ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.5

Privacy Preserving Auditing for Secure Cloud Storage

Lakshay Seth[1], Kirti Barthwal[2], Archana Sar[3], Abhishek Pokhriyal[4], Nitika Aggarwal[5]
B.Tech Student[1, 2, 4, 5], HOD[3]
Department of Computer Science and Engineering
Mahatma Gandhi Missions College of Engineering and Technology, Uttar Pradesh, India

Abstract:
Cloud computing has been anticipated as the next generation computing utility. It involves data outsourcing so as to exempt its user from the burden of physical storage and its upkeep. In cloud environment, the computing resources are under the control of service provider, the TPA ensures the data integrity over outsourced data. Here, we analyze about public key based homomorphic authenticator with random masking technique to achieve privacy preserving public auditing wherein it ensures that the Cloud Server would not acquire any knowledge about the data content stashed away in the cloud. For effective auditing process, we dig into technique of bilinear aggregate signature to extend our main result. The TPA not just eliminates the burden of Cloud User from monitoring and possible expensive auditing task but also alleviate the users' fear of outsourced data leakage.

Keywords: Cloud Computing, TPA, Homomorphic based authenticator

I. INTRODUCTION

Cloud Computing has increasingly grown in recent years due to the advantages of greater flexibility and availability of computing resources at lower cost. Security and Privacy are a concern for agencies and organizations considering migrating applications to public cloud computing environment. Cloud Computing has been envisioned as the next generation architecture of IT enterprise due to its long list of extensive advantages like on demand self service, ubiquitous network access. Our fundamental aspect of this paradigm is that data is being centralized or outsourced into the cloud. The Correctness of data is always at risk due to data integrity, hiding data or discarding data. It is one of the major security issues as it does not offer any guarantee on data integrity and availability. To efficiently verify the correctness of outsourced data without local copy of data becomes a big challenge for data storage security. Therefore, the only solution for this is to enable public audit-ability for cloud data storage so that the users may contact to a TPA who has the capability to audit the outsourced data, then the TPA generates audit report which would not only help users but also for cloud service provider to improve its platform.

CLOUD COMPUTING SERVICE MODELS

Three architectural models and the derivative combinations thereof generally describe cloud service delivery. The three individual models are often referred to as the "SPI MODEL", where "SPI" denotes to Software, Platform and Infrastructure (as a service) respectively.

SaaS (Software as a Service Model)
In the SaaS model, the user buys a subscription to some software product, but some or all of the data and code resides remotely and customers can access to this services via internet. In this model, applications could run entirely on the network, with the user interface inhabiting on a thin client. With SaaS, users must rely upon heavily on their cloud providers for security. Degree of control by providers is high and they are accountable for confidentiality, integrity and availability of their services.

PaaS (Platform as a Service Model)
This model provides the user to deploy user-built applications on the cloud infrastructure that are reinforced using programming languages and software tools hold up by the provider (e.g., Java, python, .Net). PaaS adds all the resources essential to set-up applications and services entirely from the Internet, without having to download or install software. That is, if you make an application with one cloud provider and decide to move to another provider, you may not be able to do so or you'll have to bear a soaring price. Also, if the provider goes out of business, your applications and your data will be forfeited. Degree of control by providers is moderate and they are only accountable for integrity and availability of their services. But users' responsibility is moderate and they are responsible of confidentiality and data privacy.

IaaS *(*Infrastructure as a Service Model)
IaaS model lets the development organization define its own software environment. Where SaaS and PaaS provides applications to customers, IaaS doesn't do it. It simply offers the hardware so that your organization can put whatsoever they want onto it. This basically bears virtual machine images to the IaaS provider, instead of programs, and the machines can contain whatever the developers require. Degree of control by providers is reduced and they are only liable for availability of their services. But users' responsibility is of utmost importance and they are accountable of confidentiality, data privacy and integrity. Most of the existing schemes like Proof of Possession and proof of Retrieve- ability do not consider privacy-preserving problem. Here, we talk you through the privacy of cloud server which ensures privacy from cloud server by using technique bilinear aggregate signature. The rest of the paper includes Literature Survey, which describes the existing work in

this field; most commonly used approaches as Existing System, for privacy- preserving auditing.

II. LITERATURE SURVEY

In Cloud Environment, Data Storage Security is of critical importance. The Cloud User stores bulk of data to the cloud. Any Possible leakage or forge- ability of user's outsourced data should be prohibited. TPA, on the behalf of the cloud user audits the data storage without demanding the local copy. Cong Wang [2] has proposed a privacy preserving public auditing protocol wherein an Independent TPA audits the outsourced data to check its integrity. IT achieves the auditing task by uniquely combining the public key based homomorphism authenticator with random masking. This protocol is vulnerable to existential forgeries known as message attack. To overcome this problem Wang C' et al. [3] uses Bonen-Lynn-Shacham (BLS) algorithm that utilizes technique of bilinear aggregate signature to achieve batch auditing. Wang et al. [9] proposed a privacy preserving public auditing scheme which causes the use of an independent TPA to audit the data. It utilizes the public key based homomorphic linear authenticator (HLA) with random masking techniques. But this protocol is sensitive to existential forgeries known as message attack from a malicious cloud server and an outside attacker. To overcome this problem, Wang et al. [6] proposed a new improved scheme which is more secure than the protocol proposed by G. Vidhisha et al. [9]. It is a public auditing design with TPA, which comply data auditing on behalf of users. It uses HLA which is constructed from Boneh-Lynn-Shacham short signature referred as BLS signatures. It also uses random masking for data hiding. As a result of data binding, this new design involves computationally intensive pairing operation thus making it inefficient to use. Cong Wang et al. [4] takes the challenges of minimizing auditing overhead, protect data privacy. Support data dynamics, and batch auditing. For reducing Communication overhead it resort to homomorphic authenticator. It requires additional information encoded along with the data before outsourcing. Manipulating data encryption before outsourcing is one way to diminish this privacy concern.
Kevin D. Bowers et al. [7] proposed two solutions with similar structure. The First one is privately Verifiable and builds on pseudorandom functions. The Second allows for publicly verifiable proofs and is built from signature Scheme of BLS algorithm in bilinear groups. Both solutions rely on homomorphic properties to aggregate a proof into one small authenticator value. Jachak K.B.* et al. [12] proposed a scheme of signing data block before sending it to the cloud for ensuring correctness of data and security. It is performed using BLS algorithm. TPA audits the outsourced data on user's behalf. It uses Public Key based homomorphic authenticator with random masking. To reduce Computation overhead batch auditing technique is utilized. For this purpose technology of bilinear aggregate signature is used. G. Ateniese et al. [6] achieves public adaptability in proving data possession on untrusted cloud servers. Linear Combination of blocks is used for verification using RSA based homonorphic Authenticator. To reduce Computation overhead it uses random sampling of outsourced data to ensure integrity. Abhishek Mohta* et al. [11] uses encryption technique which sending data in the cloud and at the time of retrieval, it ensures zero leakage of data during transfer. It also uses message usage to mark identity of sender outsourcing data in the cloud. H. Shacham et al. [5] uses public key based on homomorphic authenticator with random masking technology and achieve batch auditing using bilinear. It also uses keys hash function in proofs of retrieve- ability to different values of keys, different hash values are obtained. Cong Wang, Qian Wang, and Kui Ren, Wenjing Lou [14]. In this paper, the main focus was on the combination of public key based homomorphic authentication with random masking so that to achieve privacy preserving and public auditing over cloud storage system. It basically supports the method of multiple auditing task. They use Third Party Auditor who performs various multiple auditing task simultaneously and maintains the integrity of data which is stored by user on cloud. Cong Wang, Sherman S.M. Chow, Qian Wang, Kui Ren, and Wenjing Lou [15]. In this paper, they proposed a method which consist of homomorphic linear authentication with help of random masking technique for preserving privacy of data which will be stored on cloud which simultaneously reduces the burden of shared data but also avoid user's fear of data loss. Here, while using homomorphic linear authentication, third party auditor performs auditing task without asking for local copy of original data so as to remove computation and communication overhead. Qian Wang, IEEE, Cong Wang, Kui Ren, Wenjing Lou, and Jin Li [16]. In this paper, Qian Wang, Cong Wang ,etl. Proposed the various techniques so as to achieve both public auditing and dynamic data operations. To achieve dynamic data operation Merkle hash tree is to be constructed for block label authentication and for effective auditing task bilinear aggregate signature would be used, where third party auditor do multiple auditing task simultaneously. B. Wang, B. Li, and Hui Li, [17] In this paper, they have proposed a privacy preserving technique which supports shared data auditing in cloud. It uses homomorphic authentication technique with help of ring signature so as to compute and verify originality of the data stored over cloud. Sign on every data block kept private from verifiers. Mechanism is basically used so as to perform simultaneous multiple auditing task instead of verifying one by one. So as to improve efficiency of multiple auditing task a technique of batch auditing is used. C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou [18]. In this paper, they proposed a mechanism which preserves the privacy of data and public auditing for shared data in cloud i.e., ring signature so that TPA (third party auditor) is able to verify integrity of data which is shared over cloud for group of user without retrieving entire data. Here, they have provided a privacy preserving public auditing scheme that supports auditing and identify privacy on data stored in cloud. S Ezhil Arasu, B Gowri, and S Ananthi [19], Swapnali S. More Sangita Chaudhari [20]. In this paper, they have proposed a method that uses the keyed Hash Message Authentication Code (HMAC) with homomorphic tokens to enhance the security of TPA (third party auditor). It is a technique for verifying the integrity of a data transmitted between two parties that agree on a shared secret key. HMAC's are based on a key that is shared between the two parties, if either party's key is compromised, it will be possible for an attacker to create fraud messages. C. Wang, S.S. Chow, Q. Wang, K. Ren, and W. Lou [21] D. Boneh, C. Gentry, B. Lynn, and H. Shacham [22], Ms. Bhor Priti1 , Ms. Kakade Priyanka2 , Ms. Kale Ashwini3 , Miss. Dere Archarana [23], In this paper they have proposed a scheme which supports batch auditing through which efficiency is improved. It allows TPA (third party

auditor) to perform multiple auditing task simultaneously and it reduces communication and computation cost. With help of this, we can identify invalid response. It uses bilinear signature (BLS proposed by Boneh, Lynn and Shacham) to achieve batch auditing.

Features	[11]	[6]	[7]	[12]	[9]	[3]	[2]
User Identification	No	NO	NO	NO	NO	NO	NO
Linear Combination	NO	Yes	No	Yes	No	Yes	Yes
Data Dynamics	No	No	Yes	No	Yes	No	No
Integrity of Data	No	Yes	No	Yes	Yes	Yes	Yes
Increase Storage Overhead	No	Yes	Yes	No	No	Yes	Yes
Encryption	Yes	No	No	No	Yes	No	Yes

III. EXISTING SYSTEM

The ever- changing cloud shapes up due to centralization of data; multiple users can access the services via the same URL but, it's security is of utmost concern to all IT professionals who consider to outsource their data to the cloud and the concern even rises when users demand greater access. Many Cloud Service Providers (CSPs) serve its users with increased security-focused resources but, the concern retains as users lose control over their sensitive data. In some open- source clouds, users' outsourced data is not encrypted, where storage providers may access the valuable data and pose threat to privacy policy. There exists many approaches to guarantee data integrity in cloud where an un-biased Third Party Auditor (TPA) verifies the data, but, there also exists some disadvantages too. To maintain data integrity, the cloud user pre- computes Message Authentication Codes (MACs) for each block of data in the file using a secret key. The cloud server receives both data file and associated MACs while the user sends its secret key to TPA for auditing purpose such that during the auditing stage, the TPA demands for randomly selected blocks of data along with associated MACs for data integrity verification. On one hand, MACs assure data authenticity but, on the other hand, for large files it increases computation overhead of the system and retrieves users' data for auditing purpose, which violates privacy-preserving approach. In another approach, the earlier mentioned technique is modified such that the cloud user selects random number of secret keys to calculate MACs. After computing a number of MACs for data file, the cloud user sends data file along with MACs to Cloud Service Provider (CSP). TPA also receives this data along with the secret key. During auditing phase, the TPA communicates with several different keys to ensure higher degree of accuracy in verification process. This technique has its own disadvantages as once all the secret keys get used; cloud user needs to bring back the file from cloud server and re- computes MACs with new keys. Each time the keys are changed, the TPA needs to update its state. To maintain large number of MACs for multiple users may become a cumbersome and error- prone task for TPA and at the same time increasing computation as well as storage overheads.

IV. CONCLUSION

In this paper, we have used this scheme which utilizes RSA based homomorphic authenticator. Here, we are going to handle the problem of how to verify the privacy preserving TPA protocol, independent to data encryption. To address these problems, we have used the technique of public key based homomorphic authenticator which helps TPA to perform auditing task without asking for local copy of data and which reduces communication and computation overhead in parallel. By using random masking with homomorphic authenticator, it guarantees that TPA cannot alter the original or authentic data content stored in cloud server by cloud user.

V. REFRENCES

[1]. Miss Deepali D. Rane, Dr. V. R. Ghorpade, "Enabling public Auditability Assurance Supporting Data Dynamics", 2014.

[2]. Cong Wang, Qian Wang, Kui Ren, "Privacy- Preserving Public Auditing for Data Storage Security in Cloud Computing", 2010.

[3]. Wang C. et al. (2010) IEEE INFOCOM'10.

[4]. Cong Wang, Kui Ren, Wenjing Lou, Jin Li, "Toward publicly auditable secure cloud data storage services.

[5]. H. Shacham, Brent Waters, "Compact Proofs of Retrivabilty.

[6]. G. Ateniese, Randal Burns, Reza Curtmola, Joseph Herring, Lea Kissner, "Provable Data Possession at Untrusted Stores.

[7]. Kevin D. Bowers, Ari Juels, Alina Oprea, "HAIL: A High-Availability and Integrity Layer for Cloud Storage.

[8]. D Srinivas, "Privacy Preserving Public Auditing in Cloud Storage Security, 2011.

[9]. G. Vidhisha, C. Surekha, S. Sanjeeva Rayudu, U. Seshadri, "Preserving Privacy for secure and Outsourcing for Linear Programming in Cloud Computing,

[10]. Zhuo Hao, Sheng Zhong, Nenghai Yu, "A Privacy-Preserving Data Integrity Checking Protocol with Data Dynamics and Public Verifiability", 2011.

[11]. Abhishek Mohta*, Ravi Kant Sahu, Lalit Kumar Awasthi, Robust Data Security for Cloud while using Third Party Auditor".

[12]. Jachak K.B.*, Korde S.K., Ghorpade P.P., Gagare G.J., Homomorphic Authentication with Random Masking Technique Ensuring Privacy & Security in Cloud Computing,2012.

[13]. Boyang Wang, Hui Li, Ming Li, "Privacy- Preserving Public Auditing for Shared Cloud Data Supporting Group Dynamics, 2013.

[14]. Cong Wang, Qian Wang, and Kui Ren, Wenjing Lou, Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing, 2010.

[15]. Cong Wang, Sherman S.M. Chow, Qian Wang, Kui Ren, and Wenjing Lou, Privacy-Preserving Public Auditing for Secure Cloud Storage, IEEE Transactions On Computers, Vol. 62, No. 2, February 2013

[16]. Qian Wang, IEEE, Cong Wang, Kui Ren, Wenjing Lou, and Jin Li, Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing, IEEE Transactions On Parallel And Distributed Systems, VOL. 22, NO. 5, MAY 2011.

[17]. B. Wang, Student Member, IEEE , B. Li, Senior Member, IEEE, and Hui Li, Member , IEEE "Oruta: Privacy Preserving Public Auditing IEEE Transaction On Cloud Computing Vol.2, No.1, January-March 2014.

[18]. C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward secure and dependable storage services in cloud computing," Apr./Jun. 2012.

[19]. S Ezhil Arasu, B Gowri, and S Ananthi. PrivacyPreserving Public Auditing in cloud using HMAC Algorithm. International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277, 3878, 2013.

[20]. Swapnali S. More Sangita Chaudhari Privacy Preserving Third Party Public Auditing Scheme for Secure Cloud Storage International Journal of Computer Applications (0975 – 8887) International Conference on Communication, Computing and Virtualization 23

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

[22]. D. Boneh, C. Gentry, B. Lynn, and H. Shacham, Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," Proc. 22nd Int l Conf. Theory and Applications of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT03), pp. 416-432, and 2003.

[23]. Vol-1 Issue-5 2015 IJARIIE-ISSN(O)-2395-4396 1376 www.ijariie.com 25 SURVEY OF PUBLIC AUDITING IN CLOUD Ms. Bhor Priti1 , Ms. Kakade Priyanka2 , Ms. Kale Ashwini3 , Miss. Dere Archarana4