DATA INTEGRITY PROTECTION IN CLOUD COMPUTING A FORMIDABLE TASK, ESPECIALLY USERS

B. Chinna Babu[1], G. Murali[2]

[1]*M.Tech, JNTUA college of Engineering (Pulivendula), Andhra Pradesh, India*
[2]*Asst.Prof. , (HOD), JNTUA college of Engineering(Pulivendula),Andhra Pradesh, India*

Abstract

The cloud storage is the one of the large data storage. It is used for security for the stored data, especially users. Cloud is the centralized computing is called cloud computing. Cloud computing provides the security from the hackers. Using cloud storage , users data or information store on demand high quality applications and services. It gives the original data for the register users on without loss store data in cloud storage. Here we have to use Third party auditor(TPA) for given information to the users any type of modification can include our data. It provides different applications and services to use a shared pool of configurable computing resources. A Third Party auditor(TPA) is to check the integrity of another data add or not in user data. Third party auditor is to just a mediator for users, like a informer. In this paper, we propose a secure cloud storage system by supporting public privacy-preserving auditor service to the user data. so, here enable the TPA performance for multiple users efficiently. We motivate the best knowledge and our best scheme. The first support scalable and efficient public auditing in cloud. It introduce secure and efficient TPA, the auditing process should takes in no new another user data privacy. In this project a propose scheme is highly efficient.

Keywords-- *data Integrity, cloud storage, public auditing.*

----------***----------

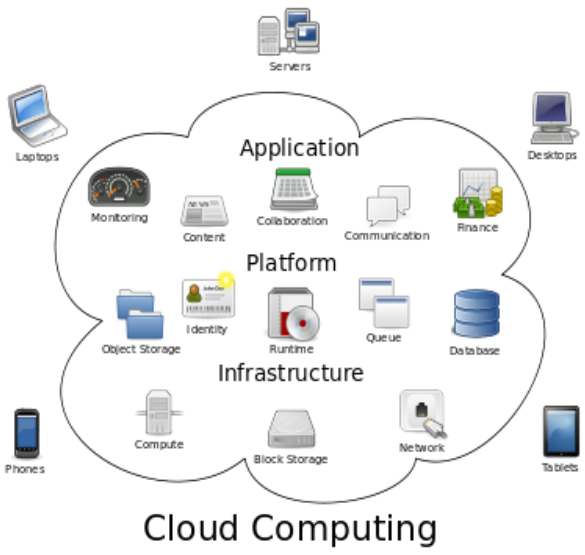
1. INTRODUCTION

The generation of cloud computing is to deliver information of users. It is both hardware and software computer resources are delivered as service on a network. Cloud Computing provides information, software and any media. It controls both Internal and External threads for user's data.

As users no longer physically possess the storage of user data and cannot be directly adopt a new treated cryptographic primitives for the data large storage, data processing, Operating systems, security protection. all the data simply Network and various types of structures, these are specified future involved in centralized services called cloud storage server. Here we have access to downloading for its integrity confirmation is not a realistic solution due to the expensiveness in I/O and show cost across the network. it is frequently presents the keywords, tabs and other media insufficient to detect the data damage only when resources. cloud is a symbol of abstraction in a data accessing ,it does not give users rightness complex network location. Cloud computing guarantee real data words for those un accessed provides a true data remote services with user data and too late to recover the data loss or damage.

So, cloud is the very high confidential and of old papers totally. The literature survey details effectively. Thus, the project may, involve based for the project helps in contrasting and relating on the Cloud server under the third party several procedures, algorithms are also different auditor(TPA).

To overcome the weaknesses of deal, over from the review in the survey. Here various routs that have executed in the research. clear and maintenance of attackers the future plan is definitely. The bellow diagram shows the structure of cloud computing.



1.1 Applications

Mainly containing applications are content, collaboration & communication between the server. These are performs individually together for the server.

1.2 Infrastructure

Infrastructure is the one of the main work maintainer in cloud storage i.e compute, block storage & network. However user information can be store in the storage in the cloud server. Which is using store and maintenance also security will be provide.

2. LITERATURE SURVEY

The survey of literature is references old algorithm and papers. Here we have refer for our development project based on this survey. It also helps and explains for in reporting summarization of old papers totally. The literature survey details for the project helps in contrasting and relating several procedures, algorithms are also different from the review in the survey. Here various routs that have executed in the research.

Study of Literature

Privacy MAC Based Solution

Privacy MAC Based verification provides user data using random data block to be authenticated.

- The cloud server online load is increase to download and upload operations in a not specified single system.
- The Third party wants awareness of user keys and over the cloud server network for verification.
- It works only for static data, and dynamic data not consider for these process.
- Data message and calculation are due to multi keys huge amount complexity maintains in the cloud server.

Third Party Based Solution

TPA is to maintenance public auditing without retrieving data block efficiently. Public auditing requires and collected constant bandwidth. Possible to compute an total multiple users by third party based solution, which verifies a linear combination of the data blocks with single performance. Here user can be transfer the data to cloud, when automatically. Third party auditor is a just performer like mediator, then TPA is going to done for especially users.

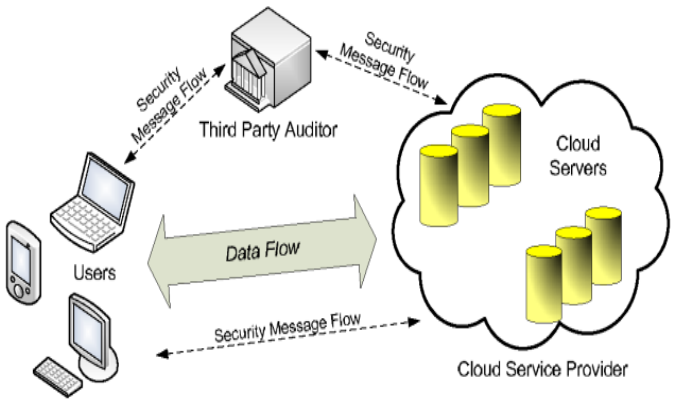


Fig. 1: The architecture of cloud data storage service

TPA can be access the data information, which is correct or not. This type of performance should be operate.

Cong Wang suggested for Privacy Preserving Public Auditing

The third party processing audit by enters privacy public auditing, to check the integrity of the real outsourced data stored on a cloud sever & third party auditing allow by Privacy Preserving, this auditing do without requesting for local copy of the data. Through this scheme, TPA can be audit the data and cloud data integrity privacy is maintained.

3. EXISTING & PROPOSED SYSTEM

3.1 Existing System

In the Existing system, the idea of public audit ability has been wished-for in the framework of ensuring remotely stored data integrity protection under security models and different system. The Public audit ability allows an external party, In additionally to the user, to prove the remotely stored data correctness. However, some type of the systems structure does not consider the privacy protection of user's data against external auditors. In this operation most of users can exposed the data auditors. In the cloud computing several problems access these protocols in computing. From the view point of protecting data privacy, the users, who own data and really TPA just for the user data storage informer security of users own data, Here users have to provide the security for the data in the cloud. In the manner existing system can be evaluate operation.

Disadvantages

- It cannot provide the security to the cloud server.
- Does not provide external security form the hackers.
- Under the cloud is more powerful reliable and effect able than personal computing devices,
- this devices facing the broad range of both external and internal threats for data integrity.
- These servers not give the multi users security at a time.
- Do exist various inspirations for CSP to behave unfaithfully toward the cloud users regarding their outsourced data status.
- Simply downloading all the user data for its integrity verification is not a practical solution, particular due to the expensiveness in Input & Output transmission cost across the network.
- As it does not give users correctness assurance is often insufficient to detect the data corruption only when accessing the data, for those un accessed data and might be too late to recover the data damage or loss.

3.2 Proposed System

In this project, To support effective handling of multiple auditing tasks, the multi users can access the number of times in the cloud. It provides the dynamic security for the user's data, from the user's data is sufficient and effective

resalable also. It Enhanced security and Fog Mitigating is secure data and perform to the cloud server. We another technique of fog security, it means to collect the correct information from the cloud server without loss users data. This technique achieves a privacy preserving public auditing in extended data. The main result is a multi-user setting system provides individual operation. Here we have to propose a multi-user system setting in the cloud server.

Advantages

Fog Security: Fog security provides a real data in the cloud, when a malicious attacker nothing but data can be protect from the hackers.

Public Auditability: Cloud servers gives areal data for the users without loss and allow the external party to verify the correctness of the cloud data on demand. The public auditing is the one of independent of user auditability.

Storage Correctness: The name itself tells the project provides on a real data in the cloud for the users, here no change user data in the cloud, after that this real information can pass the external processing.

Batch Auditing: The project is extended with multiple users auditing and secure efficient auditing capability to cope with multiple auditing operations from possibly large number of different users activities simultaneously.

4. MODULES OF THE PROJECT

System Model Module:
In this module, here we have to develop first four users show the operation in the cloud server.

Hacker and Third Party Auditor:
User: Generally user consist of both individual or single consumers and large groups. Users, who makes registration and remunerations amount to the cloud server and cloud server provides data to be stored in the cloud and really on the cloud for data and other calculation.

Hacker: Hacker is shown in the project, to extend the fog security from malicious hacking activities from hacker.

Cloud Service Provider (CSP): a CSP is also called administrator, who has significant resources and expertise in building and managing distributed cloud resources and storage servers, owns and operates live Cloud Computing systems.

Third Party Auditor (TPA): The TPA is external third party, it is the only a individual and independent operator for the users. It is also can inform the any changes in the stored cloud data. The capabilities and access the serve to make auditing of users access getting data.

TPA Module
In this module, we develop independent third party auditor external TPA. External Third Party Auditor(TPA), making the cloud storage publicly verifiable. However, as pointed out by the recent work, to securely introduce an effective TPA, the auditing process should bring in no new towards user data privacy.

Privacy Preserving Module
In this module, we develop a privacy preserving security as a secure cloud system, here we confirm that the external third party cannot derive users' data content from the information collected during the third party auditing process. The public auditing system for users, we motivate on user behalf the data storage security in cloud computing and provide a privacy-preserving auditing protocol for external dynamic auditing without copying and duplicate the users data. We are providing protocol or arrangement system visuals an external TPA auditor to audit user's cloud data without learning or copying the data content. To the best of our knowledge, we have to designed a new protocol structure is the first to support scalable and efficient privacy-preserving public storage auditing in cloud.

Batch Auditing
In this module, The batch auditing develops to enable TPA with efficient and secure auditing capability to cope with multiple access scheme auditing delegations from possibly huge number of different users simultaneously. Specially, our scheme reaches batch auditing where multiple performance auditing tasks with in the different users can be performed simultaneously by the TPA in a privacy-preserving manner.

5. CONCLUSION

In this paper, here we have to propose a privacy-preserving public auditing system for multiple user data storage in security in Cloud Computing. We use the linear random making and to warranty that the Third Party Auditor would not study any knowledge about the user data content stored on the cloud server during the efficient auditing process which not only eliminates the burden of cloud user from the deadly and possibly exclusive auditing task, but also alleviates the user's dread of their outsourced data leak. Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, we further extend our data for multi-user setting on privacy-preserving public auditing protocol, where the TPA can perform multiple performances for public auditing tasks in a batch manner for better efficiency.

ACKNOWLEDGMENTS

This work was supported in part by the US National Science Foundation under grant CNS-083, **Zero knowledge public auditing.**

The setup phase is similar to our main scheme presented. Here we present a public auditing scheme with provably zero knowledge leakage.

REFERENCES

[1]. 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.

[2] .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.
UCB-EECS-2009-28, Feb 2009.

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

[4]. 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. UCB-EECS-2009-28, Feb 2009.

[5]. 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.

BIOGRAPHIES

Mr. B. Chinna Babu, P G Student, Department Of Computer Science, JNTUA College of Engineering, Pulivendula, Kadapa(Dist.), A.P. India.

Under the guidance of:
Mr. G. Murali, M. Tech. in CSE, Assistant Professor, Head of the Department of Computer Science, JNTUA College of Engineering, Pulivendula, Kadapa(Dist.), A.P. India.