RESEARCH ARTICLE OPEN ACCESS

A Survey on Data Integrity Auditing Schemes in Cloud Computing

Purnima [1], Deepak Kumar Verma [2]
Student of MTech. [1]
Computer Science Department [2]
IEC College of Engineering and Technology, Greater Noida
Uttar Pradesh, India.

ABSTRACT
Cloud computing is an inclusive new approach on how computing services are produced and utilized. Cloud computing is an accomplishment of various types of services which has attracted many users in today's scenario. The most attractive service of cloud computing is Data outsourcing, due to this the data owners can host any size of data on the cloud server and users can access the data from cloud server when required. The new prototype of data outsourcing also faces the new security challenges. However, users may not fully trust the cloud service providers (CSPs) because sometimes they might be dishonest. It is difficult to determine whether the CSPs meet the customer's expectations for data security. Therefore, to successfully maintain the integrity of cloud data, many auditing schemes have been proposed. Some existing integrity methods can only serve for statically archived data and some auditing techniques can be used for the dynamically updated data. In this paper, we have analyzed various existing data integrity auditing schemes along with their consequences.
Keywords :— Third Party Auditor (TPA), Cloud Service Providers (CSPs), Data Outsourcing, Proof of Retrievability (POR), Provable data Possession (PDP).

I. INTRODUCTION

Cloud computing is widely embraced by many organization and individuals because of its various dazzle advantages like huge size data storage, cumbersome computation, low price service and flexible way to access the data [1], [14]. The basic concept behind cloud computing is virtualization. In cloud computing, virtualization means to create a virtual variation of a device or resource, such as a server, storage device, network or operating system where the structure divides the resource into required number of execution environments [32]. Cloud computing is a predominant service of cloud storage, which allows data owner to store their data from their local computing system to cloud. Many users store their data on cloud storage. However new protocol of data hosting service also introduces security issue [6]. Data owner would be worry that data could be lost in the cloud. Therefore, the biggest concern is how to determine whether a cloud storage system and service provider meet the customer expectations for data security [20]. Therefore, it is crucial and significant to amplify efficient auditing scheme to strengthen data owners′ faith in cloud storage. Various types of auditing models have been proposed, they can be categorized into two types Private auditing model and Public Auditing Model. Traditionally in Private auditing model data owner can verify the integrity of outsourced data based on the two-party storage auditing protocol. In this technique data owner should have expertise. It increases the overhead of data owner and sometimes it also happens both data owner and CSP cannot convince each other for the result.

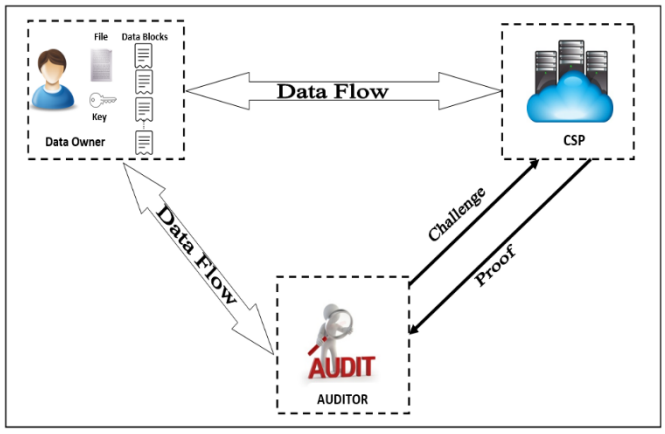

Figure 1. Cloud Auditing Model.

As public auditing is the advisable model for outsourced data verification, it additionally involves the third party to check the integrity [3], [5], [14] which can provide equitable auditing result for both data owner and CSP. Data owner send metadata to TPA instead of original data. Basically, auditing model has two phases set up phase and verification

phase. Data owner has to perform some operations prior to send data to TPA [5].

II. RELATED WORK

In the contemporary year, cloud storage auditing has attracted attention to strengthen data owners' trust and confidence in cloud storage. To verify the integrity of outsourced data many protocols have been proposed with distinct techniques [4], [7], [8], [12], [15], [16], [18], [20], [21], [22], [26]. The first auditing related work was introduced in 2007 by Juels et al. is POR (Proof of Retrievability) [4] scheme, which can check the correctness of data with the use of error correcting code. It is typically a private auditing model because there is no existence of any other third party. In the same year, Atenies et al. [16] has introduced first public Auditing Model, PDP using Homomorphic tag based on RSA. It does not support privacy preserving of data. Beside data integrity auditing there are many other significant concerns such as privacy-preserving, batch auditing, and dynamic auditing. In 2008, Atenies et al. [20] has further proposed the scheme which supports dynamic auditing but does not preserve privacy.

In 2009 Erway et al. [12] proposed dynamic PDP scheme that does not require privacy preserving. In 2010, First privacy preserving PDP was introduced by Wang et al. [6], they presented a public auditing scheme which ensures the privacy preserving for outsourced data using integrating Homomorphic authenticator with the random masking technique. In 2012 further, a new public auditing scheme Cooperative PDP (CPDP) technique proposed by Zhu et al [7], which was based on hash index hierarchy and Homomorphic verifiable scheme. It Supports public auditing, Privacy preserving and Batch auditing in the multi cloud but it has no provision for multi-user auditing. Dynamic Auditing Protocol (DAP)in 2013, Yang et al. [15] proposed further enhanced auditing schemes which supported dynamic auditing using the Index table scheme. In 2015, Identity-Based Distributed Provable Data Possession (ID-DPDP) scheme was proposed by Wang, Huaqun [26] which used bilinear pairing in random access model.

Dynamic Hash Table-Public Audit (DHT-PA) introduced by Hui Tian et al. [14] in 2016 proposed Dynamic hash table which supported public dynamic auditing. Dynamic hash table supports public dynamic auditing and employed Homomorphic authenticator with random masking to preserve the privacy of outsourced data. They used aggregate BLS signature to arrange batch auditing.

III. LITERATURE SURVEY

Data Integration Scheme	Technique	Proposed By	Year	Strength	Weakness
POR (Proof of Retrievability) [4]	Using error correcting code	Juels et al.	2007	• Private Auditing using error code • Data recovery is possible	• Increase overhead on Data Owner. • Cannot be used in the original form, preprocessing is required for encoding.
PDP (provable data possession) [16]	Use Homomorphic tag based on RSA	Atenies et al.	2007	• Support public auditing	• Not Privacy preserving • No Batch auditing • Communication overhead • Data recovery is not supported
Partially Dynamic – PDP [20]	Symmetric Key Cryptography	Atenies et al.	2008	• Supports Dynamic Auditing	• No Privacy preserving • Bounded no of

					Audits.
CPR (Compact Proof of Retrievability) [21]	HLA Built from secure BLS-Signature	H. Shacham, B. Waters	2008	• Improved POR scheme	• No Privacy preserving
DPDP (Dynamic PDP) [12]	Using ranked based authenticated skip list	Erway et al.	2009	• Dynamic data auditing • No demand of privacy-preserving	• No public auditing • Not support Batch auditing • Not Privacy preserving
PDP First privacy preserving [7]	Integrating the Homomorphic authenticator with random masking	Wang et al.	2010	• Supports public auditing • Privacy preserving	• Does not support data dynamics
Fully Dynamic PDP [22]	Combined BLS based HLA with MHT	Wang et al.	2011	• Supports Dynamic Auditing	• Not Privacy preserving
CPDP (corporative provable possession) [8]	Hash Index Hierarchy	Zhu et al.	2012	• Support public auditing • Privacy preserving • Batch auditing in multi cloud	• It does not support dynamic audit • Does not support auditing for multiuser
DAP [15]	Index table	Kan Yang et al.	2013	• Support public auditing • Privacy preserving • Support dynamic auditing • Batch auditing in multi-cloud	• High Computation cost
DPDP-MHT [19]	Based on Merkle hash tree	Wang et al.	2013	• Support public auditing • Privacy preserving • Support dynamic auditing • Batch auditing in multi-cloud	• Heavy computation cost of the TPA • Large communication overhead
IHT-PA (Index hash table-public audit) [18]	Index Hash table	Zhu et al.	2013	• Support public auditing • Privacy preserving • Support dynamic auditing	• Batch auditing is not mentioned

MUR-DPA [2]	Used Authenticated Data Structure (ADS) based on the Merkle Hash Tree (MHT)	Liu, Chang, et al.	2014	• Provides facility to verify cloud data storage with multiple replicas.	• Works only with constant-sized integrity proofs
ID-DPDP [26]	Distributed Provable Data Possession in Multi-cloud storage.	Wang, Huaqun	2015	• Bilinear pairings in random oracle model Flexible and improves the efficiency.	• Verification delay occurs
DHT-PA (Dynamic hash table-public audit) [14]	Dynamic Hash table	Hui Tian et al.	2016	• Support public auditing • Privacy preserving • Support dynamic auditing • Batch auditing in multi cloud	• Communication cost is greater than DAP and IHT-PA

Table 1: Comparison of existing data integrity auditing schemes [5]

IV. CONCLUSION

In cloud computing, a new paradigm of data outsourcing increases new security challenges. This new paradigm requires a Third-Party Auditor to check the data integrity in cloud storage. In this paper, we have compared different types of auditing schemes on the basis of Privacy preservation, dynamic auditing and batch auditing along with their strength and weakness. From all these papers, it is concluded that there is need to design some optimizing techniques that can be applied to speed up the set phase at data owner side [2], [20], [32]. In our previous paper, we have proposed a multithreading model on multi-core CPU system to generate the signature for each block [5], it is one-time operation and occurs in setup phase at data owner side.

V. FUTURE WORK

In future, we will focus on enhanced & sophisticated data setup process to reduce the computation and communication overhead at data owner side. To generate authenticator, we use multithreading framework on latest multi-core system to speed up the setup phase. We will use the multithreading model in each step of data setup phase.

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, "Secure Multi-Owner Data Storage with Enhanced TPA Auditing Scheme in Cloud Computing", International Journal 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, pp. 1-9, 2010.

[8] Y. Zhu, H. Hu, G. Ahn, and M. Yu, "Cooperative Provable 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, ″Cloud Security 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.

[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.

[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 in Information 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.

. [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, "A Simulation 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 Cloud Computing", 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 Preserving Public 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, B Balamurugan," Enhanced Attribute Based Encryption for Cloud Computing", Vol. 46, pp 689-696, 2015.