



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

A Shared Authority based Data Integrity using Multiple TPA's in Cloud

Ashish Gondkar¹, Sujit Solapure¹, Vinaya Ghorpade¹, Priyanka Awate¹, Sunil Ghadge²

Under Graduate Student, Department of Information Technology, Trinity College of Engineering and Research,
Pune, India¹

Assistant Professor, Department of Information Technology, Trinity College of Engineering and Research,
Pune, India²

ABSTRACT: Cloud computing is novel paradigm in information technology. This approach involves methods that forward services to users on demand via pay -as -you- go. Cloud computing can reduces computation and communication cost. Cloud storage allows user to remotely out source there data to the cloud , this form of storage introduces new security challenges. Most proposed schema for data integrity verification uses multiple third party auditor instead of single third party auditor. Here we propose a new scheme for securing data integrity via multiple third party auditor based mutual authentication to increase the security.

KEYWORDS: cloud computing, TPA, daIta integrity.

I.INTRODUCTION

Cloud Computing are used for collecting, storing and sharing the huge amount of data using third party auditor .Cloud computing is a technology, where we can store and retrieve of our data at anytime and anywhere with the use of internet . Cloud computing offers users several benefits, such as high flexibility when using the cloud and the elimination of the need for expensive computing hardware and software in cloud computing, cloud providers host the data and applications for cloud users. Cloud is a most important part for securing huge amount of data for organization using third party auditor.

Some users uses a third party auditor(TPA)to help a user verify the data using cloud service provider (CSP)because TPA has knows the some algorithms and some concepts for handelling the data.The Single third party auditor may degrade the system performance thats why multiple third party auditor is used to overcome this problem.

Our work also contain several security features such as confidentiality, maintenance of privacy, and efficiency. security is a important challenge for cloud .A major challenge is data storage,which is highly significant in cloud computing .our work also uses digital signature and encryption algorithm for handelling the data. this paper shows that data is securely storing on cloud using TPA's.

II.EXISTING SCENARIO

Existing system is having only one TPA for handelling the overall process on the cloud. This TPA uses a single key in encryption and decryption technique. if the key is stolen then data is lost and hacker can hack the all data.so this is a insecure method for storing the data on cloud using single third party auditor (STPA).

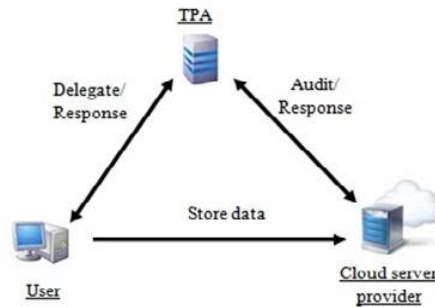
This method is cheap,less efficient and low cost ICT (Information Communication Technology) for data. Data can easily hack by the hacker and it is loss of user.So,our proposed new scenario uses multiple TPA's for storing the data on cloud.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017



III. PROPOSED SYSTEM

Our proposed scheme includes four main algorithms: KeyGen, SignGen, ProofGen, and VerifyProof. The KeyGen algorithm is used by the client during the setup process to generate the public and private keys. The SignGen algorithm is also run by the client during the setup process to generate the verification metadata, which may consist of the message authentication code, signatures, or other related information to be used for later auditing. The ProofGen algorithm is run by the CSP to generate the proof of data storage correctness. Finally, the VerifyProof algorithm is run by the TPA to verify the data storage correctness proof, which was generated by the CSP.

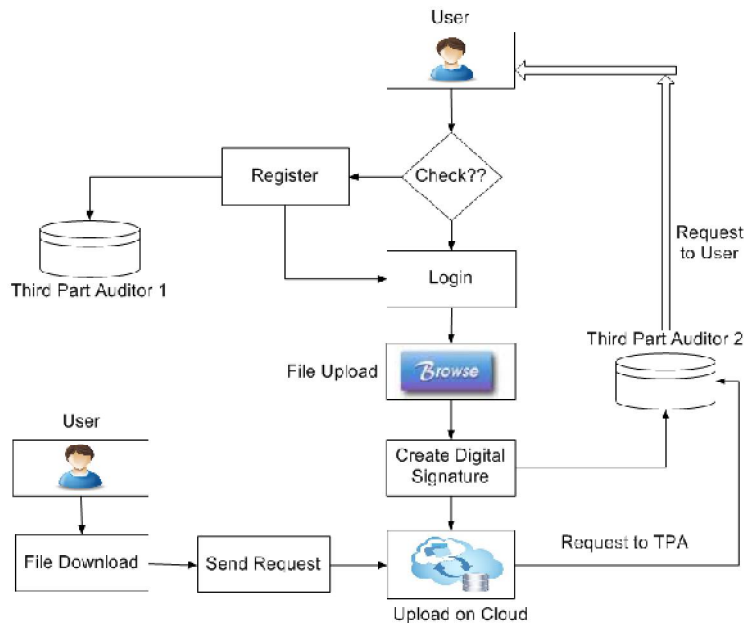


Fig. System Architecture

International Journal of Innovative Research in Computer and Communication Engineering

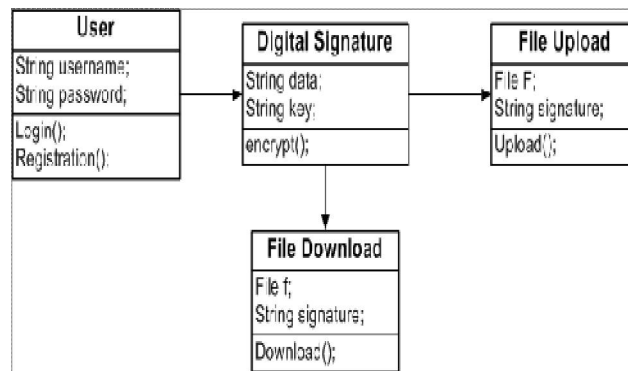
(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

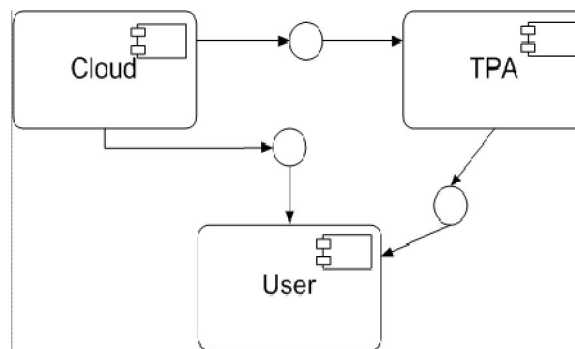
IV.UML DIAGRAMS

A. Class Diagram



The Class diagram shows the conceptual view of the overall system. The Main elements of the system are User, Digital Signature, File Download and File Upload. Class diagrams can also be used for data modeling. All the members of all the classes and methods are public.

B. Component Diagram



This diagram shows how the different components of the system are binded to each other. It connects different interfaces with each other. Here we can see the cloud component is connected to the TPA , User and TPA can send data to the cloud. Server is connected to the database, which handles the data load of the system.

V.PROJECT OUTCOME

A shared authority based data integrity using multiple TPAS in cloud data storage propose a new scheme for securing data integrity via a multiple third party auditor sbased mutual authentication to overcome the aforementioned limitation high-levelsecurity.This technology also includes several security features,such as confidentiality, maintenance of privacy, and efficiency. Cloud computing has several important security challenges. A major challenge stems from data storage, which is highly significant in cloud computing.

The technology that protect user data involve three entities that participate in the overall process flow: the cloud user ho wants to store data in the cloud , the CSP which manages and controls the data; and,the TPA, who verifies the data



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

as requested by the user and may perform operational requirements for the user. In this system, we provide a robust security scheme for users to ensure the integrity of uploaded or downloaded data. This scheme applies the concept for large files to archive encrypted data in cloud storage. In this system, we propose a remote data-storage-correctness checking scheme to support public verifiability.

VI. FUTURE SCOPE

For future work experience with handling organizational or large amount of data as indicated that there are several technical challenges to be met in deploying a pervasive system. Additionally identify the user requirement and analyze the drawback of existing system.

VII. CONCLUSION

The data storage in a cloud server facilitates computing in the cloud. However, users lose complete control of their data in remote storage. Consequently, unauthorized entities will certainly emerge in such a system. In this paper, we present a robust security scheme for users to ensure the integrity of uploaded or downloaded data. Compared with previous schemes, our proposed scheme involves a novel structure. We introduce a new approach to data integrity. MTPAs are employed to overcome the limitations of a STPA.

REFERENCES

- [1]. H. Liu, H. Ning, Q. Xiong and L.T. Yang, "Shared Authority Based Privacy Preserving Authentication Protocol in Cloud Computing," IEEE Transactions on PARALLEL AND DISTRIBUTED SYSTEMS VOL:PP NO:99 YEAR 2014.
- [2]. C. Wang, S.S.M Chow, Q. wang, K Ren and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Transactions on COMPUTERS, VOL.62, NO.2, FEBRUARY 2013.
- [3]. L. A. Dunning and R. Kresman, "Privacy Preserving Data Sharing With Anonymous ID Assignment," IEEE Transactions on Information forensics and Security, vol. 8, no. 2, pp. 402-413, 2013.
- [4]. X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Transactions on Parallel and Distributed systems. [online] ieeexplore.ieee.org/stamp/stamp.jsp?tp=arnumber=6374615, 2012.
- [5]. C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," IEEE Transactions on Services Computing, Vol.5, no. 2, pp. 220-232, 2012.
- [6]. M. Nabeel, N. Shang and E. Bertino, "Privacy reserving Policy Based Content Sharing in Public Clouds," IEEE Transactions on Knowledge and Data Engineering, [online] ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6298891, 2012.