International Journal of Allied Practice, Research and Review
Website: www.ijaprr.com (ISSN 2350-1294)

Secure Data Sharing Scheme with Attribute and Effective User Revocation

Parag R. Dupare and Dr. Emmanuel M.
ME Student, Department of Information Technology, PICT, Pune, India [1]
Professor, Department of Information Technology, PICT, Pune, India [2]

Abstract - Ciphertext policy attribute-based encryption (CP-ABE) is a promising cryptographic technique for fine-grained access control of outsourced data in the cloud. However, some drawbacks of key management hinder the popularity of its application like key escrow. We indicate that front-end devices like smart phones have limited privacy protection, so if private keys are held by them, clients risk key exposure is inherently existed in previous research. Furthermore, client decryption overhead limits the practical use of ABE. In this work, collaborative key management protocol in CP-ABE is proposed. Here construction realizes distributed generation, issue and storage of private keys without adding any extra infrastructure. A fine-grained and immediate attribute revocation is provided for key update. The proposed collaborative mechanism solves not only key escrow problem but also key exposure. Meanwhile, it helps reduce client decryption overhead. A comparison with other CP-ABE schemes demonstrates that proposed scheme has better performance in terms of cloud-based outsourced data sharing on various devices.

Keyword: CP-ABE, Cryptographic technique, key escrow, private keys, decryption overhead.

I. Introduction

Cloud computing as we know is just a one of the fundamental concepts, which provide various services; most of them are related with internet. With the help of cloud computing many companies uses computer resources such as virtual machines, storage and various applications. As a utility just like an electricity without wasting money and time in building all that on own and consuming so much of space for that. So such huge amount of information is stored on cloud storage which needs to secure for this huge set of various policies, technology as well as various types of control deploying to save information, software and hardware. Cloud security is sub-domains of cloud computing. The client's store there information in third party data centers. So the user requires fine-grained access control for sharing of their information. Technique such as Attribute-based encryption (ABE), is good and be trusted in present scenario. It offers very interesting security and sharing of information. It has one to much property, such as one key can decrypt many cipher text and multiple key can decrypt a sing cipher text. ABE techniques are of two types, which are cipher text policy attribute based encryption and key policy attribute based encryption. In ciphertext technique, private key are coded as cipher text with various attribute set. In key policy technique, the private key is embedded by access policy and cipher text is embedded by attribute.

Access policy in CP-ABE, where DO are allowed for creating of own. Policy attribute set are first of all matches to get access to a data and obtain it. Because of such property, CP-ABE is best option to choose for the building up of protected, well arrangement access control in cloud for various data sharing. ABE in practically faces many issues more specifically in private key management. As there is large number of ABE schemes, the password provider authority should be totally trusted, because provider could take out all data with help of private key not even knowing to DO. The commonly encountered problem is Key-escrow problem, that's one of the disadvantages for user's privacy. Now a days wildly use of phone applications and phone cloud services for cloud computing is have been introduced. Mostly phone front-end devices, like smartphones are very much vulnerable as compared to server in respect of privacy protection. The mishandling of private key in any respect can easily expose key to any unauthorized person. The run time must get badly unacceptable. In cloud data sharing we have proposed a novel collaborative key management protocol as CKM-CP-ABE while keeping goal in mind to increase security level and also increase efficiency of managing properly while sharing a data. Important contribution is as summarized:

1) We present a novel collaborative protocol. Here interaction between, authority, cloud server and client. They tend to get privilege to information, generation, problems as well as storing of password is made easy and safe. Without adding any separate infrastructure secure key management is guaranteed. Deployment is easy as compared to earlier multi- authority schemes.

2) Groups of attributes are introduced for making an update algorithm for private key. To each attribute group a non-repeatable attribute group key are allocated which contains clients, they shares the exactly same attributes. Whenever, attribute key is updated a well arrangement and at same time attribute revocation are given.

3) As know, password issue is always a fear for client for the private key to get exposed. But it was not properly noticed in earlier research work. As compared to earlier techniques for key management at cloud, here proposed algorithm easily solves problem with the help of collaborative key management.

4) Clients decryption overhead is reduced by collaborative mechanism because only decryption has to be managed by them.

II. Literature Survey

2.1: Fuzzy identity-based encryption (FIBE)

Sahai and Waters, at 2005 proposed this encryption technique (FIBE) that is a classic identity based encryption. Here in private key identity of receiver is present with the help of set of attributes. Only if distance between receiver and sender is shorter than threshold then only plaintext can be retrieved correctly. As this technique has some of the characteristics of ABE, it makes a theory base for various works in ABE.

2.2: Cipertext policy ABE

Bettencourt et al. creates construction of CP-ABE is proposed, here information sender could introduce access policy earlier information is encrypt. It guarantees information confidentiality and makes feel of automatic access control.

2.3: Novel attribute-based access control

Hur et al. further research CP-ABE proposed. Well-arranged key management is done by using attribute group key. It supports attribute revocation and user revocation that look front and back security.

2.4: High efficient CP-ABE

Waters, cipher text space, encrypting and decrypting period growing with difficulty of various access policies. This is more secured as compare to introduce above ones.

III. Proposed Approach

In securely sharing of data on cloud there are five entities in proposed approach. Here, Figure 3.1 shows the model of CKM-CP-ABE for cloud.

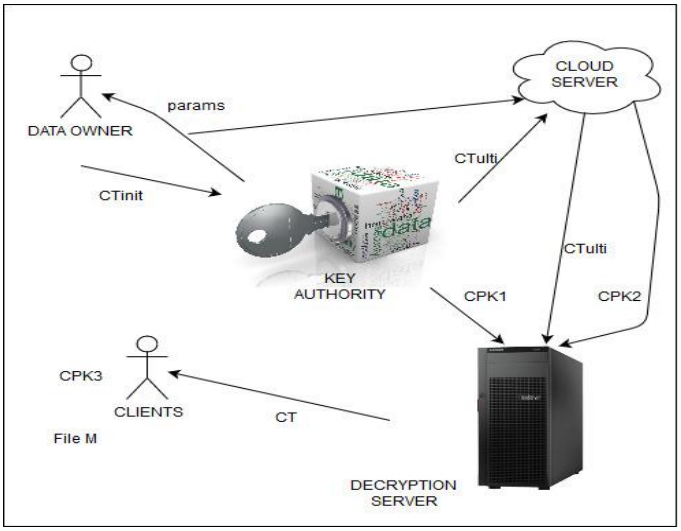

Figure 3.1: The model of CKM-CP-ABE for cloud data sharing

3.1: Client: The user who access information in cloud from various front-end devices is a client. Cell phones are mostly the front-end devices. Client will be able to access plaintext only if clients attribute set meets an access policy belonged with cipertext. Client may lose key to another person as most cell phones are performance restrained.

3.2: Key Authority: It takes many calculation tasks, such as key generation and update and shares private key to cloud server and client and one with self. When client demands for file all private keys are shared to decryption server and client for decryption of ciphertext to plaintext. Here we look after that KA is semi trusted in systems.

3.3: Cloud Server: This is also made semi trusted in this scheme. Its main job is to storage management in cloud.

3.4: Decryption Server: It has great computing potentiality. It carries most of the tasks, but not all of the decryption. It is also made to be half trusted and DS access channels are not secure, it is so because CKM-CP-ABE is enough for information security.

3.5: Data Owner: DO upload data and is authorized user. To access plaintext by client DO also introduce their own access policies.

IV. METHODOLOGY

For all systems here we introduce Client as set of U and attributes as set of L. Let G belong to attribute group of client who shares value of attribute sets. Also let K belong to Z group of an attribute, taking G. Here, G = {G| where all value of set L belongs to L}, K = {K| where all value of set L belongs to L. It is collection of all the attribute groups. Here CKM-CP-ABE scheme comprises of six algorithms, which are as follow:

5.1: Set-up work: Here security parameter is K.G1 and G2 → multiple-able cyclic group where prime order is p and g is the generators of G1.

H: {0, 1}* → G1
H1: G2 → Zp

Input → k and L sets. Output → public parameters groups are returned. Setup is comprised of three different steps:

TrustSetup: It selects random elements.

PP= {g, h1, h2… hn, H, H1}

KASetup: KA chooses random exponent.

(MKka = q, PPka=gq)

CS Setup: CS chooses random exponent.

(MKcs = ga, PPcs = e (g, g) a)

Output: public parameters param = (PP, PPka, PPcs). This public parameter is used to encrypt the plaintext file to initial ciphertext by data owner and send the file to key authority to generate keys.

5.2: Key Generation: It takes place with KA. Input: public parameter PP and client set S. Output: initial key.
PKinit = (g exponential of theta, all x belongs to S: h2 exponential of theta)

5.3: Encryption: It is done by data owner. Input: public parameters param = (PP, PPka, PPcs), access structure A and plaintext M. Outputs: CTinit = ((M, theta), C = M.e (g, g) exponential of as, C1 = G exponential of theta, where set of L all belongs to A: C* = G exponential of q and lambda. h limits to p (theta) and –theta)

5.4: Re-encryption: It is done by CS. Input: public parameters param = (PP, PPka, PPcs), initial cipertext CTinit, collection of attribute group G. Output: The ultimate ciphertext is stored in cloud.

CTulti = (Hdr, CT)

5.5: Private Key Update: Its main invention of CKM-CP-ABE. Here collaborative key management protocol is implements for creating and distributing 3 various key parts. Input: parameters param = (PP, PPka, PPcs), initial key PKinit

5.6: Decryption: This algorithm decrypts the encrypted text. Input: CL attributes set S, ultimate cipher text CTulti, private key components (CPK1, CPK2, and CPK3). Output: plaintext file M is finally obtained by the client.

V. EXPERIMENTAL SETUP

Here, system used for experiment is Lenovo ThinkPad T470. Minimum hard disk required is as per size of the dataset taken for the encryption and decryption. Here, SSD memory of 512 GB is used for the experimental work. Processor used for the work is i7 7th generation. Minimum ram required to implement is 2 GB. Various different machines where used to accomplishment the experimental setup for more efficient result for the experiment. Various software like operating system used is windows 10 and various tools like Netbeans and Eclipse are used which are good and easy to use emulation software's. Java language is used for building up of work. Together with java, MySQL database is used to store backend data for that we used wamp server, xml, CSS is also used for web designing's and templates. To implement, cloudsim 3.0.3 framework is also used to simulate the file and ciphertext size and find out the cost and time required for file to encrypt and decrypt the required file.

VI. RESULT

Here, the experimental results for proposed scheme are presented. Then comparison between the existing approaches with the proposed approach is explained. In terms of efficiency, we compare the proposed CKM-CP-ABE with other representative ABE variants detailed in methods of Bethencourt et al., Green et al., and Hur. We summarize the efficiency comparison with respect to public key, ciphertext, and private key size in below Tables. For CKM-CP-ABE, the public key size is larger than those of other schemes because our key requires a tuple of random elements associated with each authorized attribute. The CKM-CP-ABE ciphertext size, which is the smallest among the compared schemes. Similar to Green et al.'s scheme, the private key size of CKM-CP-ABE, which the number of elements is less than in the methods of Bethencourt et al. and Hur. The comparison of total decryption overhead and client decryption overhead for each method is presented in Tables. Enormous computation overhead is known to be an ABE bottleneck. Mass calculations of pairings are the main contributors to this computation load. Similar to other schemes, CKM-CP-ABE has heavy total decryption overhead. Introducing the attribute group mechanism adds more exponentiation and multiplication calculation to our scheme. Due to the collaborative mechanism, however, we decrease client decryption overhead dramatically. Authorized CLs in our scheme require only one exponentiation calculation and one division calculation because the DS undertakes enormous computation without any knowledge leakage. Differed from Green et al, CKM-CP-ABE not only outsources decryption but also provides a collaborative mechanism with reliable security.

SYMBOL	DEFINITION
$\|G_1\|$	Size of an element in G_1
$\|G_2\|$	Size of an element in G_2
$\|A\|$	Size of an access structure
$\|Z_P\|$	Size of an element in Z_P
m	Sum of all authorized attribute in system
Σ	Sum of attributes in an access structure
$\|S\|$	Sum of attributes held by a CL
v	Sum of CLs in an attribute group
$ST_\wedge$	Sum of threshold value of all "AND" gates in an access tree
SG	Sum of gates in an access tree
C_h	A calculation of pairing
C_p	A calculation of hash function
C_e	A calculation of exponentiation
C_m	A calculation of multiplication
C_d	A calculation of division

Table 6.1: Notation relevant to efficiency comparison

SYSTEM	PUBLIC KEY SIZE	CIPHERTEXT SIZE	PRIVATE KEY SIZE
Bethencourt. [2]	$\|G_1\|+\|G_2\|$	$(2\Sigma+1)\|G_1\|+\|G_1\|+\|G_1\|$	$(2\|S\|+1)\|G_1\|$
M. Green [5]	$\|G_1\|+\|G_2\|$	$(2\Sigma+1)\|G_1\|+\|G_1\|+\|G_1\|$	$\|Z_P\|+(\|S\|+2)\|G_1\|$
J. Hur [10]	$\|G_1\|+\|G_2\|$	$(2\Sigma+1)\|G_1\|+\|G_1\|+\|G_1\|$	$(2\|S+2)\|\|G_1\|$
PAPER WORK	$(\Sigma+1)\|G_1\|+\|G_2\|$	$(\Sigma+1)\|G_1\|+\|G_1\|+\|G_1\|$	$\|Z_P\|+(\|S\|+2)\|G_1\|$

Table 6.2: Comparison of size of public key, private key and ciphertext

Tables shows the time cost required for data encryption in both the schemes i.e. proposed scheme and existing scheme i.e. arbitrary state attribute based encryption with dynamic membership under the different number of attributes. It can be seen from graph; time cost for data encryption gradually increasing and approximately follows a linear relationship with the number of attributes. Also, it is clear that the time cost of data encryption using proposed scheme is lesser than the existing approach under the same number of attribute. In terms of percentage, the proposed scheme reduces average time cost of data

encryption by 18.25% as compare to existing approach. So, present CKM-CP-ABE scheme is more secured as compared to other schemes of CP-ABE. This scheme gives efficient output, reducing the decryption overhead from clients.

SYSTEM	DECRYPTION OVERHEAD	C_h	C_p	C_e	C_m	C_d
Bethencourt. [2]	TOTAL	0	2Σ+1	ST^	ST^-SG	2
	CLIENT	0	2Σ+1	ST^	ST^-SG	2
M. Green [5]	TOTAL	0	|S|+2	2|S|+1	2|S|-1	2
	CLIENT	0	0	1	0	1
J. Hur [10]	TOTAL	1	2|S|+2	ST^+v	ST^-SG-v	2
	CLIENT	1	2|S|+2	ST^+v	ST^-SG-v	2
PAPER WORK	TOTAL	1	2|S|+2	2|S|+v+1	2|S|+v-1	2
	CLIENT	0	0	1	0	1

Table 6.3: Comparison of decryption overhead

VII. CONCLUSION

CP-ABE is one of the excellent cryptographic methods for properly arrangements in secured cloud storage. For cloud data sharing system we proposed a collaborative key management protocols. By which we get a good protection and accuracy of key handling at CP-ABE. Not adding any new infrastructure, distributing key generating issue and preserving of key is properly managed and resolved. Here attribute groups are introduced to create a private key update algorithms to get fine-grained and revocation. Also key-escrow problem is resolved along with that key exposure problem is also resolved, which was not earlier noticed. Client experience has been optimizing because only decryption step has to be taken by them. With respect to security and efficiency the proposing schemes performs good at sharing of information on cloud in front end devices by serving massive performance–restrained. In future work cipher text size, encryption cast and decryption cost can be reduced. In future with help of cloud, can be work on many different real time scenarios like health record management and many more. Personal health record application uses this technique.

VIII. REFERENCES

[1] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc. EuroCrypt, vol. 3494, pp. 457-473, 2005.

[2] J. Bethencourt, A. Sahai, and B.Waters, "Cipher text-policy attribute-based encryption," in Proc. IEEE Symposium on Security and Privacy, pp. 321-334, 2007.

[3] N. Attrapadung and H. Imai, "Conjunctive broadcast and attribute-based encryption," in Proc. Int. Conf. Pairing-Based Cryptography, vol. 5671, pp. 248-265, 2009.

[4] B. Waters, "Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization," in Proc. Public Key Cryptography, vol. 6571, pp. 53-70, 2011.

[5] M. Green, S. Hohnberger, and B. Waters, "Outsourcing the decryption of ABE ciphertext," in Proc. USENIX on Security., pp. 34, 2011.

[6] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," IEEE Trans. Inf. Forens. Security, vol. 8, no. 8, pp. 1343-1354, 2013.

[7] S. Lin, R. Zhang, H. Ma, and M. Wang, "Revisiting attribute-based encryption with verifiable outsourced decryption," IEEE Trans. Inf. Forens. Security, vol. 10, no. 10, pp. 2119-2130, 2015.

[8] M. Chase, and S. S. M. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in Proc. ACM CCS, 121-130, 2009.

[9] G. Zhang, L. Liu, and Y. Liu, "An attribute-based encryption scheme secure against malicious KGC," in Proc. TRUSTCOM, pp. 1376-1380, 2012.

[10] J. Hur, "Improving security and efficiency in attribute-based data sharing," IEEE Trans. Knowl. Data. Eng., vol. 25, no. 10, pp. 2271-2282, 2013.

[11] P. P. Chandar, D. Mutkurman, and M. Rathinrai, "Hierarchical attribute based proxy reencryption access control in cloud computing," in Proc. ICCPCT, pp. 1565-1570, 2014.

[12] X. A. Wang, J. Ma, and F. Xhafa, "Outsourcing decryption of attribute based encryption with energy efficiency," in Proc. 3PGCIC, pp. 444-448, 2015.

[13] L. Cheung, and C. Newport, "Provably secure ciphertext policy ABE," in Proc. ACM CCS, pp. 456-465, 2007.

[14] J. Hur, and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 7, pp. 1214-1221, 2011.

[15] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attribute-based systems," Journal of computer security, vol. 18, pp. 799-837, 2010.

[16] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in Proc. ACM CCS, pp. 417-426, 2008.

[17] A. Xiong, C. Xu, and Q. Gan, "A CP-ABE scheme with system attributes revocation in cloud storage," in Proc. ICCWAMIP, pp. 331-335, 2014.

[18] Q. Wu, "A generic construction of ciphertext-policy attribute-based encryption supporting attribute revocation," China Commun., vol. 11, no. 13, pp. 93-100, 2014.

[19] S. S. M. Chow, "Removing escrow from identity-based encryption," in Proc. Int. Conf. Practice and Theory in Public Key Cryptography, vol. 5443, pp. 256-276, 2009.

[20] M. S. Ahmad, N. E. Musa, R. Nadarajah, R. Hassan, and N. E. Othman, "Comparison between android and iOS operating system in terms of security," in Proc. CITA, pp. 1-4, 2013.

[21] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. ACM CCS, pp. 89-98, 2006.

[22] S. Rafaeli, and D. Hutchison, "A survey of key management for secure group communication," ACM Computing Survey, vol. 35, no. 3, pp. 309-329, 2003.

[23] Chudaman Devidasrao Sukte, Emmanuel M. and Ratnadeep R Deshmukh." Novel Approach for improving Security and Confidentiality in Public Clouds using Certificate less Encryption" IJCA Proceedings on International Conference on Cognitive Knowledge Engineering ICKE 2016(1):8-12, January 2018.

Author[s] brief Introduction

Parag R. Dupare, received BE degree in CSE, from SGBAU Amravati. Now pursuing ME Degree in Department of Information Technology from Pune Institute of computer technology, Pune. Area of interest is cloud computing and network security.

Dr. Emmanuel M, Professor of Information Technology Department, Pune Institute of Computer Technology, Pune. He has received PhD degree in Computer Science & Engineering. His research interests include Data Mining, Big data, Cloud Computing and Medical Image Processing.