Secure Data Sharing in Cloud Computing

Sobia Tahniath, Master of Technology, Sharnbasva University, Faculty Of Engineering & Technology, Department of Computer Network & Engineering Kalaburagi-585103, Karnataka

Patil Yogita Dattatrya, Professor, Sharnbasva University, Faculty Of Engineering & Technology, Department of Computer Science & Engineering Kalaburagi-585103, Karnataka

Abstract -

Cloud computing provides convenient way in real time data sharing. Identification based encryption has been used in the data sharing. The data has to be traversed form one end to other end and in secured way or path. The structured and also the unstructured data will be generated every second in the real time by the multiple users and hence managing is important as it can be of many type of data like business, government media etc . A revocable-storage identity-based encryption (RS-IBE); has been proposed in the forward and the backward security for the cipher text which will update simultaneously. The implementation will give the results of proposed scheme for the implementation of data security in practicability.

***Key Words*: CLOUD COMPUTING, DATA SHARING, REVOCATION**

1. INTRODUCTION

Cloud computing is considered an emerging field as it allow the user to access the data from remote location. The security and flexibility are the features of the good cloud environment. The storage of the data at a remote location is very efficient for any user to access the same data. They user is allowed to access the data by password or key which will be passed through the key management known as the Auditing of the key. The user will be able to access the data. A revocable storage is proposed to enable the data sharing which provides the ID based encryption of the data.

1.1 PROBLEM STATEMENT

Failure of the Data exchange in the cloud environment in the system will play the negative role in the real time data transmission between end users. The data which has been transmitted from source to the destination has to be traversed between the node s y the fixed route and path by using the specific routing protocol like AODV. The management of the data in the RS-IBE assisted network by the secured encoding decoding scheme will be vital for data delivering in the cloud database.

1.2 OBJECTIVE

The main objective of the proposed work is to address the data security by ID based data encryption in the cloud network based data transmission over the cloud environment by using the re-routing algorithms. The user must be assured if the data delivery in revoke storage of cloud, as it adopts the system in multiple scenario of attacking. The loopholes of the data transmission have to overcome by using the multilevel security checks.

2. LITERATURE SURVEY

[1] This paper discusses the concept of Cloud Computing. Author has state the concept of dividing the data D into the number of blocks N in such a way that the complete data can be re-constructed at the receiver end by using the entire N Grids paradigm. Due to any Grid the N-1 paradigm is missed or deleted or destroyed than the data cannot be completed and will be in unreadable format. The use of the Grid paradigm which is the better exploit of the good relation between the Grid and Cloud approaches.

[2] The use of the dynamic "Social Cloud," has been proposed. In social networking the grouping of the heterogeneous data, a construction scheme including additive homomorphism, encryption scheme which no need of the extra round of interaction. In proposed scheme by author the total costs of the computation and also the cost for the storage is equal and also it is resilient for user size .The use of the social storage cloud has been used in the Face book.

[3] For accessing the remote data the cloud is very important aspect. They have chosen the use of the TPA: Third party approach in this work. The remote cloud based data access of the data has been proposed in the concept of data upload by the bandwidth. The encryption has been used by the author in the proposed concept extensively for the secure data de-duplication, the issue of making the convergent based on the data encryption in the practical which will manage the convergent keys by the data security. The Amazon service cloud has been used for the remote access of the data in the cloud.

[4] The data owner is considered to be the data owner. The data outsourcing, in the new paradigm of data hosting service given the new security challenges, collects the data it tends to work in efficiently and unreliably and it is design novel key mechanism by imaging a smart structured grid which will indeed secured data access, the total amount of the energy utilized in the total secured exchange of the data. Auditing paradigm helps in making sure the data is secured in auditing.

[5] Data storage and the real time data sharing services in cloud environment for the exchange of the data in the group. The use of the data supplier will be used in measuring the data in flow by use of the sensor nodes. Depending in the type of the data the sharing will provide the secure data and read and aggregate in the way cloud

has been designed by the user without worry of any type of the individual type of data. Experiments show the good and efficient of user revocation.

3. SYSTEM ANLYSIS

3.1 Existing System

There are many systems which are in the real time environment. Few of the successful concepts are Boneh and Franklin uses the cipher text, non-revoked key authority, binary tree to manage ID based on RIBE scheme, in the cloud environment has been proposed in the past.

DISADVANTAGES:

- Achieves selective security.
- Can't control the collusion of revoked, non-revoked users.
- Key authority needs to maintain table.

3.2 Proposed System

To overcome the disadvantage and to provide the higher security we have proposed the secured management of the data in the RS-IBE assisted network. It is secured in the ID based encoding decoding scheme will be vital for data delivering in the cloud database. The use of the data revoke in the cloud computing has been used to exchange data with the auditing key management.

ADVANTAGES:

- Construction of RS-IBE in concrete environment.
- Provide both the confidentiality & security.
- It can withstand decryption key exposure.
- Provide ID based encryption so higher security.

4. METHODOLOGY

- Construction of the System Module
- End to End Data Provider
- Cloud domain User
- Secret Key Authority (Auditor)

MODULES DESCSRIPTION:

Construction of the System Module:

In the proposed work the generation of the Cipher Text is made by the user at the end. The encoded message over cloud has to be processed and stored later. The communication line will be opened.

Data Provider:

File uploading by end user has to be in the cloud server. The data is uploaded with key generated Cipher Text. The user uploads the file to the end user and transmits to their end user. The server using revocable storage allows the end user to store the data to access it later. The auditor followed to provide access.

Cloud User:

The Cloud User module allows users to Signup initially for authentication and option of file searching has been provided. Then cloud user feature used to send the Request to Auditor to access file from cloud. Decrypt key obtained from the Auditor later to access the File. The cloud user enabled file downloading. After the completion of the process user logout the session.

Secret Key Authority (Auditor):

The cloud network Auditor Login to the Auditor's page. User verifies the pending requests of any person. Based on the request of the user the key is generated as the master key for process of the encrypt and the cloud based Secret key for the process of the decrypt. Later; after successful data exchange over the cloud environment the Auditor will logout the session.

5. SYSTEM ARCHITECTURE

Fig-1: Basic block diagram

In fig-1 it shows the basic block diagram, where first the data provider uploads the cipher text of the file to the cloud storage server. When the user needs the shared data file, it sends request for key authority. The key authority accepts the request for the respective user and sends the secret key to the corresponding user maid id. Later, the user login by user name and password, after the successful verification user can access the file. In some case, user authorization gets expired; the data provider will decrypt then re encrypt the file to the cloud server such that the unauthorized user cannot be able to access the file.

5. DATA FLOW DIAGRAM

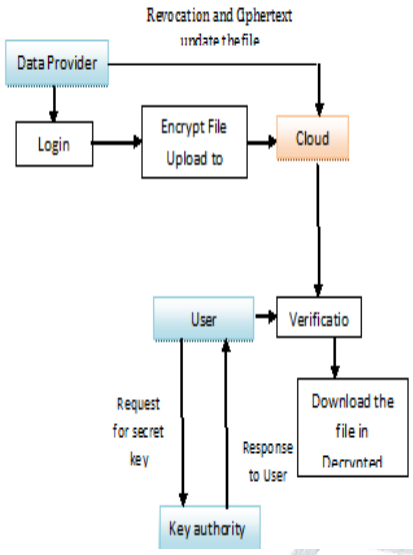

Fig-2: Data flow diagram

6. RESULTS

Fig 6.1- Figure shows the data provider login page. The data provides first needs to register, then login with the respective user name and password.

Fig 6.2- Figure shows the uploaded file details done by the data provider.

Fig 6.3- Figure shows the user request for file access. First, the user needs to register and login with the username and password.

Fig 6.4- The auditor has the authority to send the secret key to the user mail id.

Fig 6.5- The user will login and copies the secret key from the mail id and gets the respective file download.

Fig 6.6- In some case,if user authorization gets expired, the data provider shown in figure does the revoation and

chiper text update such that the expired user has no access to that file.

Fig 6.6- Now if the user tries to access that file it shows the pop up message as secret key does not matched. So, the unauthorized user can no longer access to that file.

7. CONCLUSION

Cloud Computing concepts have brought the convenience for the remote people. The use for the RS-IBE used the ID based encryption for the generation of the cipher text has to be generated simultaneously. The cipher text is generated based on the key generated to exchange the data over the cloud. The proposed work has given the efficient way of accessing the data in secured way. The use of the revocable storage has allowed the auditing of the files over the cloud in the decisional ℓ-DBHE assumption. Proposed work is more feasible for the practical applications compared to other works.

REFERENCES

[1] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," *ACM SIGCOMM Computer Communication Review*, vol. 39, no. 1, pp. 50–55, 2008.

[2] K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana, "Social cloud computing: A vision for socially motivated resource sharing," *Services Computing, IEEE Transactions on*, vol. 5, no. 4, pp. 551–563, 2012.

[3] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy preserving public auditing for secure cloud storage," *Computers, IEEE Transactions on*, vol. 62, no. 2, pp. 362–375, 2013.

[4] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 24, no. 9, pp. 1717–1726, 2013.

[5] B. Wang, B. Li, and H. Li, "Public auditing for shared data with efficient user revocation in the cloud," in *INFOCOM, 2013 Proceedings IEEE*. IEEE, 2013, pp. 2904–2912.