"Review On Security Analysis Of Cloud Computing Data"

Javed Akhtar Khan[1], Dr.MR Aloney[2]
[1, 2] Dept of Computer Science & Engineering
[1, 2] Bhagwant University Ajmer (India)

Abstract- *In this review article we are include the formal introduction part of cloud computing technology along with its security related issue. Every data in this digital era is very important, so security of these data is also very important . In this era maximum techno person are using cloud platform for develop the new application , software, software , App application so many more. These new technologies we are using regularly etc . So these all about directly related with the security of data or information ,in this paper we are make proper analysis of some existing security of cloud data.*

Keywords- Cloud computing , Cloud server, Cloud model, Cloud storage.

I. INTRODUCTION

Cloud computing is one of the latest developments in IT industry also known as on-demand computing. Computing is being transformed into a model consisting of services that are commoditized and delivered in a manner similar to utilities such as water, electricity, gas, and telephony. In such a model, users access services based on their requirements, regardless of where the services are hosted. It provides the full scalability, reliability, high performance and relatively low cost feasible solution as compared to dedicated infrastructures. It is the application provided in the form of service over the internet and system hardware in the data centers that gives these services. Cloud computing is the most recent emerging paradigm promising to turn the vision of "computing utilities" into a reality. Cloud computing is attach no logical advancement that focuses on the way we design computing systems, develop applications, and leverage existing services for building software. When you store your data some information digital or e- data like photos online instead of on your home computer, or use webmail or a social networking site, you are using a "cloud computing" service. If you are an organization, and you want to use, for example, an online invoicing service instead of updating the in-house one you have been using for many years, that online invoicing service is a "cloud computing" service. National Institute of Standards and Technology (NIST) is produce the formal definition of cloud computing .Characteristics of cloud Computing The characteristics of cloud computing include on-demand self service, Broad network access, Resource pooling, Rapid elasticity and Measured service. On-demand self service means that customers (usually organizations) can request and manage their own computing resources. Broad network access allows services to be offered over the Internet or private networks. Pooled resources means that customers draw from a pool of computing resources, usually in remote data centers. Services can be scaled larger or smaller; and use of a service is measured and customers are billed accordingly.Service models The cloud computing service models are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).Deployment of cloud services: Cloud services are typically made available via a private cloud, community cloud, public cloud or hybrid cloud.Cloud services are popular because they can reduce the cost and complexity of owning and operating computers and networks. This section is include the basic infroamtion about the clodu computing along with cloud characterstics service model and deployment cloud services .

II. REVIEW AND ANALYSIS OF CLOUD COMPUTING SECURITY SOLUTION

[Ref-1] This paper introduce the basic definition of cloud, author are also introduce many challenges related to cloud and security and integrity threats toward user' outsourced data, in this paper author proposed protocol achieves full stateless and transparent verification, for this work author are constructing a sequence-enforced Merkle Hash Tree Technique .in this paper author are introduce the batch auditing task using the bilinear map method .In this paper, researcher develop an efficient auditing mechanism, which support batch au-diting for multiple data files in multi-cloud environment. By utilizing the bilinear map, the proposed protocol can aggregate the verification task from different users to re-duce the computing overhead of the auditor. By constructing a sequence-enforced Merkle Hash Tree, the proposed protocol can resist the replace attack. In addition, our protocol protects the position information of the data blocks by generating fake data blocks to confuse the organizer, so as to achieve full stateless and transparent verification.

[Ref-2] Ateniese, G. et al.In order to address the issue above, various Provable Data Possession (PDP) pro-tocols have been proposed. PDP is a probabilistic proof technique for checking the availability and integrity of outsourced data with randomly sampling a few file blocks. In this paper author are introduce the PDP model with public verification , for this author are introduce the RSA based Homorphic linear authentication HLA and suggested random-ly sampling method . Ateniese etal. propose a partially dynamic version of the prior PDP scheme that uses only symmetric key cryptography. This mechanism can support update and delete operations on data, however, insert operations are not available in this mechanism. Because it exploits symmetric keys to verify the integrity of data, it is not public verifiable and only provides a user with a limited number of verification requests.

[Ref- 3]Wang et al. also proposed a dynamics PDP scheme based on combining Boneh–Lynn–Shacham signa-ture (BLS)-based HLA with Merkle Hash Tree (MHT) structure .

[Ref- 4] Erway et al. presented a skip list-based dynamics PDP model with fully data dynamic operation. The scheme supports both the public stateless verification and fully dynamic data update. developed a skip lists based scheme to enable provable data control with fully dynamics support. However, all their protocol requires the linear combination of sampled blocks just as, and thus does not support privacy preserving auditing on users outsourced data.

[Ref -5] Juels and Kaliski describe a proofs of irretrievability (POR) model, which not only can verify data possession but also ensure retrieve ability of raw data files when abnormality is detected. Although they describe a straight forward Merkle-tree construction for public PoRs, this approach only works with encrypted data. The first scheme is built from BLS signatures, and the second one is based on pseudorandom functions.

[Ref -6] In this paper author are introduce the Privacy preserving between cloud and TPA has to be addressed to avoid the data leakages, for this work author are used the advanced encryption standards(AES) encryption algorithm instead of RSA, to increase the efficiency and security. To speed up the auditing by TPA batch auditing scheme is introduced, which has the ability to audit the files batch wise. In this paper author also make secure roll of TPA . for this work author are used the Genproof algorithm is run on the cloud server to check the data storage correctness in the cloud, and for auditing the proof TPA uses to audit the proof. Algorithms for preserving privacy between the user and the cloud. Homomorphism Linear Authenticator (HLA) With random masking technique is used. This technique guarantee that during auditing process TPA will not demand for the local copy of data and will not be able to learn any knowledge about the data.

[Ref -7] Recently, Franz et al. proposed an oblivious out source storage scheme based on Oblivious RAM techniques, which is able to hide users' access patterns on outsourced data from an un trusted cloud.

[Ref – 8] [Ref -9]To prevent special attacks exist in remote data storage system with de duplication, Halevi et al[8]. Introduced the notation of proofs-of-ownership (POWs), which allows a client to prove to a server that she actually holds a data file, rather than just some hash values of the data file. Zheng et al.[9] further discussed that POW andPDP can co-exist under the same framework.

[Ref- 10] Chenet al.also introduced a mechanism for auditing the correctness of data with the multi-server scenario, where these data are encoded by network coding instead of using erasure codes.

III. CONCLUSION

Most of the above PDP schemes mainly address integrity verification issues at a single CSP. As a more feasible application scenario, users may store their data in multi cloud with a distributed manner to reduce the threats of data integrity and availability . In this scenario, multi cloud is composed of multiple private or public clouds. Each CSP has a different level of quality of service as well as a different cost associated with it. Hence, the users can store their data files on more than one CSP according to the required level of security and their affordable budgets. Within multi cloud, an organization can offer and manage in-house and out-house resources .

Comparative Analysis Table

Reference	Integrity Task	Batch Auditing	Auditing Task	Data Block	Single Cloud	Multiple Cloud	TPA Authentication	User registration	Key generation Algorithm used for the TPA	Cloud Type	Methodology used /Technique used	Result Summary
Ref-1	NO	Yes	Single	Yes	NO	Yes	NO	yes	1.Two hash functions 2. signature function	Private	1.Merkle Hash Tree Technique 2. Bilinear map method	-No TPA Authentication - only applicable for the Private cloud
Ref-2	Yes	NO	Single	NO	Yes	NO	NO	yes	1-RSA based Homographic linear authentication HLA 2- suggested random-by sampling method	Private	probabilistic proof technique symmetric key cryptography	-No Batch Auditing Task - No data block fragmentation - Un trusted TPA -only for the private cloud
Ref-3	Yes	NO	Multip le	yes	yes	No	NO	NO	classic Merkle Hash Tree	Private	Boneh–Lynn–Shacham signature (BLS)-based HLA with Merkle Hash Tree (MHT) structure	-Un trusted TPA -NO user Authentication at on cloud or TPA verification -only for private cloud
Ref-4	Yes	NO	Single	Yes	Yes	NO	NO	NO	authenticated dictionaries based on rank information.	Un trusted server	skip list-based dynamics PDP model	-single auditing task that increases auditing time -un trusted
Ref-5	Yes	NO	Single	NO	Yes	NO	NO	yes	1-pseudorandom functions 2-BLS signatures	semi-trusted	proofs of irretrievability (POR) model Merkle-tree construction for	-single auditing task same issue mention ref 4 -semi trusted cloud

											public PoRs	
Ref-6	NO	NO	Single	NO	NO	NO	NO	NO	1-advanced encryption standards(AES) encryption algorithm	Un trusted	Genproof algorithm Homomorphic Linear Authenticator (HLA) With randaom masking technique	-No data integrity - No auditing task -applicable for single cloud -un trusted
Ref-7	yes	yes	single	NO	NO	Yes	NO	NO	RSA	Un trusted cloud	Oblivious RAM techniques	-data integrity -single cloud -RSA used
Ref-8 Ref-9	Yes	yes	Single	NO	NO	yes	NO	NO	1-Hash values	hash signatures 2-Merkle trees and specific encodings,	proofs-of-ownership (POWs),	-data integrity -single server auditing -Hash values is used -optimize the auditing up to 17 % in some parameter
Ref-10	Yes	NO	Multiple	NO	NO	Yes	NO	NO	KEYGEN algorithm	the multi-server POSD scheme	encoded by network coding	-auditing task for multi data block in the multiple cloud

REFERENCES

[1] Ref[1]-Advanced Science and Technology Letters Vol.50 (CST 2014), pp.67-73 http://dx.doi.org/10.14257/astl.2014.50.11 Batch Auditing for Multiclient Data in Multicloud Storage Author Zhihua Xia, Xinhui Wang, et .al.

[2] Ref[2]- Ateniese, G. et al.: Provable data possession at untrusted stores. Proceedings of the 14th ACM conference on Computer and communications security, 2007, pp. 598-609.

[3] Ref[3] - Wang, Q. et al.: Enabling public auditability and data dynamics for storage security in cloud computing. Parallel and Distributed Systems, IEEE Transactions on, vol. 22, pp. 847-859, 2011.

[4] Ref[4]- Erway, C. et al.: Dynamic provable data possession. Proceedings of the 16th ACM conference on Computer and communications security, 2009, pp. 213-222.

[5] Ref[5]- A. Juels and B. S. Kaliski Jr.: PORs: Proofs of retrievability for large files," in Proceedings of the 14th ACM conference on Computer and communications security, 2007, pp. 584-597

[6] Ref[6]- PRIVACY PRESERVING AND BATCH AUDITING IN SECURE CLOUD DATA STORAGE USING AES
1SANTOSH P. JADHAV, 2B. R. NANDWALKAR

[7] Ref[7]- M. Franz, P. Williams, B. Carbunar, S. Katzenbeisser, and R. Sion, “Oblivious Outsourced Storage with Delegation,” in Proc. Finan-cial Cryptography and Data Security Conference (FC), 2011, pp. 127– 140.

[8] Ref[8]-S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg, “Proofs of Ownership in Remote Storage Systems,” in Proc. ACM Conference on Computer and Communications Security (CCS), 2011, pp. 491–500.

[9] Ref[9]-Q. Zheng and S. Xu, “Secure and Efficient Proof of Storage with Deduplication,” in Proc. ACM Conference on Data and Application Security and Privacy (CODASPY), 2012.

[10] Ref[10]-B. Chen, R. Curtmola, G. Ateniese, and R. Burns, “Remote DataChecking for Network Coding-based Distributed Stroage Systems,”in Proc. ACM Cloud Computing Security Workshop (CCSW),2010, pp. 31–42.