievability," of Cryptology, vol. 26, no. 3, pp. 442–483, 2013.