A Framework for Secure Data Sharing in Cloud Computing using RS-IBE Mechanism

Mr. Pranav R. More[1]

[1]Prof.Pranav R. More Professor Computer Science & Engineering Department, Amity University Mumbai, MH, India
[1]pranavmore2530@gmail.com.

ABSTRACT- Cloud computing provides higher security in data storage & processing**.** We have developed secure information sharing in cloud computing system using revocable storage identity based encryption. We have used AES (Advanced Encryption standard) technique to encrypt information as well as decrypt the information using analytical approach. We have analyzed different features like information sharing, high security, confidentiality and forward secrecy. In this paper, we used RS- IBE (Revocable Storage Identity- Based Encryption) and KUNode algorithm for the information security and highly secure transmission of data. We have also used the re-encryption technique for advanced secure data sharing in cloud computing mechanism.

The key function mechanism such as Public key and private key are used to encryption and decryption of information respectively. Normally forward secrecy or backward secrecy provided for higher security and data sharing mechanism in securely manner. In this paper, Forward secrecy is used for advanced security data transmission. Revoke user can't access the previous or subsequent data so that revocable identity based encryption technique is highly secure mechanism.

Our main approach is that time periods is provided to download or access the data using KUNode and Re-encryption technique gives advanced secure sharing of information in cloud computing.

Keyword - Cloud computing, Data Sharing, RS_IBE, AES, encryption key and decryption key.

1. INTRODUCTION

Cloud computing is type of internet based computing. Most of time data will be share using cloud computing. Cloud is big area to access any type of data, and information. We all share the data based on cloud computing. Cloud provides the mechanism for shared computer processing resources. Security is important in today's environment. Provide extra security among data sharing in cloud computing is one of the big challenge. Encryption Technique is used for sharing secure data between senders to receive. In this paper proposes re-encryption technique to providing extra-large security in cloud computing. Key is used to encrypt any type of data. Key function provide random key to data provider and number of user. More security will be providing based on the key technique. Hacked data between data sharing is the big issue. Unauthorized user access data without any authentication. So data is hacked by the hacker. These problems are overcome in that paper. In this paper, advance security provides in cloud computing using the re-encryption technique. Cloud Storage server is responsible for storing the data. Data Provider is nothing but the server and data provider is responsible for the upload the data or files to storage sever. Number of user access the uploaded data of files or download the files using the key as well as opt code.

2. RELATED WORK

Public key and private key are used to encryption and de-cryption respectively in this paper, AES algorithm as well as KUNode algorithm is used. Normally forward secrecy or backward secrecy provided for security. In this paper, Forward secrecy is used for advanced security. Revoke user can't access the previous or subsequent data so that revocable identity based encryption technique is used. Data providers upload the files into storage server using the encryption technique. For the encryption key is used and this key provide by the key authority. Key authority

is responsible for sending the key to data provider. In this paper, random function used for generating the key to encryption as well as decryption. Storage server stores the files which are uploaded by data provider. And users download or access the file as per their need. Download the file is done through decryption process. In this paper, time quantum also provided for downloading the data. Firstly for downloading file key will be send and this key is send again key authority. If key will be match between data provider and user then user will authorized to download the data. Else key does not match then the user cannot download the file. After matching key OTP will be send to the user. At this stage, time limit should be provided because of more security for accessing the data using cloud computing. Within a time period user can type the OTP. If OTP is type within time then user can access this file. Else time period is expired then user cannot access this file. And one more condition is that, if OTP is wrong then user enters into revoke list .In this paper, extra mechanism provided for the secure data sharing in cloud computing.

3. SYSTEM DESIGN

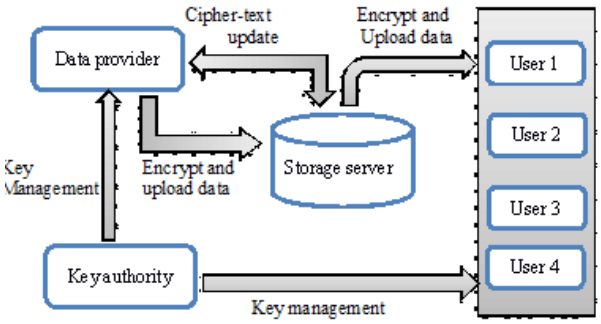


Figure-1: System Architecture

In this system first data provider upload the file. And upload file convert into the encrypted format using key encryption algorithm. I.e. AES algorithm. Then storage server responsible not only storing the data or files but, also give permission for unrevoked user to access the data or files through cloud computing. User send request for accessing data permission to data provider via storage server. Then key authority generates the key as per user requested data. These generated key is send to user. After receiving key, data provider key and user key will be match. If key will be match then user is authorized to download the data. Else it cannot the file. After matching of key again OTP will be send to user for extra security. User can write the OTP within time period. Again user will write the OTP within a time period. Then user can download the required file successfully. Else it cannot download the needed file. This whole process provide large security in cloud computing. In this paper, extra security for data sharing in cloud computing should be provided. There for sharing data through cloud computing is securely.

3.1 DATA PROVIDER

Data provider is working as a cloud and it provides important data. Cloud computing is based on internet computing it provides data and resources to the computer very securely. This model is for enabling ubiquitous to share a pool of configurable computing resources for *e.g.* Server, application, and computer network. For obtaining information user request to the data provider then data provider accept the request of the user and then work on data analysis. Next data is encrypting by the data provided by using the key and sequence key provide by key authority. The Time quantum is also set by data provider. Key updating can be done by data provider.

3.2 NUMBER OF USER

Multiple users can access their data from cloud at a one time. Each user have different key for decryption. Each user can access the data in particular time quantum. Users can access meaningful information from cloud. Key authority manager provide the key to user for decryption purpose. In this paper, additional thing is OTP, and time period is provided for the writing the key.

3.3 STORAGE SERVER

In the data sharing concept storage server is most important module. The storage data store the huge amount

of data. This data is securely store in storage server. The storage server is securely store the data. It also store encrypted data and key which used for data encryption. When the user requires his data, user requests to the storage server. There are two keys used for encryption and decryption purpose. Data sharing can be done by this server.

3.4 KEY AUTHORITY

The key which is used for encryption as well as decryption is generated by key authority. There are two algorithm is used for key generation. KUNodes algorithm and RS_IBE algorithm these two algorithms are used for key authority. In this paper, matching a key is important for security. Key authority generates the key and it will provide to the user as well as data provider. And both key matched to each other for sharing the secure data in cloud computing.

4. ALGORITHM

4.1 RS-IBE

Boneh and Franklin [2] first proposed the RS-IBE (Revocable Storage Identity Based encryption). Goyal and Kumar [3] introduced a novel approach to achieve efficient revocation.

In case of unauthorized person can use the authorized person data. Then hacking is occurred in this case. So overcome this problem using the revocation technique.

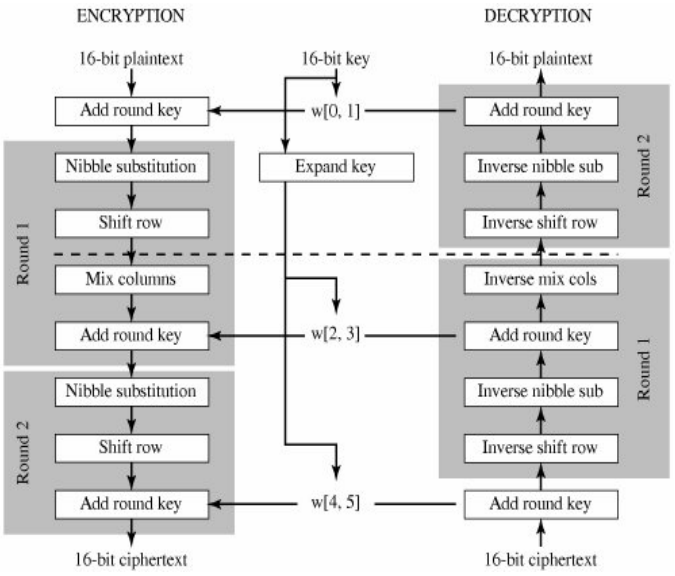
4.2 KUNodes

At the time of data sharing various nodes are participate. That is like data provider, number of user, storage server, and key authority. All these members are collaborating with each other. Each members or modules are connected to each other because of sharing of data securely in cloud computing. All modules are dependent to each other.

4.3 AES

Advanced Encryption Standard (AES) is a symmetric key block cipher published by the NIST in December 2001 [1]. The AES algorithm is used for encrypt data as well as decrypt data. In this paper, the AES algorithm is provide more security using re-encryption technique. Key is used for encryption and decryption purpose. Generate the key by using random function. Encryption key is collection of integer value and string value and same concept is applied on decryption key. The AES algorithm worked based on attributes.

4.3.1 Encryption & Decryption



5. RESULT ANALYSIS

5.1 MATCH KEY

In this paper, key authority sends the key to data provider and users. Key authority is responsible for generating the key. If the data provider receive key and user receive key is match the user will permitted to download the data. Otherwise her/him is cannot download the needed file. Matching key mechanism provide advanced security to sharing data in cloud computing. Key match operation will be failed then according to general mechanism unauthorized user accesses the authorized person account. Therefore, matching of key in important to secure data sharing in cloud computing.

5.2 TIME PERIOD

The time period is taken to users to download the data.

As per the time period user will write the OTP. Normally, size of OTP code is the 4 to 6 digit. In this paper, 6 digit integer number provided fir OTP. Each and every time OTP will be changed. So for that purpose, more security will provided. In case of within a time period OTP will not write then time will expired. And user cannot download the required files. For all this time period mechanism provide large security.

CONCLUSION

We have studied and implement a system for secure data sharing in cloud computing. We have used RS-IBE and AES algorithm to revoke as well as encryption, re-encryption and decryption. We have given time period to users for downloading data.

REFERENCES

[1] This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCC.2016.2545668, IEEE Transactions on Cloud Computing

[2] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," *SIAM Journal on Computing*, vol. 32, no. 3, pp. 586–615, 2003.

[3] International Journal of Scientific & Engineering Research Volume 3, Issue 3, March -2012 ISSN 2229-5518

[4] J. Yu, R. Hao, F. Kong, X. Cheng, J. Fan, and Y. Chen, "Forwardsecure identity-based signature: security notions and construction," *Information Sciences*, vol. 181, no. 3, pp. 648–660, 2011.

[5] iCloud. (2014) Apple storage service. [Online]. Available: https://www.icloud.com/

[6] Revocable Identity-Based Encryption Revisited: Security Model and Construction ∗ Jae Hong Seo*y* and Keita Emura*y* January 10, 2013

[7] A preliminary version of this paper appears in Proceedings of the 14th ACM Conference on Computer and Communications Security, CCS 2008, ACM Press, 2008. This is the full version.

[8] A preliminary version of this paper appears in Proceedings of the 14th ACM Conference on Computer and Communications Security, CCS 2008, ACM Press, 2008. This is the full version.

[9] Identity-based Encryption with Efficient Revocation Alexandra Boldyreva ∗ School of Computer Science Georgia Institute of Technology Atlanta, GA aboldyre@cc.gatech.edu