www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 1 January 2015, Page No. 9929-9932

Privacy Preserving Public Auditing and Recovery Using Backup & Restore Method for Secure Cloud Storage

[1]Priya Rupeja , [2] Prof. Kalyani Waghmare

[1]Pune Institute of Computer Technology,
Department of Computer Engineering, Pune
rupeja1122@gmail.com

[2]Pune Institute of Computer Technology,
Department of Computer Engineering, Pune
Kalyani_mehunkar@yahoo.com

Abstract: ***As cloud computing provides many relinquish characteristics to users like on demand self-service, storage, multi-tenancy, pay-as-you go and access information from shared pool of configurable computing resources without any burden. So that users stores their data remotely anywhere and enjoy on demand services of cloud. Cloud computing is capable of handling mass data storage and intense computing tasks so that, user can store huge amount of data on cloud without any storage capacity limitations. Despite this, users no longer have a physical possession of the outsourced data which make data integrity and availability in cloud a dreadful task, for those which has limited computing resources. Besides also, user can use cloud storage as it is local without any worry for its integrity check. Thus, to avoid this burden from user so there is need of public auditing for cloud storage. So users can rely on third party auditing (TPA) to check its outsourced data integrity. TPA should effectively do its auditing process without any risk towards user data privacy and provide no additional online burden to user. In this paper, we propose secure cloud storage system which will maintain outsourced data confidentiality and integrity by supporting privacy preserving public auditing. We further extend our system to provide recovery of lost data and also identify which block is lost from which file and recovery of that block or file to maintain data availability in cloud server.***

Keywords: Cloud computing, Data Storage, privacy-preserving, TPA.

1. Introduction

Cloud computing has became a buzz word in today's era**.** It is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [2]. It has been envisioned as the next-generation information technology (IT) architecture for enterprises, due to its long list of unprecedented advantages in the IT history [1]. Users or enterprise store their data on cloud and it will be stored in centralized manner. They can get their outsourced data from anywhere and cloud service providers (CSP) will charged them pay-as-you go. Users can upload huge amount of data on cloud without any burden of capacity and maintenance. As a disruptive technology with profound implications, Cloud Computing is transforming the very nature of how businesses use information technology. One fundamental aspect of this paradigm shifting is that data is being centralized or outsourced to the Cloud [1].

From users' perspective, including both individuals and IT enterprises, storing data remotely to the cloud in a flexible on-demand manner brings appealing benefits: relief of the burden for storage management, universal data access with independent geographical locations, and avoidance of capital expenditure on hardware, software, and personnel maintenances, etc [5]. As cloud computing provides many advantages but it also brings security threads towards user's outsourced data. As users no longer physically possess the storage of their data, traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted [6]. Hence due these many attacks on outsourced data is possible. As a result, the correctness of the data in the cloud is being put at risk due to the following reasons. First of all, 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. Even though, there do exist various motivations for CSP to behave unfaithfully towards the cloud users regarding the status of their outsourced data. For examples, CSP might reclaim storage for monetary reasons by discarding data that has not been or is rarely accessed, or even hide data loss incidents so as to maintain a reputation will eliminate any data.

To avoid this problem, we introduce an effective third party auditor (TPA) to audit the user's outsourced data when needed [1]. TPA is the third party auditor who will audit the data of data owner or client so that it will let off the burden of management of data of data owner. TPA eliminates the involvement of the client through the auditing of whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for Cloud Computing. The released audit report would not only help owners to evaluate the risk of their subscribed cloud data services, but also be useful for the cloud service provider to improve their cloud based service platform. This public auditor will help the data owner that his data are safe on cloud [3]. Public auditability allows anyone, not just the client (data owner), to challenge the cloud server for the correctness of data storage while keeping no private information. Hence TPA will help data owner to make sure that his data are safe in the cloud and management of data will be easy and less burdening to data owner. Besides, with the prevalence of Cloud Computing, a foreseeable increase of auditing tasks from different users may be delegated to TPA. As the individual auditing of these growing tasks can be tedious and cumbersome, a natural demand is then how to enable the TPA to efficiently perform multiple auditing tasks in a batch manner, i.e., simultaneously [1]. It will inform whether integrity is lost or not but didn't provide exactly which file lost and how this happened so this will our contribution in this system.

2. Motivation

Cloud computing becomes a successful and popular business model due to its charming features. In addition to the benefits at hand, the former features also result in serious cloud-specific security issues. The people whose concern is the cloud security continue to hesitate to transfer their business to cloud. Security issues have been the dominate barrier of the development and widespread use of cloud computing. Cloud customers have their data and program outsourced to cloud servers. As a result, owners lose direct control on the data sets and programs. Loss of physical control means that customers are unable to resist certain attacks and accidents. For example, data or software may be altered, lost, or even deleted; in addition, it is difficult and impractical to ensure data/computation integrity and confidentiality with traditional methods. With outsourced computation, it is difficult to judge whether the computation is executed with high integrity. Since the computation details are not transparent enough to cloud customers, cloud servers may behave unfaithfully and return incorrect computing results. The main challenge of integrity checking is that tremendous amounts of data are remotely stored on untrustworthy cloud servers; as a result, methods that require hashing for the entire file become prohibitive. In addition, it is not feasible to download the file from the server and perform an integrity check due to the fact that it is computationally expensive as well as bandwidth consuming [17]. So there is need for certain mechanism which will help to eliminate these issues. Hence, auditing mechanism will be useful to solve above problem at some extend. To fully ensure the data integrity and save the cloud users' computation resources as well as online burden, it is of critical importance to enable public auditing service for cloud data storage, so that users may resort to an independent third party auditor (TPA) to audit the outsourced data when needed. The TPA, who has expertise and capabilities that users do not, can periodically check the integrity of all the data stored in the cloud on behalf of the users, which provides a much more easier and affordable way for the users to ensure their storage correctness in the cloud [1]. Audit result from TPA will also play a vital role for the cloud service provider to improve cloud services. In above papers, TPA will give idea about integrity of data. But not exact information of data like which file is lost and which block got change from which attack and recovery of that file. All this will be covered in proposed system. Users will be aware of their information lost and from which attack it's happened. Meanwhile CSP will also get this information to improve their service and increase their security level.

3. Literature Survey

Cloud Computing has been envisioned as the next-generation architecture of IT Enterprise. It moves the application software and databases to the centralized large data centres, where the management of the data and services may not be fully trustworthy [7]. As many user switch towards cloud storage so there should be certain mechanism by confidentiality and integrity must be maintained. For that many authors proposed different protocols and techniques to secure data on cloud. So, many authors has given their own idea toward data security issues. Below is the list of that mechanism along with their protocol.

A. MAC Based Solution

It is used to authenticate the data. In this, user upload data blocks and MAC to CS provide its secret key SK to TPA. The TPA will randomly retrieve data blocks & Mac uses secret key to check correctness of stored data on the cloud. Problems with this system are listed below as

- It introduces additional online burden to users due to limited use (i.e. Bounded usage) and stateful verification.
- Communication & computation complexity
- TPA requires knowledge of data blocks for verification
- Limitation on data files to be audited as secret keys are fixed
- After usages of all possible secret keys, the user has to download all the data to recomputed MAC & republish it on CS.
- TPA should maintain & update states for TPA which is very difficult
- It supports only for static data not for dynamic data[1] – [16]

B. HLA Based Solution

It supports efficient public auditing without retrieving data block. It is aggregated and required constant bandwidth. It is possible to compute an aggregate HLA which authenticates a linear combination of the individual data blocks [1].

C. Privacy Preserving Public Auditing Proposed by Cong Wang

Public auditing allows TPA along with user to check the integrity of the outsourced data stored on a cloud & Privacy Preserving allows TPA to do auditing without requesting for local copy of the data. Through this scheme [1], TPA can audit the data and cloud data privacy is maintained. It contains 4 algorithms as

1) *Keygen:* It is a key generation algorithm used by the user to setup the scheme.

2) *Singen:* It is used by the user to generate verification metadata which may include digital signature.

3) *GenProof:* It is used by CS to generate a proof of data storage correctness.

4) *Verifyproof:* Used by TPA to audit the proofs

D. Using Virtual Machine

Abhishek Mohta proposed Virtual machines which uses RSA algorithm, for client data/file encryption and decryptions [8]. It also uses SHA 512 algorithm which makes message digest and check the data integrity. The Digital signature is used as an identity measure for client or data owner. It solves the problem of integrity, unauthorized access, privacy and consistency.

E. Non Linear Authentication

D. Shrinivas suggested Homomorphic non linear authenticator with random masking techniques to achieve cloud security [10]. K. Gonvinda proposed digital signature method to protect the privacy and integrity of data [9]. It uses RSA algorithm for encryption and decryption which follows the process of digital signatures for message authentication.

F. Using EAP

S. Marium proposed use of Extensible authentication protocol (EAP) through three ways hand shake with RSA. They proposed identity based signature for hierarchical architecture. They provide an authentication protocol for cloud computing (APCC) [11]. APCC is more lightweight and efficient as compared to SSL authentication protocol. In this, Challenge – handshake authentication protocol (CHAP) is used for authentication. When make request for any data or any service on the cloud. The Service provider authenticator (SPA) sends the first request for client identity. The steps are as follows
1) When Client request for any service to cloud service provider, SPA send a CHAP request / challenge to the client.
2) The Client sends CHAP response/ challenges which is calculated by using a hash function to SPA
3) SPA checks the challenge value with its own calculated value. If they are matched then SPA sends CHAP success message to the client.

I. Analysis of protocol proposed by C. Wang which contains security flaws:

Researchers of [15] analyses the Protocol proposed by Wang et al and find security flaws in their protocol. A Public auditing protocol is a collection of 4 polynomial time algorithm as (Keygen, TagBlock, Genproof, and CheckProof)

a. Keygen: User executes Keygen for key generation.

b. TagBlock: User executes TagBlock to produce verification metadata.

c. Genproof: Cloud server executes Genproof for proof of possession.

d. CheckProof: TPA will validate a proof of possession by executing CheckProof.

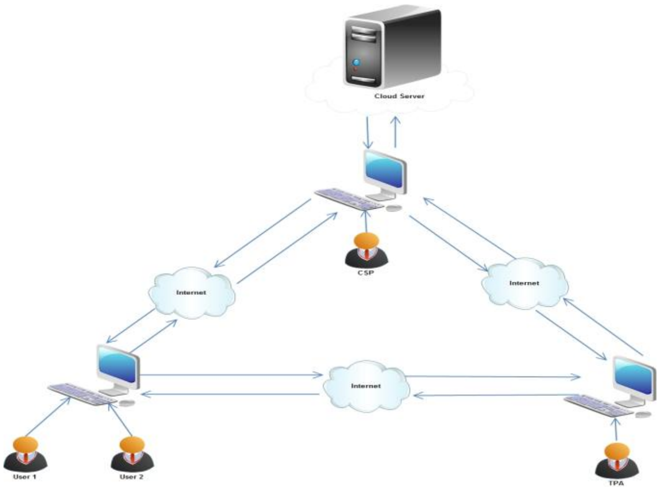
The Problem with this system is that cloud server might be malicious which might not keep data or might delete the data owned by cloud users and might even hide the data possessions.

J. Automatic Protocol Blocking with 3-D Password Authentication

In this protocol, public auditing can be achieved using the Automatic Protocol Blocking for the secure cloud storage, which improves the efficiency of the user storage. Thus the 3-d password will improve the user level security in Cloud Server and the data level security will be effectively provided using the GCM based encryption and decryption algorithms. Thus the public auditing ensures that the data leakage and data loss will be reduced and more number of users will be improved [3].

4. Existing system

We consider a cloud data storage service involving three different entities, the cloud user (U), who has large amount of data files to be stored in the cloud, the cloud Server (CS), which is managed by the cloud service provider (CSP) to provide data storage and has significant storage space and computation resources., the third party Auditor (TPA), who has expertise and capabilities that cloud users do not have and is trusted to assess the cloud storage service security on behalf of the user request [3]. Fig1. shows the entire architecture of the system. User can upload or download to/from the cloud and whenever feels that data is corrupted then user directly call TPA for integrity check. On behalf of user TPA will check and give report to user as well as CSP to inform that data is lost on cloud server. As contribution work we can add value to TPA. We can notify user which file get changed and also which block of that file get changed from which attack and its recovery.



5. Conclusion

In this paper, we studied all techniques used for a privacy-preserving public auditing system for data storage security in Cloud Computing. As TPA will inform about data integrity and not providing exact idea about how data is lost. So we proposed our solution to solve that problem and also report the file which changed and corrupted and also will report from which attack it happened. Also provides recovery of that corrupted file.

References

[1] Cong Wang, Sherman S.-M, Qian Wang, Kui Ren, Wenjing Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage", IEEE Trans. on Cloud Computing, March-2013

[2] P. Mell and T. Grance, "Draft NIST working definition of cloud computing," Referenced on Nov. 22rd, 2014 Online at http://csrc.nist.gov/groups/SNS/cloud-computing/index. html, 2014.

[3] P. Selvigrija, D. Sumithra," Public Auditing & Automatic Protocol Blocking with 3-D Password Authentication for Secure Cloud Storage", D. Sumithra et al, International Journal of Computer Science and Mobile Applications,Vol.2 Issue. 1, January- 2014, pg. 1-8

[4] Cong Wang, Qian Wang, and KuiRen "Ensuring Data Storage Security in Cloud Computing" Email: {cwang, qwang, kren}@ece.iit.edu.-pg:2,3

[5] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley view of cloud computing," University of California, Berkeley, Tech. Rep

[6] A. Juels and J. Burton S. Kaliski, "Pors: Proofs of retrievability for large files," in *Proc. of CCS'07*, Alexandria, VA, October 2007, pp. 584–597.

[7] Wang, Q., Wang, C., Ren, K., Lou, W., & Li, J. 2011. "Enabling public auditability and data dynamics for storage security in cloud computing". Parallel and Distributed Systems, IEEE Trans. on, 22(5), 847-859.

[8] Abhishek Mohta, Lalit Kumar Awasti, "Cloud Data Security while using Third Party Auditor", International Journal of Scientific & Engineering Research, Volume 3, Issue 6, ISSN 2229-8 June 2012.

[9] K Govinda, V. Gurunathprasad and H. sathishkumar*, "* Third Party Auditing for Secure Data Storage in Cloud Through Digital Signature Using RSA*",* International Journal of Advanced science and Technical Research, vol 4,no. 2, ISSN: 2249-9954,4 August 2012

[10] D. Shrinivas, "Privacy-Preserving Public Auditing in Cloud Storage security", International Journal of computer science nad Information Technologies, vol 2, no. 6, pp. 2691-2693, ISSN: 0975-9646, 2011

[11] S. Marium, Q. Nazir, A. Ahmed, S. Ahthasham and Aamir M. Mirza, "Implementation of EAP with RSA for Enhancing The Security of Cloud Computig", International Journal of Basic and Applied Science, vol 1, no. 3, pp. 177 183, 2012

[12] XU Chun-xiang, HE Xiao-hu, Daniel Abraha,"Cryptanalysis of Auditing protocol proposed by Wang et al. for data storage security in cloud computing", http://eprint.iacr.org/2012/115.pdf, and cryptologyeprintarchieve: Listing for 2012.

[13] Balkrishnan. S, Saranya. G, Shobana. S and Karthikeyan. S, "Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud", International Journal of computer science and Technology, vol. 2, no. 2, ISSN 2229-4333 (Print) | ISSN: 0976-8491(Online), June 2012

[14] Jachak K. B., Korde S. K., Ghorpade P. P. and Gagare G. J. ,"Homomorphic Authentication with Random Masking Technique Ensuring Privacy & Security in Cloud Computing", Bioinfo Security Informatics, vol. 2, no. 2, pp. 49-52, ISSN. 2249-9423, 12 April 2012

[15] B. Dhiyanesh "A Novel Third Party Auditability and Dynamic Based Security in Cloud Computing" ,International Journal of Advanced Research in Technology, vol. 1,no. 1, pp. 29-33, ISSN: 6602 3127,2011

[16] Tejashree Paigude , Prof. T. A. Chavan," A survey on Privacy Preserving Public Auditing for Data Storage Security", International Journal of Computer Trends and Technology-volume4Issue3- 2013

[17] Zhifeng Xiao and Yang Xiao, Senior Member, IEEE*,"* Security and Privacy in Cloud Computing*",* IEEE Communication Surveys & Tutorials, Vol. 15, No. 2, Second Quarter 2013

Author Profile

1. Priya Rupeja had BE from Sipna College of Engineering & Technology From Amravati University. Now pursuing ME in Pune Institute of Computer Engineering from Pune University. Currently Live in Pune.