iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** III **Month of publication:** March 2019

DOI: http://doi.org/10.22214/ijraset.2019.3133

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue III, Mar 2019- Available at www.ijraset.com

Reliable and Effectual Solitude Conformable Data Ownership in Cloud Computing

K. Suja Rajeswari[1], S. Kaviya[2], S. Haripriya[3]
[1]*Assistant Professor,* [2, 3]*Student, Department of CSE, PIT, Chennai-600123*

Abstract: ***Cloud computing is a paradigm which provide secure and pliable infrastructure enabling the data owners to store their data and they can access from cloud servers. This paradigm reduces storage and cost of maintenance. The user loses the physical control and ownership of data which leads to certainty risks. So to label these difficulty this work proposes a reliable and effectual solitude conformable data ownership in cloud computing. Further this scheme is extended to brace multiple owners' data dynamics and batch verification.***

Keywords: Integrity Verification, Storage as a Service, Privacy Preserving, Dynamic Auditing, Batch Auditing.

I. INTRODUCTION

Storage as a resource has emerged as a commercial replacement for storage of local data. This is because of some attributes which includes low initial foundation setup and get rid off from maintenance. Even though it provides many well being like saving cost, penetrability, usability, synchronizing and sharing, it undergoes many reliability threats because the data is under the dominance of the cloud service provider [1],[2].CSP can dispose the seldom accessed data. This is done in order to save storage space and earn more profit. However checking the possession of data in cloud storage is necessary. Checking the integrity in data involves traditional cryptographic solutions which either need the local copy of the data or permit the users to download the entire data [7],[8]. Preserving privacy is crucial to prevent third party auditor to surmise the data while auditing In this work we propose a reliable and effectual data possession scheme for storage in cloud [2],[3]. It operates in three phases namely key generation, signature generation and auditing phase.

II. RELATED WORK

Protocols for remote data integrity can be broadly designated into kinds. One is deterministic covenant based strategies. This strategy verifies each block of data so that it requires only considerable amount of Two different integrity mechanisms are designed for verification.

One uses pseudo random function while other uses boneh Lynn sachem signatures. Pseudo random function fails to provide public verifiability. It fails to provide reliability of the data owners' data but both the schemes support block less verification. Public auditing scheme is designed to maintain reliability of the data owner. Multiple auditing request can be performed concomitantly by the third party auditor [11],[12],[13].

As it responds to many requests it fails to support data dynamics. If one block is updated, deleted or inserted other blocks of corresponding verification must be updated. The proposed scheme uses hash table. IHT is used to support data dynamics in public monitoring mechanism which reduces the update overhead. Secure auditing protocol achieves all necessary features of public auditing. Also it consumes lesser communication cost and manipulation. Pairing based cryptography requires huge attestation cost.

III. SYSTEM MODEL

Public auditing for cloud data storage consist of four entities namely data owner, data user, cloud service provider and third party auditor. Data users handle and ingress on those data kept at cloud service provider [4],[6]. Users are the entities who store their data in the cloud.

But when we operate on the incorrect data it leads to faulty result which creates disorder of remotely stored data. Third party auditor is used to verify the integrity of outsourced data. Initially a secret key is shared by data owner with third party owner through a reliable channel using any standard technique like SSL/TSL. Outsourced data of every block is tagged with a signature manipulated using the private key of data owner.

A challenge is send by the third party auditor to the cloud service provider and it turns the cloud service provider respond to proof possession of data. Thus it is a category of challenge response protocol. Cloud service provider is assumed to be semi trusted. Protocol is executed without affecting data integrity.

©IJRASET: All Rights are Reserved

IV. DESIGN GOALS

1) *Assurance for Storage Correctness:* Audit phase can be passed by the cloud service provider only if it is same as uploaded by data owner.
2) *Guarantee for Reliable Preserving:* Third party auditor fails to infer the data from the response provided by cloud service provider.
3) Block less verification: Verification can be done by the auditor by checking the desired blocks at once.
4) *Public Auditablity:* Any third party other than data owner should be able to correctly verify the integrity of the data stored in cloud service provider without downloading the entire outsourced data.
5) *Assurance for Unforgetablity:* It must be manipulatively infeasible for cloud service provider to forge a response in the auditing phase.
6) *Batch Auditing:* TPA should be capable enough to deal with the multiple number of verification requests from different data users simultaneously [15],[17],[18].
7) *Data Dynamics:* The scheme should facilitate the data owners to perform insert, modify, and delete operations on a particular block of data without the change in meta data of other blocks.

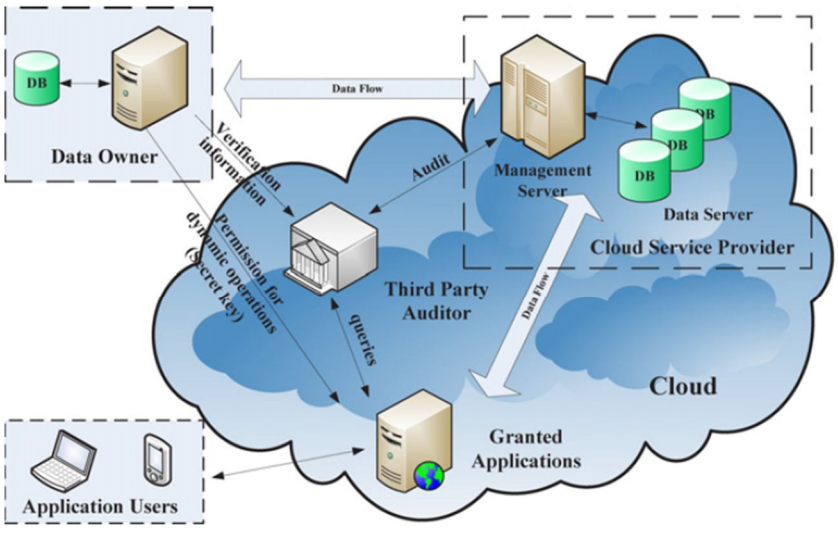
V. EXISTING SYSTEM

Firstly outsourcing data to cloud server implies that data is out of control of users [14],[15]. This may cause users hesitation since the outsourced data usually contain valuable and sensitive information. Secondly data sharing is often implemented in an open and hostile environment and cloud server would become a target of attacks. Although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they are still facing the broad range of both internal and external threats for data integrity.

The existing system faces lots of security risk over the data sharing and integrity checking. To address these issues in auditing we introduce a third party auditor [2],[6]. Number of schemes has been proposed to check the integrity of data. Idea of signature exchange is also adopted for correctness of metadata [3],[4],[8]. To access data from cloud a number of VPH applications have been designed. Thus an effective and reliable dynamic auditing protocol is desired to persuade data owners that the data are correctly stored in the cloud [6][7].

VI. PROPOSED SYTEM

In this section, a proposed scheme called reliable and effective data possession scheme is introduced. This work consists of three phases namely key generation phase, signature generation phase and auditing phase. In simple first it is described with a single data owner then it is extended to support multiple data owners [12],[15].



Audit system architecture for cloud computing

FIG:1

©IJRASET: All Rights are Reserved

Encryption of blocks is done using AES algorithm followed by message digest using
Secure hash algorithm. This message digest is later send to third party auditor. Auditing is performed by third party auditor on the demand by client. Integrity of data is checked by third party auditor [2],[5],[7].

Here we use a cryptographic technique to verify the integrity of data. It is done in a random manner. Since multiple auditing tasks is done to support the efficiency a technique called bilinear aggregate signature is extended for multiple users.

VII. MODULES

A. Audit Service System

It provides cloud service providers with a way to make their performance and security data readily available for potential customers.

B. Data Storage Service System

The data stored in the cloud is accessible to data users over the network.

C. Audit Outsourcing System

Clients no longer have physical possession data indicates that they are facing a potentially security risk. Audit services are critical to ensure the integrity and availability of outsourced data and credibility in cloud computing.

D. Secure And Performance Analysis

Some guarantee should be assured when client host data to the cloud. The access is specific to only limited users. With the security, mechanism for data integrity should be implemented.

VIII. CONCLUSION

In this paper, an effective audit service for the integrity of data is addressed. For the interactive system a third party auditor knew as agent of data owners.

To realize the audit model, security of the system is essential. Hence to replace the traditional hash system our technology can be easily used in cloud computing environment. This approach reduces our work greatly. Our experiments could clearly show that our approach could minimize manipulation and communication overheads.

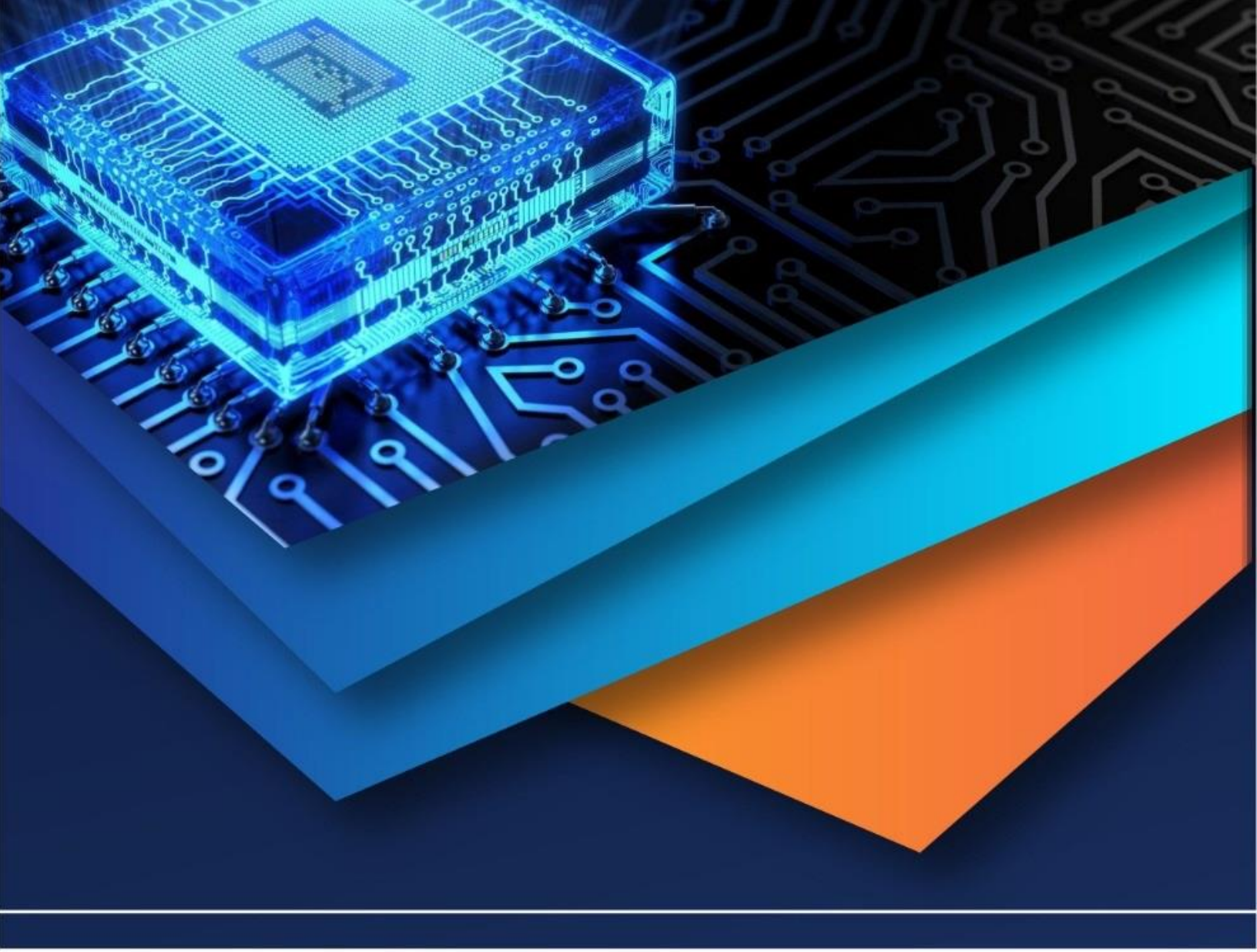
REFERENCES

[1] K. Yang and X. Jia, "Data storage auditing service in cloud com- puting: challenges, methods and opportunities," World Wide Web, vol. 15, no. 4, pp. 409–428, 2012.
[2] B. Wang, B. Li, H. Li, and F. Li, "Certificateless public auditing for data integrity in the cloud," in Proceedings IEEE Conference on Communications and Network Security (CNS), 2013, pp. 136–1
[3] H. Shacham and B. Waters, "Compact proofs of retrievability," inProceedings of 14th ASIACRYPT, 2008, pp. 90–107.
[4] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in Proceedings of 29th IEEE Conference on Computer Communications (INFOCOM), 2010, pp. 1–9.
[5] L. Yuchuan, F. Shaojing, X. Ming, and W. Dongsheng, "Enable data dynamics for algebraic signatures based remote data possession checking in the cloud storage," China Communications, vol. 11, no. 11, pp. 114–124, 2014.
[6] A. F. Barsoum and M. A. Hasan, "Provable multicopy dynamic data possession in cloud computing systems," IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, pp. 485–497,
[7] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy- preserving public auditing for secure cloud storage," IEEE Trans- actions on Computers, vol. 62, no. 2, pp. 362–375, 2013
[8] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peter- son, and D. Song, "Provable data possession at untrusted stores," in Proceedings of the 14th ACM conference on Computer and commu- nications security, 2007, pp. 598–609.
[9] B. Wang, H. Li, X. Liu, F. Li, and X. Li, "Efficient public verification on the integrity of multi-owner data in the cloud," Journal of Communications and Networks, vol. 16, no. 6, pp. 592–599, 2014.
[10] Y. Zhu, H. Hu, G.-J. Ahn, and M. Yu, "Cooperative provable data possession for integrity verification in multicloud storage," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 12, pp.
[11] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 9, pp. 1717–1726,2013. in cloud computing," IEEE trans- actions on Services Computing, vol. 5, no. 2, pp. 220–232, 2012.
[12] H. Wang, "Proxy provable data possession in public clouds," IEEE Transactions on Services Computing, vol. 6, no. 4, pp. 551–559, 2013.
[13] ——, "Identity-based distributed provable data possession in mul- ticloud storage," IEEE Transactions on Services
[14] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward secure and dependable storage services

©IJRASET: All Rights are Reserved

[15] Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and C.-J. Hu, "Dynamic audit services for outsourced storages in clouds," IEEE Transactions on Services Computing, vol. 6, no. 2, pp. 227–238, 2013.
[16] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, "Dynamic audit services for integrity verification of outsourced storages in clouds," in Proceedings of the 2011 ACM Symposium on Applied Computing. ACM, 2011, pp. 1550–1557.
[17] F. Sebe´, J. Domingo-Ferrer, A. Martinez-Balleste, Y. Deswarte, and J.-J. Quisquater, "Efficient remote data possession checking in criticaL information infrastructures," IEEE Transactions on Knowledge and Data Engineering, vol. 20, no. 8, pp. 1034–1038, 2008.
[18] D. L. Gazzoni Filho and P. S. L. M. Barreto, "Demonstrating data possession and uncheatable data transfer." IACR Cryptology ePrint Archive, vol. 2006/150, 2006.
[19] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," in Proceedings of 7th ASIACRYPT, 2001, pp. 514–532
[20] P. Adusumilli, X. Zou, and B. Ramamurthy, "Dgkd: Distributed group key distribution with authentication capability," in Proceed- ings of the Sixth Annual IEEE SMC Information Assurance Workshop. IEEE, 2005, pp. 286–293.
[21] M. Nabeel, M. Yoosuf, and E. Bertino, "Attribute based group key management," in Proceedings of the 14th ACM symposium on Access control models and technologies, 2014, pp. 115–124.
[22] B. Lynn, "The pairing-based cryptography library," Internet: crypto. stanford. edu/pbc/[Mar. 27, 2013], 2006.[23] Amazon Elastic Compute Cloud (Amazon EC2) Available:

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)