Proxy driven data upload and Remote Integrity checking using MD5 Algorithm.

Ashutosh Ingle[1], Shivani Bondre[2], Rutuja Kanjane[3]

[1] *Student, Department of Computer Engineering, NBNSSOE, Maharashtra, India*
[2] *Student, Department of Computer Engineering, NBNSSOE, Maharashtra, India*
[3] *Student, Department of Computer Engineering, NBNSSOE, Maharashtra, India*

ABSTRACT

In today's modern world internet has became an important source of information. Various methods or techniques are invented to extract useful information from the internet and one of the important field is Cloud Computing. It is the most reliable computing platform in these modern era .These clouds are used for storage purpose and various other purposes. Though it provides storage the data on the clouds needs to be safe and that's why encryption is needed .The data from the cloud server should be checked whether it is being uploaded or it is downloaded. There are various threats like data stealing , data altering , etc. due to such type of threats "Proxy-Oriented Data Uploading and Remote Data Integrity Checking in Public Cloud" is taken under consideration. Cryptographic Proxy Oriented Data uploading secures the internal and external environment by avoiding the data from a invalid source. Though cloud services may be popular but due to high security the data which was uploaded from a illegal source or from a unauthorized user will be restricted. To counter this user can update their proxy or modify them and do the uploading task. The existing system cannot counter such type , so for this purpose the proposed system is to be taken under consideration .It does not provide access to unauthorized users . Proxy alteration makes it easier for the attackers to steal the data or to inject malwares into the cloud environment . The integrity of data also plays important role in data security . The proposed system checks the integrity of the data without actually downloading the actual data . Unlike other systems, data is to be downloaded and checked the integrity, this system does it remotely.

Keyword: - *: Cloud Computing, Data Integrity, Proxy oriented, Key Generation, Encryption and Decryption*

1. INTRODUCTION

Now a days in era of this technology the extensive use of networks social media and data sharing among internet devices has use of its maximum level .The vast use of internet enables user to use data ,sharing and access on internet. The cloud computing is most popular among them ,many of customers preferably use the cloud service to store and access the data which is cost effective and its ability to store data .but the issue of data security is taken into the considerations to avoid loss of data integrity, confidentiality, availability.

Proxy oriented data uploading and remote data integrity preserving and checking mechanism in public cloud can ensure data will be protected .we use ID-PUIC protocol for preservation of data integrity.ID-PUIC protocol is flexible and efficient.

Cloud storage technology is used to store huge data which is helpful for business data storage in cost effective manner. many of users transfer data or store data in public cloud where chances of tamp ration of data is possible.

The cryptographic proxy oriented data which uploaded to cloud can avoids the problem of losing integrity of data.

ID-PUIC protocol where the encryption decryption mechanism limits the access used while uploading the file to the cloud storage. Proxy server separately stores the copy of data ,because there is possibility of data loss . That's why we introduced secure system model for protecting data.

2. PROPOSED SYSTEM

In this paper, firstly concentrate on data uploading technique it uses data integrity and proxy. Using public key identity based technique, our organized system is cost effective because management of certification in procedure is removed. The ID-PUIC protocol is basically proxy-aimed data uploading and remote data integrity based version on public cloud. We provide the official structure and safety version of existing ID PUIC protocol. For this reason our organized structure is more reliable.

2.1 CONCRETE ID-PUIC PROTOCOL

This protocol has four different servers:

- Middle server
- Encryption - Decryption server
- Checksum server
- Proxy Server

As our system point of view, the structure of concrete protocol is represented in below figure 2. Firstly, the configuration is worked on every servers which is included in our structure after that the client give the permission to upload the data.

Data are uploaded via computer, before uploading some data candidate receives the One Time Password i.e. OTP which is created by the algorithm of key generation for candidate validation. After that the actual data will sent to middleware server. For data encryption, it will send to the encryption server, That encrypted data again send to the middleware server. Using checksum server we can calculate the checksum of specific data. Now the encrypted file is in proxy server. Using proxy server the data will securely uploaded on DRIVEHQ cloud. whenever candidate need to check their data, it will send the request for checking the integrity of particular file, and candidate can check the integrity of data without downloading specific data safely.

2.2 PRIVATE CHECKING and DELEGATED CHECKING

In our organized structure non public checking and delegated checking are assured. Data uploading using proxy-aimed states that each candidate can upload any data on cloud storage using specific proxy. On the basis of representation, our planned system help to examine the integrity of data and upload secured data on the cloud storage .we can check the data integrity without downloading the particular data. After that, using key cryptography method our organized system is more effective because the management of certificate is removed.

2.3 AES ALGORITHM

Advanced Encryption Standard(AES) is basically permutation and substitution method. This algorithm is a union of permutations and substitution. Its worked on 128 bit of size. Size of each block is 12.192,256 bits. The AES input is used for converting the plaintext message in cipher text. It has various rounds which is 10 cycles hold 128 bit key, 12 cycles hold 192 bit key, 14 cycles hold 256 bit keys.
The steps in the AES algorithm are given below -

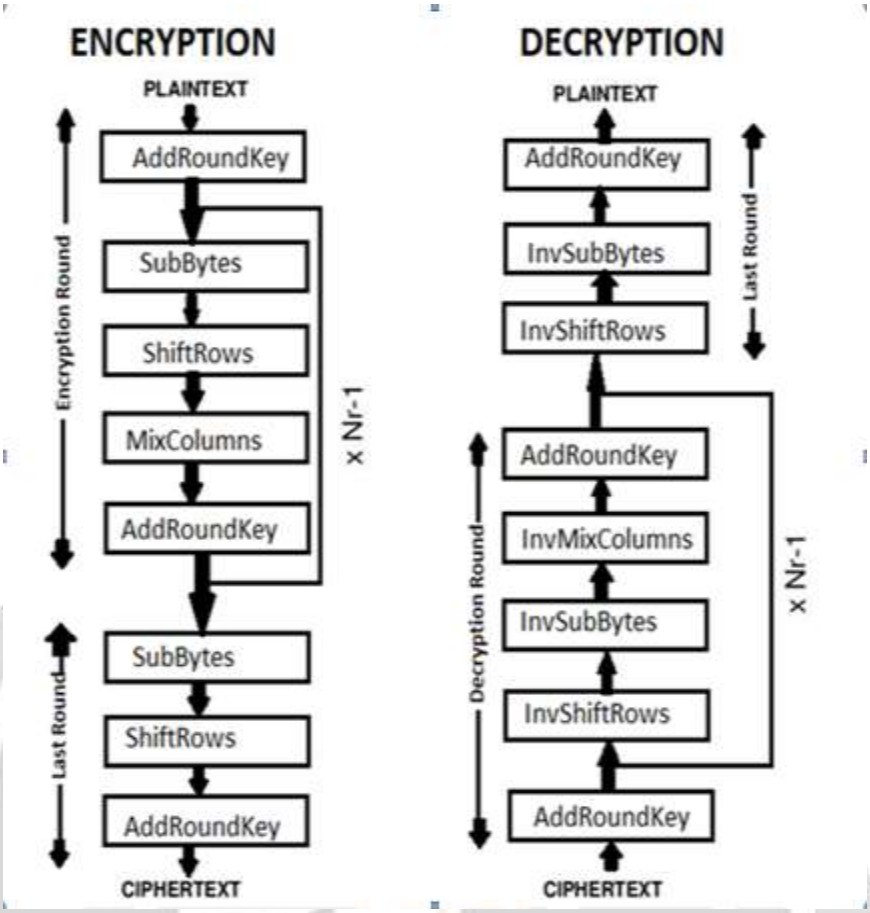

Fig -1: AES Algorithm

2.4 MD-5 ALGORITHM

Message digest five is basically uses hash function which is very responsible for producing the 128 bit hash value .it is used or design of this MD5 algorithm is to use as the cryptographic hash function. its main function which states that to process the variables length of message into the fix size variable. Its mechanism is to detect the integrity of files or data. Integrity itself is how correct data is.while transferring data within network the MD5 algorithm calculates checksum of data and transfers along with data from sender side at receivers side data is evaluated along with checksum how corrupted is that data is?

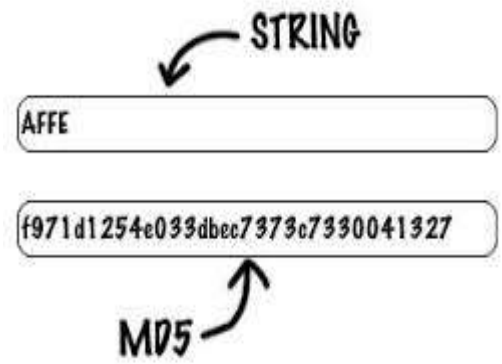

Fig -2: Input and output for MD 5 algorithm

2.5 CHECKSUM SERVER AND INTEGRITY FUNCTION

It is one of the server which is to be activated for file transfer to the cloud. The file during uploading or transfer goes from this server . The main purpose of this server is to calculate the checksum of the file which is being uploaded . Integrity check function which is resides on the Checksum Server, is activated for checking and calculating the checksum of file to process the intactness of the file. It is one of the servers which is to be initialized before sending data or file to the cloud storage and to request for integrity check. Its basic aim is to compare the string value calculated before data transfer and after value of the same string or file , and pass the result to the user .

2.6 PROXY SERVER

In the networks of computer system which is responsible for the sharing data between the clients and cloud server proxy server acts as the intermediate system which handle the clients requests to access the data resources from cloud server between the internet and client this server has its position. the third party machine or client cant able to access the resources ,it acts as the single proxy where the communication mechanism regarding data access process happens.

2.7 ENCRYPTION-DECRYPTION SERVER

These types of servers which is responsible for the encryption and decryption mechanism ,there role and responsibility are only dedicated for the security of files or the data. The data encryption mechanism is handled by AES algorithm after that data uploading is process done. This is just to process the integrity policy of cloud service. At decryption side ,the decryption mechanism starts its process before downloading file to check its integrity ,after this decryption process of file the data then sent to the user who is authenticated to access that file.

2.8 MIDDLEWARE SERVER

Middleware servers are the medium between system networks and the applications that are of many types such as web servers and also directories. Every data sharing between the applications and servers has to happen from the middleware server. Basically middleware server is the middle agent which is responsible for the sending files, encrypted data ,checksum values from one server to another server.

3. SYSTEM ARCHITECTURE

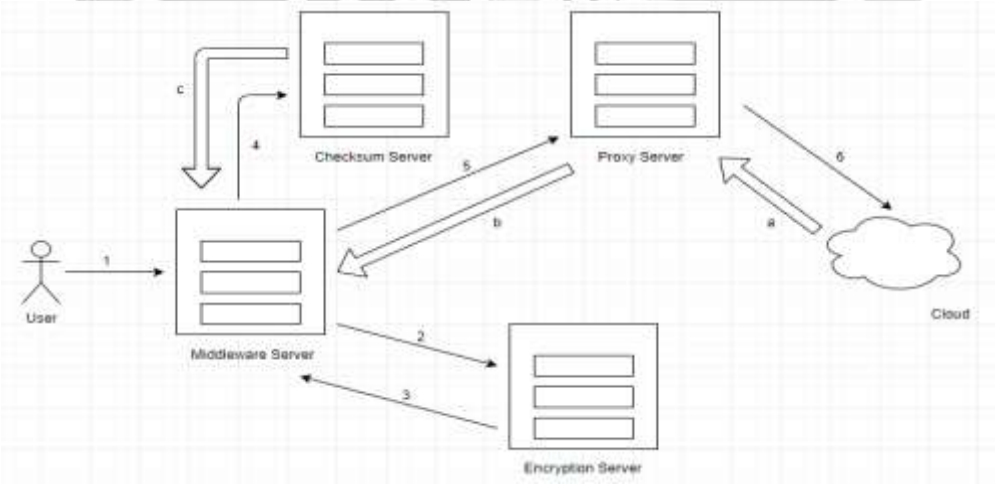

Fig-3: System Architecture

4. CONCLUSION AND FUTURE WORK

The mechanism is motivated by the concept of ID-PUIC protocol mechanism ,this paper posses the concept of ID-PUIC in the public cloud environment, this paper states that the ID-PUIC model analysis which includes authentication integrity and the prevention of access from the third parties which are not authenticated to access the data. It also recognizes the remote data integrity based on authorization of the user, thus proposed system is positively beneficial to upload file in secure manner.

5. REFERENCES

[1]. Z. Fu, X. Sun, Q. Liu, L. Zhou, and J. Shu,"Achieving efficient cloud search services: Multi-keyword ranked search over encrypted cloud data supporting parallel computing," IEICE Trans. Communication, vol. E98-B, no. 1, pp. 190–200, 2015.

[2]. Y. Ren, J. Shen, J. Wang, J. Han, and S. Lee, "Mutual verifiable provable data auditing in public cloud storage," J. Internet Technol., vol. 16, no. 2, pp. 317–323, 2015.

[3]. M.Mambo, K. Usuda, and E. Okamoto, "Proxy signatures for delegating signing operation," in Proc.CCS, 1996, pp. 48–57.

[4]. E.-J. Yoon,Y. Choi, and C. Kim, "New ID-based proxy signature scheme with message recovery," in Grid and Pervasive Computing (Lecture Notes in Computer Science), vol. 7861. Berlin, Germany: Springer- Verlag, 2013, pp. 945–951.

[5]. B.-C. Chen and H.-T.Yeh, "Secure proxy signature schemes from the weil pairing," J. Super computer, vol.65, no. 2, pp. 496–506, 2013.

[6]. X. Liu, J. Ma, J. Xiong, T. Zhang, and Q. Li, "Personal health records integrity verification using attribute based proxy signature in cloud computing," in Internet and Distributed Computing Systems (Lecture Notes in Computer Science), vol. 8223. Berlin, Germany: Springer-Verlag, 2013, pp. 238–251.

[7] H. Guo, Z. Zhang, and J. Zhang, "Proxy re-encryption with unforgeable re-encryption keys," in Cryptology and Network Security (Lecture Notes in Computer Science) vol. 8813. Berlin, Germany: Springer-Verlag, 2014, pp. 20–33.

[8] E. Kirshanova, "Proxy re-encryption from lattices" in Public-Key Cryptography (Lecture Notes in Computer Science), vol. 8383. Berlin, Germany: Springer-Verlag, 2014, pp. 77–94.

[9] P. Xu, H. Chen, D. Zou, and H. Jin, "Fine-grained and heterogeneous proxy re-encryption for secure cloud storage," Chin. Sci. Bull, vol. 59, no. 32, pp. 4201–4209, 2014.

[10] S. Ohata, Y. Kawai, T. Matsuda, G. Hanaoka, and K. Matsuura, "Re-encryption verifiability: How to detect malicious activities of a proxy in proxy re-encryption" in Proc. CT-RSA Conf., vol. 9048. 2015, pp. 410–428.