ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 19, April 2017

Encrypted data deduplication with secure access control using MA-ABE

[1]J.Joselin Sahaya Sheeba, [2]M.Senthil, [3]Abishek Udayashankar
[1,3]PG Scholar, CSE Department, SRM University
[2]Asst Professor in CSE Department, SRM University,Chennai
Email: [1]jssheeba.09@gmail.com
[2]senthil.m@rmp.srmuniv.ac.in
[3]abishek.u@gmail.com

Abstract: Attribute based encryption (ABE) is a encryption technique used most recently in cloud computing, social networks and other technologies that provides security and privacy. From different types of ABE, Multi-authority attribute based encryption (MA-ABE) scheme is used in this paper. In MA-ABE system there can be n number attribute authorities and k no. of users. Based on the attribute authority selected by the user , the corresponding decryption keys are generated by the MA-ABE scheme. It also deduplicate the duplicated data stored in the cloud. The data owner has the highest priority for data storage management.

Keywords: ABE, Multi-Authority Attribute based encryption, Deduplication.

1. Introduction

Multi-Authority Attribute based encryption system use different set of attributes for encryption and decryption. The multiple attribute authorities provide the secret attribute key to the users based on their identities.Both Deduplication and secure access control is provided by MA-ABE.

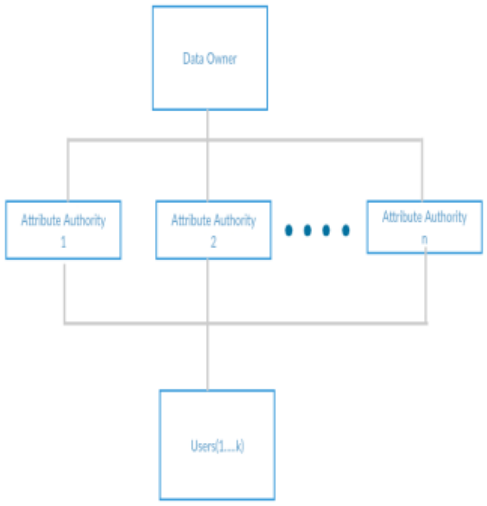

Fig 1: Multiple Authority Attribute based encryption

1.1. Problem Statement

Attribute based encryption use attributes for encryption and decryption of data.But these attributes are managed by only a single authority.If the authority fails then it affects the system.The single authority is responsible for providing secret key to the users,so the single authority can decrypt any cipher text in the system.The drawback of this system is the "Key Escrow " Problem. In order to avoid these drawback Multi-Authority attribute based encryption is proposed .This system consist of Multiple Attribute Authorities.These multiple attribute authorities are responsible for providing the secret attribute key for decryption based on the user's attribute.MA-ABE is more flexible for both deduplication and secure data access at the same time.

2. Literature Survey

2.1. Related Work

Sahai and Waters [11] introduced the notion of attribute-based encryption (ABE), and then Goyal et al. [12] formulated key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE) as two complimentary forms of ABE.

The notion of Multiple authority attribute based encryption scheme was first proposed by Chase[13]. The system uses the principles of trusted

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 19, April 2017

central authority (CA) and global identifiers (GID). The system also contains K attribute authorities. Each attribute authority is assigned a value dk.[13]. Message-locked encryption (MLE) aims to solve the problem in deduplcating the encrypted data..[1,2]. The most prominent manifestation of MLE is convergent encryption,[2] which is used in a wide variety of commercial and research storage service systems. Let M be a file's contents.

A client A first computes a key K ← H(M) by applying a cryptographic hash function H() to M, and then computes the ciphertext C ← E(K, M) via a deterministic symmetric encryption scheme. A second client B encrypting the same file M will produce the same C, enabling deduplication. However, because convergent encryption is deterministic and keyless, it's subject to an inherent security limitation—namely, susceptibility to offline brute-force dictionary attacks.[1] Secure convergent encryption is only possible when the target M is drawn from a space too large to exhaust. Mihir Bellare and his colleagues proposed DupLESS, which provides secure deduplicated storage to resist brute-force attacks.[3]

In DupLESS, a group of affiliated clients encrypt their data using a key server that's separate from a storage service. Clients authenticate themselves to the key server but don't leak any information about their data to it. As long as the key server remains inaccessible to attackers, DupLESS can ensure high security.Convergent encryption also suffers from another access control problem. It isn't flexible to control data access, especially for data revocation, since it's hard for data holders to generate the same new key for data reencryption. An image deduplication scheme adopts two servers to achieve verifiability of deduplication[.4]

A convergent encryption-based scheme described elsewhere combines file content and user privilege to obtain a file token with unforgeability[.5] However, the schemes we've described directly encrypt data with a convergent encryption key, so suffer from the access control problem we've described. To resist attacks involving manipulation of a data identifier, Pierre Meye and his colleagues proposed adopting two servers for intra-user deduplication and interdeduplication[.6] In their scheme, the ciphertext C of convergent encryption is further encrypted with a user key and transferred to the servers.

However, it doesn't deal with data sharing after deduplication among different users. ClouDedup also aims to cope with the inherent security exposure of convergent encryption, but it can't solve the problem caused by data deletion.[7] A data holder that removes the data from the cloud can still access that data if it isn't completely removed from the cloud since it still knows the data encryption key.

Other work proposed using proxy reencryption (PRE) to achieve encrypted data deduplication by applying an authorized party.[8] In many situations, data owners want to control data storage and access by themselves and track their own data's usage status. However, the solutions described here can't support this requirement in a flexible way.

3. Analysis of Framework

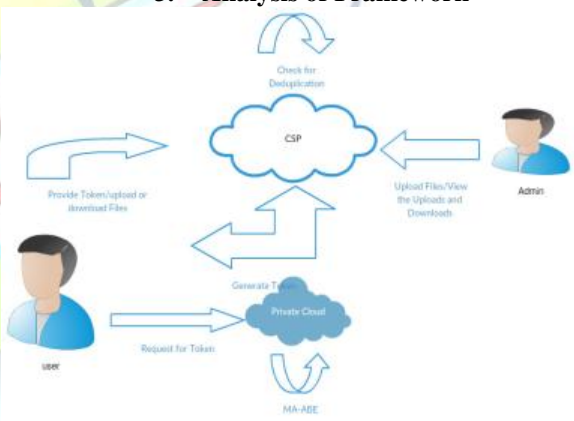

Fig 2: System Architecture

The system architecture expresses the overall workflow of proposed framework along with MA-ABE (Multi Authority-Attribute based Encryption) algorithm. This system is divided in three sections namely as

i)Private Cloud: it accepts user request & activate the user to perform the operation in cloud based on given rights. To authenticate the user, private cloud generates the token using MA-ABE algorithm along with their application handling rights. This information is communicated through registered user's email by private cloud.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 19, April 2017

ii) User: user operates the application in cloud environment, after getting the token. User can encrypt the data using MA-ABE technique, before uploading in cloud environment. Using Multi-Authority Attribute based encryption; file is uploaded in cloud server. Once, Server receives the encoded content then it will check the content from storage to avoid de-duplication. File duplication restricted and file stored in encrypt format from cloud service. Here, user can download, and view the content with valid key.

iii) **Admin:** Admin can view the list of user and their activity like file updating, file upload and file download with log details. This system avoids malicious or external attacks. It prefers secure and efficient data transmission in un-trusted cloud environment. [5] discussed about a method, In vehicular ad hoc networks (VANETs), because of the nonexistence of end-to-end connections, it is essential that nodes take advantage of connection opportunities to forward messages to make end-to-end messaging possible.

3.1. Algorithm

MA-ABE determines decryption ability based on a user's attributes. In a multi-authority ABE scheme, multiple attribute-authorities monitor different sets of attributes and issue corresponding decryption keys to users and encryptions can require that a user obtain keys for appropriate attributes from each authority before decrypting a message. In MA-ABE method data holder will fix the authentication policy based content sharing (which kinds of content for whom). The scheme can be constructed with the help of content details with descriptions. In this scheme encrypted data can is confidential even th ough server is un-trusted. A user can encrypt data in terms of any Boolean formula over attributes issued from any chosen set of authorities. During content transfer, any misleading is going to happen in either cloud server parts or external attack then proposed approach will update the key of content and send updated key to user automatically. It also send alert message to data holder as well trusted user Proposed scheme is simple, efficient and secure against collusion attacks. MA-ABE scheme consists of the following four techniques.

- **Setup:** This algorithm takes input parameter *k* and revert the public key *PK* as well as a system master secret key *MSK*. *PK* is utilized by message content senders for encryption. *MSK* is used to generate data holder's secret keys and it is known by authorized user only.
- **Encryption:** This algorithm accepts a message content *M*, the public key *PK*, and a set of attributes γ as input. It performs the ciphertext *CT*.
- **Key Generation:** This algorithm receive as input an access mechanism A, and the master secret key *MSK*. It provides a content secret key *SK* which enables trusted user to decrypt a encrypted message content under a set of attributes γ if and only if γ matches A.
- **Decryption:** It accept as input the data holder's secret key *SK* for access mechanism A and the cipher text *CT*, which was encrypted under the content attribute set γ. This approach performs the message content *M* if and only if the set of attribute γ assures the data holder's access mechanism *A*.

ContentBupdate(I, MSK)

// assume current version of attribute i is k ¡ 1;randomly pick $a'_i \xleftarrow{R} Z_{p;}$ Compute $A'_i \leftarrow g\ t'_i$ 'and $\gamma\ k_i \leftrightarrow i'$ $\longleftarrow \frac{a'_i}{a_i}$;Output a'_i, $A'_{i,\ and}$ $\gamma\ k_i \leftrightarrow i'$.

ContentBaseFileupdate(i, CT_i,AHL_i)

if i has the latest version, exit;
Search AHL_i and locate the old version of // assume the latest version of i in MSK is $a_i(n)$.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 19, April 2017

$k_i \leftrightarrow i(n) \longleftarrow \gamma_{k_i} \leftrightarrow i'. \ \gamma_{k_i'} \leftrightarrow$

$i'' \ldots . \gamma_{k_i(n-1)} \leftrightarrow i(n) = \frac{a_i(n)}{a_i}$;

Compute $CT_i^{(n)} \longleftarrow (CT_i) \ \gamma_{k_i} \leftrightarrow i(n) = g^{a_i(n)}$s.Output $CT_i^{(n)}$.

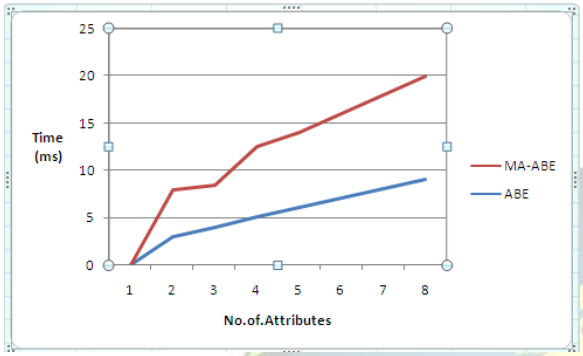

Fig 3: Comparision of ABE and MA-ABE

4. Conclusion

The Purpose of using MA-ABE scheme is to develop a secure, robust, privacy and efficient multi-authority attribute based encryption system. The field of MA-ABE scheme is a vast and ever evolving one with its wings stretched to the areas of IoT and Social Networks.

5. References

1. M. Bellare, S. Keelveedhi, and T. Ristenpart,"Message-Locked Encryption and Secure Deduplication," Advances in Cryptology (EUROCRYPT 13),LNCS 7881, 2013, pp. 296–312.

2. J.R. Douceur et al., "Reclaiming Space from Duplicate Files in a Serverless Distributed File System,"Proc. 22nd Int'l Conf. Distributed Computing Systems,2002, pp. 617–624.

3. M. Bellare, S. Keelveedhi, and T. Ristenpart, "DupLESS: Server-Aided Encryption for Deduplicated Storage,"Proc. 22nd Usenix Conf. Security, 2013, pp. 179–194.

4. Z.C. Wen et al., "A Verifiable Data Deduplication Scheme in Cloud Computing," Proc. Int'l Conf. Intelligent Networking and Collaborative Systems, 2014, pp. 85–90.

5. Christo Ananth, Kavya.S., Karthika.K., Lakshmi Priya.G., Mary Varsha Peter, Priya.M., "CGT Method of Message forwarding", International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE), Volume 1, Issue 1, August 2015,pp:10-15

6. P. Meye et al., "A Secure Two-Phase Data Deduplication Scheme," Proc. IEEE 6th Int'l Symp. Cyberspace Safety and Security, IEEE 11th Int'l Conf. Embedded Software and Systems (HPCC, CSS, ICESS), 2014, pp. 802–809.

7. P. Puzio et al., "ClouDedup: Secure Deduplication with Encrypted Data for Cloud Storage," Proc. IEEE 5th Int'l Conf. Cloud Computing Technology and Science, 2013, pp. 363–370.

8. Z. Yan, W. Ding, and H. Zhu, "Manage Encrypted Data Storage with Deduplication in Cloud," Proc. Int'l Conf. Algorithms and Architectures for Parallel Processing (ICA3PP), 2015, pp. 547–561.

9.Dr. M.Newlin Rajkumar1, Ancy George2, Brighty Batley C"An Overview of Multi-Authority Attribute Based Encryption Techniques"International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 9, September 2014.

10. Z .Yan, W. Ding, and H. Zhu, "Manage Encrypted Data Storage with Deduplication in Cloud," Proc. Int'l Conf. Algorithms and Architectures for Parallel Processing (ICA3PP), 2015

11. A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques,Aarhus, Denmark, May 22-26, 2005, Proceedings, ser. Lecture Notes in
Computer Science, vol. 3494. Springer, 2005, pp. 457–473.

12. V.Goval, O.Pandey, A.Sahai, and B.Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS 2006, Alexandria, VA, USA, october 30 – November 3, 2006, ser.Lecture Notes in Computer Science, vol.5126. Springer, 2006,pp.89-98.

12. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS 2006, Alexandria, VA, USA, Ioctober 30 -November 3, 2006, ser. Lecture Notes in Computer Science, vol.5126. Springer, 2006, pp. 89–98.

13. M. Chase. "Multi-authority attribute based encryption". In *TCC*, pages 515-534, 2007.