European Journal of Molecular & Clinical Medicine
ISSN 2515-8260 Volume 07, Issue 08, 2020

Honey Encryption Technique For Access Control In Public Cloud Environment

Mr.Nagendran.K[1], Mr.Aravindha Hariharan.M[2], Gowtham.G[3], Kabilan.S[4]
[1]*Assistant Professor, Department of Information Technology, Sri Krishna College of Engineering and Technology,* ***nagendrank@skcet.ac.in***
[2]*Student, Department of Information Technology, Sri Krishna College of Engineering and Technology, 18euit009@skcet.ac.in*
[3]*Student, Department of Information Technology, Sri Krishna College of Engineering and Technology, 18euit042@skcet.ac.in*
[4]*Student, Department of Computer Science and Business Systems, Sri Krishna College of Engineering and Technology, 18eucs144@skcet.ac.in*

Abstract-

In the present scenario, the difficult task is to handling the data and control the access of data. Attribute Based Encryption (ABE) is an encryption method which will be mainly applicable for access outsourced data. By using ABE-based schemes not supports access with collaboration. This paper proposed attribute-based control technique in this the users can collaborate by getting the access permission from data owner for all its attribute sets. We propose a technique which will improve data security and confidentiality.

Key Terms: CP-ABE, Cloud Computing, Honey Encryption

1. INTRODUCTION

This concept mainly Deals with leasing of resources in order to reduce the maintenance cost for cloud users. Cloud resources and services can be used at anywhere and anytime due to the cloud policy of pay only for the data used.

To utilize the benefits of cloud, more individuals and organizations are ready to adopt their applications with cloud environments. Data are managed and administered by third party on remote cloud servers in order to access public cloud storage.

For controlling the access in cloud storage environment which is public, the CP-ABE schemes are devoted in this the attribute sets are associated with each users and cipher text is embedded with chosen attributes along with access structure. The access structure is to access policy which is needed to access the contents of data.

If the access structure, get satisfied with user's attribute set which can decrypt the cipher text and embedded in the cipher text. CP-ABE is used in public cloud storage for flexible and secure data access. Assigning access permission to user who has their own attribute sets which satisfy the access policy. Single users alone can't be able to obtain the secret information; It is needed to share the files among multiple users with various responsibilities to maintain data confidentiality [1].

Collaboration between the users with different responsibilities needed to permit data access request. Each user must be labelled with attribute set based upon his/her responsibility for fine grained access control. It must need to meet the conditions: 1.Individual must satisfy an access structure with sufficient attribute set.2.The users must collaborate with users who have different integrated set of attributes to access the required data. This scheme allows the users to collaborate inside the group even if is not allowed by the data owner. To provide collaborative access and confidentiality, the users within the same project group are

allowed to collaborate. Translation nodes are designed in access structure to provide collaboration in access structure [2]. In order to maintain unwanted collision, the collaborating users attribute sets are not relevant with translation nodes.

The following problems are addressed as 1.Collaborative data access control and attribute-based controlled collaborative access control mechanism are proposed.2.Mechanism to modify secret keys and cipher text by designating translation nodes in policy trees. 3. Divide the users into particular groups to restrict access and provide security [3].

EXISTING SYSTEM

- It allows the users to utilize remote resources instead of buying new hardwares to reduce maintenance cost.
- Apply CP-ABE to provide secure and flexible data access control for public cloud storage.
- To satisfy the access policy the users are assigned with own attribute sets using existing CP-ABE.

2.1 DISADVANTAGE OF EXISTING SYSTEM

- Low Security
- More time consumption
- Utilization of CP-ABE algorithm

3 PROPOSED SYSTEM

- Access for data will be allowed when collaboration occurs between multiple users with various responsibilities.
- Collaboration will be restricted for the user in the same group to the same project.
- To provide collaborative access control and confidentiality, the individuals responsible for same project only allowed collaborating. Data owners designate translation nodes within the access structure to allow collaboration [4].

4 PROBLEM DEFINITION

- Propose collaborative access control scheme based on attribute set to provide data access control.
- Access policies defined with data owners expected collaboration.
- Designate translation nodes in policy trees and modify secret keys and cipher texts to allow collaboration.
- Translation key embedded inside the secret key with translation value for each translation node cipher text.
- To restrict collaboration and provide security ,the users must be divided into groups

4.1 ADVANTAGE OF PROPOSED SYSTEM

- More Secure
- Time Consumption is very less.
- Easy data accessibility.

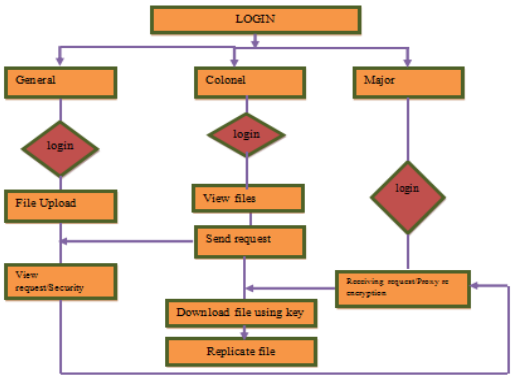


Fig. 1.Data flow Diagram

4.2 ALGORITHM

- Honey Based Encryption Algorithm is used to improve the security and confidentiality.
- Honey encryption is an encryption scheme, which produces a cipher text, when decrypted with fault key as guessed by the attacker, represents incorrect plaintext.
- Honey Encryption tool is to carry out a brute force attack to identify if he has correctly guessed a key for encryption.
- Decryption will be carried out for the file using secret keys when the user is permitted to send the request.

5 MODULE DESCRIPTION

5.1 Certification of files

File certification is needed to upload a file in the cloud. After certification the data owner can upload the files in the cloud in encrypted format for providing data security.

Fig. 2.Certification of files

5.2 Privacy protection

Encrypted file will be uploaded by the data owner to provide security. A random key is generated for data uploading. After the file uploaded into the cloud by data owner, some data can be hidden by the data owner [5] .The hidden files can be changed into unmasked format if data owner wants to display the hidden data.

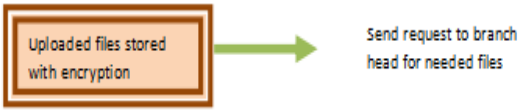


Fig. 3.Uploading files with security.

5.3 Request generation

Except hidden file present in the server, the remaining data/ files can be view by the user. The data owner must grant permission for the user to access the data or a file. The data owner verify the user requests and then forward the requests to an authenticator to send TTP for the user.

Fig. 4.Request Generation

5.4 Forward security

Data owner transfer the secret key to the third party after verification of the request. The unauthorized users not allowed to access the data .Using the secret key send by the authenticator to user mail ID and the users can access the restricted data.

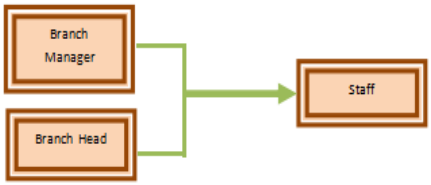


Fig 5.Forward Security

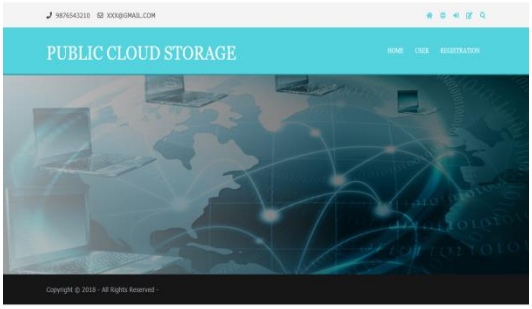
5.5 Access the files

Authenticator mailed the secret key to particular user then the user can access the file or a data in the server using the secret key and also to decrypt and download the file from the server.

Replicate Files

The overall user details in data centre of cloud will be viewed by the admin to maintain the details. Based on the frequent access the file is reduced .In order to maintain efficiency the optimized energy is preserved on files.

6 IMPLEMENTATION AND RESULTS




PUBLIC CLOUD STORAGE
HOME USER REGISTRATION
Submit Query
Copyright © 2018 - All Rights Reserved -

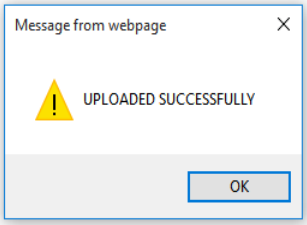

PUBLIC CLOUD STORAGE

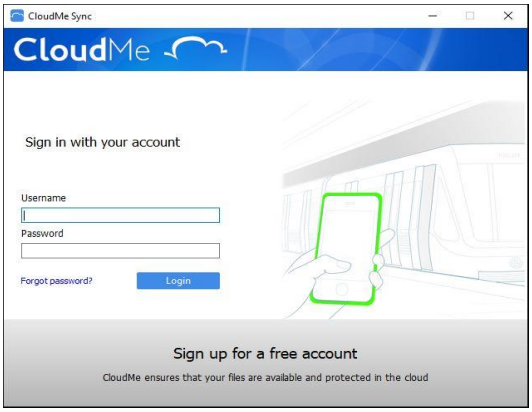

PUBLIC CLOUD STORAGE
HOME USER REGISTRATION
Secret Key...
Submit Query
Copyright © 2018 - All Rights Reserved -

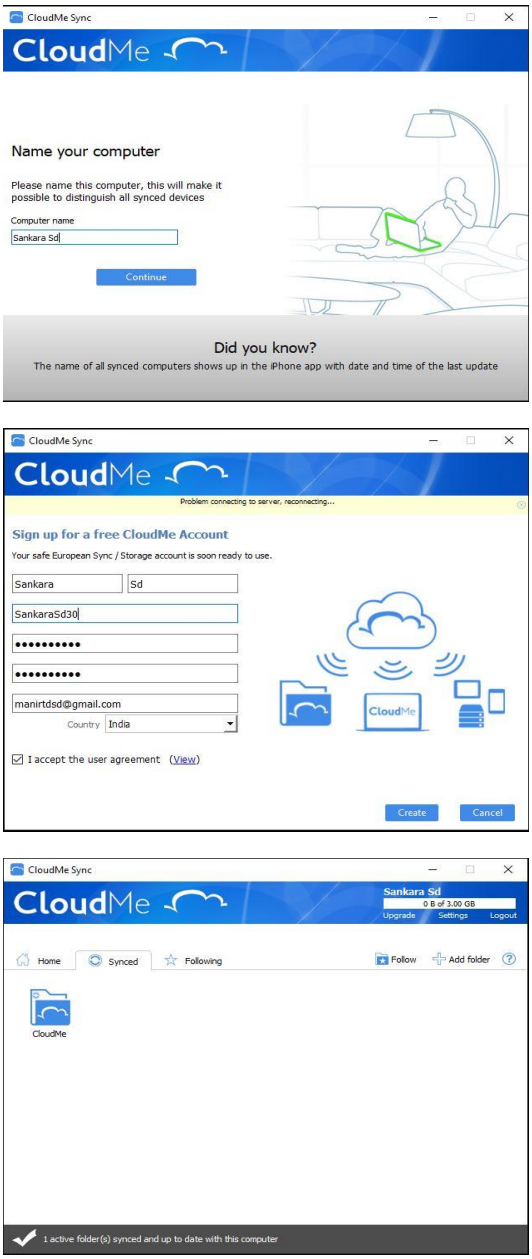

PUBLIC CLOUD STORAGE
HOME UPLOAD VIEW REQUEST LOGOUT
Logged as : Saikara
Copyright © 2018 - All Rights Reserved -


PUBLIC CLOUD STORAGE
HOME
UPLOAD
VIEW REQUEST
LOGOUT
UPLOAD


PUBLIC CLOUD STORAGE
HOME
UPLOAD
VIEW REQUEST
LOGOUT
UPLOAD


Message from webpage
UPLOADED SUCCESSFULLY
OK


CloudMe Sync
CloudMe
Sign in with your account
Username
Password
Forgot password?
Login
Sign up for a free account
CloudMe ensures that your files are available and protected in the cloud



CONCLUSION

- Translation keys are embedded inside secret keys to provide data confidentiality and collaboration control within the same group. Data owner designate translation node in access structure to provide data security in access .policy
- Proposed scheme provides effective access control in collaboration in which the data need to be accessed by multiple users.

FUTURE WORK

The cost of computation in cloud for file downloading is independent of number of users. The data files needs some algorithm to decrypt .The file cost not depends on the size of file. Our scheme encrypted message is irrelevant to requested file size and cloud operations for decryption.

REFERENCES

1. K. Yang, X. Jia, K. Ren, and B. Zhang, "DAC-MACS: Effective data access control for multi-authority cloud storage systems," in Proceedings of the 32nd IEEE International Conference on Computer Communications (INFOCOM). IEEE, 2013, pp. 2895–2903.

2. Y. Wu, Z. Wei, and H. Deng, "Attribute-based access to scalable media in cloud-assisted content sharing," IEEE Transactions on Multimedia, vol. 15, no. 4, pp. 778–788, 2013.

3. K. Xue, Y. Xue, J. Hong, W. Li, H. Yue, D. S. Wei, and P. Hong, "RAAC: Robust and auditable access control with multiple attribute authorities for public cloud storage," IEEE Transactions on Information Forensics and Security, vol. 12, no. 4, pp. 953–967, 2017.

4. K. Xue, W. Chen, W. Li, J. Hong, and P. Hong, "Combining data owner-side and cloud-side access control for encrypted cloud storage," IEEE Transactions on Information Forensics and Security, vol. 13, no. 8, pp. 2062– 2074, 2018.

5. A. Shamir, "How to share a secret," Communications of the ACM, vol. 22, no. 11, pp. 612–613, 1979.