Melange Publications
International Innovative Research Journal of Engineering and Technology (IIRJET)
Volume 1, Issue No. 1

# An Efficient Auditing Technique for Secure Cloud Computing Using Asymmetric Cryptographic Algorithm

C.Ashwini[1], J.Muthu[2], B.Karthikeyan[3], V.Vinith Raj [4]

[1]*Asst.Prof, Dept. of Computer Science and Engineering, Karpaga Vinayaga College of Engineering & Technology.*
[2] *B.E Students, Dept. of Computer Science and Engineering, Karpaga Vinayaga College of Engineering & Technology*
[3] *B.E Students, Dept. of Computer Science and Engineering, Karpaga Vinayaga College of Engineering & Technology*
[4]*B.E Students, Dept. of Computer Science and Engineering, Karpaga Vinayaga College of Engineering & Technology*

***Abstract*-The intensification of Cloud computing is increasing in business and IT organization. Rapid growth of Cloud moves all kind of database to the datacenters. An online providers contributes to keep users files, photos, email and other backup files in cloud. To guarantee that protect data of customers and maintain integrity cloud auditing is essential. Information present in datacenter may not be reliable. It reduces inducement of rely on online services. Third party auditing is essential in auditing online services. It estimates the customer risk and increases the efficiency. Using internal and external auditing inducing the cloud service provider and maintains data authentication. It improves the truthfulness of data and helps to prevent from data loss.**

***Keywords- Auditing, Access Control, Authentication.***

## I.INTRODUCTION

Cloud computing provides online based service based on user demand. It can provide computing service through network. Cloud is pay-per-service, based on demand and usage user has to pay. It could provide services like software, platform and infrastructure [1]. The cloud platforms are Amazon Elastic Compute Cloud (EC2) and Amazon Simple Storage System [2], Microsoft Azure [3], and Google App Engine [4]. Some Cloud storage providers are Dropbox, Google Drive, Sky Drive, etc. In future, a growth of cloud computing techniques moves many business into the cloud [5].

Cloud storage is used to preserve data into the cloud for data security. Owing to traditional cryptographic method, to protect security of cloud environment cannot be directly implemented [6]. A data security problem is solved by using third party auditor to measure and represents risk of cloud storage service based on user's request. In traditional method, third party auditor is functioned by an institute not to cloud service provider. It produces wastage of resource and takes slow response user request. At the same time, slowdown performance of the third party auditor may causes uncertainty to the system.

In this paper, third party auditor is working to audit the data security of cloud. Moving the function of third party auditor into cloud create smore trustful to data and it provides security. It reduces response time and bandwidth allocation between auditor and cloud. So, the complexity of cloud is also reduces.

## II. AUDITING

Auditing is the process of gathering and checking proof regulates whether a system protect their resources, maintains data integrity, complete its business aim efficiently and effectively. A trusted Third party auditor is audits the cloud environment. Service Level Agreement is maintained between customer and cloud service provider. An auditor must know about service level agreement. With proper security, auditor can check provider can able to work with multiple users without information leakage [7].

Auditing can be classified into external auditing and internal auditing. Using externally existing interface, quality of service can be calculated by an external audit. It also predicts the future output from the available limited input samples. To confirm whether the objective of service level agreement are meets the structure and methods present within the service are estimated by an internal audit.

To provide any online services both external and

internal audits are required. External audit uses only the past activities so it uses internal audit to predict the future risks and problems. By using external audits result, internal audit are checked whether is working properly or not [8].

## III. Problem Statements

The conventional architecture for cloud is shown in Figure 1.

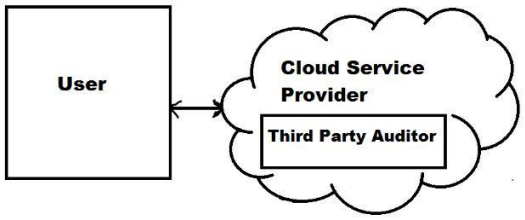


Figure 1. Architecture Diagram

It consists of users, cloud service provider and third party auditor [9]. Users are active candidates. All the information located in the cloud and trusts the cloud for data maintenance. Any individual consumer and business organizations can be the users.

Cloud service provider allocates storage space resources to users. Service provider has knowledge to build and manage storage server. Based on the users' request, third party auditor is to expose risk in cloud. While storing large size file, user can relieve from storage burden.Data is stored in the cloud should be safe. Cloud service provider provides storage and resources through online. Third party auditor is regularly checks data access control regularly in online.

The proposed architecture for cloud storage has two parts: Users and Advanced cloud service provider. It is represented in Figure 2.

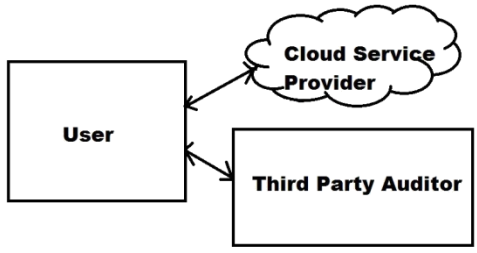


Figure 2. Proposed Architecture

The difference between our architecture and conventional is third party auditor is combined with cloud service provider.

In this work, we assume that user and advanced cloud service provider has point-to-point communication channel and it resist from attacks. User can add, modify, delete and append their information in cloud. Data present in the cloud is reliable against malicious data modification, Byzantine failure and server colluding attacks [10].

To provide data security to information stored in the cloud has to design a mechanism for move auditor function into cloud. It achieves the following goals: Access control safety, Authentication data trustful in cloud storage servers and Authentication information efficiently in use. Access control safety gives privilege to communication between user and service provider.

Authentication data trustful is used to prevent authentication to information present in cloud. To transfer the information between users and to makes provider works effectively.

## IV A Novel Third Party Auditor Scheme

Third party auditor moves their function into cloud service provider to achieve data independent and security it uses an asymmetric cryptographic algorithm like RSA and Bilinear Diffie-Hellman [11]. In advanced cloud service provider, RSA algorithm is used to encrypt data stored in it. For exchanging the keys Bilinear Diffie-Hellman is used. RSA is asymmetric cryptographic method. It can be used for long keys and it kept up-to-date information to protect our data. Bilinear Diffie-Hellman key exchange algorithm allows to two people can exchange their secret key without no prior knowledge about each other in an insecure communication. In front of each file packet message header is added with it. By using a message header, both user and service provider can be able to communicate directly. The cloud server can add and update the information of the user through it.

| Notation | Description |
|---|---|
| PK | Public Key |
| SK | Secret Key |
| CUID | User's identification in certain server |
| SID | Unique identification for server in Cloud |
| H-x | Message Header of message X |
| SIDCC | Check code of SID |
| TTL | Time To Live of the H-x |
| CUIDCC | User's identification in certain server |
| HCC | Check code of H-x |

Figure 3. Notation used in our scheme

Each user has uses a pair of key that can be exchanged between user and cloud service provider by using Bilinear Diffie-Hellman key exchange. Data packet can be encrypted with RSA algorithm. The following notations are used in message header.

The architecture has two parts. One is interoperation between the users and cloud service provider and other is cloud service provider and trusted third party.

**1. Interoperation between the users and cloud service provider**

Setup: Initially user communicates with one of cloud service provider in cloud for storing information. Cloud service provider receives request and generate a couple of keys for individual user should be distinctive. The couple of keys are PK, SK and CUID used for secure authentication.

New File Packet: Initially create message header for uploading data file on cloud and encrypt original data with the help of PK and SK. Encrypting file does not contain any message header (H-x).

| | | | | | |
|---|---|---|---|---|---|
| SID | SIDCC | TTL | CUID | CUIDCC | HCC |

Figure 4. Message Header Format

File storage: Finally cloud service provider checks whether received data contain any message header and capturing SID information. The purpose of SID information helps to communicate with the cloud service provider. SID information not available server will avoid the user request. And further communication cannot be carried.

**2. Interoperation between the cloud service provider and trusted third party auditor**

Setup: Using individual SID each cloud service provider can communicate each other. User key is updated and distributed by cloud service provider. Third party auditor is responsible for data present in cloud.

Key and information exchange: User download any file from cloud service provider then an auditor checks HCC, SIDCC and CUIDCC. If all details are correct then it return the information to user. Otherwise, it discard the user request.

## V. Analysis of Proposed Scheme

Analysis of performance and security with following properties

1 Access control: By using authentication module, only authorized people can access the function of other modules. This module is operated based on user request.

2 Authentication data trustful: Information stored in the cloud can be evaluated only by auditor.

3 Authenticate efficiently: H-x in message header is used to send user request. It result shows valid authentication information.

sk represents total audit time per individual tasks. Task 3 denotes the invalid task.

It shows the comparison of individual auditing, batch auditing by reducing the cost as 12% and 15% of individual task time is kept for block is 300 and 460.

## VII. Conclusions

This paper helps to designing a third party auditor technique in cloud. It identifies data security problem in cloud for data storage. It will decrease the difficulty of the cloud and provide secure access control to information. RSA and Bilinear Diffie-Hellman methods can be used to solve data trustful and authentication problem. Besides, designing a message header helps to decreases the cost. Privacy and accountability can be achieved by giving privilege to user. The third party auditing technique is efficient in secure cloud environment.

Third Party Auditor should audit cloud user file. It is guarantee that TPA does not reveal data to others. It also alleviates the users' fear of their outsourced data leakage. In the future implementation extend auditing for multiple users in same time. That result will give better efficiency.

The client file has been modified to clients does not show what modification is done in client file by server, if the user need to know the modification only way to download the corresponding file. In future will show what modification is done in the client file by server to the client. The user can view their file details such as upload files, download files. Modification files can be viewed through accessing with the help of mobile or email.

## References

[1] M. Armbrust, S. 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.

USB-EECS-2009-28, Feb 2009.

[2] Amazon Web Services, online at http://aws.amason.com.

[3] Microsoft Azure, Online at http:// www.microsoft.com/ azure/

[4] Google App Engine, Online at http://code.google.com/appengine/.

[5] Shucheng Yu, Cong Wang, KuiRen, Wenjing Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", IEEE INFOCOM 2010 Proceeding.

[6] M. R. Tribhuwan, V. A. Bhuyar, ShabanaPirzade, "Ensuring Data Storage Security in Cloud Computing through Two-way Handshake based on Token Management", IEEE ARTCom 2010.

[7] J. C. Mogul, "Operating Systems Should Support Business Change", In Proc. HotOS X, June 2005.

[8] Mehul A. Shan, Mary Baker, Jeffrey C. Mogul and Ram Swaminathan, "Auditing to Keep Online Storage Services Honest".