File Hierarchy Attribute Based Encryption Scheme in Cloud Computing

Prof. K. R. Pathak[1], S. G. Game[2]

[1] *Assistant Professor, Computer Engineering Department, PREC Loni, Maharashtra, India*
[2] *Student, Computer Engineering Department, PREC Loni, Maharashtra, India*

ABSTRACT

To solve the issue of secure data sharing in cloud computing, Cipher-text policy attribute based encryption (CP-ABE) has been preferred encryption method. The shared data files in most cases have the features of multilevel hierarchy, specifically in the area of healthcare and the military. However, the hierarchy system of shared files has not been explored in CP-ABE. In this paper, an effective file hierarchy attribute-based encryption method is proposed in cloud computing. The layered access structures are included into a single access structure, and then, the hierarchical files can be encrypted with the integrated access structure. The cipher text components similar to attributes could be shared by the files. Therefore, both cipher text storage and time cost of encryption is preserved. Moreover, the proposed scheme is proved to be secure under the entire assumption. Experimental simulation shows that the proposed method is more capable in terms of encryption and decryption. With the number of the files increasing, the benefits of our method more and more clear.

Keyword : - *Cloud Computing, data sharing, file hierarchy, cipher text-policy, attribute –based encryption.*

1. INTRODUCTION

With the growing of network technology and mobile terminal, online data sharing has become a new "pet", such as Facebook, Myspace, and Badoo. Meanwhile, cloud computing is one of the best assuring application platforms to solve the dangerous expanding of data sharing. In cloud computing, to protect data from lossing, users need to encrypt their data before being shared. Access control in dominant as it is the first line of defense that prevents unauthorized access to the shared data. Recently, attribute-based encryptions (ABE) have been attracted much more concentrated since it can keep data privacy and realize fine-grained, one-to-many, and non-interactive access control. Cipher text-policy attribute based encryption (CP-ABE) is one of appropriate schemes which has much more adjustability and is more applicable for most of applications.

2. System Architecture

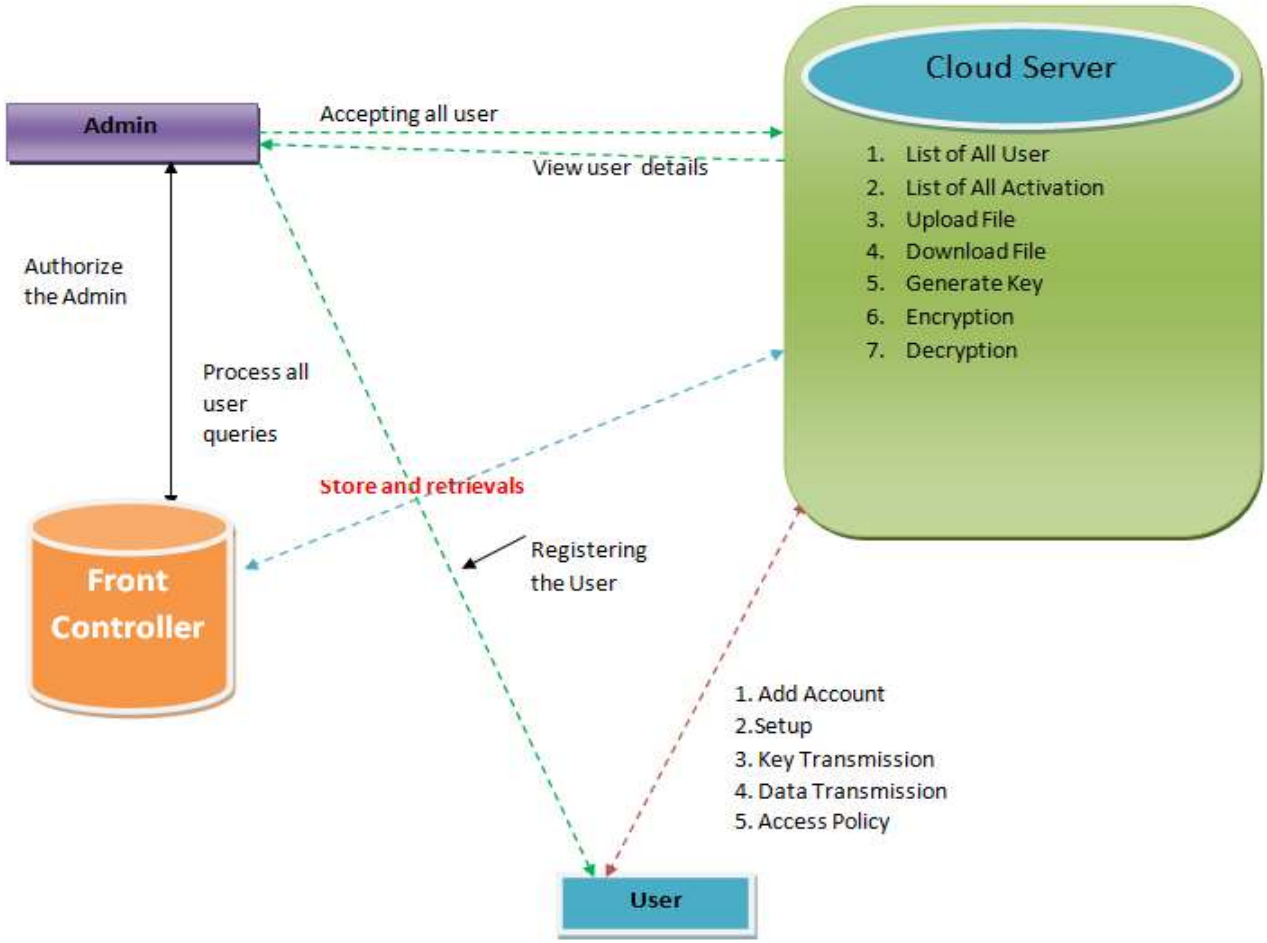


Figure-1: **System Architecture**

Data Owner:
Register with cloud server and login (username must be unique).Send request to Key transmission to generate ABE Key on the user name. Browse file and request Private Key to encrypt the data, Upload data to service provider. Verify the data from the cloud.

Public Key Generator (Key Transmission):
Receive request from the users to generate the Key, Store all keys based on the user names. Check the username and provide the private key. Revoke the end user (File Receiver if they try to hack file in the cloud server and un revoke the user after updating the private key for the corresponding file based on the user).

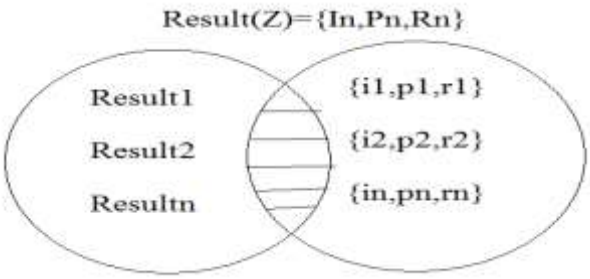
End User:
1. In this module receiver first has to Register and login, Request secret key, Request available files in the cloud and receive files.
2. Every key come respective unique id.

Data Sharing:
1. Data Share group wise as per authorized account.
2. Every File key changeable.

3. Mathematical Model

- Set theory : Let S = I,P,R,O,K
- Where,
- S: Public integrity auditing system.
- I: Set of inputs.
- P: Set of processes.
- R: Rules or constraints.
- K: Keyword
- O: Set of outputs/Final output.
- I = i1, i2,.....,in
- Where,
- i1,i2,...,in = Files shared by the users.
- P=p1, p2, p3, p4, p5, p6, p7
- Where,
- p1: Key generation
- p2: Generate commitment string
- p3: Open
- p4: Verify
- p5: Update.
- p6: Proof Update.
- R = r1
- Where,
- r1: Revoked user should not be able to access files shared by users.
- r2: Proper keyword should be extracted.
- Where,
- O1: Valid user cloud access any file.

  Output:-
- Result(Z) ={In,Pn,Rn}
- In->i1,i2,i3,.....in(Share file)
- Pn-> p1,p2,p3,....pn(process)
- Rn-> r1,r2,r3.....Rn(Revocation)
- Result(Z) = {pi, 0<I<k}.....set of probability
- ~Result(Z) = {pi,(K,mi),{false otherwise}}
- here , K(Z) = {ki, 0<I<n} Set the keyword.



4. Conclusion

To proposed a variant of CP-ABE to efficiently share the hierarchical files in cloud computing. The hierarchical files are encrypted with an integrated access structure and the cipher text components related to attributes could be shared by the files. Therefore, both cipher text storage and time cost of encryption is saved. The proposed scheme has an advantage that users can decrypt all authentication files by computing secret key once. Thus, the time cost of

decryption as also saved if the user needs to decrypt multiple files. Moreover, the proposed scheme is proved to be secure under DBDH assumption.

5. REFERENCES

[1] C.-K. Chu ,W.-T. Zhu, J. Han, J. –K. Liu, J. Xu, and J. Zhou, Security concerns in popular cloud storage services, IEEE Pervasive Computing., vol.12,no.4,pp.5057,Oct./Dec.2013.
[2] T. Jiang , X. Chen, J. Li, D. S. Wong, J. Ma, and J. Liu, TIMER: Secure and reliable cloud storage against data re-outsourcing, in Proc. 10th Int. Conf. Inf. Secure.Pracr.Exper.,vol.8434.May 2014,pp.346358.
[3] K. Liang, J. K.. Liu, D. S. Wong, and W. susilo, An efficient cloud based revocable identity-based proxy re-encryption scheme for public clouds data sharing, in Proc.19th Eur.Symp.Res.Comput.Secure.,vol.8712.Sep.2014,pp.257272.
[4] T.H. Yuen, Y. Zhang, S.M. Yio, and J.K. Liu, Identity-based encryption with post-challenge auxiliary inputs for secure cloud applications and sensor networks, in Proc. 19th Eur.Symp. Res. Comput. Secure., col. 8712.Sep.2014,pp.130147.
[5] K. Liang et al., A DFA-based functional proxy re-encryption scheme for secure public cloud sharing, IEEE Trans. Inf. Forensics Security, vol.9, no.10, pp.16671680, Oct.2014.
[6] T.H. Yuen, J. K. Liu, M. H. Au, X. Huang, W. Susilo, and J. Zhou, k-times attribute-based anonymous access control for cloud computing, IEEE Trans.Comput.,vol.64,no.9,pp.25952608,Sep.2015.
[7] J.K. Liu, M.H. Au, X. Hiang ,R. Lu, and J. Li, Fine-grained two factor access control for Web-based cloud computing services, IEEE Trans. Inf. Forensics Security,vol.11,no.3,pp.484497,Mar.2016.
[8] A. Sahai and B. Waters, Fuzzy identity-based encryption, in Advances in Cryptology. Berlin, Germany: Springer, May 2005, pp.457473.
[9] V. Goyal, O. Pandey, A. Sahai, and B. Waters, Attribute-based encryption for fine-grained access control of encrypted data, in Proc.13th ACM Conf. Comput. Commun. Secur., Oct.2006,pp.8998.
[10] W. Zhu, J. Yu, T. Wang, P. Zhang, and W. Xie, Efficient attribute-based encryption from R-LWE, Chin. J. Electron., vol.23, no.4, pp.778782, Oct.2014.