ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

A Survey on File Hierarchy Based Encryption and Geo Encryption Scheme for Efficient Data Sharing in Cloud

Priyanka H.V[1], Prasanna kumar M [2], Abhinav N. D[3]

PG Student, Dept. of C.S.E., SIET, Visvesvaraya Technological University, Belagavi, India[1]

Assistant Professor, Dept. of C.S.E., SIET, Visvesvaraya Technological University, Belagavi, India[2]

PG Student, Dept. of C.S.E., SIET, Visvesvaraya Technological University, Belagavi, India[3]

ABSTRACT: Data sharing in cloud is very popular. In the cloud consists of different types of files. Normally in cloud for encryption cipher-text policy attribute based encryption(CP-ABE) method can be used. But it can only suitable for normal files. But the shared file is having the property of multi-level hierarchy. so for this type of file cipher - text policy attribute encryption(CP-ABE) is not possible particularly in health and military organization. More and more security is needed for this kind of organization. In this paper policy based file hierarchy encryption scheme and geo encryption scheme is used for shared file in cloud. In this the layer access structure are combine into one access structure and then the hierarchy are encrypt with combined structure.Here the ciphertext element related to attribute shared by files.Therefore both the ciphertext data and cost of encryption saved. More over the proposed scheme is proved to be secure under the standard assumption of geo Encryption and the proposed scheme is more powerful in both encryption and decryption.

KEYWORDS*:* cloud computing , Data sharing , File Hierarchy , GeoEncryption , Cipher-text policy Attribute-Based Encryption(CP-ABE)

I. INTRODUCTION

In the recent technology cloud computing is most powerful application in data sharing. In cloud computing [1]-[5] the data is protected from leaking. The user encrypt the data before sharing into the cloud.
Normally cipher-text policy attribute based encryption is a technique[1]-[2] it more and more security and it is useful for general application[6]-[7]. In cipher text policy user private key is associated with the set of attributes with in the system. A user will be able to decrypt a ciphertext if and only if attributes satisfy the policy of respective ciphertext.the policies defined over attributes using conjuction and disjunction.

In data sharing Normally the keys which can be generated by the Authority and Data owner encrypt file and upload to cloud service provider . user download and decrypt the ciphertext from cloud service provider.
In geoencryption the decryption of the data with the specific location,time or position of the receiver.it provides on additional layer of security and it supports for data sharing and the distribution policies.[8]

In the cloud the shared files generally have Hierarchial structure that is group of files divided into subgroup at different access levels and with geo encryption with the help of GPS devices it enhances the power of the data security.
For the hierarchial structure let us take the example of personal health record[9].To securely share the records in the cloud computing , it divides into two parts m1 and m2.the files present in personal health record adopts the cipher text attribute based encryption scheme to encrypt the information at different access policies.so here the multiple files are integrated into the single integrated access structure.so the computation complexity encryption and storage ciphertext reduced

DOI: 10.15680/IJIRCCE.2017. 0503178

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

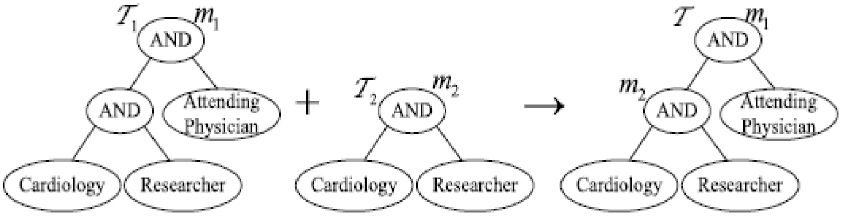

Fig 1: The integrated access structure T1 and T2 are access structures of m1 and m2 respectively.T is the integrated access structure of m1 and m2

II. RELATED WORK

Sahai and Waters[10] proposed fuzzy Identity-Based Encryption (IBE) in 2005, which was the prototype of ABE. Latterly, a variant of ABE named CP-ABE was proposed.
Gentry and Silverberg[11] proposed the first notion of hierarchical encryption scheme, many hierarchical CP-ABE schemes have been proposed.
*Wang et al.[*12] proposed a hierarchical ABE scheme by combining the hierarchical IBE and CP-ABE. Later, Zou gave a hierarchical ABE scheme, while the length of secret key is linear with the order of the attribute set. ciphertextpolicy hierarchical ABE scheme with short ciphertext is also studied.In these schemes, the parent authorization domain governs its child authorization domains and a top-lev el authorization domain creates secret key of the next-level domain. The work of key creation is distributed on multiple authorization domains and the burden of key authority center is lightened.Other CP-ABE schemes with specific features have been presented.
Hur [13] proposed a data sharing scheme to solve the problem of key escrow by using an escrow free key issuing protocol between the key generation center and the data storing center.
Green et al. [14] and Lai *et al.* [15] proposed CP-ABE schemes with outsourced decryption to reduce the workload of the decryption user.
Fan et al. [16] proposed an arbitrary-state ABE scheme to solve the problem of the dynamic membership management. *Guo et al.* [17] proposed a novel constant-size decryption key CP-ABE scheme for storage-constrained devices. *Hohenberger and Waters* [18] proposed an online/offline ABE scheme to improve the speed of key generation and encryption, where each computation work in the two processes is split into two phases offline phase (a preparation phase) and online phase.

III. PROPOSED SYSTEM

In this we propose the layered model of access structure for the hierachial files.In this the file is encrypted with one integrated access structure.
We also proposed geo scheme it will given the enhanced security for the hierachial files when the files are encrypting and decrypting.

IV. ADVANTAGES OF PROPOSED SYSTEM

- FH-CP-ABE feasible schemes which has much more flexibility and is more suitable for multilevel hierachial files.
- Multiple hierarchical files sharing are resolved using layered model of access structure.
- In proposed system both ciphertext storage and time cost of encryption are saved.
- The proposed scheme has an advantage that users can decrypt all authorization files by computing secret key once. Thus, the time cost of decryption is also saved if the user needs to decrypt multiple files.
- The computation cost of decryption can also be reduced if users need to decrypt multiple files at the same time.

- The proposed scheme is proved to be more secure under standard assumption of geo encryption

V. ARCHITECTURE

In Architecture it consists of three phases

- Geo locking phase
- Geo encryption phase
- FH-CP-ABE phase

GEO LOCKING PHASE

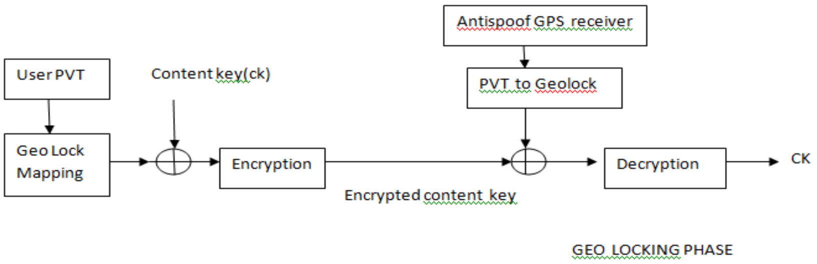

Fig 2:It shows the Geo locking phase

- In this it firstly sets the user place or velocity or time.
- After the above attributes gets geo locked with the user randomnly generated content key(ck) with the help of geo lock mapping.
- Then this content key is Encrypted with attributes.
- Again the attribute is obtained with the help of geolock.
- with the help of GPS device it compare the firstly given attribute and the geolocked attribute. if the Both are same the content key is released for decryption.

GEO ENCRYPTION PHASE

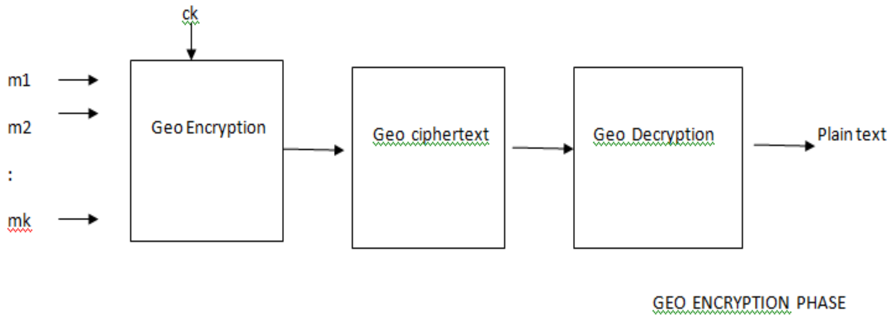

Fig 3:It shows Geo encryption phase

It consists of four modules
1. Authority 2. Data owner 3. Cloud service provider(CSP) 4. User

1. Authority: It is the trusted Entity for the user and it generates setup and keygeneration operations
2. Data owner : In my scheme it defining the access structure and executing encrypt operation and upload ciphertext.
3. Cloud service provider(CSP) : it is the semitrusted entity and perform the assigned task and return correct result.
4. User: It is the Entity first download ciphertext and execute decrypt operation

- The data owner chooses the content key(ck) and encrypt file (m1,m2....mk)with randomly generated content key by hybrid encryption algorithm.

- Next the geociphertext will be obtained.
- Next the ciphertext is decrypted the plain text is generated

FH-CP-ABE PHASE

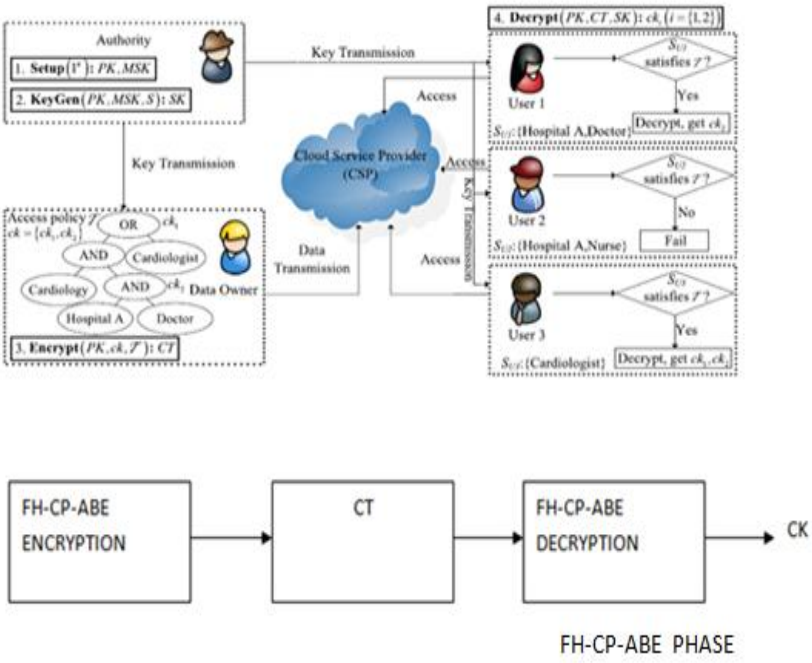

Fig 4 :It shows FH-CP-ABE scheme

In this the dataowner encrypt content key using FH-CP-ABE scheme.

- In setup it takes K as input and output publickey(PK) and mastersecret key(MSK).
- In Keygeneration it takes input PK,MSK and set of attributes S and creates a secret key SK.
- The dataowner inputs PK,CK and the Hierachial access tree and create integrated ciphertext of content key CT
- Then it gives to the cloud service provider(CSP)
- Next the user download ciphertext and CT from Dataowner
- Then the content key can be decrypted if and only if the user's attribute satisfies part on T.In the above figure the user1 can decrypt ck to obtain m2.The user2 cannot decrypt any message and the user 3 can decrypt ck.

BLOCK DIAGRAM

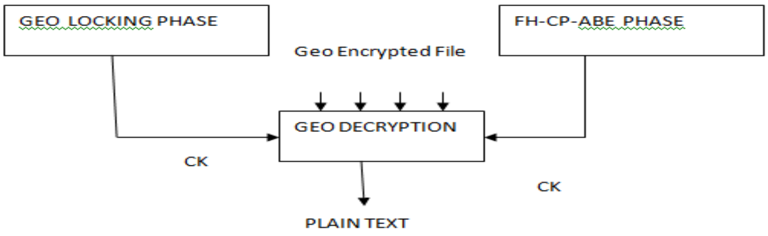

Fig 5: It shows the block diagram of proposed scheme

- In Geo-locking phase it gets locked with the geo lock then encrypt.if the place or attributes match with the GPS server the CK is released.
- In FH-CP-ABE if the access structure policy is Matched with attributes the CK is produced
- If Both the content key is matched then only the ciphertext is decrypted and the plain text is obtained.

VI. CONCLUSION

In this paper we proposed the file Hierachy based Encryption scheme and geoencryption. In file Hierachy the Hierachial files are encrypted with combined access structure and the elements of attribute easily shared by the files.so ciphertext storage and the cost is saved. And with geo encryption assumption more and more security is enhanced.

VII. FUTURE WORK

In our discussion , we used geoencryption assumption for security purposes.In future it can be solved with by doing research and implement with higher upcoming encryption and decryption techniques.

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 Comput.*,vol. 12, no. 4, pp. 50–57, 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. Secur. Pract. Exper.*, vol. 8434. May 2014, pp. 346–358.

[3] K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, "An efficient cloudbased revocable identity-based proxy re-encryption scheme for public clouds data sharing," in *Proc. 19th Eur. Symp. Res. Comput. Secur.*, vol. 8712. Sep. 2014, pp. 257–272.

[4] T. H. Yuen, Y. Zhang, S. M. Yiu, 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. Secur.*, vol. 8712. Sep. 2014, pp. 130–147.

[5] K. Liang *et al.*, "A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 10, pp. 1667–1680, Oct. 2014.

[6] C.-I. Fan, V. S.-M. Huang, and H.-M. Ruan, "Arbitrary-state attributebased encryption with dynamic membership," *IEEE Trans. Comput.*,vol. 63, no. 8, pp. 1951–1961, Aug. 2014.

[7] H. Zheng, Q. Yuan, and J. Chen, "A framework for protecting personal information and privacy," *Secur. Commun. Netw.*, vol. 8, no. 16, pp. 2867–2874, Nov. 2015.

[8] Geo-encryption;using GPS to Enhance Data Security by Scott,Logan,GPS world,April 2003,pp.40-49(.pdf)

[9] F. Xhafa, J. Wang, X. Chen, J. K. Liu, J. Li, and P. Krause, "An efficient PHR service system supporting fuzzy keyword search and fine-grained access control," *Soft Comput.*, vol. 18, no. 9, pp. 1795–1802, Sep. 2014. [10] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology*. Berlin, Germany: Springer, May 2005, pp. 457–473.

[11] C. Gentry and A. Silverberg, "Hierarchical ID-based cryptography,"in *Advances in Cryptology*. Berlin, Germany: Springer, Dec. 2002, pp. 548–566.

[12] G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in *Proc. 17th ACM Conf. Comput. Commun. Secur.*, Oct. 2010, pp. 735–737.

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

[14] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryption of ABE ciphertexts," in *Proc. 20th USENIX Conf. Secur.*, Aug. 2011, pp. 1–16.

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

[16] C.-I. Fan, V. S.-M. Huang, and H.-M. Ruan, "Arbitrary-state attributebased encryption with dynamic membership," *IEEE Trans. Comput.*, vol. 63, no. 8, pp. 1951–1961, Aug. 2014.

[17] F. Guo, Y. Mu, W. Susilo, D. S. Wong, and V. Varadharajan, "CP-ABE with constant-size keys for lightweight devices," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 5, pp. 763–771, May 2014.

[18] S. Hohenberger and B. Waters, "Online/offline attribute-based encryption," in *Proc. 17th Int. Conf. Pract. Theory Public-Key Cryptogr. (PKC)*, vol. 8383. Mar. 2014, pp. 293–310.