Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 8, August : 2023

Data Blinding-based Data Integrity Audit For Cloud And Fog Environment

D. Bujjibabu 1, Gadamsetti Venkata Naga Anitha 2

#1Professor in the department of MCA at QIS College of Engineering and Technology (Autonomous), Vengamukkapalem, Prakasam (DT)
#2MCA Student in the department of MCA at QIS College of Engineering and Technology (Autonomous), Vengamukkapalem, Prakasam (DT)

ABSTRACT_ Cloud-fog computing is an innovative computing concept that extends the capabilities of cloud computing by delivering multiple services via fog nodes. Traditional data integrity auditing has issues with data security, data processing speed, and communication efficiency. This study presents a data integrity audit scheme based on data blinding to address these issues. To reduce transmission time, this strategy employs edge devices in the transmission node to create a fog computing layer between the cloud service provider and the data owner. To reduce transmission time, the subordinate distribution relationship and weight between fog nodes dynamically allocate the appropriate path and send the data. To prevent data leakage, a blind element is added to the integrity audit throughout the evidence creation process. Based on computational Diffie-Hellman (CDH) assumptions, this study provides a security model and security proof. The experimental findings reveal that the fog computing layer and blind factor are incorporated into the data integrity audit process, which effectively reduces data communication delay and improves data audit security.

1. INTRODUCTION

As of late, as the wealth of data has developed, the capacity and figuring prerequisites on cell phones, PCs, and other terminal gadgets have expanded. To decrease the capacity tension on terminal gadgets, a few clients store their information in the cloud [1]. Notwithstanding, some cloud specialist co-ops could erase a rarely utilized information to decrease server above. Erased information may not be recovered, bringing about cloud information misfortune. As clients transfer information, the information is put away on the cloud server rather than the nearby gadget [2]. Remotely checking the uprightness of the information transferred by clients has turned into a critical issue. Because of the above issues, the idea of Distant Information Ownership Checking (RDPC) is proposed, which incorporates verification of retrievability

(POR) and provable information parade (PDP) [3]-[5]. Nonetheless, according tothe point of view of information review, it tends to be isolated into private and public reviews. The examiner of the confidential review is the information proprietor, while the evaluator of the public review can be any approved outsider review. Because of the greater adaptability of public examining techniques, the vast majority of them will pick public evaluating [6]. As the web has found its direction into individuals' lives, distributed computing appreciates rising notoriety among people, everything being equal. An ever increasing number of clients store their information in the cloud for simple use whenever, anyplace. Notwithstanding, in the customary distributed storage model, the cloud specialist organization requirements to lay out an association with every client, which imperceptibly builds the heap tension on the cloud specialist co-op [7]. In this way, how to diminish the processing and burdenstrain of cloud specialist co-ops has turned into a dire issue to be settled.

2. LITERATURE SURVEY

1. H. Yan, J. Li, and Y. Zhang, ‘‘Remote data checking with a designated verifier in cloud storage,’’ IEEE Syst. J., vol. 14, no. 2, pp. 1788–1797, Jun. 2020.

Abstract:

Remote data possession checking (RDPC) supplies an efficient manner to verify the integrity of the files stored in cloud storage. Public verification allows anyone to check the integrity of remote data so that it has a wider application in public cloud storage. Private verification just allows the data owner to verify the data integrity, which is mainly applied for the verification of secret data. However, in many real applications, the data owner expects a specific user to check the files in cloud storage, whereas others cannot execute such work. It is obvious that neither public verification nor private verification can satisfy such a requirement. To solve this issue, Ren et al. provided a designated-verifier provabledata possession (DV-PDP) protocol. Unfortunately, the DV-PDP is insecure against replay attack launched by the malicious cloud server. To overcome this shortcoming, we present a new RDPC scheme with the designated verifier, in which the data owner specifies a unique verifier to check the data integrity. Based on the computational Diffie-Hellman assumption, we prove the security for our RDPC scheme in a random oracle model. The theoretical analysis and experiment results indicate that our scheme has less communication, storage, and computation

overhead while achieving high error detection probability.

2. J. Chang, H. Wang, F. Wang, A. Zhang, and Y. Ji, ‘‘RKA security for identity-based signature scheme,’’ IEEE Access, vol. 8, pp. 17833–17841, 2020

Related-key attack (RKA) is a kind of side-channel attack considered for kinds of cryptographic primitives, such as public key encryption, digital signature, pseudorandom functions etc. However, we note that the RKA-security seems to be not considered for identity-based signature (IBS), which is an important primitive for identity-based cryptography and proposed by Shamir in 1984. In this paper, for the first time, we introduce the RKA security into IBS schemes and try to define the security model for it. More specifically, weconsider the RKA occurs in the users’ signing key or the master key of the key- generation center (KGC), which derives two kinds of RKA securities for IBS. Meanwhile, we illustrate that the most efficient Schnorr-like IBS scheme proposedby Galindo and Garcia is RKA-insecure bylaunching a simple RKA. However, a slightmodification of it yields a RKA-secure IBSscheme, for which we give the detailed security proof in the random oracle. Finally, the performance analysis shows that the modified scheme is still extremely efficient but has higher security.

3.PROPOSED SYSTEM

This study presents a data integrity audit scheme based on cloud and fog architecture, as well as a data transmission model for cloud and fog networks. In this concept, fog nodes send and calculate data to locate the shortest communication channel, lowering communication overhead. Simultaneously, a blind element is introduced in the integrity audit's evidence production step to prevent the adversary from calculating the ciphertext in the two interrogations and increase the integrity audit's security.

The following are the primary contributions of this study.

1) This work provides a data integrity audit methodology in a cloud and fog environment that can effectively reduce communication overhead in the transmission process as well as the cloud service provider's computational strain.
2) A blind element is introduced in the data integrity audit to eliminate data leaking caused by repeated submissions of malevolent auditors while questioning data.
3) Using the provided security model, this article demonstrated the scheme's

security. The experimental results suggest that this system performs better and is more feasible.

3.1 IMPLEMENTATION

3.1.1 Data Owner

In this module, the data owner uploads their encrypted data in the Cloud server. For the security purpose the data owner encrypts the data file and then store in the server. The Data owner can have capable of manipulating the encrypted data file and performs the following operations Register and Login, Upload File, View Files, Update File, Verify File's Block(Data Integrity Auditing).

3.1.2 Cloud

The Cloud manages which is to provide data storage service for the Data Owners. Data owners encrypt their data files and store them in the Server for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the Server and then Server will decrypt them. The server will generate the aggregate key if the end user requests for file authorization to access and performs the following operations such as Login, View and Authorize User, View and Authorize Owner, View Files By Block chain, View All Transactions, Search Requests, Download Requests, View All Attackers, View File Rank Chart, View Time Delay Results, View Throughput Results.

3.1.3 User

In this module, the user can only access the data file with the secret key. The user can search the file for a specified keyword. The data which matches for a particular keyword will be indexed in the cloud server and then response to the end user and performing the following operations Register and Login, Search, Download, View Files, Search Request, Download Request.

3.1.4 TPA

responsible for Login, View File's Meta Data, View Files & Generate Secret Key, CPU Speed.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 8, August : 2023

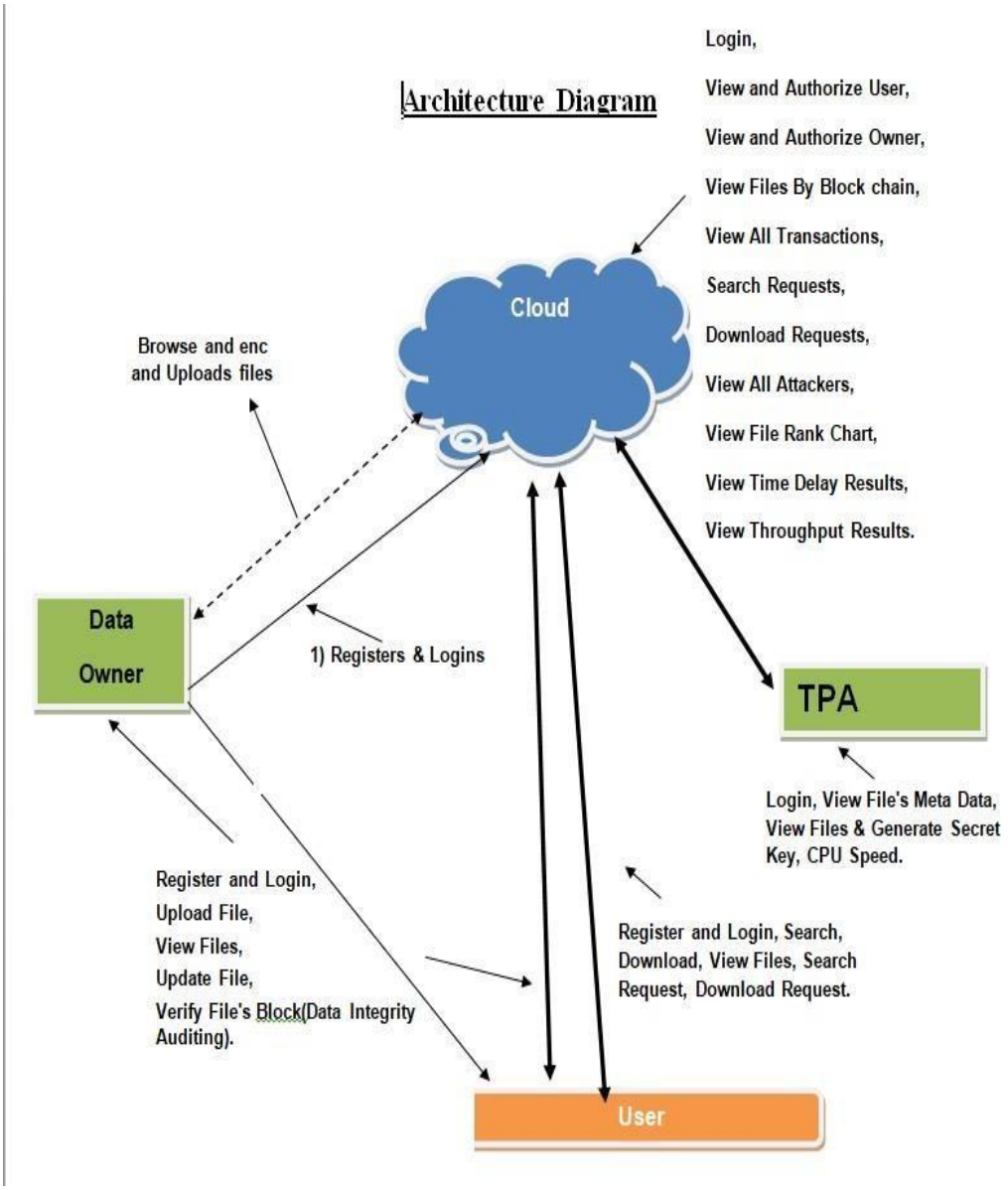

Fig 1:Architecture

4.RESULTS AND DISCUSSION

Table 1:Comparison of communication cost

Protocol	DOtoCSP	TPAtoCSP	CSPtoTPA
PPDP	$n\|G_1\| + \|F\| + \|\psi\|$	$3\|Z_q^*\| + \|\psi\| + \|Sign(\psi)\|$	$\|G_1\| + \|Z_q^*\|$
RDPC	$n\|G_1\| + \|F\|$	$3\|Z_q^*\|$	$\|G_1\| + \|Z_q^*\|$
Ours	$n\|G_1\| + \|F\| - \tau(n\|G_1\| + \|F\|)$	$3\|Z_q^*\| - \tau(3\|Z_q^*\|)$	$\|G_1\| + \|Z_q^*\| - \tau(\|G_1\| + \|Z_q^*\|)$

* $|\psi|$ and $|Sign(\psi)|$ represent the warrant size and its signature size.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 8, August : 2023

Table 2:Comparison of computation cost

Protocol	TagGen	ProofGen	Verify
PPDP	$T_p + (2n+1)T_{exp} + nT_{mul} + Sign$	$cbT_{exp} + (cb-1)T_{mul} + Ver$	$3T_p + (cb+2)T_{exp} + cbT_{mul}$
RDPC	$(2n+1)T_{exp} + nT_{mul}$	$cbT_{exp} + (cb-1)T_{mul}$	$2T_p + (cb+2)T_{exp} + cbT_{mul}$
Ours	$2nT_{exp} + nT_{mul}$	$cbT_{exp} + (cb-1)T_{mul}$	$3T_p + (cb+1)T_{exp} + cbT_{mul}$

* *Sign* and *Ver* represent the computational cost of the signature and verification method in PPDP.

This scheme's communication overhead was compared to that of the PPDP and RDPC schemes in Table 1. When compared to the PPDP approach, this scheme lowers the overhead of the warrant size during the DOtoCSP stage. The cloud-fog node's overhead is also lower than that of the other two techniques (n|G1| + |F|)). The communication overhead of a challenge block and two random number seeds communicated in the cloud-fog node is lowered in the TPAtoCSP stage, which is (3|Z *q |), in comparison to the other two methods. By reducing the communication burden of the warrant size and signature size, this technique only requires the challenge block number and random number seeds to be sent during the challenge stage. The proof block and proof label are returned by CSP in the CSPtoTPA stage, hence the communication overhead is |G1| + |Z ∗ q |. This method lowers the transmission overhead in the cloud-fog node as compared to the first two methods. The quantity of data needed for communication is simplified by this system, which also has a lower communication overhead in the three stages than the PPDP and RDPC schemes do.

Let Tp, Texp and Tmul represent the bilinear mapping, multiplication and exponential operations on the multiplication cyclic group G1. Since the calculation cost of operations such as hashing and pseudo-random number generation is meager, they are ignored in calculating the overhead. In the tag generation stage, the data owner runs the TagGen algorithm, and its computational cost is 2nTexp + nTmul. For the ProofGen algorithm, the computational cost of cbTexp + (cb − 1)Tmul is required. However, in the verification stage, the verifier runs the Verify algorithm, and the computational cost is 3Tp + (cb + 1)Texp + cbTmul. Table 2 compares the computation overhead of our scheme with PPDP and RDPC scheme. According to Table 2, this scheme reduces the operation steps in the calculation and verification process

without reducing the security. In the TagGen algorithm, this scheme reduces the computational cost of bilinear mapping, signature and multiplication compared with the PPDP scheme, and reduces the computational overhead of multiplication compared with the RDPC scheme. In the proof generation algorithm, this scheme reduces the computational cost of the verification part compared with the PPDP scheme. In terms of the computational cost of verification, the cost of this scheme is close to that of the PPDP and RDPC schemes.

5.CONCLUSION

In this study, we present a DBCF protocol for use in cloud and fog environments. In the case of data integrity auditing, this protocol can ensure data security. This approach includes a blind component into the data verification process and adds random values to each verification, preventing the adversary from making multiple requests for user information. At the same time, the fog computing layer is built, and the cloud and fog structure is employed to update the transmission network's architecture. This can significantly cut communication overhead. Furthermore, the security model is provided and demonstrated to be secure under the random oracle model proposed by CDH. Finally, the performance study indicates that this technique will be more efficient in practise. The architecture model of the fog computing layer can be enhanced in future work to make it more efficient..

REFERENCES

[1] K. Hao, J. Xin, Z. Wang, and G. Wang, ``Outsourced data integrity

veri_cation based on blockchain in untrusted environment," World Wide

Web, vol. 23, no. 4, pp. 2215_2238, Jul. 2020.

[2] Y. Fan, X. Lin, G. Tan, Y. Zhang, W. Dong, and J. Lei, ``One secure data

integrity veri_cation scheme for cloud storage," Future Gener. Comput.

Syst., vol. 96, pp. 376_385, Jul. 2019.

[3] H. Wang and J. Zhang, ``Blockchain based data integrity veri_cation for

large-scale IoT data," IEEE Access, vol. 7, pp. 164996_165006, 2019.

[4] Z. Miao, C. Ye, P. Yang, R. Liu, B. Liu, and Y. Chen, ``A scheme for

electronic evidence sharing based on blockchain and proxy re-encryption,"

in Proc. 4th Int. Conf. Blockchain Technol. Appl., Dec. 2021, pp. 11_16.

[5] F. Kefeng, L. Fei, Y. Haiyang, and Y. Zhen, ``A blockchain-based _exible

data auditing scheme for the cloud service," Chin. J. Electron., vol. 30,

no. 6, pp. 1159_1166, Nov. 2021.

[6] K. He, J. Shi, C. Huang, and X. Hu, ``Blockchain based data integrity

veri_cation for cloud storage with T-Merkle tree," in Proc. Int. Conf. Algo-

rithms Archit. Parallel Process. Cham, Switzerland: Springer, Oct. 2020,

pp. 65_80.

[7] Y. Lei, Z. Jia, Y. Yang, Y. Cheng, and J. Fu, ``A cloud data access

authorization update scheme based on blockchain," in Proc. 3rd Int. Conf.

Smart BlockChain (SmartBlock), Oct. 2020, pp. 33_38.

[8] Y. Yuan, J. Zhang, W. Xu, and Z. Li, ``Identity-based public data

integrity veri_cation scheme in cloud storage system via blockchain," J.

Supercomput., vol. 78, pp. 8509_8530, Jan. 2022.

[9] S. Wang, D. Zhang, and Y. Zhang, ``Blockchain-based personal health

records sharing scheme with data integrity veri_able," IEEE Access, vol. 7,

pp. 102887_102901, 2019.

[10] A. Liu, Y. Wang, and X. Wang, ``Blockchain-based data-driven smart

customization," in Data-Driven Engineering Design. Cham, Switzerland:

Springer, 2022, pp. 89_107.

[11] K. Dhyani, J. Mishra, S. Paladhi, and I. S. Thaseen, ``A blockchain-based

document veri_cation system for employers," in Proc. Int. Conf. Comput.

Intell. Data Eng. Singapore: Springer, 2022, pp. 123_137.

[12] K. Xu, W. Chen, and Y. Zhang, ``Blockchain-based integrity veri_cation

of data migration in multi-cloud storage," J. Phys., Conf. Ser., vol. 2132,

no. 1, Dec. 2021, Art. no. 012031.

[13] G. Xu, S. Han, Y. Bai, X. Feng, and Y. Gan, ``Data tag replacement

algorithm for data integrity veri_cation in cloud storage," Comput. Secur.,

vol. 103, Apr. 2021, Art. no. 102205.

AUTHOR PROFILES

Dr.D.Bujji Babu, currently working as a Professor and Head in the Department of Master of Computer Applications, QIS College of Engineering and Technology, Ongole, Andhra Pradesh. He did his M.Tech(CSE) from JNTUK, Kakinada and Ph.D(CSE) from Acharya Nagarjuna University. He published more than 50 research papers in reputed peer reviewed Scopus indexed journals. He also attended and presented research papers in different national and international journals and the proceedings were indexed IEEE, Springer Link series.He visited the countries Kuching, Malaysia for attending and presenting his research articles. 3 Patent journals are published and in pipeline for grant. He wrote more than an dozen of monographs and published by the Technical Publishers. He Published Two Course content modules for the students of Acharya Nagarjuna University. He is the recognized research supervisor under JNTUK, Kakinada and guided several UG and PG Projects, currently supervising 3 research scholar under JNTUK. His area of interest is Software Engineering, Data Mining, Data Science, Big Data and Programming Languages. He is the Principal Investigator for the DST Sponsored Project and Co-PI for another DST Project.

Ms.G.V.N. Anitha as MCA Student in the department of Qis College of engineering and Technology (autonomous), Vengamukkapalem, Prakasam(DT).She has Completed B.Sc. in Computer Science from Nagarjuna Degree &p.g College. Her areas of interests are Cloud Computing & Machine learning.