RESEARCH ARTICLE OPEN ACCESS

Remote Data Integrity Checking with Third Party Auditor in Public Cloud using a Proxy Server

S. SwamyAyyappa*, Prof P.S. Avadhani**

*(Student, Computer Science and Systems Engineering, AU College of Engineering, Andhra University,Visakhapatnam
Email: sas118cct@gmail.com)

** (Professor, Computer Science and Systems Engineering, AUCollege of Engineering, Andhra University, Visakhapatnam
Email :psavadhani@yahoo.com)

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

Abstract:

Rapid development of cloud computing enabled many users to store data to PCS (public cloud servers). Enormous amount of data in cloud brought up the need of new security problems to be solved in allowing more clients process their data in a public cloud. At times the owner or the administrator fails to dispose its duty, upon the delegation that is handled by a proxy to process the data and upload them. Alongside the remote data integrity checking with third party auditor is also possible in public cloud storage. Proxy makes an internal communication with the client as well as end user in disposing the data with security. We propose a method of remote data integrity checking with third party auditor using IDPP (Identity based proxy server processing).This IDPP protocol is designed to enhance secure transactions and works on CDH (computational Diffie-Hellman) problem. IDPP can realize the remote data integrity checking possible upon the authorization by the administrator or owner.

Keywords **—Cloud Computing, Identity based Cryptography, Proxy, Remote data, Integrity.**

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

I. INTRODUCTION

Over-headed computation and communication techniques generated huge amount of data.

These data require more computation resources and greater storage space. Cloud computing realized the data centricity with independence to data. Major problem arises at providing security to data being uploaded and downloaded. Cloud computing applications provided with storage, computing, data security, etc. By using the public cloud platform, the clients are relieved of the burden for storage management, universal data access with independent geographical locations, etc. There increased the demand for cloud services with lowest burden of storing and accessing.

Cloud computing provides the users all the hardware, storage space and application software to access and process data. Cloud computing uses the internet and remote central servers for data and applications to organize this pattern. This is broadly categorized into two models.

- Deployment model
- Service model

Deployment model manage the entire cloud service. In Fact, they define the type of access to the cloud. There are 4 major deployment models. They are

- Public cloud model
- Private cloud model
- Community cloud model
- Hybrid cloud model

Service models are user centric and define the model of service to the consumers. This is application driven model and design is a subset of automating the resource.

They are 3 service models. They are

- Platform as a service (PaaS)
- Software as a service (SaaS)
- Infrastructure as a service (Iaas)

Cloud Computing has client infrastructure, Internet, application, services, Cloud runtime, Storage, Infrastructure, and security blocks in the architecture. Below figure shows the architecture of Cloud Computing

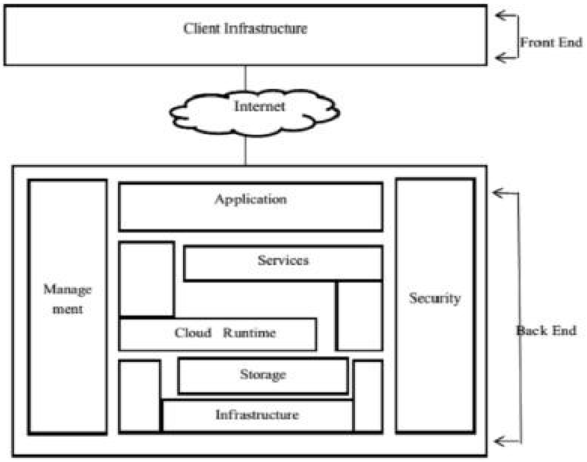

Fig. 1Cloud Computing Architecture

Security of the cloud refers to the data uploaded by the user in remote public cloud servers since the data stored is out of user's reach in terms of confidentiality, integrity and availability of data and service. Remote data integrity checking is an essential task in convincing the users of the cloud that their data is kept safe. Some special cases the actual user may be restricted due to administrational problems, and the same is realized by the Identity based Proxy server Processing (IDPP).

II. LITERATURE REVIEW

WentingShen[1]proposed a new model for the integrity check on the cloud computing environment and the use of TPA (Third party auditor) and digital signaturetechnique for achieving the integrity over cloud computing. They also brought up a new method of encrypting a file with the concept of "Sanitization". This is again broughtby[6] where the concept of "sanitizable signatures" was explained. The sanitizable signatures idea led to the development of sanitization.

B.Wang[4] discussed the "public auditing for shared data for efficient user revocation in cloud services". This analysed the concepts of users in cloud and their bound of access in a protected cloud environment.

All the services that cloud provide, basic security but identifying the user based on the ID and auditing of data in cloud have the efficient method of data handling.

BhalePradeepkumar[7] made the part of functional algorithms used in this paper in auditing and data integrity checking in cloud while all this is done by a third-party auditor. They used concepts like Third party auditor and MD5 algorithm in generating message block of 32-bit length key.

J.Sun[3] showed the cross-domain distribution of files especially the electronic health records and relevant permission access to use them.

This in return showcased the concepts that are used in WentingShen[1] that project on electronic health records and the partly encrypted files were pushed into the cloud using specified sanitization techniques. These both allowed us to think over the domain and area of research.

In this paper the proposed algorithm is using the entire cloud service with a proxy, both uploading and downloading alongside the auditing and data integrity checking. These concepts were motivated by many earlier published papers and the core algorithm in generating the keys was designed in showing a concreteness in development. This uses IDPP protocol depending on the Diffie Hellman key algorithm keeping in mind the CDH (computational Diffie Hellman problem).

III. MOTIVATION

The earlier proposed WentingShen[1] showcased a challenging problem of partial encryption with "Sanitization" and advancing the cloud usage. Further study at this process of upload and usage of data is clear and struck with at problem of initial uploader, which is the motivation for this paper.

Generally, all the users of the cloud upload their data to the public cloud and check the data integrity by Internet and direct applications provided by the cloud. If a particular user who is a head of any institution, by administrational problem couldn't reach the network, then the manager's transactions will be affected. To assist this sort of problems, he has to delegate his duty to a proxy. He even has to appoint data integrity mechanism to ensure the security of data. Our proposed model performs all required aspects at one platform.

IV. PROPOSED WORK

The security in a cloud is a remote task performing the connectivity between the cloud and its corresponding applications which are at default by the services of cloud computing. This paper is a combination of Remote data integrity check by a Third-party auditor and push and pull of data through an additional layer called Proxy server in disguise of actual manager to the cloud,which take multiple inherited functions namely,

- Identity - based encryption
- Remote data Integrity check

A. Identity – based Encryption

Identity based encryption takes the user's *ID* and with the help of a master key *MSK*, produces a unique Private key *Kp* with what the encryption process is done where message *MSG* is encrypted with *Kp* and the decryption process follows with the Ciphertext *C* being decrypted with the unique key *Kp*. Security is a great concern as the user parameters changes for every user and they are unique in generating the encryption and decryption keys.

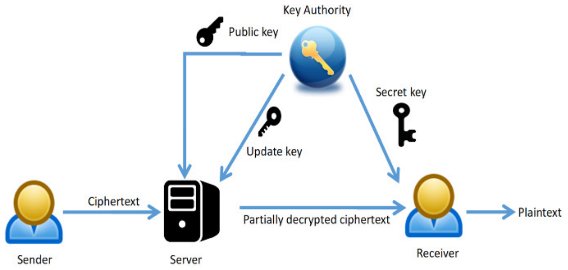

Fig. 2Identity based Encryption Architecture

B. Remote Data Integrity Check

Remote data integrity check is the non-local function, where the check is at the Cloud site maintaining the privacy of user files. The data in cloud has to follow the CIA - triad (Confidentiality, integrity, availability). The remote data integrity is realized by assigning the function of data integrity check. This entity takes in the user parameters including the file in encrypted format and regenerate the signature (Sig) and tries to validate it with the initially generated signature.

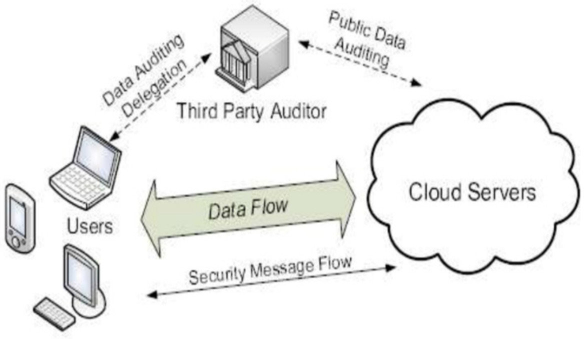

Fig. 3 Remote Data Integrity Check Using TPA

V. SYSTEM ARCHITECTURE

We propose an *IDPP* protocol to secure data in public clouds. *Bilinear pairings* technique makes Identity-based cryptography practically possible. This protocol comprises of five procedures:

- Set - parameters
- Seeking
- Proxy- key generation
- Labelling
- Proof

A. Set Parameters

Let *G1* and *G2* be two groups and *e* be the bilinear pairings which have the same order *q*. Let g be a generator g of the group *G1.* Two cryptographic hash functions are given below

$H: \{0,1\}^* \text{ --> } Z^*q,\ h : Z^*q \ X\ \{0,1\}^* \text{ --> } G1$

B. Seeking

Taking in the original client's identity *IDo, KGC* generates a random key and sends the *sk(id)* to the original client by the secure channel. Let *sk(id)* be the original client's private key.

C. Proxy-key Generation

KGC generates its master key and is kept confidential by *KGC.*

D. Labelling

Taking in the file *F* and proxy-key, the proxy generates the corresponding tag for each file *Fi*. Then it uploads the block-tag pair to *PCS*.

E. Proof

Proof is an interactive system between Public Cloud and Original client. At the end of the interactive proof protocol, Original Client output a bit *{0|1}* denoting "success" or "failure" after the remote data integrity check is over.

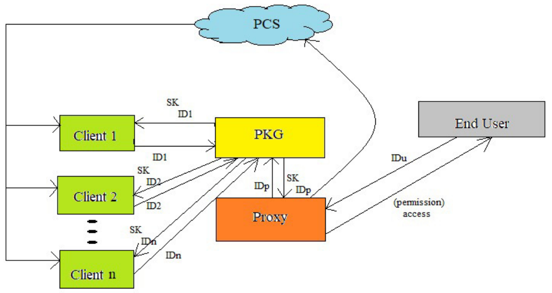

Fig 4 IDPP Protocol

VI. SYSTEM MODEL

IDPP protocol in the application generated consists of few entities each performing certain functions. There are four entities similar to them

A. ***Client:*** This is an entity which uploads massive data to the PCS (Public Cloud Server), by the delegated proxy which can perform the data integrity checking.

B. ***PCS (Public Cloud Server)***: This is maintained by the cloud service provider and has significant storage and computation capacity. User's data is securely managed in the cloud.

C. ***Proxy***: This is delegated and authorized by the manager to process the Client's data and upload them. This verifies the signature signed by the Client and processes it when the same is satisfied, otherwise it cannot perform the procedure.

D. ***KGC (Key Generation Centre)***: This is an entity that generates the private key upon seeking the data and all inputs from the Client.

This procedure provides the Client to interact directly with the PCS to check the remote data integrity. Thus, delivering the integrity check and securing the data in a specified design method.

VII. CONCLUSION

Motivated by the security needs, we proposed a novel security concept of IDPP implemented on public cloud. The concrete IDPP protocol is designed by using the bilinear pairings technique. This protocol is provably secure and efficient by using the formal security proof and efficiency analysis. This finally accomplishes the managerial tasks with updated security mechanisms.

REFERENCES

[1] Wenting Shen, Jing Qin, Jia Yu , Rong Hao, and Jiankun Hu, Enabling Identity Based Integrity Auditing And Data Sharing With Sensitive Information Hiding for Secure cloud Storages, IEEE transactions vol 14 , February 2019

[2] G. Ateniese et al., "Provable data possession at untrusted stores," in Proc. 14th ACM Conf. Comput. Commun. Secur., 2007, pp. 598–609.

[3] J. Sun and Y. Fang, "Cross-domain data sharing in distributed electronichealth record systems," IEEE Trans. Parallel Distrib. Syst., vol. 21, no. 6,pp. 754–764, Jun. 2010

[4] B. Wang, B. Li, and H. Li, "Panda: Public auditing for shared data with efficient user revocation in the cloud," IEEE Trans. Serv. Comput.,vol. 8, no. 1, pp. 92–106, Jan./Feb. 2015.

[5] Y. Yu et al., "Identity-based remote data integrity checking with perfectdata privacy preserving for cloud storage," IEEE Trans. Inf. ForensicsSecurity, vol. 12, no. 4, pp. 767–778, Apr. 2017.

[6] G. Ateniese, D. H. Chou, B. de Medeiros, and G. Tsudik, "Sanitizable signatures," in Proc. 10th Eur. Symp. Res. Comput. Secur. Berlin, Germany: Springer-Verlag, 2005, pp. 159–177.

[7] Bhale Pradeepkumar Gajendra, Vinay kumar singh, More Sujeeth, " Achieving cloud security using third party auditor, MD5 and Identity based encryption"