© 2016 IJSRST | Volume 2 | Issue 2 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

Data Security in Cloud Using Semi Trusted Third Party Key Manager

M. Akhila, E. Hemalatha, S. Parvathi, Karthikeyan. L

Department of Information Technology, Dhanalakshmi College of Engineering, Chennai, Tamilnadu, India

ABSTRACT

In our project Off-site data loading is an request of cloud that releases the clients from focusing happening data storing scheme. However, subcontracting facts to a third-party directorial switch involves grave security concerns. Data leak might occur owing to bouts by additional operators and tackles in the cloud. Wide of facts by cloud ability worker is yet another problem that is met in the cloud location. Thus, top of security events is requiring. In this paper, we offer Data Safety for Cloud Setting with Semi Trusted Third Party (DaSCE), a data security system that provides (a) key management (b) access control, and (c) file assured deletion. The DaSCE utilizes Shamir's (k, n) threshold scheme to manage the keys where k out of n shares are required to generate the key.

Keywords : ABE, RSA, Diffie-Hellman, Elgammal, DES, Shamir(k,n) Techniques

I. INTRODUCTION

Cloud computing is a promising evaluating standard and has shown large potential for managing hardware and software placed at third party, Which relieves the customer from managing complex infrastructure [1, 10] Storing Data in cloud has many advantages as Cloud has efficient access mechanism of data and an efficient retrieval mechanism. In addition, Attribute Based Encryption (ABE) has proved to be efficient in data security. As the name suggests this encryption makes The data available to users whose attributes satisfy the access policies defined by the data owners. Currently when access policies are changed, cloud has to upload the data in it to the local site, change the access policy and then add back the data. This involves heavy communicational and computational load.

II. METHODS AND MATERIAL

A. Related Work

Firstly, in this user has to register to become a member in cloud, and the registration process is in java. Once they registered user has to choose some attributes (e.g. name, email, address etc..,) and also give some user defined attributes to encrypt their policy file which is created while the process of uploading. This Attribute Based Encryption performed using Elgammal algorithm. Attribute Based Encryption is used while policy setting. After finishing the above procedure, authentication process takes place between user and the key manager with the help of Diffie-Hellman algorithm. Then the user will encrypt their file using secret key provided by Cloud to the user based, on user attributes and then it will upload into cloud and the policy file is generated concurrently and it contains username, filename and access permission by default user will be allowed for the process. Now user breaks up secret key into n shares (S1,S2...Sn) using Shamir key sharing technique and user encrypts their i-th key share with public key if i-th key manager.

In addition, the keys are splitted and given to the key manager in the encrypted form. If users need to download their file, then they will send request to key-manager with appropriate attributes. Key- manager will check their attributes and decrypt the appropriate users policy file and check the users file admit approval validate user, now key- manager will decrypts user secret key by using their own private key and provide decrypted i-th share to the requested user. The secret key will be reformed by shamir secret scheme only if the attributes and credentials are proven. Now user will

receive their secret key, download their file, and decrypt using their secret key.

In this phase user will set revocation and renewalling of policies, for policy revocation user send revocation request to the key manager. Revocation is nothing but user will remove all the policies that he/she set before. User policy revocation request send to key manager, they delete all the policies of the user, in policy renewal key manager will allow to renew the user existing policy. Once he/she got approval from key manager user will renew their policy. Now key manager will generate new set of keys and encrypt the user's policy file by using user's new policy.

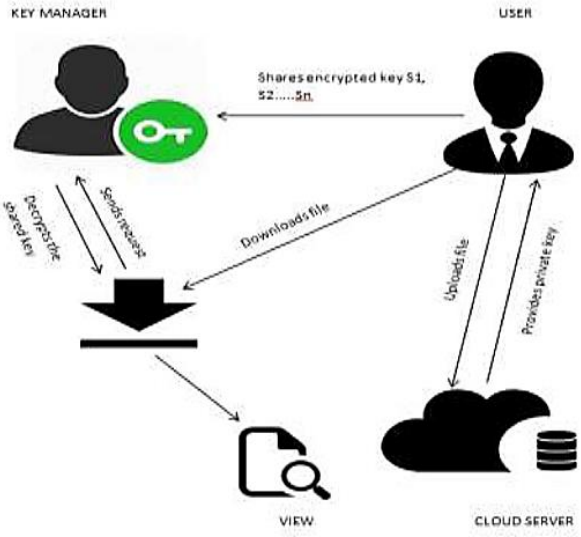

Figure 1. Architecture Diagram

Now, the above architecture diagram explains how the app works. The user has to Login by their default, user defined attributes, and policy file is created simultaneously. While uploading the file, secret key will be generated and is provided to the user. User breaks the secret key and encrypts their key share with public key of key manager. Now key manager will decrypt user secret key by using their own private key and they provide decrypted share to the user. If users need to download their file, then they will send request to Key-Manager with appropriate attributes. Key-Manager will check their attributes and decrypt the appropriate user policy file and check the user's file access permission for authenticate user. User policy revocation request send to key manager, they delete all the policies of the user, in policy renewal key manager will allow to renew the user existing policy.

B. DaSCE

The DaSCE makes usage of both symmetric and asymmetric keys. The privacy and honor services for fact are providing through symmetric key that are protected by expending asymmetric keys.

For secure show of keys, a conference key is recognized between client and KM through STS protocol. To evade man-in the middle attack. Together client and KM are genuine by using cardinal signatures.

1. User starts term formation and needs for asymmetric keys.
2. User and Key manager validate each other and create term.
3. Key manager makes asymmetric keys and sends open part to client.
4. User makes encryption actions over facts and symmetric keys.
5. User sends encrypted keys to the cloud.
6. Eradicates duplicate of keys.

III. RESULT AND DISCUSSION

Experimental Results

The first screen is a register screen wherein we can register ourselves. After registering, we have to upload a data in cloud for security .Then it will generate secret keys to user and shared to key manager in encrypted form the user can download as long as he is defined to be a user who can download by the policy. The user is verifies whether authorized by with the help of ABE key. If he is a user who tries to download, send request to key manager with appropriate points. Key manager checks and provide permission to user.

IV. CONCLUSION

Hence, we proposed and developed the DaSCE protocol, a cloud storage security system that provided key-management, access control, and file deletion. The key management was accomplished using (k, n) threshold secret sharing mechanism.

V. FUTURE ENHANCEMENTS

Policy File Encryption Policy files are generated When user upload their files in cloud. Inside the policy file contains username, filename that is upload by the user and access permission then Key Manager will encrypt the policy file by using user attributes.

VI. REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Ktaz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoics, and M. Zaharia, "A View of Cloud Computing" Communications of ACM, Vol. 53, No. 4, 2010, pp.50-58

[2] M. S. Blumenthal, "Is Security Lost in the Clouds?"Communication and Strategies, No. 81, 2011, pp. 69-86.

[3] C.Cachin-+and M.Schunter, "A cloud you can trust," IEEE Spectrum,Vol. 48,No. 12, 2011,pp. 28-51.

[4] C.Cremer's, "The Scyther Tool: Verification, falsification and analysis of security protocols." In Computer Aided Verification, Springe Berlin Heidelberg,2008,pp.414-418

[5] Cloud Security Alliance http://downloads.cloudsecurityalliance .org/initiatives/cdg/CSA_ CCAQIS_ Survey.pd f (accessed March 24, 2013).

[6] W. Diffie, P. C. V. Oorschot, and M. J. Wiener, "Authentication and authenticated key exchanges," Designs, Codes and Cryptography, Vol. 2, No. 2, 1992, pp. 107-125.

[7] M. Ali, K. Bilal, S. U. Khan, B. Veeravalli, K. Li, and A. Y. Zomaya, "DROPS: Division and Replication of Data in the Cloud for Optimal Performance and Security," IEEE Transactions on Cloud Computing, 2015,DOI:10.1109/TCC.2015. 2400460

[8] N. En and N. Srensson, "An extensible SAT-solver,"Lecture Notes Computer Science, vol. 2919, Springer, 2003, pp. 502-518.

[9] C P. Gomes, H. Kautz, A. Sabharwal, "Satisfia-bility solvers," In Handbook Of Knowledge Representation, Elsevier, 2007.

[10] M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges," Information Sciences, Vol. 305, 2015, pp. 357-383.

[11] A. Juels and A. Opera, "New Approaches to security and Availability for cloud data," Communications of the ACM, Vol. 56, No. 2, 2013, pp. 64-73.