ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 2, Issue 3, pp: (47-51), Month: September-December 2015, Available at: www.noveltyjournals.com

A Review on Security for Accessing Data Using Real Cloud Computing

[1]Bakare Ninad, [2]Rasal Vishal, [3]Borse Sushmita, [4]Prof. Sujit Ahirrao, [5]Ladke Pallavi

[1,2,3,4,5] Department of Computer Engineering Sandip Institute of Engineering & Management Nashik, (India)

Abstract: **Cloud computing is future of data storage. In case of such storage, data is outsourced to third-party and user no longer has physical possession of it. This reduces the maintenance and securing work demanding in case of locally stored data. Such systems are expected to work as if data is stored locally without worrying about to verify the reliability of data. Therefore, public auditability of data is important so that the user can route to third party for integrity checking and be tension free. Such auditing system is expected to introduce no new vulnerability to the users' data privacy and should not add any extra network burden. In this project, we explore ring signature to compute the verification information need to verify reliability of that shared data. In the mechanism introduced in this project, the uniqueness of signer in each block is kept remote from third party auditor, who can still verify the integrity of publicly shared data without retrieving the entire file.**

Keywords: **signature; auditability; vulnerability.**

I. INTRODUCTION

Cloud Computing is used as a long lasting source for storing files as it has many advantages in information technology architecture. Cloud computing has changed the nature of business in information technology. Data can be stored on cloud in a very flexible way and on-demand manner makes many benefits along with relief the burden of storage management. Various types of files can be stored on the cloud at a time. The files may contain documents, images, audios, videos, etc. The data is stored on cloud thinking that it is secure and cannot be accessed by any unauthorized person. But the current situation is that the data stored on cloud is not at all secure mostly which is stored on public cloud [4]. Hence to secure the data on cloud we have proposed a system which will act as a middleware between user and cloud. This system will encrypt the data using AES algorithm and then the data will be stored on the cloud. The ring signatures of the same will be generated using SHA- 1 algorithm and will be stored in a database. There consists a Third Party Auditor (TPA) [7] which will verify the ring signatures of the original file stored and file on cloud which may get attacked. If both the signatures are same then the file can be decrypted else the TPA will give an error message that the file on cloud is been attacked and cannot be accessed.

II. LITERATURE SURVEY

A cloud is most widely used service for storing data. This data can be in various forms such as images, documents, audio, video, etc. Cloud is a place where data can not only be stored but can also be shared to various users. User thinks that data stored on cloud is safe and secure. But the current scenario is that data on the cloud can be accessed by unauthorized people. So to make the data on the cloud secure, we have proposed a system which will encrypt the data before storing on cloud. Moreover a signature will also be generated of the data which will be stored on cloud. Still if the data is attacked on cloud, the signature of the data will change. Thus the signature of the uploaded data and attacked data will be verified by the Third Party Auditor (TPA). If both signature matches, the data is safe for sharing and if it does not matches then TPA will notify that data is attacked and cannot be shared.

Xiaofeng Chen Et. [1], The cloud services are improved in a large extend from couple of years. The method of sharing the important data from the cloud to third person is been focused as a part of security. More precautions are taken while sharing the important data. So to make simple the sharing of data, an efficient process is needed. This paper consist of such process which will take care of security of data while sharing it to third person. The algorithm used is the best one in terms of smoothness in working and easy to verify the data.

Ning Cao, Et. [2], With the approach of cloud service, the users are now storing their important data on the public cloud instead of storing it on private cloud. The user first needs to buy his own cloud and then store his important data for the security purpose. But the approach of public cloud takes good care of security of all the data due to which the user need not to buy private cloud for storing important data. This leads to saving of money and increase smoothness in working. In public cloud, before uploading the important data it has to be encoded. In this proposed module, a set of similar keyword are taken for matching. Same is used for data verifying in the cloud.

Hong Liu, Et. [3], This work consist of recommender system which is constructed as online application and it generates a personalized list of attractions which user may like. The modern technologies like collaborative filtering are considered effective in tourist domain. The recommendation process of attractions divided into three steps: 1. Representation of tourist information. 2. Finding similar tourists. 3. Recommending attractions. The cosine method is used for finding similar tourists. And then recommendations are generated by referring history of similar tourists.

Boyang Wang, Et.[4], Mostly cloud is used for storage of data but now a day the cloud service is also used for sharing the data with multiple users. However it becoming very difficult to maintain the identity privacy.

For this, authors used public auditing scheme. In this they took advantage of Ring Signature to compute the Verification data. This data is required to audit the Integrity of data. Here they offered the public auditing on the data which is stored on the Cloud. This experiment results to effectiveness and efficiency when auditing such Cloud data.

Qiang Tang [5], Current encryption algorithms allows user to share cipher data on the cloud and can be searched on behalf of user. This scenario is not Suitable for the multiple users where they gives right to access to the particular users. There is also possibility that the Cloud server may affected by the unwanted users. So it becomes a big task to secure the data stored on the cloud which can be accessed by multiple end user. Thus authors proposed the system which provides the data security using bilinear property of Type 3 pairings.

Cong Wang, Et. [7], User should store the data on cloud remotely without any burden of local data storage. Moreover if the cloud storage is local then user can use this system and public auditing is performed by Third Party Auditor. In this paper, they proposed a secured system and supporting privacy for public auditing. Third party can perform audits of multiple user simultaneously.

Ming Li, Et.[8], PHR (Personal health record) is exchange of patient health information records, which is stored at another place(third party). The patient health information records share between only third party servers and unauthorized party and that PHR means patients health information record is in encrypted formatted before it stored on another place because it is risk, suppose we stored that information as it is on any place then any one can access it. In this paper, they proposed system for security of patient information records which encrypted using (ABE) attribute based encryption is.

Jens-Matthias Bohli Et.[9],Cloud security is the most important challenges. Cloud is set of research activity having security. Cloud is the distinct set of concepts which is new set of unique concepts which is easily accessed by everyone, in this paper they provides security for cloud using multiple different clouds and it having the different services IaaS, PaaS, SaaS. This paper mainly focused on high security for cloud. The different clouds having their privacy capabilities.

Qin Liu Et.[10], Key strategy is used by the users to store data on the cloud is Encrypt it first and then store it after that issue decryption key to only authorized users. When user tries to access data, the owner will re-encrypt the data to prevent it from being accessed. Re-encryption command will also generate new decryption key for valid user so that they will be able to access the particular data. But Cloud computing formed by many Cloud Servers. It becomes troublesome to execute such commands. Here they proposed the scheme where Cloud Server does data re-encryption automatically.

Dawei Suna Et.[11], Cloud computing is used in large scale in this world of technology. But still its performance is not up to the mark. The security issues are a big problem in the current system due to which the requirement of today's users is not fulfilled. The files containing various types of data and application are uploaded on cloud and then executed in the form of virtual machine. This files have to face many security problems. It is difficult to apply security for the files stored on cloud. In this paper this security issues are tried to apply on the files uploaded on cloud so in future we can use a secured cloud to upload our data.

III. PROPOSED SYSTEM

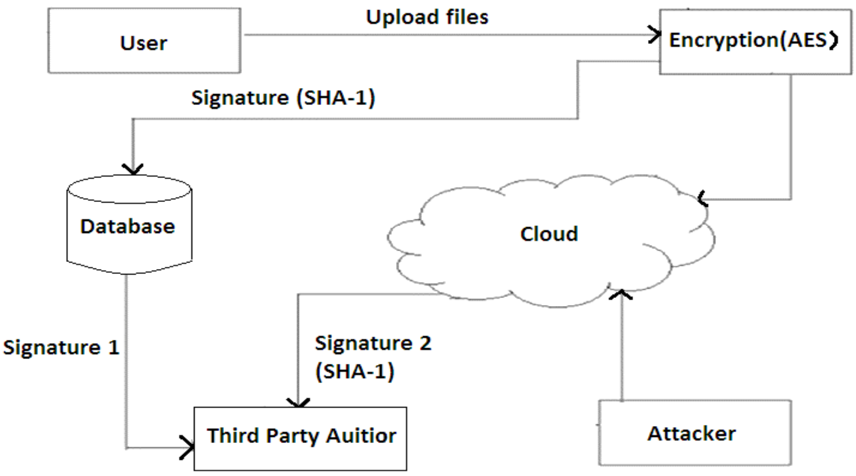

Figure 1: System Architecture

Our System contains the

1. User

2. Encryption

3. Cloud

4. Database

5. Third Party Auditor

6. Attacker

In above system architecture the user will upload multiple files on cloud. Before uploading the files will get ciphered by using AES algorithm and signature will be generated using SHA-1 algorithm. The ciphered data will be stored on cloud and Signature will be stored in separate database. Attacker may access data unauthorized stored on cloud which will manipulate the original data that results into the change in signature.

There exist a TPA which will compare the modified signature and original signature Stored in Database. If both the signature gets matched then the files can be decrypted and accessed. If both the signature does not match then the TPA will produce an Error message and data will not be accessed.

IV. MATHEMATICAL MODEL

Let S be a cloud storage security that maintain the integrity of users data on cloud. Such that,

$S= \{K, A, V, U, T, C, D, F\ |^{\phi}\ s\}$

Where,

K – Represents key generation set of $K= \{k0, k1\ |^{\phi}\ k\}$

Where k0= public key, k1=secret key

C- Represents the set of cloud C= {c0 | ϕC} Where

c0= cloud service provider.

A – Represents the set of signature

A= {a0, a1|ϕA} where a0= signature generated by user,

a1=signature generated by cloud.

V - Represents the set of signature to verify

V= {v0 ϕV} Where v0= verify the signature.

U- Represents the set of user

U= {u0….un| ϕU} Where u0= number of user.

T- Represents the third party auditor

T= {t0 | ϕT} Where t0= third party auditor.

F- Represents set of files

F= {f0…… fn |ϕ F}

Where f0…. fn - number of files.

D- Represents database

D= {d0 |ϕ D} Where d0- Database

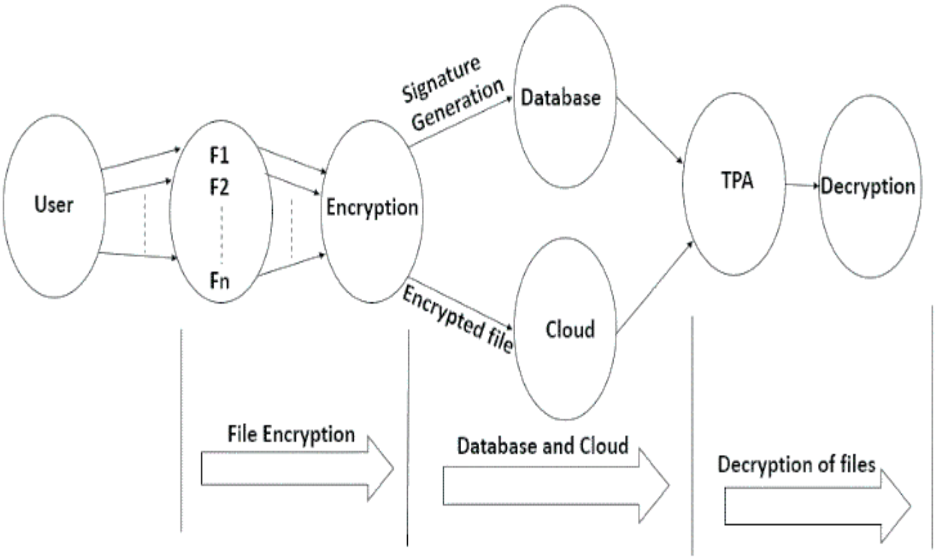

Figure 2: Mathematical Model of Proposed System

V. CONCLUSION

In proposed system ring signature utilize by TPA to audit integrity of data. To improve efficiency of verification for various reviewing task batch auditing is used. Therefore this system is preserving privacy while auditing shared data stored on cloud.

REFERENCES

[1] Xiaofeng Chen, Jin Li, Jianfeng Ma, Qiang Tang, and Wenjing Lou, “New Algorithms for Secure Outsourcing of Modular Exponentiations" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 9, SEPTEMBER 2014, pp. - 2386-2396

[2] Ning Cao, Cong Wang, Ming Li, Kui Ren and Wenjing Lou, “Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data”, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 1, JANUARY 2014, pp. - 222-223

[3] Hong Liu, Huansheng Ning, Qingxu Xiong,, and Laurence 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, pp. - 1-11

[4] Boyang Wang, Baochun Li and Hui Li, Me “Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud” IEEE 5TH INTERNATIONAL CONFERENCE ON CLOUD COMPUTING YEAR 2014.

[5] Qiang Tang ”Nothing is for Free: Security in Searching Shared and Encrypted Data” IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 11, NOVEMBER 2014, pp. - 1943-1953.

[6] Yong Yu, Jianbing Ni, Man Ho Au, Yi Mu, Boyang Wang, and Hui Li “On the Security of a Public Auditing Mechanism for Shared Cloud Data Service” IEEE Transactions on Services Computing Citation information: DOI 10.1109/TSC.2014.2355201, pp. – 1-2.

[7] Cong Wang, Sherman S.-M. Chow, Qian Wang, Kui Ren, and Wenjing Lou, “Privacy-Preserving Public Auditing for Secure Cloud Storage” IEEE TRANSACTIONS ON COMPUTERS VOL: 62 NO: 2 YEAR 2013, pp. – 1-12.

[8] Ming Li, Shucheng Yu, Yao Zheng,” Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption” IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 1, JANUARY 2013, pp. – 131-143.

[9] Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen,” Security and Privacy-Enhancing Multicloud Architectures” IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 10, NO. 4, JULY/AUGUST 2013, pp. – 212-225.

[10] Qin Liu†‡, Chiu C. Tan ‡, Jie Wu ‡, and Guojun Wang† “Reliable Re-encryption in Unreliable Clouds” IEEE Communications Society subject matter experts for publication in the IEEE Globecom 2011.

[11] Dawei Suna,*, Guiran Changb, Lina Suna and Xingwei Wanga “Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments” Procedia Engineering 15 (2011) 2852 – 2856, pp. – 2852-2856.