Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 1, pp: (121-123), Month: January-April 2016, Available at: www.noveltyjournals.com

Improving Cloud Data Storage Security Using Data Partitioning Technique

[1]B. C. Julme, [2]Amruta Aphale, [3]Avinash Deshmukh, [4]Omkar Shirsalkar, [5]Yogita Naral

[1]HOD, Department Of Computer Engineering, PVG's College of Engineering and Technology, Savitribai Phule Pune University, Pune, Maharashtra, India
[2,3,4,5] Savitribai Phule Pune University, PVG's College of Engineering and Technology, Pune, Maharashtra, India

Abstract: **In this paper we propose a secured cloud storage system for ensuring security and dynamic operation in the environment using data partitioning technique. The main focus of this paper lies on seed block algorithm. This seed block algorithm uses the X-OR operation to partition the data and generate the recovery copy of data. The SHA-1 algorithm is for creating the digital signature for each partition which are generated by seed block algorithm. The AES algorithm is use to encrypt the data then third party auditor stores those partitions on different servers. Data can be retrieve in exactly reverse order and in case of any damage, data can be recovered from recovery server.**

Keywords: **SHA-1, AES algorithm, Seed block algorithm, Third party auditor, Data integrity.**

1. INTRODUCTION

Cloud storage system enables storing of data in the cloud server efficiently and makes the user to work with the data without any trouble of the resources. In the existing system, the data are stored in the cloud using dynamic data operation with computation which makes the user need to make a copy for further updating and verification of the data loss.

An efficient distributed storage auditing mechanism is planned which overcome the limitations in handling the data loss. In this the partitioning method is proposed for the data storage which avoids the local copy at the user side by using partitioning method. This method ensures high cloud storage integrity, enhanced error localization and easy identification of misbehaving server. If any of the server compromised, we can recover damaged files.

The main focus of this paper is to ensure high cloud storage integrity, enhanced error localization and easy identification of misbehaving server. If any of the server compromised, we can recover damaged files.

2. EXISTING SYSTEMS

Third party cloud storage and access permissions play a vital role in security analysis and user access control. User access control and data verification are the important revolutionary technologies to provide security and control unauthorized users. Third party cloud servers are built without proper security measures and user control mechanisms. User can access the data such as documents, media or other type of files using third party generated authentication key and secret information.

Traditional cloud security mechanisms are independent of data integrity verification to the authorized data users. Third party cloud servers are vulnerable to different type of message integrity attacks. Traditional message integrity algorithms are depend on the file size, hash size and security parameters.

Satheesh K S V A Kavuri, Dr.Gangadhara Rao Kancherla, Dr.Basaveswara Rao Bobba proposed a system in which DUPHA algorithm is used which creates 512 bit hash key. In this process, each user has to store the data in the cloud by using hash and encryption algorithms.

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 1, pp: (121-123), Month: January-April 2016, Available at: www.noveltyjournals.com

Each user's data is given input to hash algorithm to calculate 512-bit hash value. In the next process, generated hash value is given input to improved attribute based encryption model for data encryption. Both the encrypted data and its hash value are stored separately in the cloud storage. Similarly, the reverse process can be used to restore the original data through data integrity method C. Selvakumar G. Jeeva Rathanam M.R.Sumalatha proposed system which uses RSA which create public and private RSA key for encrypting the files, and stored in cloud. The generated private key length is 2048 bits.

3. PROPOSED SYSTEM

The focus of our idea is to recover the data and provide the integrity on public cloud. World Wide Web is usually visualized as numerous cloud servers and hosting third party users; therefore the term cloud computing is used for computation can be done through the internet at remote server. Authorized Cloud users can access cloud resources over the internet from anywhere, without concentrating on any resource management or maintenance. Besides, instances in cloud are certainly dynamic and scalable. The cloud has evolved by the different technologies including parallel computing, distributed computing, virtualization, grid computing and utility computing. Virtualization optimizes the performance in a cost efficient manner.

Cloud data user who wish to store the data in cloud first generate the hash code and send data along with hash to the remote cloud server. The partitioning method is proposed for the data storage which avoids the local copy at the user side by using partitioning method. Even though the data is damaged it can be recovered through recovery system.

The overall system design consists of following modules:

1. Data Partitioning.
2. Data Encryption.
3. Data Distribution.
4. Data Updating.
5. Data Retrieval.

Data Partitioning:

This is the process of dividing the data into different chunks or partitions. This process happens in the TPA machine. During this process, the criteria such as security and size of data are usually being considered.

Data Encryption:

This is the process of encrypting the data using AES algorithm into the encrypted language to provide the data confidentiality. For this process clients are needs to store their data onto TPA with having trust on to it.

Data Distribution:

The process of allocating different data chunks or partitions into two different clouds or one cloud having two or more servers.

In this system we are having two servers. In this process the key is calculated using AES algorithm and for each partition of encrypted data, the digest or digital signature is calculated using SHA-1 and store in database for providing the data integrity. After the data distribution, XORing operation is perform on distributed encrypted data, and that outcome is store on RS in encrypted format using seed block algorithm. If one of the server gets fails or if data is lost then it is recover from RS by decoding it.

Data Updating:

This process allows the clients to update their data, without any overhead with having security.

Data Retrieval:

This is the reversal process of data distribution and data partitioning, known as data reconstruction. In this the data is retrieve from S1 and S2, compare their digest with newly created one using SHA-1, decrypt it using AES and finally the data is back to the client as it is with free of cost.

Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 1, pp: (121-123), Month: January-April 2016, Available at: www.noveltyjournals.com

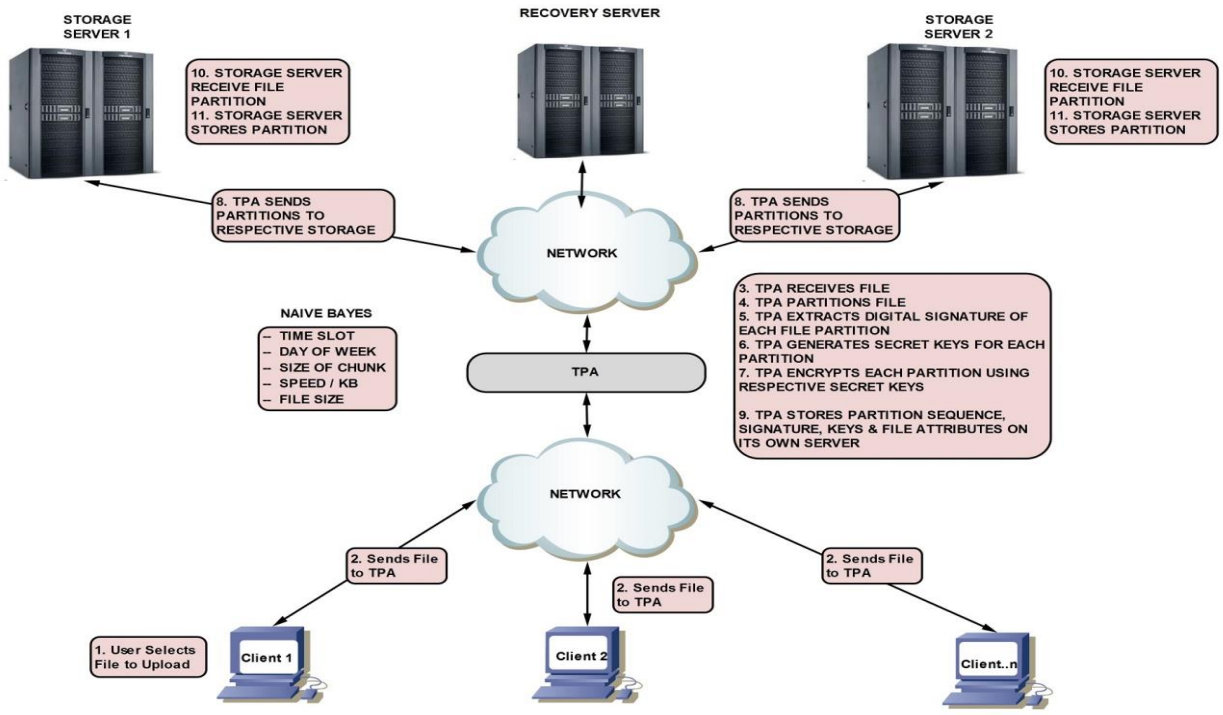

Figure No. 1 .System Architecture

In order to overcome the security related issues in commercial cloud servers, an improved hash based message integrity verification process was proposed in this paper. Proposed message integrity algorithm was tested on attributed based encryption process. Proposed cloud based hash algorithm generates 160 bit size hash value to each data partition in the third party cloud servers. Only authorized users can access the required files using his/her identity along with the message integrity value. Experimental results show that proposed cloud based hash algorithm outperformed

4. CONCLUSION

To secure the cloud and public storage we can use data partitioning method which provide more security to data by splitting the data and encrypting it then storing it on different servers the result of this project will show the higher security for user's data.

We are also creating the recovery file using Seed Block algorithm which will ensure that, if the data is loosed then the TPA can recover the data through recovery file, and user will get his/her original data.

We propose an efficient data storage security in cloud service. The partitioning of data enables storing of the data in easy and effective manner. It also gives way for flexible access and there is less cost in data storage. The space and time is also effectively reduced during storage. The main key concept or focus is on, in case if one of the storage server get fails or breakdown, then without any data loss and knowing to clients, the proper data should be provide to the clients from recovery server with very ease of use. Also the remote data integrity checking detects the threats and misbehaving server while storing the data in cloud ensuring data security.

Our goal is to provide higher level of security and searching mechanisms for outsourced computations in cloud services.

REFERENCES

[1] Data Authentication and Integrity Verification Techniques for Trusted/Untrusted Cloud Servers, Satheesh K S V A Kavuri, Dr.Gangadhara Rao Kancherla, Dr. Basaveswara Rao Bobba. 2014 International Conference Advances in Computing, Communications and Informatics (ICACCI) IEEE Dec 2014.

[2] Dynamic Secure Storage System in Cloud Services. G.JeevaRathanam IEEE Dec2014.