International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 4 475 - 479

Privacy Preserving For Secure Cloud Storage

Miss. Ankita R. Makode[†]
Student, Computer Science and Engineering,
P.R. Patil COET, Amravati,
Maharashtra, INDIA. +

Prof. V. B . Bhagat [‡]
Assistant Professor, Computer Science and Engineering,
P.R. Patil COET, Amravati,
Maharashtra, India. ‡

Abstract:- Cloud Computing is one of the large and essential environment now a days to work for the storage collection and privacy preserve to that data. Cloud data security is most important and major concern for the client while use of the cloud services provided by the different service providers. There can be some major security concern and conflicts between the client and the service provider. To get out from those issues, a third party auditor uses as an auditor for assurance of data in the environment. Storage systems for the cloud has many fundamental challenges still today. All basic as well critical challenges among which storage space and security is generally the top concern in the cloud environment. To give the appropriate security issues we have proposed third party authentication system. The cloud not only for the simplified data storage but also secure data acquisition in cloud environment .At last we have perform different security analysis as well performance analysis. It give the results that proposed scheme has significant increases in efficiency for maintaining highly secure data storage and acquisition. The proposed method also helps to minimize the cost in environment and also increases communication efficiency in the cloud environment.

Keywords: *Cloud Computing, Storage technology, security, database, storage management*

*****

I. INTRODUCTION

The Cloud computing is very fast growing and evolving IT service model. It finds way into the business world for growth and development. Use of cloud differs from one person to another person in certain ways. The technological view is simply common in environment. In Cloud computing moving services and computation data to different parts. It is location transparent. [1] Cloud provides the function of deployment scalable resources in environment. Cloud computing provide different application and services without worrying actual cost of the actual infrastructure. It helps in business to avoid capital and operation expenses. The basic advantage is user need to pay for what he had used. It helps to save money which can be use for more services. [11] Cloud computing different from traditional approaches. In the traditional there were lot of supporting needed for setup like servers and devices for storing. There are many security concern with the data and servers. Cloud has no secure guarantee at all time. Cloud provide services as IAAS,PAAS,SAAS. All the tasks are mainly important with different situations. At the point of concern all the categories help in growing world. [4].

1 Infrastructure As A Service

Many cloud provider support virtual servers. It gives separate IP address to each user in environment. Customer pays only what he had used. Like Dish TV is an example.

2 Platform As A Service

It is development tool and software provided by server on cloud. The developer makes own application which run on cloud API considering many constraints. Now Google Apps is the most usable platforms as provider in today's cloud environment [5].

3 Software As A Service

The provider allow user to use his application as he want. Interaction happens with user interface. In the world applications like Gmail and yahoo. In the environment the benefits of cost not more clear. Each time provider come up with new model [12].

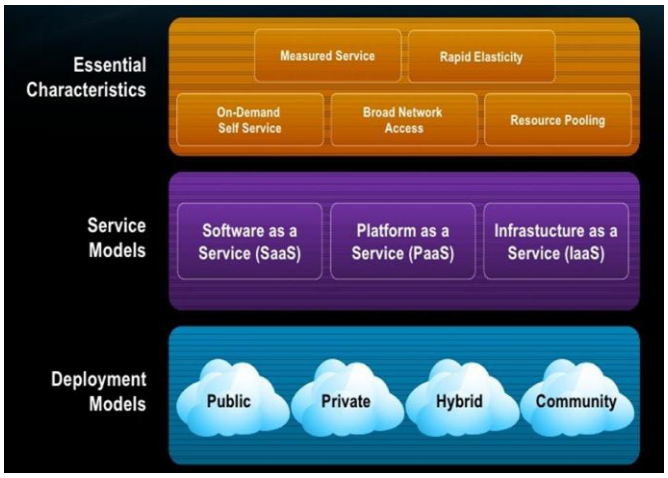


Fig 1 cloud computing

II. LITERATURE SURVEY-

A[1] challenge is to secure the specific data and also to built highly efficient architecture in hole system. Also to allows batch processing during auditing process.

Author put analysis on the system and proves that system is provably secure with implement but User's files are not encrypted on some open source like cloud storage systems. In

paper concept is homomorphic linear authenticator is used. At same time random masking techniques is used. In system TPA has no knowledge about content stored on the cloud server. At end of author performed an extensive analysis that proves the proposed schemes is secure and highly efficient Author put analysis on the system and proves that system is provably secure with implement but User's files are not encrypted on some open source like cloud storage systems. In proposal main focus on eliminate burden of user in environment. Helps from more difficult work and possibly the expensive auditing tasks as perform .Author put proof that system for data storage with security. It also prevent outsourced data mishandling or leak here. The result shows that multiple tasks in batch to get efficient auditing. It reports better output. Author made with the use of Amazon EC2 cloud for demonstration.

B[2] challenge of this paper was to maintain data correctness of data and design the system in a way that it will be highly efficient. Also it is resilient against the attacks like the malicious data modification attacks. Here also black hole attacks, Byzantine failure and also Server colluding done with implementation provable.

Author's analysis about this method shown that system is built to maintain data correctness in all tasks .This scheme also proves that system is provably secure for data but User's files are not encrypted on the some open source cloud storage systems. In the paper author explained the Cloud storage and process to remotely storage of data in particular cloud. The on demand high quality cloud computing applications without the more burden of any local hardware with fault and also software management. He had explained the benefits of the same on the system.

In a paper author proposed a flexible or a movable distributed storage integrity auditing mechanism at different level, which utilizes the homomorphic token. The second scheme was distributed erasure coded data scheme. Authors scheme help to audit with minimum communication as lightweight process. Main concern is correctness in cloud data. The system has efficient and resilient feature against different attacks.

C[3] Challenge was to ensure the data correction, storage correction and also error localization, storage management over the cloud storage. Authors implementation shown that system helps to ensure in data correction and storage. It also error locater but anyone can modify the data files. Mainly when they are internally consistent in environment. Here author had not used any encryption scheme.

This is effective as well flexible distributed scheme with dynamic data support. It keep accurate data in cloud without any misplace. The proposed method helps data correcting code in a file distribution. It provides guarantee data decency in all time.

It reduces communication, storage overhead when compare with replica based technique in cloud. Technique used homomorphic token which uses distributed verification of the erasure coded data in storage. The system is efficient and also the resilient against different attacks also at server collusion. The storage consistency increases .

D[4] challenge was to supports dynamic operations. Batch auditing should be done. Proposed scheme of the paper provides consistent place to save a valuable data and documents but owner's files are not encrypted on an open source cloud storage systems in environment.

Author has studied about the data owners and data consumers and also their access privileges and basic security challenges that come with cloud computing over the storage. The data integrity done on cloud with auditing. Some existing remote integrity checking is explained. It serves for static data management system. This is not sufficient because data on cloud always dynamic.

In the proposed system an authors explained auditing protocol. He makes own protocol and design framework. He proposed an efficient auditing protocol which helps secure data. They extend their auditing protocol which support to data dynamic operations. Further they work for batch auditing .This is done without trusted user.

III. PROPOSED SYSTEM

In paper we proposed different architecture for cloud environment and also TPA. Result shows effective and flexibility of scheme. It supports dynamic data to confidante correctness of user's data over the cloud. Third party authenticator, who has the expertise in auditing and also authorities that users data, may read only operations. It is trustful and exposes the risk on cloud. Cost is very less.

Fig2. Architecture diagram[9]

 ISSN: 2321-8169
475 - 479

We propose a new method for the auditing. It support for batch auditing also. At the multiple users over cloud so privacy preserved . TPA shows data is secured or not under the proposed model. TPA works without any knowledge about data to modify over cloud. It shows the correctness of data without copy of data or replica We ensured TPA had only read the data over cloud cannot modify. At the same time method is flexible and effective. It works for dynamic data auditing .It guarantees that correctness of user data on cloud. Our goal is to minimize the cost over cloud. For this we will be using an effective encryption technique to provide data security on data storage. [9] As shown in fig 2 there are mainly three actors data such as tpo,hr and student .

All of them have different tasks. The admin who approve tpo and hr. Tpo approves all the student. Admin also approve TPA i.e. third party authenticator who performs all batch auditing .Main moto of TPA is to handle the security issues. It gives assurance of correctness of data in the cloud. With use of TPA system provides mainly effective users data and the correctness of it. It takes very less communication time.

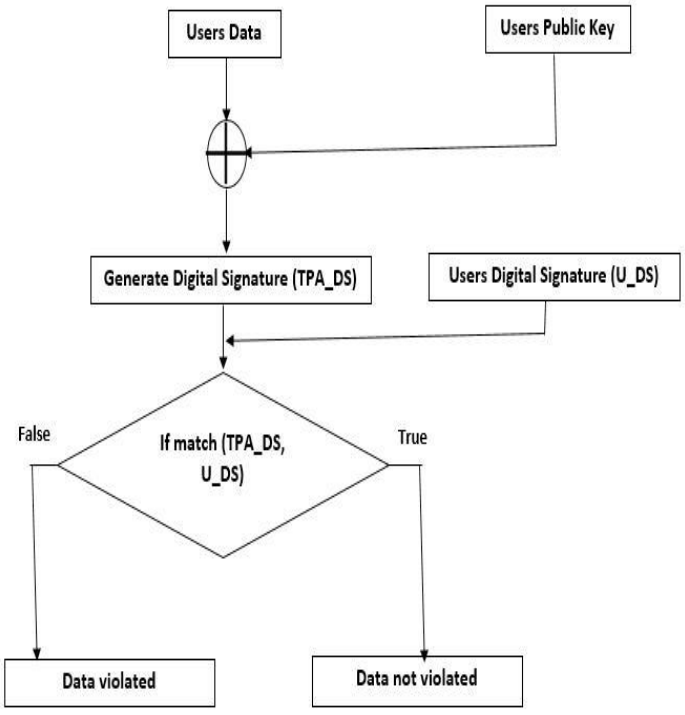


Fig 3 : TPA

Many years involved in cloud computing which gives experience as massive growth in the business industry. Our aim is to build a different TPA which should provide more security service. Our TPA should be trusted; TPA would lead to providing only security services. Also achieve and provide the security to data in public domain cloud by focusing on important issues Integrity and Privacy

As shown in fig 3. A user generates his signature with a use of private key. It stores valid signature and user data on the public cloud. TPA generates its own signature using user's public key. After generated it check whether signatures matched. If two signature not match then data has been violated else data integrity is maintained.

Detailing it further.

1. Constructing a Web portal which helps us to assure the data integrity verification of all system consumer data.

2. It helps to define access function for sharing data with security to get specific bandwidth of individuals.

V. RESULT

Cloud Computing is not only related with third party data auditor task. The data over the cloud frequently changes Authorized user also changes data in cloud. In the assurance of storage update frequently hence TPA tasks important. In this section we have evaluated graphs that depicts the performance of TPA.

Key generation

DS Generator

In this model we create the student data and private key equal to DS (insert into student detail table) and RSA algorithm are used key pair generation. And signature generated used in private key automatically integrity are provided confidently.

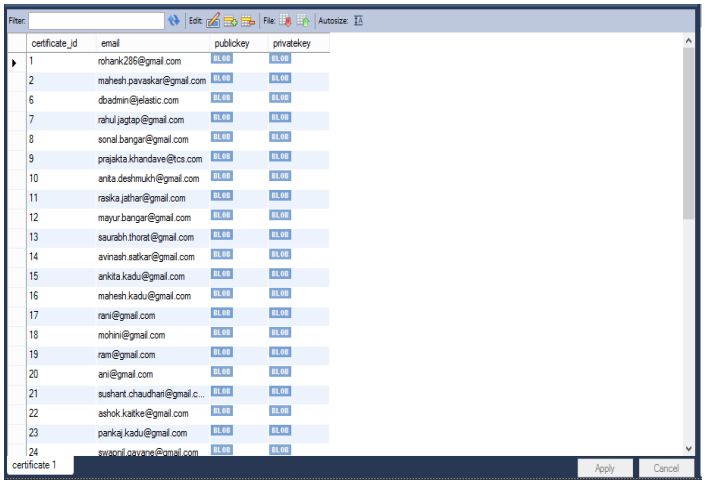


Fig 4. key pair generation

Registration

After registration when admin and tpo accepts then approval gets 1.This shows that the particular user can access further otherwise he cannot look into further accessing system. Registration detail shows a particular system and he has separate digital signature with the data. Each one has unique login id and password.

 ISSN: 2321-8169
475 - 479

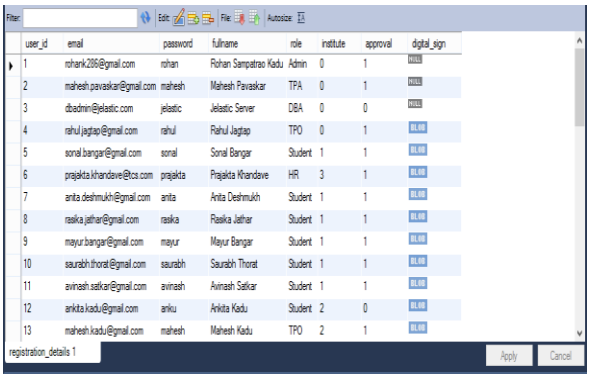


Fig 5. registration detail

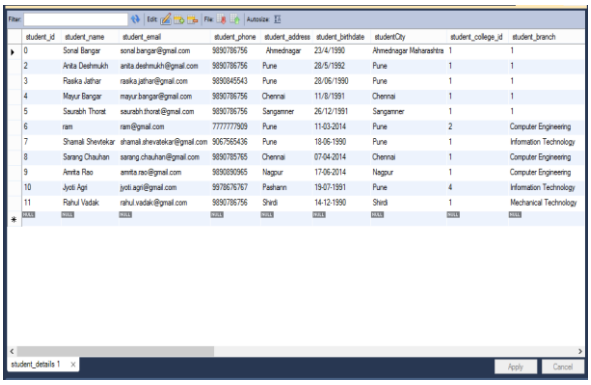


Fig 6. student detail

diagrams the student data stores. At the time of digital signature all data is used. Digital signature generate with the all data. It uses the users private key.

TPA verification

1. STUDENT VERIFICATION

In further the student data from student detail table and get student public key from certificate table. and student detail contain and student public key equal to third party auditor used in DS. Get old DS from student detail in table. And verify (TPA-DS AND OLD-DS) if the data are matched then verified, if else the data are violated and condition are satisfied.

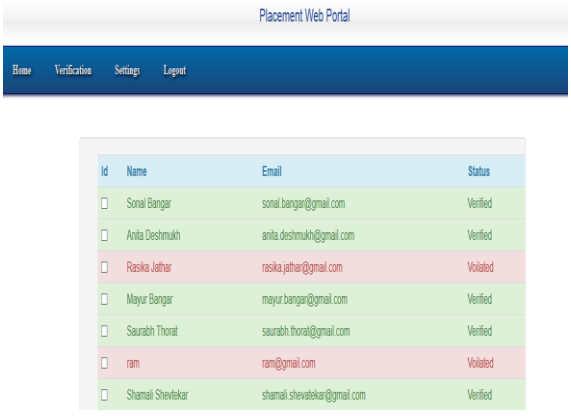


Fig 7. TPA data verification

2. DOCUMENT VERIFICATION

In further get student document from document details in table and used in student public key from certificate table. the student document detail and student public key are generated used in TPA-DS.

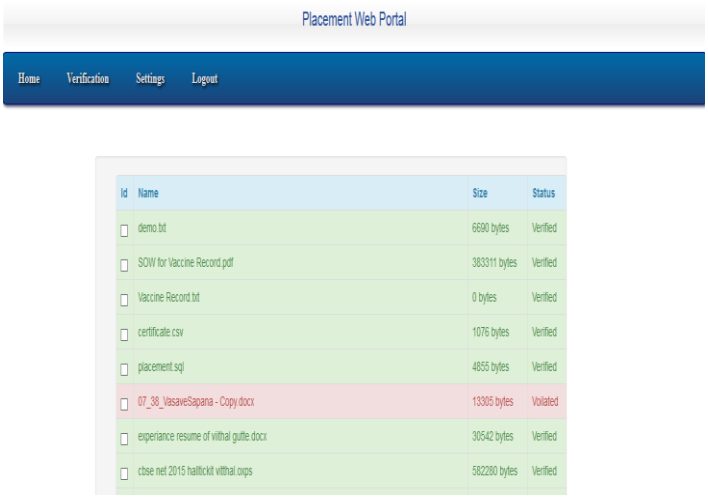
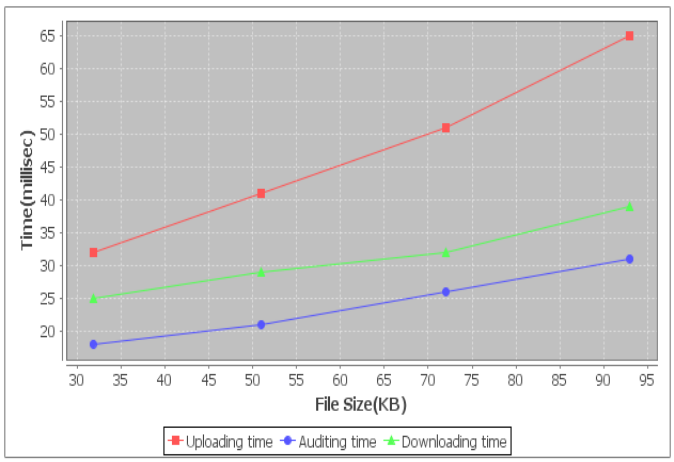


Fig 8. TPA document verification

It proves that the data is tempered by someone or not. If data get modified by unauthorized user then it gets violated. It shows in pink color. Authorize user can change data any times it's not violated. It always shows in verified format. All happens with same with document attached by student also.

In individual auditing the user can upload different size of data, as here we take four different types of user with their different file size TPA auditing time and download time is calculated as compare to both auditing time and its execution very fast.

File Size	Total time of upload file cloud (ms)	TPA auditing (ms)	Download time (ms)
31.80 KB	32	18	25
51 KB	41	21	29
72 KB	51	26	32
93 KB	65	31	39



IV. CONCLUSION

In many organizations main concern with maintaining and providing the security. We provide authentication, privacy and integrity for all users. TPA verifies data integrity and correctness. Digital signature for verification proves effective method. Burden on TPA minimizes with implementation. So that cost also get minimizes. Communication efficiency increases as the invalid response decreases. Each time TPA generate digital signature so that efficiency also increases. We proposed new scheme for Cost minimizes and increase communication efficiency in auditing. It helps in maintaining data integrity in cloud computing. It helps to eliminate the burden of cloud from tedious and expensive auditing tasks. It guarantee that no leakage of data in cloud. Considering the TPA perform different task concurrently. It handles multiple audit tasks at same time from many users. Our basic experiment conducted on jelastic public cloud instance.

REFERENCES

[1] Cong Wang, Qian Wang ,Kui Ren, Wenjing Lou "Privacy-Preserving Public Auditing for Secure Cloud Storage" IEEE TRANSACTIONS ON COMPUTERS, VOL. 62, NO. 2,FEBRUARY 2013

[2] Cong Wang , Qian Wang, Wenjing Lou, Ning Cao "Towards Secure and Dependable Storage Services in Cloud Computing" IEEE Transactions on (Volume:5 , Issue: 2) page 220 - 232 , 30 May 2012 .

[3] Cong Wang, Qian Wang, and Kui Ren "Ensuring Data Storage Security in Cloud Computing" Quality of Service, 2009. IWQoS. 17th International Workshop on ISSN 1548-615X

[4] Kan Yang and Xiaohua Jia "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing" ,IEEE Transactions on Parallel and Distributed Systems, Volume:24,2012

[5] B. Wang, B. Li, and H. Li, "Public Auditing for Shared Data with Efficient User Revoation in the Cloud," In the proceeding IEEE INFOCOM 2013, pp. 2904–2912 , 2013.

[6] "Dynamic Audit Services for Outsourced Storages in Clouds", IEEE Transactions on Services Computing, Volume:6 , pp.227 – 238, 2013.

[7] Sarfraz Nawaz Broh, "Design And Implementation Of A Privacy Preserved Off-Premises Cloud Storage", Journal of Computer Science 10 (2): 210-223, 2014

[8] Boyang Wang, Baochun Li and Hui Li, "Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud".

[9] vitthal gutte, Priya deshpande "Privacy preserving technique to secure cloud" IJSWS 15-153.

[10] Sathiya Moorthy Srinivasa Manonmaniam "providing dynamic audit services using homomorphism authenticators in cloud infrastructure" JATIT ISSN: 1992-8645 Vol. 67 No.3 30th September 2014.

[11] Michael armbrust (2010), "A view of cloud computing" Communications of the ACM, Volume 53, p-50-58.

[12] Cloud Security Alliance,(Dec 2009), "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1"https://mail.google.com/mail/?ui=2&view=bsp&ver=1qygpcgurkovy