Public Integrity Auditing through Trusted Third Party Auditor for Storage Security in Cloud Computing

Prof. Nupoor M. Yawale , Prof. Nilima V. Pardakhe, Prof. Sushant A. Patinge

Abstract— Cloud can provide service to access their applications and data from anywhere at any time and data should be fully secured as it is stored in encrypted form. Many users place their data on the cloud, so correctness of data and security is a prime concern. To ensure the correctness of data, we consider the task of allowing a third party auditor (TPA) for verifying the integrity of the data stored in the cloud. Data integrity checking is a decisive technology in cloudcomputing. TPA can save encrypted data on cloud and perform data integrity validation through challenge & challenge verification. Here, system supporting privacy-preserving public auditing and TPA to perform audit efficiently with Encryption Algorithm

Index Terms— Cloud computing, Data Integrity, Encryption, privacy-preserving, public auditability, RC5 Algorithm, Third Party Auditor (TPA).

1 INTRODUCTION

1.1 Cloud Computing

“The cloud will change IT as nothing before it has” and that is because the cloud offers businesses the opportunity to do more things faster and better.Cloud is a large group of interconnected computers, which is a major change in how we store information and run application[1]. The advantage of cloud is cost savings. The disadvantage of cloud computing is security. As security is not provided in cloud, many companies develop their unique security structure. The data which is placed on the cloud is accessible to everyone but security is not guaranteed. To ensure security, cryptographic techniques cannot be directly adopted. To avoid this problem, we introduce a third party auditor to audit the user’s outsourced data when needed. TPA performs the auditing task for each user.[2]

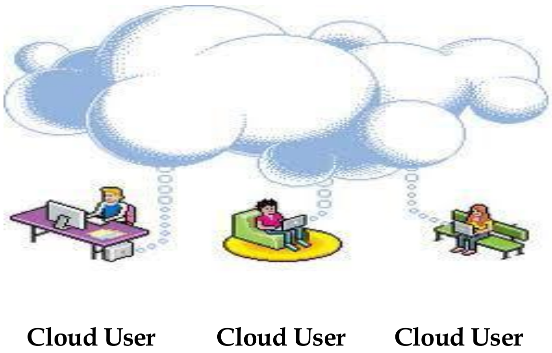

Figure 1: Cloud Architecture

1.2 Third party Auditor (TPA):

Third Party Auditor is act as an inspector. To let off the burden of management of data owner, TPA will audit the data of client. TPA helps data owner to make sure that management of data will be easy and less burdening to data ownerand also his data are safe in the cloud.

TPA has privileges to encrypt the user’s data and save it on cloud. Also auditor can view data which is uploaded by various users. TPA can encrypt data and send it to Cloud service provider (CSP) for storage and auditor can view encrypted data of every user.

Objectives:

- To provide Data Storage Security.
- To design a scheme, which will provide a monitoring system to preserve the confidentiality of the data.
- To support data integrity & validation.
- To established security for user’s outsourced data.

2 RELATED WORK

2.1 Existing System:

Cloud improves due to centralization of data, increased security focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels. Security is often as good as or better than other traditional systems, in part because providers are able to devote resources to solving security issues that many customers cannot afford. To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on line burden to the cloud user; 2) The third party auditing process should bring in no new vulnerabilities towards user data privacy.

- *Prof. Nupoor M. Yawale is assistant professorat at PRMIT &R Badnera, Amravati. Email id is nupoory1@gmail.com*
- *Prof. Nilima V. Pardakhe is assistant professorat at PRMIT &R Badnera, Amravati. Email id is nilimapardakhe@gmail.com*
- *Prof. Sushant A. PAtinge is assistant professorat at Sipna COET, Amravati. Email id is spatinge@gmail.com*

We consider a cloud data storage service involving three different entities, as illustrated in Fig. 2.14: the cloud user (CU), 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 service 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 reliability on behalf of the user upon request. Users rely on the CS for cloud data storage and maintenance. They may also dynamically interact with the CS to access and update their stored data for various application purposes. To save the computation resource as well as the online burden, cloud users may resort to TPA for ensuring the storage integrity of their outsourced data, while hoping to keep their data private from TPA.

We consider the existence of a semi-trusted CS as [16] does. Namely, in most of time it behaves properly and does not deviate from the prescribed protocol execution. However, for their own benefits the CS might neglect to keep or deliberately delete rarely accessed data files which belong to ordinary cloud users. Moreover, the CS may decide to hide the data corruptions caused by server hacks or Byzantine failures to maintain reputation. We assume the TPA, who is in the business of auditing, is reliable and independent, and thus has no incentive to collude with either the CS or the users during the auditing process. However, it harms the user if the TPA could learn the outsourced data after the audit. To authorize the CS to respond to the audit delegated to TPA's, the user can sign a certificate granting audit rights to the TPA's public key, and all audits from the TPA are authenticated against such a certificate. These authentication handshakes are omitted in the following presentation.

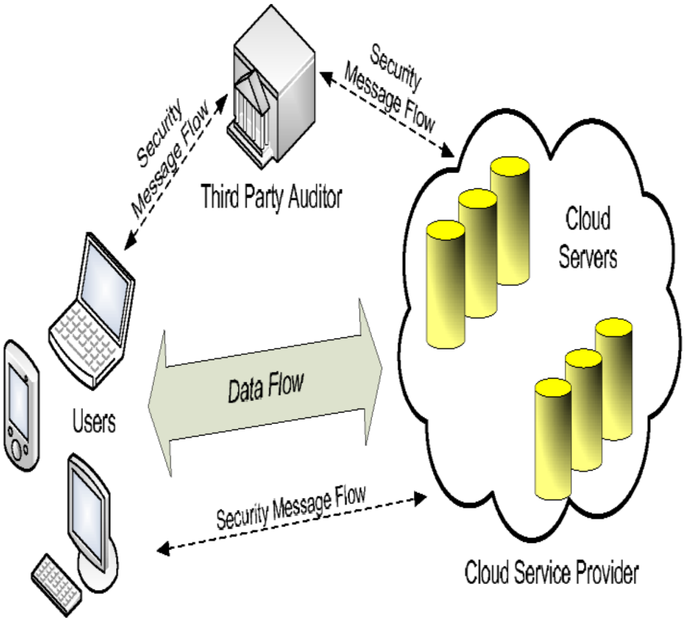

Figure 2: The architecture of cloud data Storage service

2.2 Limitation of Existing System:

- User's files are not encrypted on some open source cloud storage systems. So, privacy is not preserve.
- The storage service provider can easily access the user's files. This brings a big concern about user's privacy.
- The user has no supreme control over the software applications including secret data. User has to depend on the provider‘s action, maintenance and admin it.

3 SYSTEM IMPLEMENTATION

3.1 Basic **Idea:**

The TPA will properly monitor confidentiality ofthe data and uniquely integrate it with encryption technique to achieve a privacy-preserving public auditing system for cloud data storage security while keeping all above requirements in mind. Extensive security and analysis shows the proposed schemes are secure.

Cloud computing can be applied to the data transmission security. If the data is stolen, there is no corresponding key to be restored. Only the TPA knows the key, the CSP do not know the key. User's privacy is protected because user's files are stored in encrypted form in cloud storage.

3.2 System Implementation Methodology:

Cloud computing is evolving as a revolution. In cloud computing, cloud security is most challenging tasks. Cloud computing entrusts services with users data, software and computation on a published application programming interface over a network. The cloud provides a platform for many types of services.

To enable privacy-preserving public auditing for cloud data storage under the mentioned model, our system should achieve the following security and performance guarantees. Public auditability to allow TPA to verify the correctness of the cloud data on demand without retrieving a copy of the whole data or introducing additional online burden to the cloud users. Privacy-preserving to ensure that the TPA cannot derive users data content from the information collected during the auditing process.

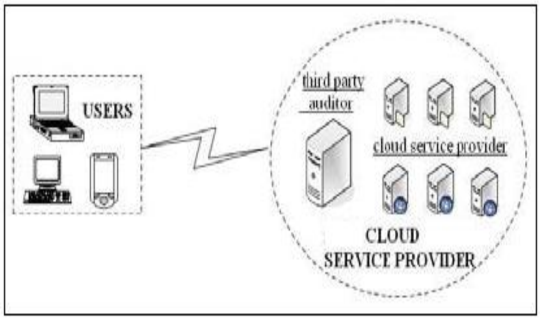

Figure 3: TPA with Cloud Service Provider

In proposed method we use RC5 algorithm for encryption and decryption. Our protocol contains three main participants. As discussed above

(i) Third Party Auditor (TPA): The Third party auditor (TPA) has expertise and capabilities that cloud users do not have and is trusted to assess the cloud storage service reliability on behalf of the user upon request.

(ii) User:The cloud user or data owner (CU), who has large amount of data files to be, stored in the cloud. Users rely on the TPA for cloud data storage and maintenance.To save the resource as well as the online burden, cloud users may resort to TPA for ensuring the storage integrity of their outsourced data and their data private.

(iii) Cloud Service Provider: Cloud service provider (CSP), provides data storage service and has significant storage space and computation resources.

We assume the TPA, who is in the business of auditing, is reliable and independent, and thus has no incentive to collude with either the CSP or the users during the auditing process.

One of the best ways to ensure confidential data is protected in the cloud is to utilize encryption for data. Almost all cloud service providers support encryption for data storage, but few offer support for data at rest. The cloud encryption capabilities of the service provider need to match the level of sensitivity of the data being hosted. To protect a user's confidential data in the cloud, encryption is a powerful tool that can be used effectively. Only user can confidently utilize cloud providers knowing that their confidential data is protected by encryption.

4 Advantage

i)The audit activities are efficiently scheduled in an audit period, and a TPA needs merely access file to perform audit in each activity.
ii) User can store any file or application on cloud and received the original decrypted data from cloud.
iii) TPA can save encrypted data on cloud and perform data integrity validation through challenge & challenge verification.
iv) CSP can provide simply the space for storing the file and it doesn't have privilege to see the content of file as it is stored in encrypted form.

5 Applications

i) Clients would be able to access their applications and data from anywhere at any time and data should be fully secured as it is stored in encrypted form.
ii) This system can be deployed in school for students. The admin will store electronic teaching materials on cloud servers. This will not only make it possible for students to use online teaching materials during class but they will also be able to access these materials at home, using them to prepare for and review school lesson.
iii) This system can be implementing in Banking Sector for storing confidential data on cloud.
iv) The system can be used in various corporate applications which are seeking for the confidentiality & Integrity of the data in cloud environment.

6 Conclusion

Cloud Computing is an area full of challenges and of paramount importance, is still in its infancy now, and many research problems are yet to be identified. System uses encryption/decryption keys of user's data and stores it on remote server. Each storage server has an encrypted file system which encrypts the client's data and store. The system ensures that the client's data is stored only on trusted storage servers and it cannot be accessed by administrators or intruders. TPA can perform auditing tasks. Resulted encrypted method is secure and easy to use. Third party auditor can be a trusted third party to resolve the conflicts between the cloud service provider and the client. This research paper provides data security using third party auditor.

We can implement this model in various cloud computing platforms to get the more efficient way of cloud computing such as SaaS, AaaS etc. we will alsowork on authentication of users password. In future, we can work for session key implementation for displaying the number of list uploaded by user and also display the encrypted image & multimedia messages.

.

References

[1] P. Mell and T. Grance, "Draft NIST working definition of cloud computing" Referenced on June. 3rd 2009 [cited 30 April, 2010]; Available from: http:// www.wheresmyserver.co.nz/storage/media/faq-files/cloud-def-v15.pdf. [Online, Access: 15 Oct 2013]

[2] A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, M. Zaharia, "Above the clouds: A berkeley view of cloud computing," University of California, Berkeley, Tech. Rep, 2009.

[3] Balakrishnan S, Saranya G, et al. (2011). Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud, International Journal of Computer Science and Technology, vol 2(2), 397–400.

[4] Yu, S., Wang, C., Ren, K., Lou, W.: Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing. In: Proc. IEEE INFOCOM. pp. 534–542 (2010)

[5] STRACHEY, CHRISTOPHER (JUNE 1959). "TIME SHARING IN LARGE FAST COMPUTERS". PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON INFORMATION

PROCESSING, UNESCO. PAPER B.2.19: 336–341.

[6] SIMSONGARFINKEL (3 OCTOBER 2011). "The Cloud Imperative". TECHNOLOGY REVIEW (MIT). RETRIEVED 31 MAY 2013.

[7] G.Ateniese et al., ―Provable Data Possession at Untrusted Stores,‖ Proc. ACM CCS ‗07, Oct. 2007, pp. 598–609.

[8] RYAN; FALVEY; MERCHANT (OCTOBER 2011). "Regulation of the Cloud in India". JOURNAL OF INTERNET LAW15 (4)

[9] "July, 1993 meeting report from the IP over ATM working group of the IETF". CH: SWITCH. RETRIEVED 2010-08-22.

[10] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in Proc. of ESORICS'09, volume 5789 of LNCS. Springer-Verlag, Sep. 2009, pp. 355–370.

[11] 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.

[12] "Jeff Bezos' Risky Bet". BUSINESS WEEK, November 12, 2006.

[13] "Amazon's early efforts at cloud computing partly accidental". IT KNOWLEDGE EXCHANGE. TECH TARGET. 2010-06-17

[14] M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, "Auditing to keep online storage services honest," in Proc. Of HotOS'07. Berkeley, CA, USA: USENIX Association, 2007, pp. 1–6.

[15] H. Shacham and B. Waters, "Compact proofs of retrievability," in Proc. of Asiacrypt 2008, vol. 5350, Dec 2008, pp. 90–107.

B ROCHWERGER, J CACERES, RS MONTERO, D BREITGAND, E ELMROTH, A GALIS, E LEVY, IM LLORENTE, K NAGIN, Y WOLFSTHAL, E ELMROTH, J CACERES, M BEN-YEHUDA, W EMMERICH, F GALAN. "THE RESERVOIR MODEL AND ARCHITECTURE FOR OPEN FEDERATED CLOUD COMPUTING", IBM JOURNAL OF RESEARCH AND DEVELOPMENT, VOL. 53, NO. 4. (2009)

[17] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," J. Cryptology, vol. 17, no. 4, pp. 297–319, 2004.

[18] A. L. Ferrara, M. Greeny, S. Hohenberger, and M. Pedersen, "Practical short signature batch verification," in Proceedings of CT-RSA, volume 5473 of LNCS. Springer-Verlag, 2009, pp. 309–324.

[19] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proc. Of SecureComm'08, 2008, pp. 1–10.

[20] C.Wang, Q.Wang, K. Ren, and W. Lou, "Ensuring data storage security in cloud computing," in Proc. of IWQoS'09, July 2009,pp. 1–9.

[21] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in Proc. of CCS'09, 2009, pp. 213–222.

[22] R. C.Merkle, "Protocols for public key cryptosystems," in Proc.of IEEE Symposium on Security and Privacy, Los Alamitos, CA, USA, 1980.

[23] D KYRIAZIS, A MENYCHTAS, G KOUSIOURIS, K OBERLE, T VOITH, M BONIFACE, E OLIVEROS, T CUCINOTTA, S BERGER, "A REAL-TIME SERVICE ORIENTED INFRASTRUCTURE", INTERNATIONAL CONFERENCE ON REAL-TIME AND EMBEDDED SYSTEMS (RTES 2010), SINGAPORE, NOVEMBER 2010