A Survey on Attribute based encryption in Cloud storage

G.Mamatha
Asst.professor, Chaitanya Bharathi Institute of Technology, Hydreabad, India.
Email: mamathagouni@gmail.com

Abstract: *Cloud computing has attracted extensive attentions from both academics and IT industry. It can provide low-cost, high quality, flexible and scalable services to users. Cloud storage is a great service of cloud computing which offers services for data owners to host their data in the cloud and through cloud servers to provide the data access to the data consumers. It allows the users to access their data from cloud storage anywhere and anytime, so security is very important factor in this access in cloud computing many schemes are there to secure the data in cloud storage. In this Attribute based encryption methodology is the best encryption system. There are Many Attribute based encryption schemes which can be divided into Key policy Attribute based encryption (KP-ABE) and cipher text Attribute based encryption CP-ABE.*

Key Words: *Cloud storage, Key policy Attribute based encryption, cipher text Attribute based encryption.*

1. INTRODUCTION:

Cloud computing is the important aspects of computer world. It enables flexible, on-demand, and low-cost of computing resources. But the data is outsourced to some cloud servers, and various privacy concerns emerge from it. The one of the essential services of cloud computing is the storing capacity of cloud which enables users (data owner) to host their data in cloud by means of cloud server. It provides the data access to data consumers. It can also provide on demand resources for storage which can help service providers to reduce their maintenance costs [15]. Normally users store his/her data in trusted servers. These data are controlled by a trustable administrator [2]. The cloud storage can gives the permission to users to access their data from anywhere on any device in efficient manner. The user's secret key is stored in their personal computer [11]. In cloud computing there are several schemas is proposed to secure the cloud storage. The attribute based encryption methodology is the one among types of encryption system [6]. In this type of system, each user has the user secret key is issued by the authority. This encryption method is the powerful flexible approach which implements attribute-based access control (ABAC) by using data or subjects' attributes as data access policies as well as public keys [10].

Attribute-Based Encryption (ABE) is a promising approach for cloud storage that offers fine-grained access control policy over encrypted data [12]. Attribute-based Encryption (ABE) is regarded as one of the most suitable schemes to conduct data access control in public clouds for it can guarantee data owners' direct control over their data and provide a fine-grained access control service. It deals with authenticated access on encrypted data in cloud storage service [8].There are many ABE schemes proposed, which can be divided into two categories: Key Policy Attribute-based Encryption (KP-ABE), Cipher text-Policy Attribute-based Encryption (CPABE) [2]. In the KP-ABE, a cipher text is associated with a set of attributes, and a private key is associated with a monotonic access structure [3] [14]. Compared with KP-ABE, CP-ABE is a preferred choice for designing access control for public cloud storage. The CP-ABE is used for data owners and based on access policies, to provide flexible, fine-grained and secure access control for cloud storage systems [3]. In CP-ABE scheme, there is an authority that is responsible for attribute management and key distribution. There are two types of CP-ABE systems: single-authority CP-ABE where all attributes are managed by a single authority, and multi-authority CP-ABE [4].

CP-ABE is used to data access control for cloud storage, some multi-authority CP-ABE schemes, has proposed. Specially, in DAC-MACS [1], besides proposing a multi authority CP-ABE scheme for cloud storage, the authors claimed that the attribute revocation mechanism [5]. The user's access permission depends on the attributes the user holds in the CP-ABE based access control system, and each attribute may be possessed by multiple data users [7]. CP-ABE scheme was proposed to completely hide the access policy. However, the scheme only supported the simple 'AND' gate access structure [9].In order to improve the system security, protect user privacy and save the storage overhead of cipher text, for cloud storage [13].

2. RELATED WORK:

Huang *et al.* [16] have proposed with the increasing trend of outsourcing data to the cloud for efficient data storage, secure data collaboration service including data read and write in cloud computing was urgently required. However, it introduced many new challenges toward data security. The key issue was how to afforded secure write operation on cipher text collaboratively, and the other issues include difficulty in key management and heavy computation overhead on user since cooperative users might read and write data using any device. They proposed a secure and efficient data collaboration scheme, in which fine-grained access control of cipher text and secure data writing operation could be afforded based on attribute-based encryption (ABE) and attribute-based signature (ABS) respectively. In order to relieved the attribute authority from heavy key management burden, our scheme employed a full delegation mechanism based on hierarchical attribute-based encryption (HABE). Further, they also proposed a partial decryption and signing construction by delegating most of the computation overhead on user to cloud service provider. The security and performance analysis showed that our scheme was secure and efficient.

Li *et al.* [17] have proposed that data sharing became an exceptionally attractive service supplied by cloud computing platforms because of its convenience and economy. As a potential technique for realizing fine-grained data sharing, attribute-based encryption (ABE) had drawn wide attentions. However, most of the existing ABE solutions suffered from the disadvantages of high computation overhead and weak data security, which had severely impeded resource-constrained mobile devices to customize the service. The problem of simultaneously achieved fine-grandness, high-efficiency on the data owner's side, and standard data confidentiality of cloud data sharing actually still remains unresolved. That paper addressed the challenging issue by proposed a new attribute-based data sharing scheme. It was suitable for resource-limited mobile users in cloud computing. The proposed scheme eliminated a majority of the computation task by adding system public parameters besides moving partial encryption computation offline. In addition, a public cipher text test phase is performed before the decryption phase, which eliminated most of computation overhead due to illegitimate cipher texts. For the sake of data security, a Chameleon hash function was used to generate an immediate cipher text, which would be blinded by the offline cipher texts to obtain the final online cipher texts.

Cui *et al.* [18] have recommend with the advent of cloud computing, it was becoming increasingly popular for data owners to outsource their data to public cloud servers while allowing indented data users to retrieved these data stored in cloud. For security and privacy concerns, data owners usually encrypted their data before outsourcing them to the cloud server. At the same time, users often need to found data related to specific keywords of interest to them, so that motivated the research on the searchable encryption technique. In that paper, they focused on a different yet more challenging scenario where the outsourced dataset could be contributed from multiple owners and were searchable by multiple users. Researching on attribute based encryption (ABE), they proposed an attribute-based keyword search with efficient revocation scheme (AKSER). Our scheme had a high efficiency in terms of user revocation and could achieved fine-grained authorization of the search under the distributed multiple attribute authorized institution. Proofing of security analysis, the proposed scheme AKSER could achieved keyword semantic security, keyword secrecy, trapdoor unlink ability and collusion resistance.

Thouraya *et al.* [19] have described that the data confidentiality in the Cloud Computing was a very challenging task. Encryption was one of the most secure methods ensuring this task, and searchable encryption techniques were used to search on encrypted data without the need for decryption. But, despite that secure measure some leaks might appear when searching over data. In that article, they proposed to improve confidentiality of outsourced data. They were particularly interested in reinforcing the access control on the search result, when the search was performed over encrypted data. The property behind that aspect of security was known as ACAS (Access Control Aware Search) principle. They present a hybridization of Searchable Encryption and Attribute Based Encryption techniques in order to satisfy the ACAS property. The proposed model supports a personalized and secure multi-user access to outsourced data, presenting high search performance. It deals with multi-keywords searches and was designed to speed up the search time by taking advantage of High Performance Computing, which was widely used in Cloud Computing. Two Attribute Based Encryption techniques were considered on the side of the Cloud and some conducted experiments showed the efficiency of the proposed method.

Qiaoyan *et al.* [20] have recommended that the cloud, for achieving access control and keeping data confidential, the data owners could adopt attribute-based encryption to encrypt the stored data. Users with limited computing power were however more likely to delegated the mask of the decryption task to the cloud servers to reduce the computing cost. As a result, attribute-based encryption with delegation emerged. Still, there were caveats and questions remaining in the previous relevant works. For instance, during the delegation, the cloud servers could tamper or replaced the delegated cipher text and respond a forged computing result with malicious intent. They might also cheat the eligible users by responding them that they were ineligible for the purpose of cost saving. Furthermore, during the encryption, the access policies might not be flexible enough as well. Since policy for general circuits enabled to achieve the strongest form of access control, a construction for realizing circuit cipher text-policy attribute-based hybrid encryption with verifiable delegation had been considered in our work. In such a system, combined with verifiable computation and encrypt then MAC mechanism, the data confidentiality, the fine-grained access control and the correctness of the delegated computing results were well guaranteed at the same time. Besides, our scheme achieved security against chosen-plaintext attacks under the k-multi linear Decisional Diffie-Hellman assumption. Moreover, an extensive simulation campaign confirms the feasibility and efficiency of the proposed solution.

Liu *et al.* [21] have proposed that the notion of attribute-based signature was one of important security primitives to realized anonymous authentication. In an attribute based signature (ABS), users could generate a signature on a message with their attributes. With that signature, any verifier would be convinced that such a signature was generated from a signer with these attributes. However, the identity of the signers would be hidden from the verifier. ABS was useful to design anonymous authentication and attribute-based messaging system. However, existing work of attribute-based authentication usually requires huge computation during signing, which grows linearly with the size of the attributes. Thus, these methods result heavy computation overhead on the users and were not suitable for devices with only small computation ability. Cloud computing was an emerging computing paradigm in which resources of the computing infrastructure were provided as outsourcing services over the Internet. In that paper, they first addressed the challenging issue of securely outsourcing ABS, which enabled users largely eliminates the computational costs of ABS generation. The security model was formally defined to protect the privacy of users' signing key while outsourcing the computation of signing. An efficient and secure outsourcing algorithm of ABS was also proposed. Extensive analysis showed that our scheme was secure in the proposed model and saves more than 90% computation overhead on the user side.

Liang *et al.* [22] Proxy Re-Encryption (PRE) was a useful cryptographic primitive that allowed a data owner to delegate the access rights of the encrypted data stored on a cloud storage system to others without leaking the information of the data to the honest-but-curious cloud server. It provides effectiveness for data sharing as the data owner even using limited resource devices (e.g. mobile devices) can offload most of the computational operations to the cloud. Since its introduction many variants of PRE had been proposed. A Cipher text-Policy Attribute-Based Proxy Re-Encryption (CP-ABPRE), which was regarded as a general notion for PRE, employs the PRE technology in the attribute-based encryption cryptographic sets such that the proxy was allowed to convert an encryption under an access policy to another encryption under a new access policy. CP-ABPRE was applicable to many network applications, such as network data sharing. The existing CP-ABPRE systems, however, leave how to achieve adaptive CCA security as an interesting open problem. That paper, for the first time, proposed a new CP-ABPRE to tackle the problem by integrating the dual system encryption technology with selective proof technique. Although the new scheme supporting any monotonic access structures is built in the composites order bilinear group, it is proven adaptively CCA secure in the standard model without jeopardizing the expressiveness of access policy. They further make an improvement for the scheme to achieve more efficiency in the re-encryption key generation and re-encryption phases.

3. OBJECTIVE :

Multi-authority attribute-based access control system for a cloud is proposed for handling the data in a cloud based on Cipher text-policy ABE (CP-ABE). In this method, rather than only using secret keys, some attributes also used for access the data for decrypting the cipher-text. However, it has some difficulties that must be overcome for providing better efficiency and performance. Here, some of them are given, in this existing technique, attributes and the keys are used for providing better security scheme for user authentication towards the data. However, if the unauthorized user entered the wrong attributes or the keys the access will be denied. The role of multiple authorities is inevitable to send the attributes towards the user therefore; the possibilities of occurring data collision are high. In existing ABE schemes involve only one authority to maintain the whole attribute set, which can bring a single-point bottleneck on both security and performance. The ability and the performance of the existing system should be improved.

These are the main drawbacks of various existing works, which motivate us to do this research on Multi-authority attribute-based access control system. In single authority user can easily decrypt the data.

4. CONCLUSION:

In this paper we consider different attribute based encryption strategies attribute-based encryption (ABE), Cipher text-Policy Attribute-Based Proxy Re-Encryption, Proxy Re-Encryption. The main access polices are key policy ABE, Cipher text policy ABE how they work and how secure the data in cloud storage.

REFERENCES:

1. Li, Xiaoyu, Shaohua Tang, Lingling Xu, Huaqun Wang, and Jie Chen (2017), "Two-Factor Data Access Control with Efficient Revocation for Multi-Authority Cloud Storage Systems", IEEE Access 5: 393-405.
2. Li, Wei, Kaiping Xue, Yingjie Xue, and Jianan Hong (2016). "TMACS: A robust and verifiable threshold multi-authority access control system in public cloud storage." IEEE Transactions on parallel and distributed systems 27, no. 5: 1484-1496.
3. Xue, Kaiping, Yingjie Xue, Jianan Hong, Wei Li, Hao Yue, David SL Wei, and Peilin Hong (2017). "RAAC: Robust and auditable access control with multiple attribute authorities for public cloud storage." IEEE Transactions on Information Forensics and Security 12, no. 4: 953-967.
4. Yang, Kan, and Xiaohua Jia. (2014) "Expressive, efficient, and revocable data access control for multi-authority cloud storage." IEEE transactions on parallel and distributed systems 25, no. 7: 1735-1744.

5. Hong, J., K. Xue, and W. Li. (2015) "Security analysis of attribute revocation in multi-authority data access control for cloud storage system." IEEE Trans. Inf. Forens. Security 10, no. 6: 1315-1317.
6. Jung, Taeho, Xiang-Yang Li, Zhiguo Wan, and Meng Wan (2015). "Control cloud data access privilege and anonymity with fully anonymous attribute-based encryption." IEEE Transactions on Information Forensics and Security 10, no. 1: 190-199.
7. Xia, Zhihua, Liangao Zhang, and Dandan Liu. (2016) "Attribute-based access control scheme with efficient revocation in cloud computing." China Communications13, no. 7: 92-99.
8. Yuen, Tsz Hon, Joseph K. Liu, Man Ho Au, Xinyi Huang, Willy Susilo, and Jianying Zhou. (2015) " k $-Times Attribute-Based Anonymous Access Control for Cloud Computing." IEEE Transactions on Computers 64, no. 9: 2595-2608.
9. Yundong, Fan, Wu Xiaoping, and Wang Jiasheng (2017). "Multi-authority attribute-based encryption access control scheme with hidden policy and constant length cipher text for cloud storage." In Data Science in Cyberspace (DSC), 2017 IEEE Second International Conference on, pp. 205-212. IEEE,.
10. Zhu, Yan, Dijiang Huang, Chang-Jyun Hu, and Xin Wang (2015). "From RBAC to ABAC: constructing flexible data access control for cloud storage services." IEEE Transactions on Services Computing 8, no. 4: 601-616.
11. Liu, Joseph K., Man Ho Au, Xinyi Huang, Rongxing Lu, and Jin Li. (2016) "Fine-grained two-factor access control for web-based cloud computing services." IEEE Transactions on Information Forensics and Security 11, no. 3: 484-497.
12. Liu, Zechao, Zoe L. Jiang, Xuan Wang, Siu-Ming Yiu, Chunkai Zhang, and Xiaomeng Zhao (2016), "Dynamic Attribute-Based Access Control in Cloud Storage Systems", In Trustcom/BigDataSE/I SPA, 2016 IEEE, pp. 129-137. IEEE,.
13. Yundong, Fan, Wu Xiaoping, and Wang Jiasheng.(2017) "Multi-authority attribute-based encryption access control scheme with hidden policy and constant length cipher text for cloud storage." In Data Science in Cyberspace (DSC), 2017 IEEE Second International Conference on, pp. 205-212. IEEE,.
14. Jung, Taeho, Xiang-Yang Li, Zhiguo Wan, and Meng Wan. (2015) "Control cloud data access privilege and anonymity with fully anonymous attribute-based encryption." IEEE Transactions on Information Forensics and Security 10, no. 1: 190-199.
15. Zhou, Lan, Vijay Varadharajan, and Michael Hitchens (2013). "Achieving secure role-based access control on encrypted data in cloud storage." IEEE transactions on information forensics and security 8, no. 12: 1947-1960.
16. Huang, Qinlong, Yixian Yang, and Mansuo Shen. (2017) "Secure and efficient data collaboration with hierarchical attribute-based encryption in cloud computing." Future Generation Computer Systems 72: 239-249.)
17. Li, Jin, Yinghui Zhang, Xiaofeng Chen, and Yang Xiang. (2017). "Secure attribute-based data sharing for resource-limited users in cloud computing" Computers & Security.
18. Cui, Jie, Han Zhou, Hong Zhong, and Yan Xu (2017) "AKSER: Attribute-based Keyword Search with Efficient Revocation in Cloud Computing " Information Sciences,.
19. Bouabana-Tebibel, Thouraya, and Abdellah Kaci (2015). "Parallel search over encrypted data under attribute based encryption on the Cloud Computing" Computers & security 54, pp.77-91,.
20. Xu, Jie, Qiaoyan Wen, Wenmin Li, and Zhengping Jin.(2016) "Circuit cipher text-policy attribute-based hybrid encryption with verifiable delegation in cloud computing " IEEE Transactions on Parallel and Distributed Systems 27, no. 1, pp. 119-129,.
21. Liu, Zhusong, Hongyang Yan, and Zhike Li (2015) "Server-aided anonymous attribute-based authentication in cloud computing" Future Generation Computer Systems 52, pp. 61-66,.
22. Liang, Kaitai, Man Ho Au, Joseph K. Liu, Willy Susilo, Duncan S. Wong, Guomin Yang, Yong Yu, and Anjia Yang (2015) "A secure and efficient cipher text-policy attribute-based proxy re-encryption for cloud data sharing" Future Generation Computer Systems 52, pp.95-108,.