IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 1, January 2022

DOI: 10.17148/IJARCCE.2022.11137

Privacy Preserving in TPA for Secure Cloud-Survey

Miss. Shreya Mugal[1], Prof. K. K. Chhajed[2], Prof. A. R. Ladole[3]

Dept of CSE, PR POTE COEM Amravati[1,2]
Dept. of CSE, SIPNA COET, Amravati, Maharashtra,India[3]

Abstract- Cloud users can remotely store their data and appreciate the on-demand high quality applications and services from a shared pool of configurable computing resources, regardless of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in Cloud computing a formidable task, especially for users with constrained computing resources. This paper study the the problem of ensuring the integrity of data storage in Cloud Computing. In particular, we task of allowing a third-party auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. To securely introduce an effective third-party auditor (TPA), and determine various techniques and algorithms for strengthen the Security.

Keywords- TPA, Cloud Computing, CSP, RSA

INTRODUCTION

In today's era, Cloud Computing is attaining more and more generosity in both intellectual and industrial community. The significance of cloud computing is that you don't need to buy the any kind of hardware, or even the software, you need anymore, rather you rent some computational power, storage, databases, and any other resource you need by a provider according to a pay-as-you-go model, making your investment smaller and oriented to operations rather than to assets acquisition.

Mainly users can abandon the maintenance of IT services to cloud service providers (CSP), who is apt in providing knowledge and maintains the large amount of IT resources. Cloud computing compel many new security issues and challenges on assuring the integrity and privacy of users data in cloud. To entice these issues, work of this research uses the concept of secret key which is based on symmetric key cryptography, in which it allows the TPA to execute the auditing without exacting the local copy of user's stored data and hence sharply analyze the transmission and reckoning overhead as related to the straightforward data auditing approaches.

Cloud provides users to store huge amount of data and to accomplish application over cloud also provides better flexibility of storing and computation of data but, Such applications can be processed, huge volume processing data sets are to be generated. However, numerous potential customers are still hesitant to take the advantage of cloud due to security and privacy concerns.

It is the long-term idea of computing as a utility and storage that include the economical benefits to transmute the IT industry which will assist for making software products even more service oriented. It is nothing but the grouping of networks, hardware, services, storage that can be coupled with each other to provide computing as a service.

Need of Privacy

Cloud computing is an rising technology which offers an novel business model for the organizations with immense data without upfront investment, but most of the organizations still hesitate to explore their business over cloud due to security. It is one of the major hurdles which limit the growth of cloud. So there is need to work on it and find the appropriate solution.

Third Party Auditor (TPA)

For an organization, it is important that, cloud which allows delivering from single party audit, the commerce data to ensure data security and save the user's reckoning and data storage. It is essential to maintain the public auditing services for cloud data storage in the way that user can trust an autonomous third party auditor (TPA). On the behalf of users, TPA polls the integrity of the data within cloud, and also maintains the users to poll the validity of data in cloud. In addition, public auditing provides the external party to verify as well the correctness, of already stored data across the external attacks to the user. However these systems, as in [1] don't relate the privacy protection of the data.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 1, January 2022

DOI: 10.17148/IJARCCE.2022.11137

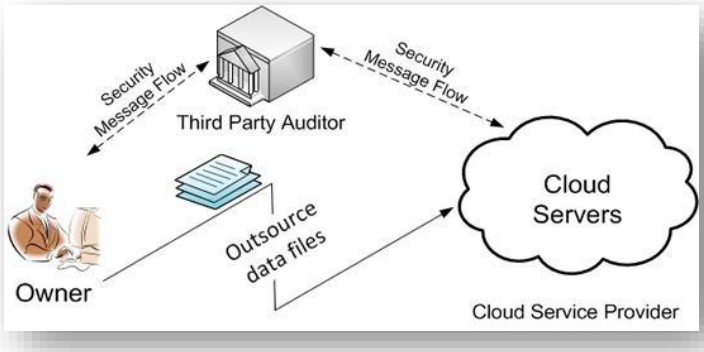

Figure 1- TPA architecture

LITERATURE SURVEY

Privacy-Preserving Public Auditing for Secure Cloud Storage [01], in this paper researcher stated that, Using Cloud Storage, users can remotely store their data and enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. Propose a secure cloud storage system supporting privacy-preserving public auditing. They further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently.Public auditing schemes consist of four algorithms. KeyGen, SigGen, GenProof, Verify Proof.

Privacy-Preserving Public Auditing using TPA for Secure Cloud Storage [02], in this paper they explain, by using Cloud storage, users can access applications, services, software whenever they requires over the internet.The cloud must have to ensure data integrity and security of data of user. The issue about cloud storage is integrity and privacy of data of user can arise. To maintain to overkill this issue here, they are giving public auditing process for cloud storage that users can make use of a third-party auditor (TPA) to check the integrity of data. They also extend our concept to ring signatures in which HARS scheme is used. Merkle Hash Tree is used to improve block level authentication. Further they extend our result to enable the TPA to perform audits for multiple users simultaneously through Batch auditing. This paper used HARS contains three algorithms: KeyGen, RingSign and RingVerify

Secure Privacy Preserving Public Auditing for Cloud storage [03], in this paper they explain, Cloud storage provides users to easily store their data and enjoy the good quality cloud applications need not install in local hardware and software system.In cloud environment the computing resources are under the control of service provider, the third party auditor ensures the data integrity over out sourced data. In this paper they proposed Encryption and Proxy encryption algorithm to protect the privacy and integrity of outsourced data in cloud Environments.

Sathiskumar R, Dr.Jeberson Retnaraj [5] clarified general society review capacity is a primary downside of distributed computing innovation. In this paper secure open examining plan for distributed storage give greater security thought about past innovation. In this paper open Auditing framework and talk about two direct plans and their bad marks. In this paper a public auditing scheme consists of four algorithms (KeyGen, SigGen, GenProof, VerifyProof) used.

T. Prasanthi, C. Balasubramanian, [6] described to ensure the integrity of dynamic data stored in the cloud, external Third Party Auditor (TPA) is acquainted in a cloud infrastructure. For enabling public auditing in cloud data storage security, users can resort to an external auditor to check integrity of an outsourced data. This paper used the DES algorithm to encrypt the data to ensure that the file will not be intercepted by an unauthorized person to get the file Content.

Sadia Marium [7] they research on Cloud computing is fast growing technology used by modern world but needs to be covered some open area which is affecting its robust features. In cloud computing users have very serious concerns about its open nature of privacy and security. To ensure the security of client data in cloud, they purpose the implementation of Extensible Authentication Protocol through three way hand shake with RSA

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 1, January 2022

DOI: 10.17148/IJARCCE.2022.11137

Table 1- Comparative analysis of TPA techniques

Sr. no	Author	Concept	Algorithm Used
1	Bilal Ahmed, Pushpalatha M.N	propose a secure cloud storage system supporting privacy-preserving public auditing. also extend result to enable the TPA to perform audits for multiple users simultaneously and efficiently.	KeyGen, SigGen, GenProof, erifyProof
2	Jyoti R Bolannavar	To maintain privacy and integrity of data public auditing process for cloud storage that users can make use of a third-party auditor (TPA) to check the integrity of data.	KeyGen, RingSign and RingVerify
3	Salve Bhagyashri, Prof. Y.B.Gurav	To maintain integrity of databy TPA, they proposed Encryption and Proxy encryption algorithm to protect the privacy and integrity of outsourced data in cloud Environments.	Proxy algorithm
4	R. Sathiskumar, Dr.Jeberson Retnaraj	this paper secure open examining plan for distributed storage give greater security thought about past innovation. In this paper open Auditing framework and talk about two direct plans and their bad marks	KeyGen, SigGen, GenProof, verifyProof
5	T. Prasanthi, C. Balasubramanian	For enabling public auditing in cloud data storage security, users can resort to an external auditor to check integrity of an outsourced data.	DES algorithm
6	Sadia Marium	To ensure the security of client data in cloud, they purpose the implementation of Extensible Authentication Protocol through three way hand shake with RSA	RSA algorithm

CONCLUSION:

TPA are capable to publicly certifying the integrity of the data to be shared away from retrieving the whole data within the cloud. The public verifiers (TPA) are adept at correctly verifying the integrity of data to be shared. The public verifier (TPA) cannot distinguish the identity of the user on each block which shared data during the process of auditing.the overview from above review it is comes to the conclusion that more firmed security can be provided by a asymmetric algorithm like RSA.

REFERENCES

[1] Bilal Ahmed, Pushpalatha M.N, “A Novel Privacy-Preserving Public Auditing For Secure Cloud Storage”, 10th IRF International Conference, 04th October-2014, Bengaluru, India, and ISBN: 978-93-84209-56-8.

[2] Jyoti R Bolannavar, “Privacy-Preserving Public Auditing using TPA for Secure Cloud Storage”, International Journal of Scientific Engineering and Research (IJSER) ISSN (Online): 2347-3878 Volume 2 Issue 6, June 2014.

[3] Salve Bhagyashri, Prof. Y.B.Gurav, “Privacy-Preserving Public Auditing For Secure Cloud Storage”, IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, pISSN: 2278-8727, Volume 16, Issue 4, Ver. III (Jul – Aug. 2014), PP 33-38

[4] Sathiskumar R, Dr.Jeberson Retnaraj, “Secure Privacy Preserving Public Auditing for Cloud storage”, International Journal of Innovative Research in Science, Engineering and Technology, Volume 3, 1st January2014, International Conference on Engineering Technology and Science-(ICETS’14) On 10th & 11th February

[5] T. Prasanthi, C. Balasubramanian, "An Efficient Auditing Protocol for Secure Data Storage in Cloud Computing", Proceedings of the World Congress on Engineering 2014 Vol I, WCE 2014, July 2 - 4, 2014, London, U.K

[6] 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, Volume 1, 2012, no. 3, ISSN 177- 183.

DOI: 10.17148/IJARCCE.2022.11137

[7] Abhishek R. Ladole, K. K. Chhajed,alesh M. Shelke, "A Survey on Privacy Preserving Techniques in Cloud Environments", 2018 International Conference on Current Trends towards Converging Technologies (ICCTCT), doi:10.1109/ICCTCT.2018.8551019

[8] Krebs, "Payment Processor Breach May Be Largest Ever," Online at, http://voices.washingtonpost.com/securityfix/2009/01/payment processor breach may b.html, Jan. 2009.

[9] 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.

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

[11] G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, L. Kissner, Z. N. J. Peterson, and D. X. Song. Provable data possession at untrusted stores. In Proceedings of the 2007 ACM Conference on Computer and Communications Security, CCS 2007, pages 598–609, 2007.

[12] Cloud Security Alliance, "Security guidance for critical areas of focus in cloud computing," 2009, http://www. cloudsecurityalliance.org.

[13] Dr. P. K. Deshmukh, Mrs. V. R. Desale, Prof. R. A. Deshmukh, "Investigation of TPA (Third Party Auditor Role) foe Cloud Data Security", International Journal of Scientific and Engineering Research, vo. 4,no. 2,ISSn 2229-5518, Feb 2013.

[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

