Key Generation & Access Control Policy in Cloud Data Sharing

Prashant Gutte, Jeevan Vinay Wankhade and Shailendra Mote

February 5, 2020

Key Generation & Access Control Policy in Cloud Data Sharing

Prashant H Gutte[1*], Jeevan V Wankhade[1], Shailendra B Mote[2],

[1]Government Polytechnic, Hingoli,
India
gutte.p50@gov.in, jeevanwankhade@gmail.com,
shailendramote@gmail.com

Abstract. In this paper we discussed the access control policy and data sharing mechanisms in cloud environment. In 21th century Cloud computing is the best & proficient way to handle our valuable data remotely. Now a day's Data Confidentiality is one of the prime and crucial problem. Security vulnerability feature also matters while data exchanging with others. Whenever we are using a cloud like platform trust factor plays an important role. Ample of unauthorized user communities try to access & steal the classified data. In the 21st century encryption technologies are used to secure data. Exchanging cloud data in group of users at a best level is still a critical problem, especially when dealing with dynamic user group. In this paper we proposed a mechanism which deals with revocation and data privacy & make Access Control Policy (ACP) in dynamic user group problem.

Keywords: Data Sharing, ACP, Data Confidentiality.

1 Introduction

Cloud computing and information sharing is mainly required and quickly developing trends in this current era. We can get to and share information from various areas with the assistance of internet. Additionally it prepared gives client adaptable infrastructure, storage space and hardware similarity to accomplish better execution. Information privacy and execution are vital factor in cloud storage environment. Cryptographic methods are utilized to secure information from unauthorized access. In cloud computing third parties are likewise assuming primary job in giving us secure channel to exchanging the data from information proprietor to other requested different end clients or customers. Existing system uses the cipher text policies. In which confidentiality of the data are made by using three factors data, encryption algorithm & the size of key. As well existing concepts third parties are used such as key as well as digital certificate providers & verifiers. Still it is not a piece of cake to keep fully trust over these service providers & third parties. Not everything except rather some of them might have the capacity to attempt to take our information and keys. Group sharing concept is works like broadcasting particular data among the set of peoples. But while sharing encrypted or sensitive data need to share its key also for decryption purpose. Sometime access is given to the set of user and one of them might be leave the group or change the group that time its access should be revoked otherwise it can be able to take unauthorized access from outside also.

In literature review we discussed on the relevant existing topics.

2 Literature Survey

There are numerous approaches are characterized in regards to data sharing & data security in cloud computing which are mentioned in our literature.

2.1 Secure Fine-Grained Access Control and Data Sharing for Dynamic Groups:

Cloud computing additionally brings numerous security issues since cloud service providers (CSPs) are not in the same trusted domain as users. To ensure information protection against untrusted CSPs, existing arrangements apply cryptographic techniques (e.g., encryption mechanisms).challenging issue, particularly when managing dynamic client group. They proposed [1] a secure and efficient fine grained access control and data sharing scheme for dynamic user groups by (1) defining and enforcing access policies based on the attributes of the data; (2) permitting key generation center (KGC) to efficiently update user credentials for dynamic user groups; and (3) allowing some expensive computation tasks to be performed by untrusted CSPs without requiring any delegation key. They first designed an efficient revocable attribute-based encryption (RABE) scheme along with the property of ciphertext delegation by exploiting and uniquely combining techniques of identity-based encryption (IBE), Attribute-based Encryption (ABE), subset-cover framework and ciphertext encoding mechanism.

2.2 Lightweight Policy Preserving EHR Sharing Scheme:

In CP-ABE, access policy is attached to the ciphertext, however, the access policy is not protected, which will also cause some privacy leakage. In this paper, authors proposed [3] a policy preserving EHR system on the basis of CP-ABE. Specifically, authors designed an algorithm which able to hide the entire access policy as well as recover the hidden attributes from the access matrix. The subsequent evaluation of element insert, lookup and recovery shows that their proposed scheme only introduces light-weighted overhead cost. They constructed their scheme by utilizing the Waters CP-ABE as a building block. Apparently, their scheme can easily extend to other CP-ABE schemes with the structure expressed in LSSS form.

2.3 Efficient Policy-Hiding Attribute-Based Access Control:

With the rapid development of the Internet of Things (IoT) and cloud computing technologies, smart health (shealth) is expected to significantly improve the quality of healthcare. The fine-grained access control, ciphertext-policy attribute-based encryption (CP-ABE) has the potential to ensure data security in s-health. To address these problems, authors introduced [4] PASH, a privacy-aware s-health access control system, in which the key ingredient is a large universe CP-ABE with access policies partially hidden. In PASH, attribute values of access policies are hidden in encrypted SHRs and only attribute names are revealed. In fact, attribute values carry much more sensitive information than generic attribute names. Author’s security analysis indicates that PASH is fully secure in the standard model. Performance comparisons and experimental results show that PASH is more efficient and expressive than previous schemes.

2.4 Key-Policy Attribute-Based Encryption with Equality Test:

In this article, public key encryption with equality test is concatenated with key-policy ABE (KP-ABE) to presented KP-ABE with equality test (KP-ABEwET). This proposed [6] scheme not only offer fine-grained authorization of cipher-texts but also protects the identities of users. In contrast to ABE with keyword search, KP-ABEwET can test whether the cipher-texts encrypted by different public keys contain the same information. Moreover, the authorization process of the presented scheme is more flexible than that of Ma et al.'s scheme. Furthermore, the proposed scheme achieves one-way against chosen-ciphertext attack based on the bilinear Diffe-Hellman (BDH) assumption. In addition, a new computational problem called the twin-decision BDH problem (tDBDH) is proposed in this paper. tDBDH is proved to be as hard as the decisional BDH problem. Finally, for the first time, the security model of authorization is provided, and the security of authorization based on the tDBDH assumption is proven in the random oracle model.

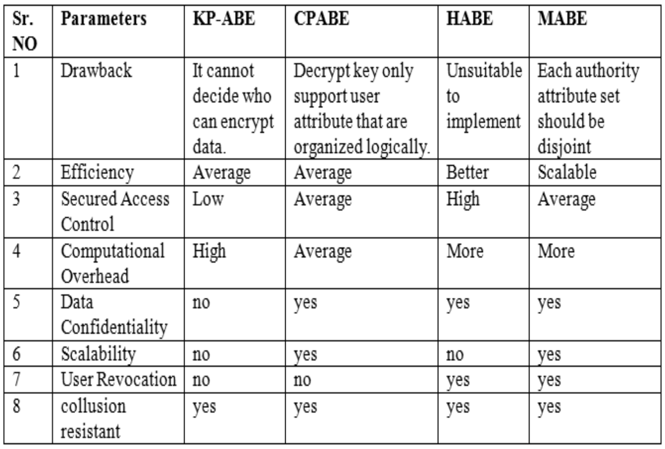
2.5 Attribute-Based Data Sharing Scheme Revisited:

Ciphertext-policy attribute-based encryption (CPABE) is a very capable encryption technique for secure data sharing. CP-ABE is limited to a potential security risk that is known as key escrow problem whereby the secret keys of users have to be issued by a trusted key authority. Besides, most of the existing CP-ABE schemes cannot support attribute with arbitrary state. They proposed [9] an improved two-party key issuing protocol that can guarantee that neither key authority nor cloud service provider can compromise the whole secret key of a user individually. Authors proposed an attribute-based data sharing scheme for cloud computing applications, which is denoted as ciphertext-policy weighted ABE scheme with removing escrow (CP-WABE-RE). It successfully resolves two types of problems: key escrow and arbitrary-sate attribute expression. This proposed system enhanced data confidentiality and privacy in cloud system against the managers of KA and CSP as well as malicious system outsiders, where KA and CSP are semi-trusted. are integrated into a single access structure, and then the hierarchical files are encrypted with the integrated access structure. Hence, both ciphertext storage and time cost of encryption are saved. Additionally, the proposed scheme is proved to be secure under the standard assumption. Experimental model shows that the proposed scheme is highly efficient in terms of encryption and decryption. With the number of the files increasing, the advantages of this proposed scheme become more and more conspicuous. In this study, an efficient encryption scheme based on layered model of the access structure is proposed in cloud computing, which is named file hierarchy CP-ABE scheme (or FH-CP-ABE, for short). FH-CP-ABE extends typical CPABE with a hierarchical structure of access policy, so as to achieve simple, flexible and fine-grained access control Moreover, the proposed scheme is proved to be secure under DBDH assumption.

2.6 Secure and Verifiable Access Control Scheme for Big Data Storage:

Traditional approaches are either completely ignore the issue of access policy update or delegate the update to a third party authority; but in practice, access policy update is important for enhancing security and dealing with the dynamism caused by user join and leave activities. In this paper, authors proposed [7] a secure and verifiable access control scheme based on the NTRU cryptosystem for big data storage in clouds. NTRU cryptosystem is a type of lattice-based cryptography. The proposed a new NTRU decryption algorithm to overcome the decryption failures of the original NTRU. It allows the cloud server to efficiently update the cipher text when a new access policy is specified by the data owner, who is also able to validate the update to counter against cheating behaviors' of the cloud. It also enables (i) the data owner and eligible users to effectively verify the legitimacy of a user for accessing the data, and (ii) a user to validate the information provided by other users for correct plaintext recovery.

- **Comparison of ABE Schemes**



Sr. NO	Parameters	KP-ABE	CPABE	HABE	MABE
1	Drawback	It cannot decide who can encrypt data.	Decrypt key only support user attribute that are organized logically.	Unsuitable to implement	Each authority attribute set should be disjoint
2	Efficiency	Average	Average	Better	Scalable
3	Secured Access Control	Low	Average	High	Average
4	Computational Overhead	High	Average	More	More
5	Data Confidentiality	no	yes	yes	yes
6	Scalability	no	yes	no	yes
7	User Revocation	no	no	yes	yes
8	collusion resistant	yes	yes	yes	yes

2.7 An Efficient File Hierarchy Attribute-Based Encryption Scheme:

In this article, an efficient file hierarchy attribute-based encryption scheme is proposed [11]. The layered access structures are integrated into a single access structure, and then the hierarchical files are encrypted with the integrated access structure. Hence, both ciphertext storage and time cost of encryption are saved. Additionally, the proposed scheme is proved to be secure under the standard assumption. Experimental model shows that the proposed scheme is highly efficient in terms of encryption and decryption. With the number of the files increasing, the advantages of this proposed scheme become more and more conspicuous. In this study, an efficient encryption scheme based on layered model of the access structure is proposed in cloud computing, which is named file hierarchy CP-ABE scheme (or FH-CP-ABE, for short). FH-CP-

ABE extends typical CPABE with a hierarchical structure of access policy, so as to achieve simple, flexible and fine-grained access control Moreover, the proposed scheme is proved to be secure under DBDH assumption.

3 Proposed work

We go for implementation of cloud based system which deals with complexity of access control policy & dynamic group data sharing problem. Access control is the better one security mechanism in cloud computing. In this propose Attribute based access control scheme we provides a lightweight approach that allows data owners to easily define and undefined the access policies for the respective data share over the groups. Propose system will also include the re key generation concept for making decryption key unique for each end user. Also in propose system we will build up the system to deal with the major problem of dynamic group sharing i.e User revocation. Revocation is becomes mandatory when the particulars want leave the assigned or joined group that time its access policies should be revoked with its dynamic behavior.

4 Conclusion

Cloud computing is most favorable and preferable fashion for the users which provides several useful services. Yet, some place, there is some security or assurance is required against the information put away or action done over the cloud. This paper provides a review of attribute based encryption mechanisms for cloud computing in which a number of security features are provided. Also we review the different attribute based access control mechanisms used in existing systems. It consist four different attribute based encryption schemes such as KP-ABE (Key-policy attribute-based encryption), CP-ABE (ciphertext-policy attribute-based encryption), HABE (Hierarchical Attribute Based Encryption), MA-ABE (Multi-Authority Attribute Based Encryption). Access Controls are associated with attributes and data . These data & attribute are associated with keys and just those keys that the related to attributes which satisfy the policy associated with the data. Also we discussed about problems within the group sharing concept. Revocation and reassignment both the things are more important while data is sharing inside the group of peoples.

References

1. Shengmin Xu, Guomin Yang, Yi Mu and Robert H. Deng Fellow, "Secure Fine-Grained Access Control and Data Sharing for Dynamic Groups in Cloud", IEEE Transactions on Information Forensics and Security, 1556-6013 (c) 2018 IEEE.
2. YAN YANG, XINGYUAN CHEN, HAO CHEN, AND XUEHUI DU, "Improving Privacy and Security in Decentralizing Multi-Authority Attribute-Based Encryption in Cloud Computing", IEEE Access ,2169-3536 (c) 2018 IEEE.
3. YING ZUOBIN, WEI LU, LI QI, LIU XIMENG AND CUI JIE, "A Lightweight Policy Preserving EHR Sharing Scheme in the Cloud", IEEE Access, 2169-3536 (c) 2018 IEEE.
4. Yinghui Zhang, Member, IEEE, Dong Zheng, Robert H. Deng, "Security and Privacy in Smart Health: Efficient Policy-Hiding Attribute-Based Access Control", IEEE INTERNET OF THINGS JOURNAL, VOL. 3, NO. 1, APRIL 2018
5. Hu Xiong and JianfeiSun , "Comments on Verifiable and Exculpable Outsourced Attribute-Based Encryption for Access Control in Cloud Computing", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 14, NO. 4, JULY/AUGUST 2017
6. HUIJUN ZHU , LICHENG WANG, HASEEB AHMAD, AND XINXIN NIU, "Key-Policy Attribute-Based Encryption With Equality Test in Cloud Computing", IEEE Access, 2169-3536 2017 IEEE.
7. Mr.Sourabha Vijaykumar Pashte, Mr.Chetan J. Awati, "Overcome Key Escrow Problem with Attribute-Based Data Access Policy & Efficient Cloud Environment", 978-1-5386-4008-1/17,2017 Third International Conference on Computing, Communication, Control And Automation©2017 IEEE

8. Javier Herranz, "Attribute-based encryption implies identity based encryption",IET Inf. Secur., 2017, Vol. 11 Iss. 6, pp. 332-337 © The Institution of Engineering and Technology 2017

9. Shulan Wang, Kaitai Liang, Joseph K. Liu, Jianyong Chen, Jianping Yu, WeixinXie, "Attribute-Based Data Sharing Scheme Revisited in Cloud Computing", IEEE Transactions on Information Forensics and Security,1556-6013 (c) 2016 IEEE.

10. Long Li, TianlongGu, Liang Chang, ZhouboXu, Yining Liu, JunyanQian, "A Ciphertext-Policy Attribute-Based Encryption Based on an Ordered Binary Decision Diagram", IEEE Access, 2169-3536 (c) 2016 IEEE.

11. Shulan Wang, Junwei Zhou, Joseph K. Liu, Jianping Yu, JianyongChen,WeixinXie, "An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing", IEEE Transactions on Information Forensics and Security,1556-6013 (c) 2015 IEEE.

12. Kan Yang, Qi Han, Hui Li, KanZheng, Zhou Su and Xuemin (Sherman) Shen, "An Efficient and Fine-grained Big Data Access Control Scheme with Privacy-preserving Policy", IEEE Internet of Things Journal,2327-4662 (c) 2016 IEEE.

13. SikharPatranabis, YashShrivastava and DebdeepMukhopadhyay, "Provably Secure Key-Aggregate Cryptosystems with Broadcast Aggregate Keys for Online Data Sharing on the Cloud",IEEE Transactions on Computers, 0018-9340 (c) 2016 IEEE.

14. Jun Ho Huh, Rakesh B. Bobba, Tom Markham, David M. Nicol, Julie Hull, Alex Chernoguzov, HimanshuKhurana, and Kevin Staggs ,Jingwei Huang, "Next-Generation Access Control for Distributed Control Systems", IEEE INTERNET COMPUTING ,1089-7801/16 © 2016 IEEE

15. ChunqiangHu,WeiLi, XiuzhenCheng, JiguoYu, ShenglingWang, and RongfangBie, "A Secure and Verifiable Access Control Scheme for Big Data Storage in Clouds", IEEE TRANSACTIONS ON BIG DATA,2332-7790 (c) 2016 IEEE.