JCSE International Journal of Computer Sciences and Engineering Open Access

Review Paper Vol.-6, Issue-7, July 2018 E-ISSN: 2347-2693

A Survey on Cloud Computing Security and Data Integrity Auditing Schemes in Cloud Platform

L.Ramesh[1*], R.A.Roseline[2]

[1,2]Department of Computer Applications, Government Arts College, Coimbatore, India

Available online at: www.ijcseonline.org

Accepted: 03/Jul/2018, Published: 31/Jul/2018

***Abstract*-**Cloud computing is a comprehensive new approach on how processing administrations are created and used. Cloud computing is an achievement of different kinds of administrations which has pulled in numerous clients in the present situation. The most appealing administration of distributed computing is Information outsourcing, because of this the information proprietors can have any size of information on the cloud server and clients can get to the information from cloud server when required. The new model of information outsourcing likewise faces the new security challenges. However, clients may not completely believe the cloud specialist organizations (CSPs) in light of the fact that occasionally they may be untrustworthy. It is hard to decide if the CSPs meet the client's desires for information security. In this way, to effectively keep up the respectability of cloud information, numerous evaluating plans have been proposed. Some current trustworthiness strategies can serve for statically chronicled information and some inspecting methods can be utilized for the progressively refreshed information. In this paper, we have dissected different existing information uprightness evaluating plans alongside their results.

***Keywords*-**Third Party Auditor (TPA), Cloud Service Provider(CSPs), Information Outsourcing, Proof of Retrievability (POR), Provable Data Possession (PDP).

I. INTRODUCTION

Distributed computing is generally grasped by numerous organization and people on account of its different stun favorable circumstances like huze size information stockpiling, lumbering calculation, low price benefit and adaptable approach to get to the information [1], [14]. The essential idea driving distributed computing is virtualization. In distributed computing, virtualization intends to make a virtual variety of a gadget or asset, for example, a server, stockpiling gadget, organize or working framework where the structure separates the asset into required number of execution conditions [32]. Distributed computing is an overwhelming administration of distributed storage, which enables information proprietor to store their information from their neighborhood processing framework to cloud. Numerous clients store their information on distributed storage. However new convention of information facilitating administration additionally presents security issue [6]. Information proprietor would be stress that information could be lost in the cloud. In this manner, the greatest concern is the way to decide if a distributed storage framework and specialist organization meets the client desires for information security[20].Therefore, it is vital and huge to open up auditing scheme to fortify information owners′ confidence in cloud storage. Different sorts of inspecting models have been proposed, they can be ordered into two kinds Private Auditing model and Public Auditing Model. Generally in Private Auditing model information proprietor can confirm the trustworthiness of outsourced information in view of the two-party stockpiling auditing protocol. In this procedure information proprietor ought to have aptitude. It builds the overhead of information proprietor and some of the time it likewise happens the two information proprietor and CSP can't persuade each other for the outcome. As Public Auditing is the fitting model for outsourced information confirmation, it furthermore includes the outsider to check the uprightness [3], [5], [14] which can give impartial auditing result to the two information proprietor and CSP. Information proprietor send metadata to TPA rather than original information. Essentially, auditing model has two stages set up stage and verification stage. Information proprietor needs to play out a few operations preceding send information to TPA [5].

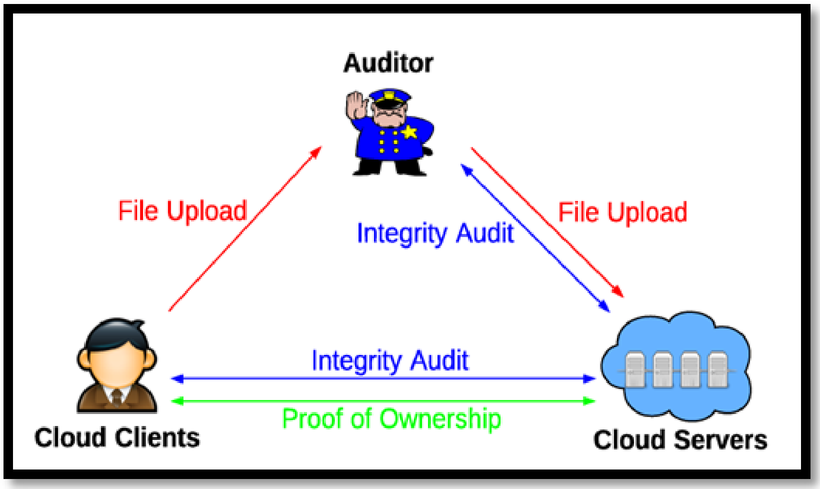

Fig 1 Cloud Computing Model

1.1 Challenges in Cloud Computing

As cloud provides many advantages but as every coin has 2 side, and cloud computing is no exception, it also has certain challenges. Every day, a fresh news item, latest publication, blog entry, highlights the cloud computing's challenges and issues. In each technology there are some security issues that affect the usage and the behavior below some of these concerns in the cloud: [2]

- Access: When there is an unauthorized access to the data, the ability of altering on the client data arise.
- Availability: The data must be available all the time for the clients without having problems that affect the storage and lead to the client data lose.
- Network Load: The over load capacity on the cloud may drop the system out according to the high amount of data between the computers and the servers.
- Integrity: The data correctness, legality and security is the most fields that influence on the cloud and have major lay on the service provider.
- Data Location: The client does not know the actual place that the data saved or centered in because it distributed over many places that led to confusion.

One of the important concerns in the cloud computing that need to be addressed is to assure the customer of the integrity, accordingly in the next section will discuss about data integrity.

1.2 Data Integrity

Integrity, in terms of data security, is nothing but the guarantee that data can only be accessed or modified by those authorized to do so, in simple word it is process of verifying data. Data Integrity is very important among the other cloud challenges
. As a result, data owners need to be convinced that their data are correctly stored in the Cloud. So, one of the biggest concerns with cloud data storage is that of data integrity verification at untrusted servers. In order to solve
the problem of data integrity checking, many researchers have proposed different systems and security models
. Rest of the paper is organizes as follows, Section I is contains Introduction of cloud computing ,Section II contains the related work of data integrity schemes, Section III contains Comparative study of the data integration scheme, Section IV Concludes research work and Section V describes future directions.

II. RELATED WORK

In Cloud computing the issue of data integrity is still done by numerous scientists. There is part of research as yet going ahead in this field to give secure and productive data integrity in distributed computing. Scientists have given numerous answers for center around settling the issues of data Integrity.

This area will endeavor to center around couple of such techniques .This paper give overview on the diverse strategies of data integrity and there limitations. The fundamental plans for data Integrity in cloud are Provable Data Possession (PDP) and Proof of retrievability (PoR). The accompanying area depicts the protection systems for data integrity.

This area will endeavor to center around couple of such techniques .This paper give overview on the diverse strategies of data integrity and there limitations. The fundamental plans for data Integrity in cloud are Provable Data Possession (PDP) and Proof of retrievability (PoR). The accompanying area depicts the protection systems for data integrity.

2.1 Proof of Retrievability (PoR):

Proof of Retrievability (POR) is a cryptographic technique for remotely checking the trustworthiness of records put away in the cloud, without keeping a duplicate of the client's unique documents in neighborhood stockpiling. In a plan, client reinforcements his information document together with some verification information to a possibly unscrupulous distributed storage server. Client can check the information for its trustworthiness put away with CSP utilizing the verification key, without recovering back the information record from cloud.

Limitations:

- It just works with static informational indexes.
- It underpins just a set number of questions as a test since it manages a limited number of check pieces.
- A POR does not give in counteractive action to the record put away on CSP.

2.2 Provable Data Possession (PDP)

Provable Data possession (PDP) is a technique for assuring data integrity over remote servers. In PDP A client that has stored data at an unfaithful server can verify that the server possesses the original data without retrieving it. Ateniese et al. are the first to consider public audit ability in their defined “provable data possession” model for ensuring possession of files on untrusted storages.

Limitations:

- Lack of error-correcting codes to address concerns of corruption.
- Lack of privacy preservation.
- No dynamic support.

In the contemporary year, distributed storage examining has pulled in thoughtfulness regarding reinforce information proprietors' trust and trust in distributed storage. To confirm the uprightness of outsourced information numerous conventions have been proposed with particular methods [4], [7], [8], [12], [15], [16], [18], [20], [21], [22], [26]. The principal reviewing related work was presented in 2007 by Juels et al. is POR (Proof of Retrievability) [4] plot, which can check the accuracy of information with the utilization of blunder rectifying code. It is ordinarily a private inspecting model on the grounds that there is no presence of some other outsider. Around the same time, Atenies et al. [16] has presented first open Auditing Model, PDP utilizing Homomorphic label in light of RSA. It doesn't bolster protection safeguarding of information. Alongside information uprightness evaluating there are numerous other noteworthy concerns, for example, security saving, bunch reviewing, and dynamic examining. In 2008, Atenies et al. [20] has additionally proposed the plan which underpins dynamic inspecting yet does not safeguard security.

In 2009 Erway et al. [12] proposed dynamic PDP plot that does not require security safeguarding. In 2010, First security saving PDP was presented by Wang et al. [6], they exhibited an open examining plan which guarantees the protection safeguarding for outsourced information utilizing coordinating Homomorphic authenticator with the arbitrary concealing system. In 2012 further, another open evaluating plan Cooperative PDP (CPDP) method proposed by Zhu et al [7], which depended on hash list progression and Homomorphic evident plan. It Supports open examining, Privacy safeguarding and Batch inspecting in the multi cloud however it has no arrangement for multi-client evaluating. Dynamic Auditing Protocol (DAP) in 2013, Yang et al. [15] proposed additionally upgraded inspecting plans which bolstered dynamic examining utilizing the Index table plan. In 2015, Identity-Based Distributed Provable Data Possession (ID-DPDP) plot was proposed by Wang, Huaqun [26] which utilized bilinear matching in irregular access display.

Dynamic Hash Table-Public Audit (DHT-PA) presented by Hui Tian et al. [14] in 2016 proposed Dynamic hash table which upheld open dynamic reviewing. Dynamic hash table backings open dynamic evaluating and utilized Homomorphic authenticator with arbitrary masking to protect the security of outsourced information. They utilized total BLS mark to organize bunch auditing.

PPOA scheme presented by Tengfei,Lurao et al.[33] in2017 proposed PPOA which is used the technique user focus outsourced auditing scheme. In 2017 certificate less public Auditing was proposed by Bayouvan Kang,Jiagiang wang et al. [34] which is used to maintain privacy preserving.Auditing for shared dynamic cloud data [35] in 2017 by used the technique Group Signature. Dynamic data operation technique presented by Santhosh Kumar and Latha Parthipan [36] in 2017 proposed 1^k,Dbase which is used to resistant against collusion.

III. COMPARITIVE STUDY

This Comparative examination gives a brief clarification of all the techniques that have been talk about so far in this paper.

Table 1: Comparison of existing data integrity auditing schemes

S.No	1	2	3	4	5	6
Weakness	Verification delay occurs	Communication cost is greater than DAP and IHT-PA	Does not support dynamic updates	High Computation Cost	Does not support Group user revocation	Heavy Computation Cost and Verification delay occurs
Strength	Bilinear pairings in random oracle model Flexible and improves the efficiency.	Support public auditing Privacy preserving Support dynamic Auditing Batch auditing in multi cloud	No need to fetch the data from cloud outsourced Auditing Setting	Protected from being directly exposed from auditor	Data confidentiality for small groups	Resistant against collusion attacks
Year	2014	2016	2017	2017	2017	2017
Proposed By	Wang, Huaqun	Hui Tian et al.	Tengfei et al	Baoyuvan Kang et al	Shubam sing et al	Santhishkumar and Latha Parthiban
Technique	Distributed Provable Data Possession in Multi-cloud storage.	Dynamic Hash table	User focus outsourced auditing scheme	Privacy Preserving	Public integrity auditing for shared dynamic in cloud data	1 ^{k},Dbase
Data Integration Scheme	ID-DPDP [26]	DHT-PA (Dynamic hash table- public audit) [14]	PPOA Scheme [33]	Certificateless Auditing [34]	Concrete Scheme [35]	Dynamic data operation(1^{k},Dbase)

IV CONCLUSION

In the realm of Cloud computing the data integrity is most testing and consuming security issue. By thinking about the significance of data integrity, in this paper distinctive existing paper methods and their benefits and demerits are clarified. The scientific examination quickly thinks about this methods. From this survey paper it is infer that there is need to plan design efficient, dynamic secure data integrity technique which is still wide area of research.[2], [20], [32].

V FUTURE SCOPE

From the above comparative study it is clear that all these techniques which are surveyed in this paper have some advantages as well as some limitation. All those papers were lack in proper data integrity mechanisms, supporting dynamic data operations, and by high resource and computation cost The technique Dynamic data Operation Data Blocks is best suited for thin client as well as this technique provides the strong proof of retrievability. The only drawback of this technique is delay in verification process. So expanding the scope of this paper will be the future work.

REFERENCES

[1] P. Melland, T. Grance, “The NIST Definition of Cloud Computing, technical report”, Nat’l Inst. of Standards and Technology, 2009.

[2] Nandini J., Sugapriya N. P., M. S. Vinmathi, “SecureMulti-Owner Data Storage with Enhanced TPA Auditing Scheme in Cloud Computing”, InternationalJournal of Advances in Computer Science and Cloud Computing, ISSN: 2321-4058, Vol. 2, Issue: 1, MAY 2014.

[3] C. Wang, S. M. Chow, Q. Wang, K. Ren and W. Lou, ″Privacy-Preserving Public Auditing for Secure Cloud Storage, ″ vol. 62, IEEE Trans. on Computers, no. 2, pp. 362-375, 2013.

[4] A. Juels and B.S. Kaliski Jr., “PoRs: Proofs of Retrievability for Large Files,” Proc. ACM Conf. Computer and Communications Security (CCS ’07), pp. 584-597, 2007.

[5] Deepak Kumar Verma, Purnima and Rajesh Kumar Tyagi, “Optimizing the User Side Set-up Phase for Privacy Preserving Public Auditing in Cloud Storage”, (manuscript submitted for publication), 2017.

[6] K. Yang and X. Jia, “An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing”, vol. 24, IEEE Trans. on Parallel and Distributed Systems, no. 9, pp.1717-1726, ISSN: 2278 – 1323, 2013.

[7] C. Wang, Q. Wang, K. Ren and W. Lou, “Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing”, Proc. IEEE INFOCOM,pp1-9, 2010.

[8] Y. Zhu, H. Hu, G. Ahn, and M. Yu, “CooperativeProvable Data Possession for Integrity Verification in Multi-Cloud Storage”, vol. 23, IEEE Trans. Parallel and Distributed Systems, no. 12, pp. 2231-2244, 2012.

[9] J. Ryoo, S. Rizvi, W. Aiken and J. Kissell, ″CloudSecurity Auditing: Challenges and Emerging Approaches″, IEEE Security & Privacy, vol. 12, no. 6,pp.68-74, 2014.

[10] M. S. Giri, B. Gaur, D. Tomar, “A Survey on Data Integrity Techniques in Cloud Computing”, Vol. 122, No. 2, International Journal of Computer Applications (0975 – 8887), July 2015.

[11] K. Shinde, V. V. Jog, “A Survey on Integrity Checking for Outsourced Data in Cloud using TPA”, International Journal of Computer Applications (0975 – 8887), International Conference on Internet of Things, Next Generation Networks and Cloud Computing, 2016.

[12] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, “Dynamic Provable Data Possession”, proc. ACM Conf. Computer and Comm. Security (CCS’09), pp.213-222, 2009.

[13] Sumalatha M.R., Hemalathaa S., Monika R., Ahila C., “Towards Secure Audit Services for Outsourced Data in Cloud”, International Conference on Recent Trends inInformation Technology IEEE, 2014.

[14] H. Tian, Y. Chen, C. Chang, “Dynamic-Hash-Table Based Public Auditing for Secure Cloud Storage”, Vol. PP, Issue: 99, IEEE Transactions on Service Computing, Manuscript ID, DEC 2016.

[15] CH. Mutyalanna, P. Srinivasulu, M. Kiran, “Dynamic Audit Service Outsourcing for Data Integrity in Clouds”, Vol. 2 Issue 8, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), AUG 2013.

[16] G. Ateniese, R. B. Johns, R. Curtmola, J. Herring, L.Kissner, Z. Peterson and D. Song, ‘‘Provable Data Possession at Untrusted Stores,’’ Proc. 14th ACM Conf. on Comput. and Commun. Security (CCS), pp. 598-609, 2007.

[17] Mr. Pragnash G. Patel and Sanjay M. Shah, “Survey on data security in cloud computing”, Vol 1, Issue 9, International Journal of Engg Research and Tech (IJERT), ISSN: 2278-0181, NOV 2012.

[18] Zhu, H. Wang, Z. Hu, G. J. Ahn, H. Hu and S. S.Yau, “Dynamic Audit Services for Outsourced Storage in Clouds”, Vol. 6, no. 2, IEEE Trans. on Services Computing, pp. 227–238, 2013.

[19] Q. Wang, C. Wang, K. Ren, W. Lou and J. Li,‘‘Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing’’, Vol. 22, no. 5, IEEE Trans. on Parallel and Distributed Systems, pp. 847-859, 2011.

[20] A P Shirahatti, P S Khanagoudar, “Preserving Integrity of Data and Public Auditing for Data Storage Security in Cloud Computing”, IMACST, Vol. 3, Number 3,JUN 2012.

. [21] H. Shacham and B. Waters, “Compact Proofs of Retrievability”, vol. 5350, Proc. Int’l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (Asiacrypt), pp. 90-107, DEC 2008.

[22] Syed Rizvi, Katie and Abdul, “Cloud Data Integrity Using a Designated Public Verifier,” in 2015 IEEE 17th International Conference on High Performance Computing and Communications (HPCC), International Symposium on Cyberspace Safety and Security (CSS) and International Conference on Embedded Software and System (ICESS).

[23] S Lins, S Schneider, and A Sunyaev, “Trust is Good,Control is Better: Creating Secure Clouds by Continuous Auditing”, Vol. PP, Issue: 99 IEEE Transactions on Cloud Computing, TCC-2015-10-0378, JAN 2016.

[24] A Kushanpalli, V. S. Kumar, C. R. Yadav, “ASimulation Study of Outsourcing of Audit Service for Data Integrity in Cloud Computing”, Vol. 3, Issue 11,ISSN (Print): 2319-5940, International Journal of Advanced Research in Computer and Communication Engineering, NOV 2014.

[25] D. N. Rewadkar, S. Y. Ghatage, “Cloud Storage System Enabling Secure Privacy Preserving Third Party Audit”, International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), JUL 2014.

[26] Wang, Huaqun. "Identity-Based Distributed Provable Data Possession in Multicloud Storage", Services Computing, IEEE Transactions on 8.2 (2015): 328-340.

[27] S. Pearson, "Toward Accountability in the Cloud", Vol. 15, no. 4, IEEE Internet Computing, pp. 64–69, 2011.

[28] Cloud Security Alliance,”Top Threats to CloudComputing”,http://www.cloudsecurityalliance.org, 2010.

[29] C. Wang, K. Ren, W. Lou, and J. Li, “Towards Publicly Auditable Secure Cloud Data Storage Services”, Vol. 24, no. 4, IEEE Network Magazine, pp. 19-24, July/Aug. 2010

[30] S. N. Poornima, R. S. Ponmagal, “Secure PreservingPublic Auditing for Regenerating Code Based On Cloud Storage”, International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) ISSN: 0976-1353, Vol. 21, Issue: 4, APR 2016.

[31] K. Chen, J. M. Chang, T. Hou, “Multithreading in Java: Performance and Scalability on Multicore Systems”, Vol. 60, IEEE Transactions on Computers, NO. 11, NOV 2011.

[32] N. Saravana Kumar, G.V. Rajya Lakshmi, BBalamurugan,” Enhanced Attribute Based Encryption for Cloud Computing”, Vol. 46, pp 689-696, 2015.

[33] Tengfei Tu, Lu Rao, Hua Zhang, Qiaoyan Wen, and Jia Xiao “Privacy-Preserving Outsourced Auditing Scheme forDynamic Data Storage in Cloud” Security and Communication Networks Volume 2017, Article ID 4603237, 17 pages

[34] Baoyuan Kang, Jiaqiang Wang, and Dongyang Shao “Certificateless Public Auditing with Privacy Preserving forCloud-Assisted Wireless Body Area Networks” Hindawi,Mobile Information Systems Volume 2017, Article ID 2925465, 5 pages

[35] Shubham Singha, Surmila Thokchomb “ Public integrity auditing for shared dynamic cloud data ” 6th International Conference on Smart Computing and Communications, ICSCC 2017, 7-8 December 2017, Kurukshetra, India.

[36] Santhosh Kumar, Latha Parthiban “ Cloud Data Integrity Auditing Over Dynamic Data for Multiple Users” International Journal of Intelligent Engineering and Systems, Vol.10, No.5, 2017,pp.23