Security for Storing Data in Cloud

T. A. Salunke[1] V. M. Solanki[2] T. N. Raut[3] K. P. Salve[4]
[1,2,3,4]Student
[1,2,3,4]Department of Computer Engineering
[1,2,3,4]SVPM's College of Engineering Malegaon (Bk), Baramati, India

Abstract— Cloud computing is the new emerging technology which is going to play an important role in future. As the many of the services are provided by cloud such as Saas, Paas and Iaas so any one using this services has to pay for it. In this paper, we focus on cloud data storage security, which is always been an important aspect of quality of service. So while storing the data in cloud there is fear that either it is secure or not this security challenge need to handle. For that, to ensure the user we are going to propose a system that will be more helpful to the user to store the data more securely in cloud. It consist of three entities: data owner, TPA and cloud server. The data owner performs various operations such as splitting the file to blocks, encrypting them, generating a hash value for each, concatenating it and generating a signature on it. And the Data owner can check his data integrity by providing indices of blocks. Unlike most prior works, the new scheme further supports secure and efficient dynamic operations on data blocks, including: data update, delete and append.

Key words: Cloud Computing, Cloud Storage, Cloud Service Provider, Digital Signature, Third Party Auditor

I. INTRODUCTION

This paper explains Cloud computing is innovation that uses advanced procedure power and improved storage capabilities. Cloud computing may be a long unreal vision of computing utility, that modify the sharing of services over the net. Cloud may be a massive cluster of interconnected computers that may be a major advancement in however we have a tendency to store data and run application. Cloud computing may be a shared pool of configurable computing resources, on-demand network access and provisioned by the service supplier. The advantage of cloud is value savings. The prime disadvantage is security. Knowledge security is one in all the foremost important barriers to its adoption and it's followed by problems together with compliance, privacy, trust, and legal matters. Therefore, one of the necessary goal is to take care of security and integrity of data hold on within the cloud owing to the crucial nature of Cloud computing and enormous amounts of advanced data it carries. In cloud knowledge security embrace knowledge privacy, knowledge protection, knowledge availableness, knowledge location, and secure transmission.

Knowledge confidentiality is additionally necessary side from user's purpose of read as a result of they store their non-public or confidential knowledge within the cloud. The info confidentiality can be self-addressed by increasing the cloud reliableness and trustiness in Cloud computing. so security, integrity, privacy and confidentiality of the hold on knowledge on the cloud is necessary from users purpose of we have a tendency to demonstrate the info auditing that check the integrity of knowledge with the assistance of associate entity known as Third Party Auditor (TPA). The aim of this work is to develop associate auditing theme that is secure, economical to use and possess the capabilities like privacy conserving, public auditing, maintaining the info integrity in conjunction with confidentiality. TPA (Third Party Auditor) will the auditing while not retrieving the info copy, hence privacy is preserved. The info is split into components or blocks so hold on within the encrypted format within the cloud storage, therefore maintaining the confidentiality of knowledge. The info integrity is verified by TPA for the asking of the data owner by the digital signatures. It solely checks whether or not the hold on knowledge is tampered or not and informs regarding it to the user.

II. LITERATURE SURVEY

Cloud computing faces many problems on integrity and privacy of user's data stored in the cloud. Hence it requires some secure and efficient methods which can ensure the integrity of data stored in the cloud. Wang et al. [7] has proposed a protocol which makes 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 vulnerable to ex-istential forgeries known as message attack from a malicious cloud server and an outside attacker. To overcome this problem Wang et al. [5] proposed a new improved scheme which is m- ore secure than the protocol proposed in [7]. It is a public auditing scheme with TPA, which performs 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. For the sake of data binding, this new scheme involves computationally intensive pairing operation thus making it inefficient to use. This proposed scheme has been implemented practically on Amazon EC2 instance which demonstrates the fast performance of the design on both the cloud and the auditor side. But the full-fledged implementation of this mechanism on commercial public cloud is not been tested. So it is difficult to expect it to robustly cope with very large scale data [5].

Wang et al. [8] planned another protocol that supports each public auditing and information dynamics by victimisation B- LS based mostly HLA at the side of Merkle Hash Tree (MHT) It achieves the integrity of information however fails to supply confidentiality to the info keep on the cloud. Wang et al. [6] has additionally planned a style to sight the changed blocks simply victimization homomorphic token precomputation and later erasure coded technique is employed to acquire the specified blocks from totally different servers. Male monarch et al. [9] planned protocol uses an equivalent security level as Wang et. al.[5] however with higher potency. It generates a signature set that is associate degree ordered assortment of signatures on every file block, therefore acquisition computation and communication overhead. Meenakshi et al. [2] has planned a protocol that uses TPA to audit the info of the users victimisation Merkle Hash Tree algorithm. It supports information dynamics however fails to supply confidentiality. To the keep info within the cloud.

Tejaswani et al. [4] has achieved integrity of knowledge employing a Merkle hash tree by TPA and also the confidentiality of knowledge is achieved victimisation RSA based mostly cryptography algorithmic rule whereas Jadhav et al. [3] have introduced an offensive module that endlessly keeps track on knowledge alteration within the cloud. The offensive module may be a tiny code that resides on cloud server. Confidentiality of hold on knowledge is achieved by encrypting the info victimisation AES algorithmic rule. Arasu et al. [1] has projected a technique that uses the keyed Hash Message Authentication Code (HMAC) with homomorphic tokens to reinforce the protection of TPA. It's technique for corroboratory the integrity of an information transmitted between 2 parties that agree on a shared secret key. HMAC are supported a key that's shared between the 2 parties, if either party's key's compromised, it'll be durable for an resilient to make fraud messages.

III. Proposed System

The proposed system is developed to verify the correctness of cloud data by TPA, periodically or as per demand of users without retrieving the entire data blocks or without introducing additional online burden to the cloud users and cloud servers.

The proposed scheme is helpful for the maintaining storage correctness of data, integrity and confidentiality of stored data.

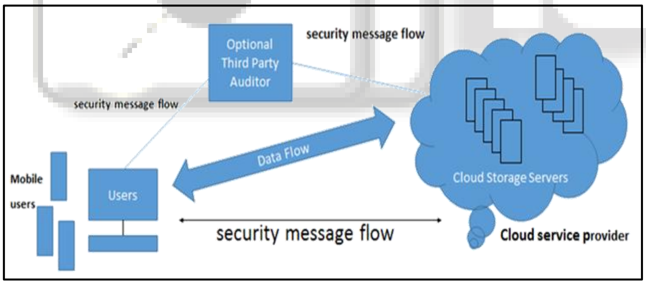

Fig. 1: Proposed system

Proposed system consists of mainly three entities.

1) Data owner – It is entity who want to store his data in cloud.
2) Cloud Service Provider (CSP): A CSP is entity, who has significant resources and expertise in building and managing cloud storage servers.
3) Third Party Auditor (TPA): An optional TPA, who has expertise and capabilities that users may not have, is perform integrity check on data stored in the cloud on behalf of the users upon request.

The information (data owner) performs varied operations like rending the file to blocks, encrypting them,

And then that blocks stored on the cloud server. Data owner has to generate digital signature on each block. TPA will also calculate hash value on the blocks stored on cloud server and it will also generate digital signature on it. TPA performs the integrity check by requesting digital signature from the data owner. It checks if both signature matches or not. Give notification to the data owner. This auditing theme makes use of Blowfish algorithm for encryption, Token pre-computations for generating the tokens (Hash) values and DSA signature for digital signature calculation.

IV. Conclusion

We investigated the matter of information security in cloud data storage that is essentially a distributed storage system. We propose security model for cloud information. The user information is split into blocks and so keep within the encrypted format once generating the Hash price within the cloud storage, thus confidentiality of knowledge is get maintained. The TPA (Third Party Auditor) can check the Integrity of the info upon request of the consumer by confirmative each the digital signatures. It solely checks whether or not the keep data is tampered or not and informs concerning it to the user. Privacy conserving and public auditing for cloud are often achieved by employing a TPA. All the modules within the system are enforced to develop an efficient auditing scheme. In future, we'd like to perform information dynamic operations on information.

References

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

[2] IK Meenakshi and Sudha George. Cloud Server Storage Security using TPA. International Journal of Advanced Research in Computer Science & Technology (IJARCST) ISSN: 2347-9817, 2014.

[3] Jadhav Santosh and B.R nandwalkar. Privacy Preserving and Batch auditing in Secure Cloud Data Storage using AES. Proceedings of 13th IRF International Conference, ISBN: 978-93-84209-37-72014.

[4] Tejaswini, K. Sunitha, and S. K. Prashanth. Privacy Preserving and Public Auditing Service for Data Storage in Cloud Computing. Indian Journal of Research PARIPEX,2(2), 2013.

[5] Cong Wang, Sherman SM Chow, Qian Wang, Kui Ren, and Wenjing Lou. Privacy Preserving Public Auditing for Secure Cloud Storage. Computers, IEEE Transactions on, 62(2):362375, 2013.

[6] CongWang, QianWang, Kui Ren, Ning Cao, and Wenjing Lou. Toward secure and dependable storage services in cloud computing. Services Computing, IEEE Transactions on, 5(2) :220-232, 2012.

[7] Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou. Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing. In INFOCOM, 2010 Proceedings IEEE, pages 19. IEEE, 2010.

[8] [8] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, and Jin Li. Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing. Parallel and Distributed Systems, IEEE Transactions on, 22(5):847-859, 2011.

[9] Solomon GuadieWorku, Chunxiang Xu, Jining Zhao, and Xiaohu. He Secure and efficient privacy-preserving public auditing scheme for cloud storage. Computers & Electrical Engineering, 40(5):1703-1713, 2014.