Secure and Scalable System by integrating CP-ABE with Proxy

Natasha D'Souza, Dolly D'Souza, Valentine Correia., Mr. Vimal Ram
B.E 8th sem, Department of Computer Science and Engineering, SJCET Palghar, India
Asst. Prof. Department of Computer Science and Engineering, SJCET Palghar
1. nats811@gmail.com
2. dolly.dsouza17@gmail.com
3. valencorreia@gmail.com

Abstract:

Data stored in the remote database should be kept in a secure and confidential manner it should not be accessed by any unauthorized user. Some changes are being made to the ABE (Attribute Based Encryption) Algorithm in order to decide the set of users to access the data. The already existing Semi-Trusted authority can be changed to complete trusted authority by only keeping a track of the logs and not the data. It will also have the ability to revoke a particular user, hence adding more security.

I. INTRODUCTION:

File servers provide the advantage of secure and trusted storage by the data manager outsourcing the data on any remote database comes with a requirement of the accessibility of the data by users.

A major concern is that the server should be able to differentiate between authorized and unauthorized users. A database manager may or may not be trusted inspite of certain protocols and obligations. Hence it's the need of the hour to enforce the security measures.

The data owner and the data user need to have two different logins. This is done in order to provide fine grained access. The owner has to decide a certain set of attributes as to who can access the data, hence preventing unauthorized data access.

The database manager has no access to read or manipulate the data for security reasons which makes it completely trusted. The database manager can only keep a track of all the logs of the data in the database and possesses the attributes. Certain group of users possess a uniform secret key, hence encouraging group keying mechanism. The data owner has the authority to change the set of attributes as per his requirements, which in turn changes the access policy, hence prompting the database manager for re-encryption, on revocation or introduction of a new user, encouraging additional security to the system.

II. RELATED WORK:

This is not a completely new concept, there were many algorithms and methods proposed, but most of the methods proposed then had various types of short comes or limitations.

- In [2], asymmetric key management system such as RSA (Authors: Rivest, Shamir and Adleman) is used, its drawback is that it needs a data owner to be present throughout and give an encrypted version of the file for every user that wants to access the file.

- Another algorithm Elliptic curve encryption (ECE) [3] was also used but it was completely dependent on a manger who uploads the encrypted file and distributes the attributes and also performs re-encryption and many other activities.

- In [7] the CP-ABE (Cipher text Policy-Attribute Based Encryption) is a very important and efficient scheme but it relies on the data owner for permission to access the data using an access tree, which requires the owner's constant availability, moreover revocation of an authorized user is complex to be done in CP-ABE.

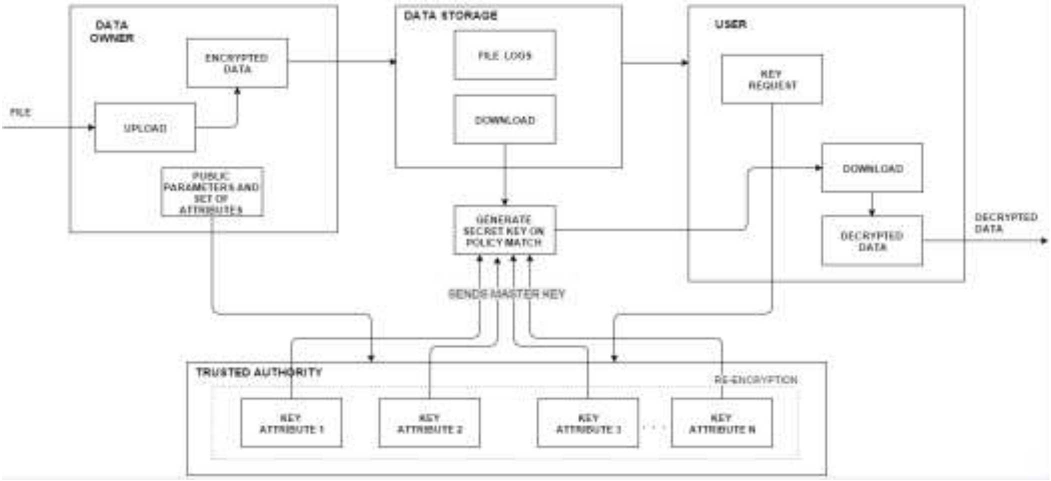
- There is yet another technique that is a combination of CP-ABE with proxy based re-encryption, but it is not does not efficient at all for users, since the decryption process needs the processing of two access sub-trees instead of one.

- Another related work in [4] proposes the integration of ABE (Attribute Based Encryption) with proxy based re-encryption that allows fine-grained access control of resources to the third-party or provider or manager during the process of re-encryption.

-In another proposal the re-encryption occurs due to attribute re-definition and this proposal is based on KP-ABE (key-policy attribute-based encryption) and not CP-ABE, where the cipher-text is associated with a policy.

Many more works have been conducted that is not of that relevance for this proposed scheme.

III. ARCHITECTURE:



The proposed architecture of this system consists of three main modules along with the data storage. The three modules are the data owner (who uploads the files to be shared among the users), the trusted authority (who works as the proxy and manages the data in the data storage) and the user (who uses the files shared by the data owner).

Initially a file is created by the owner this file is confidential and cannot be shared publicly. Hence security is provided by encrypting file by using Cipher-text Policy Attribute Based Encryption (CP-ABE). As our proposed system uses grouping mechanism, it enables the data owner to make a group of users with whom he wishes to share his data.

The trusted authority works as the manager. The trusted authority has access to all file logs of data uploaded and list of users in the groups created by the data owner. The trusted authority does not hold access to the data uploaded due to the additional security provided by CP-ABE but keeps a track of logs. The trusted authority is the proxy who decides about which user should be granted access to the data.

When a new user registers and requests to join a group, the proxy first checks its list of attributes. If the user fulfils the set of attributes, he is granted access and the system generates appropriate key using which the user can decrypt the data.

In the proposed system, we have introduced a new concept of proxy re-encryption. As we use grouping mechanism, the owner creates group of the users with whom he wants to share his data. The owner has the privilege to add new members to the group or revoke the existing members of the group. Depending on the choice of the owner, the attribute set given to the trusted authority also changes. To avoid the unauthorized use of data uploaded, the file is re-encrypted according to the new set of attributes.

This enables the system to preserve the confidentiality of the data uploaded by the data owner. During re-encryption, the keys are changed according to the new attribute set and these keys are sent to the authorised users of the system to avoid misuse of the data by the users whom the owner has revoked.

Thus the system provides users with a high level of security as well as enables fine grained data access with the data being shared to a number of authorized users using the grouping mechanism with the help of proxy.

DOI: 10.18535/ijsrm/v4i3.08

-Firstly the trusted authority runs the setup using certain security parameters, which generates a master secret key denoted by “MK” which is not shared and the master public key denoted by “PK” that is shared to all the users in the system.

-Thereafter the trusted authority enters the set of attributes sent by the data owner along with the MK which generates an output secret key denoted by “SK” according to the set of attributes provided. This SK is used to decrypt files at the user end.

-To encrypt the data, the algorithm accepts the message “M” uploaded along with the access policy assigned by the owner as well as the master public key, It generates the cipher-text stored in the data storage and shared only to authorized users.

-In case the owner changes the attributes, re-encryption is performed for re-encryption, a re-encryption key “RK” is generated. It takes the secret and the old as well as the newly generated access policy thus generating the Re-encryption key.

-For, re-encryption, the algorithm takes the cipher-text and the re-encryption key so as to generate a new cipher-text.

-While the user wants to download the file, it has to be decrypted which is done using cipher-text and secret key assigned to it according to the set of attributes given by the owner.

IV. CONCLUSION AND ON-GOING WORK:

In this paper a proposal for a key management system has been made for outsourcing important data in any database system, here, attribute-based encryption allows authorized users to access the data content in the system based on the fulfilment of the attributes. This proposal is being modified in such a way that the data owner and a trusted authority (i.e. the data manager or the proxy) co-operate with each other during the key generation and encryption processes which reduces the burden that falls on the data owner alone.

The user does not need to perform any complex activity instead, they are delegated to the manager/ third party server. Also, the manager computes the decryption key, not the data owner, and it assists with key distribution on behalf of the data owner.

Also, a mixture of protocols is proposed that optionally allows message encryption based on a group key, allowing the user membership to be further refined for highly sensitive data. Additionally, it allows re-encryption to occur, and thus revocation to become efficient without necessitating existing common; an example is the expiration of attributes specified in the attribute-based policy that leads to constant key updates as time elapses.

The proposed protocol is similar in overall performance to the original cipher-text-policy attribute-based-encryption idea, while significantly lessening the computational and traffic burden on the data owner in a system where data updates and encryption activities are frequent and dominant. Thus, the proposal is useful for securing data base computing with very large user populations

REFERENCES:

[1] P.K. Tysowski and M.A. Hasan, “Hybrid Attribute-Based Encryption and Re-Encryption for Scalable Mobile Applications in Clouds,” Technical Report 13, Centre for Applied Cryptographic Research (CACR), Univ. of Waterloo, 2013.

[2] R.L. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” Comm. ACM, vol. 26, no. 1, pp. 96-99, Jan. 1983.

[3] G. Zhao, C. Rong, J. Li, F. Zhang, and Y. Tang, “Trusted Data Sharing over Untrusted Cloud Storage Providers,” Proc. IEEE Second Int’l Conf. Cloud Computing Technology and Science (CLOUDCOM ’10), pp. 97-103, 2010.

[4] S. Yu, C. Wang, K. Ren, and W. Lou, “Attribute Based Data Sharing with Attribute Revocation,” Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS ’10),

[5]J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-Policy Attribute-Based Encryption,” Proc. IEEE Symp. Security and Privacy (SP ’07), pp. 321-334, 2007.

[6] A. Tassanaviboon and G. Gong, “OAuth and ABE Based
Authorization in Semi-Trusted Cloud Computing: Auth,” Proc. Second Int’l Workshop Data Intensive Computing in the Clouds (Data Cloud-SC ’11), pp. 41-50, 2011.

[7] K. Yang and X. Jia, “Attributed-Based Access Control for Multi- Authority Systems in Cloud

DOI: 10.18535/ijsrm/v4i3.08

Storage," Proc. IEEE 32nd Int'l Conf. Distributed Computing Systems (ICDCS), pp. 536-545, 2012.

[8]Xiaohui Liang†, Rongxing Lu†, Xiaodong Lin‡, and Xuemin (Sherman) Shen† †Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Canada ‡Faculty of Business and Information Technology, University of Ontario Institute of Technology, Canada {x27liang, rxlu, xshen}@bbcr.uwaterloo.ca; xiaodong.lin@uoit.ca