International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 03 | Mar -2017 www.irjet.net p-ISSN: 2395-0072

An Approach towards Shuffling Of Data to Avoid Tampering In Cloud

Dipak Khadse[1], Sandeep Giratkar[2], Mehul Balsaraf[3],Jyoti Gawande[4], Monali Taywade[5], Soniya Deshmukh[6]

[123456]*Department of Computer Sci. & Engg.,Priyadarshini Bhagwati College of Engineering, Nagpur, Maharashtra, India*

Abstract - *Cloud is a model which permits for on-request resource access. Apart from it, the cloud provides facilities for data storage which can be personal, confidential and business related. As the standard of technology increases, it also attracts various security threats towards itself. As cloud computing is a popular platform which is mainly used in IT industries the security plays an important role in securing the data stored in the cloud. To keep data secure we are proposing an approach by using Advance Encryption Technique (AES) and allows the admin to control the data shuffling life cycle within regular interval of time and also applying access control policies to perform various operation on the files present in cloud. Apart from it the concept of deduplication has been used to reduce memory storage.*

Key Words*: *Advance encryption technique, Shuffling, access control policies, de-duplication.

1.INTRODUCTION

The history of cloud computing starts with the invention of first Ethernet adaptor card for IBM PC in the year 1982 which has fast connections that would enable cloud computing. In the year 1989, the first public dial-up Internet service was founded which we still use it and was founded by software tools and die. The term Cloud Computing was put forward by professor Ramnath Chellappa from the University of Texas in the year 1997[1]. Since then Amazon Web Services was launched in the year 2002 followed by Google apps in April 2008 and Microsoft Azure in November 2009. Nowadays cloud is emerging for all kinds of online activities. It is capable of satisfied different needs of customers of the cloud.
Cloud computing offers many services in data storing, data accessing with congruous data management. Cloud computing started to grow its

Popularity as to reduce down overhead of maintaining data, companies commenced relying on cloud platforms. End users have benefits of cloud as they can access the data anytime and anywhere even on their mobile devices. Most common examples of such accommodations are Amazon cloud and Google engine [3]. To fluently achieve the provisioned services, cloud systems generally enhance the services by caching, replicating and/or archiving a huge volume of user data in its storage network. Despite these enhancements can upgrade the comprehensive conduct, they also provoke a huge danger to reveal the user data publicly, as the cloud-wide storage networks are commonly not protected that is they are facilely under vigorous attacks and also struggle through software/hardware faults [1].
There are many such incidents on attacks cloud servers, which were deadly and caused many troubles. One type of attack on cloud computing is a DDoS attack in Cloud, one such incident regarding this attack is a Security breach on Sony which has alerted the whole internet community. Attack has exposed 100 million account records. Attackers are not remained concentrated on this attack instead an additional attack occurred on Sony's online entertainment that exposed additional 25 million users.

Swapping across the servers and data swapping could be solutions for these threats. Data swapping implicatively insinuates transmuting the physical location of accessed data by swapping them between the numbers of involved servers. This will be done by a process which reallocates data by constant swapping between the many servers, so it will be infeasible to access the cloud confidential data by any illicit denotes.[3].

2. Problems in existing system

File security: - During supporting the text record secretly, the facts stored must not be let to be chan ged even by the controlling person. The data created must be kept secured from attacks of file confidently. The way to store the file in the cloud must not be tracked.

Data Duplication: - Duplication means which stores same data multiple times, which results in wastage of space in

the cloud. The attacker might upload the same file with diff attributes which may damage the original data file

Probity Surveying: - audits are done to verify the truth that the data provided is authentic. It also helps in maintaining correctness of data in the cloud.

Encryption and Decryption of data: - It assigns the extra protective layer to the security of data. Encryption is performed on the sender's end while decryption is performed on the receivers end.

3. Proposed Methodology

The proposed system works on reducing the security threats and avoiding duplication of the file in the cloud and also providing access control policies for the user. As the security is an important aspect for every cloud user this proposed work requires a special attention towards it. This work mainly focuses on providing maximum security to data stored in the cloud and accessing the data from the cloud. Here when the user uploads some data in the cloud it is in plain text form after encryption it gets converted into cipher text. Here for encryption, we have used AES algorithm. Using this algorithm we can encrypt the data and then send it to the cloud which keeps it secure. To provide some advancement we used the shuffling concept. With the help of shuffling the data can be moved from one server to other server or directory to directory without leaving any trace for the attacker. Admin sets the time interval for a file to stay in one server after the specified time period the file gets relocated to some random server. The relocated location is updated into admin's database.
To prevent the data theft we have provided the concept of access control policies. By using this policy only authorized user can access their files. It works as if a user wants to access his file or before performing any actions like deleting, downloading a secret key is send to the authorized user's mail which will be provided by the user at the time of registration into the cloud. The admin has the authority to approve or disapprove the registration request of the user. The user cannot perform any of the operation which until the admin approves their request.
As many IT industries rely on storage provided by cloud the demand has crossed 50 percent in recent years. Space for storing data can be a major problem. This gives rise to the technology named deduplication. This technique mainly does not allow the user to upload the files which are already stored in the cloud.

3.1 Deduplication

The deduplication technique concerns of tracing each data file and removing the file if more than one replica is found in the user's account. It maintains data reduction alike in compression where the data is compressed. There are various techniques to detect and remove the duplicate data. Some of them are explained below.

I] Data Location: - The data in the cloud are stored server side or on the client side. The deduplication is performed according to the storage location of the data. The difference in finding the data deduplication in both locations are that while the data is stored in the client location the special program is required whereas the data stored in server location can be found simply by sorting files.

II] Data Division: - In data division, the data is divided into a sequence of bytes, after that the blocks are obtained to test the redundancy in deduplication only unique block is stored[2].

3.2 Analysis of Hash Algorithm

Hash functions have a broad and consequential role in cryptography. A hash function is an alteration which takes input in bits and gives fixed-size string. This string is called as a hash value. The hash function must be able to give output in fixed length in spite of providing it the input of random length message. Here we have used the SHA-1 hash function.this algorithm is described below.

SHA-1: - SHA stands for Secure Hash Algorithm. This algorithm was proposed by National Security Agency (NSA) and published by National Institute of Standards and Technology (NIST) in the year 1995. The earlier version was SHA-0 which was published in the year 1993. SHA-1 gives 160-bit message digest and takes 80 rounds. This algorithm is used for protection of sensitive unclassified information and is also used in protocols like IPsec. Due to its time efficiency and robustness, it is it is most popular among various hash algorithm[5].

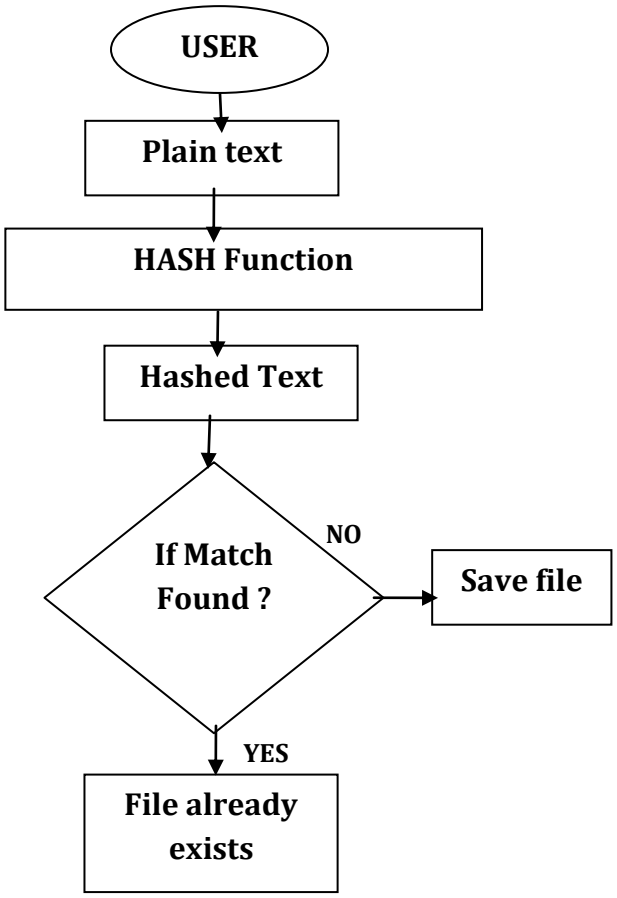

Fig: 3.2 Flowchart of Deduplication using Hashing Function

3.3 Shuffling

Shuffling is a very common technique which is used for moving data from one location to another location. This helps to avoid tampering of files. By providing the timestamp to data as soon as it enters into the cloud after that the data stays there for particular timestamp then it moves to other random location in the server. This method is used to avoid tampering of data in the cloud. Admin has the access to set the timestamp and only he knows the updated location of the file in server.

3.5AES Encryption

Advanced Encryption Standard (AES) was developed as a replacement for Data Encryption Standard. AES allows the block size of 128,168, 192, 224 and 256 bits. We have used AES-128 where both key size and block size is 128 bits. This algorithm uses the same key for encryption as well as decryption as like DES algorithm

4. Future Work

We have implemented the current system for the enrichment of security in the cloud.we need to grow and investigate every aspect of the cloud to keep it fully secured. In this proposed work we have tried to enhance the security in the cloud using multiple concepts but still gainful has not been found and we will try to enhance security in future work.

5. Conclusion

In this case study, we have discussed the way of reducing data storage space and duplication is one of the assorted techniques used for improvement. Duplication is removed with the help of hash function. Encryption methods are used to enhance the security to the data in the cloud. Shuffling of data in regular timestamp adds additional security. Hence we have tried to improve the performance, security and storage capacit

REFERENCES

[1] Lingfang Zeng, Yang Wang and Dan Feng "CloudSky: A Controllable Data Self-Destruction System for Untrusted Cloud Storage Networks" 2015 IEEE 978-1-4799-8006-2/15.

[2] S.Kaaviya, P.L.Revathi , R.Nithya , "Enhancing Data Security in Cloud using Shuffling and Distribution Algorithm", NCRTCA 2013 (0975 – 8887)

[3] Bindia, "Enhancing Security through Data Swapping and Shuffling Across the Servers in Cloud", IJETER Volume 4, Issue 5, May (2016).

[4] T.Y.J.NagaMalleswari, D.Malathi, G.Vadivu, "Deduplication Techniques: A Technical Survey", IJIRST Volume 1 | Issue 7 | December 2014 ISSN (online): 2349-6010

[5] Mr. Pratik Sawarkar, Ms. Sheetal Singh, Ms. Priti Nitnaware, Ms. Rasika Tiwari, Ms. Akriti Shrivastava, Ms. Pooja Dubey, "Securing Cloud from Tampering and Duplication", IJRITCC Volume: 4 Issue: 10 ISSN: 2321-8169 81-85.