ISSN: 0975-833X

Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 10, Issue, 12, pp.76380-76383, December, 2018
DOI: https://doi.org/10.24941/ijcr.33594.12.2018

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

RESEARCH ARTICLE

REVIEW OF EFFICIENT REVOCABLE ATTRIBUTE BASED ENCRYPTION TECHNIQUE IN DYNAMIC GROUPS

***Sonal S. Gulkari and Prof. R. V. Mante**

Department of Computer Science and Engineering, Government College of Engineering, Amravati, Maharashtra, India

ARTICLE INFO

Article History:
Received 20th September, 2018
Received in revised form
10th October, 2018
Accepted 19th November, 2018
Published online 31st December, 2018

Key Words:
Cloud Computing,
Access Control,
Dynamic Groups,
Revocation, Security.

ABSTRACT

We proposed a secure cloud-based application to enhance revocable attribute-based encryption technique. Along with it to boost the security of the document we proposed a modified AES algorithm with some pre-encryption modifications in document to make system more secure and efficient. In our paper first, there is designing of a revocable attribute-based encryption (RABE) scheme with some modification in previous RABE algorithm together with the characteristics of ciphertext relegation by some effort and exclusively combining some techniques to scale down the computation overhead. Then there is presentation of fine-grained access control together with data sharing mechanism for on-demand services along with dynamic user groups in the cloud. Specifically, in this paper the main focused on advancement of RABE scheme which plays an important role in cloud-based application. Furthermore, in this user revocation there is new concept of addition and deletion of users. The comparative data proves that our proposed innovation is more effective and scalable than existing one.

***Citation: Sonal S. Gulkari and Prof. R. V. Mante*, 2018.** "Review of efficient revocable attribute based encryption technique in dynamic groups", *International Journal of Current Research*, 10, (12), 76380-76383.

INTRODUCTION

Cloud systems can be used to enable data sharing capabilities and this can provide several benefits to the user and organization when the data shared in cloud. Since many users from various organization's contribute their data to the Cloud, the time and cost will be less compared to manually exchange of data. Cloud computing is universally accepted as a new computing standard due to its inherent resource-sharing and low maintenance aspects. Cloud computing is an emerging technology using which the customers can store their document and share them with others easily. The security of the document is very valuable for maintaining customer's trust. To improve cloud security, there are many encryption techniques has been evolved to improve cloud security. One of the well-known and popular techniques is Attribute based encryption technique. Many researchers are doing research on ABE technique. In our base paper, there are many loop holes in ABE technique regarding access permission revocation. In our base paper, revocable ABE technique (RABE) has been proposed. According to the author, RABE is efficient to manage access permissions. In RABE technique, the attributes are managed in master secrete key just like ABE technique and the timestamp (Service subscription time period) is managed separately. With the help of that master secrete key, the document is encrypted and stored on cloud. While decrypting any document, user has to submit his allotted key contains attribute key. Then the KGC will check service time span and update attribute key to form master secrete key. Using master secrete key, the document will be decrypted and given to the user. The security requirements for data sharing in cloud computing system are as follows:

Data Security: The provider must be sure that their data outsourced to the cloud is secure and the provider has to take security measures to protect their information in cloud.

Privacy: The provider must ensure that all critical data are encrypted and only authorized users have access to data in its entirety. The references of user and digital identities must be secure as any data which the provider gathered about customer activity from the cloud.

Data Confidentiality: In this concept, the information of user must remain private. It will not easily be disclosed by any illegal or unautherized one. There should not be easy access of information from the cloud.

Fine-grained Access Control: Data owner can't permit the unauthorized users for accessing the data which is redistributed to cloud. The data owner grants different access rights to a set of users to access the data, while others not allowed to access without permissions.

Corresponding author:* **Sonal S. Gulkari,
Department of Computer Science and Engineering, Government College of Engineering, Amravati, Maharashtra, India.

The access permission should be controlled with the help of owner in an un-trusted cloud environment.

User Revocation: When a user gets back the access rights to the data, it will not allow any other user to access the data at the given time. There is no effect on the other authorized users in the group by user revocation.

Scalable and Efficient: The number of Cloud users is remarkably large and the users join and left the service unpredictably, it is essential that the system maintain efficiency as well as scalability. An effective data sharing in cloud computing system must satisfy all the security requirements.

Public Cloud: Public cloud is referred as immerging services that is offered by third-party providers gone with the public internet which makes them ready to everyone who wants to use or buy them. Technically there may be some similarities in public as well as private cloud architecture, however, the concept for both are vary which are made available by a service provider for a public and when communication is effects over the non-trusted network. The management of public cloud is performed by the cloud provider.

Dynamic User Groups: Dynamic user group is the most important concept in cloud computing application, e.g., after expiring or changing of user membership in the cloud and user credentials being stolen/compromised/misused. In dynamic user groups, user revocation is a critical security issue that must be properly addressed. However, one challenging and open problem while handling user revocation in cloud storage is that a revoked user may still be able to decrypt an old ciphertext they were authorized to access before being revoked. In order to address this problem, the ciphertext stored inside the cloud storage should be updated, ideally by the (untrusted) cloud server. In our base paper, the evaluation is shown for maximum 30 attributes to reduce computation overload. The base paper only discusses revocation problem, but not addition problem. If any new user registered and subscribed the service, the cipher text needs to update with new attributes. It is very time-exhausting task to update cipher text for large size files. Therefore, to overcome this issue we proposed an efficient RABE technique with slightly changes in the algorithms described in base paper. In addition to this we proposed modified AES algorithm for remaining the document securely to make our paper strongly secured and efficient than existing one. In our paper the main focused is data sharing on dynamic groups in cloud. The secret key of another users need not to change and update even if new user joins the group or leave the group. Moreover, our innovation can carry out secure user revocation; the revoked users are not able to achieve the original data previously they are revoked though they conspire with the untrusted cloud. Revocable attribute-based encryption (RABE) supporting ciphertext delegation is a useful primitive for enabling secure data sharing via a third-party storage service provider such as cloud storage. In this paper, we revisited the most advanced level of RABE scheme supporting ciphertext delegation and proposed a new construction paradigm that gives more efficient system compared with the existing solution. We provided formal security proofs for our proposed schemes and performed experiments to demonstrate that our new schemes are indeed more efficient than the previous solution. Depends on our mechanism of fine-grained access control we can proposed on demand service. Our proposed RABE scheme with ciphertext delegation can enable secure as well as fine-grained access control in many clouds based on-demand service applications. The high effectiveness of our mechanism significantly reduces the workload of the service provider in handling user revocation that occurs frequently in many large-scale applications. Protecting encrypted media for example Videos in the cloud has been studied in the literature. In, a multimessage attribute-based encryption was proposed foe enabling the access control accomplished encrypted media based on the consumers' attributes. A secure deduplication framework for handling encrypted media in the cloud was introduced to eliminate unused storage and bandwidth charge. In this work, we focus on enabling efficient user revocation for attribute-based cloud media systems.

Literature Review

In (Zhongma Zhu and Rui Jiang, 2013) Zhongma Zhu's scheme, users are able to obtain certificate authorities from group manager as well as secure communication media. In (Nuttapong Attrapadung and Hideki Imai, 2009), Nuttapong Attrapadung allows senders for selecting even if to use either director in direct revocation mode when encrypting a message. With direct mode, the sender specifies the list of revoked users directly into the encryption algorithm. With indirect mode, sender specifies just the encrypt time. In this system, the cipher text/key size is not constant. The (NuttapongAttrapadunga *et al.,* 2011; Matthew Pirretti *et al., 2006*), focuses on ABE schemes along with cipher text having constant size. To achieve constant cipher text, author proposed KPABE method in which the attributes are stored in key. It can cause key escrow problem. The (Patil *et al.,* 2017), proposed a scheme to realize efficient and secure data integrity to audit for sharing dynamic data with multiple users modification. In (Amit Sahai *et al.,* 2005), the author develops the new concept that is Fuzzy Identity-Based Encryption based on Identity Based Encryption technique. In Fuzzy IBE the author views an identity as group of descriptive attributes. The key update efficiency improved by author (Boldyreva *et al.,* 2008) which is in the favor of trusted party. The concept which is reviewed in is an alternative for public key encryption. This scheme creates binary tree data structure hence it is more secure.

A. Fast Digital Identity Revocation

In (Aiello *et al.,* 1998), S. Micali the system of fast digital identity revocation include the revocation of some revoked users so their digital identities must be there, which helps for the efficient implementation of the system. In this infrastructure there is small bit communication between users and verifiers which are participated in the system. Here, author uses public key as well as certificate cryptography combined together. However, there is challenging issue to maintain the private key of right intended user.

B. Certificate revocation and Certificate Update

In (Naor and Nissim, 1998), certificate revocation component includes certificate authority (CA) which is trusted and useful for authentication of public keys. Second, there is directory having one or more non-trusted parties. Third is user which got certificate from CA Fourth one is variant. This method reviewed efficient verification along with efficient updates. The problem with this technique is that the probably certificate

is not revoked and certificate updation in not valid for long term period.

C. Identity-Based Encryption Scheme

In (Boneh and Franklin, 2001), according to D. Boneh elliptic curve helps to vary the Diffie-Hellman problem and also this scheme is widely used for random oracle for ciphertext security. The privacy of ciphertext is completely functional identity-based encryption. In this system, there is no sureity that identity must belongs to intended user, also user revocation is not in this proposed concept. And one more issue of scalability in this technique.

D. Subset Cover Algorithm

Naor D. (Canetti *et al.,* 2013) defines this algorithm which mainly helps in algorithm. Through disjoint subset, all non-revoked users are managed in this concept. Long term keys as well as Short-term keys plays a vital role in this framework. This algorithm is not fully efficient in terms of complexity.

E. Certificate-Based Encryption and Revocation

The (Craig Gentry, 2013) on the basis of merits of public key encryption and identity-based encryption the certificate-based encryption is developed. Certificate-Based Encryption and Revocation helps to remove third party queries on the certificate status. The effort of computation and requirement of bandwidth is not fully considerable over here, even if concept not used hash function. The (Libert and Quisquater, 2003) review the way of revocation with RSA keys. Revocation is done by the mediators and this mediator has given an instruction to stop supporting to the user for signing or decrypting message.

F. Hierarchical identity-based encryption

In HIBE according to Boneh, X. Boyen, E.-J. Goh (Boneh *et al.,* 2005), the size of ciphertext and cost of decryption are not relay on hierarchy depth. There is forward secure encryption, system is used with less size of ciphertext. Security is not efficient over here. HIBE is only for limited delegation. The (Hanaoka *et al.,* 2005) develops the advance form of attribute-based encryption and its application. Here there is labelling of ciphertext as encryptor with some group of descriptive attributes. V. Goyal (Hanaoka *et al.,* 2005) uses Key-Policy attribute-based encryption for private keys which creates the problem of key escrow.

- ***Dual- Policy Attribute Based Encryption***

N. Attrapadung (Attrapadung, 2009) propose the modification of attribute-based encryption. Dual Policy attribute-based encryption permits simultaneously CPABE and KPABE. These both are the access control schemes. Shucheng Yu () proposed scheme consists of data owner, data consumer, some cloud servers and if necessary third-party auditor (TPA). There will be not always online either user or data owner. Cloud server is operated by cloud service provider (CSP). There is constant length of CPABE for multivalued attribute. In addition, proposed scheme is able to support user accountability with minor extension not useful for big extensions.

1. Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud

In (Xuefeng Liu *et al.,* 2013) Xuefeng Liu presents the new concept of MONA which is data sharing concept having cost effective and powerful solution to share group system between cloud users. In this there is a privacy issue as untrusted cloud is there and membership of user get continuously changes. There is no identity privacy in this system. This creates system with less efficient.

Proposed Methodology

On considering all the downsides of the above literature, we proposed a modified algorithm in which the attributes are maintained on KGC server with one unique attribute key. Instead of maintaining the attributes in secrete key, we will maintain the attribute key in master secrete key to remain the length of ciphertext constant upto end. For that we will use modified RABE technique. The main motive of our system is to remain constant ciphertext till end if even if new user add or revoked.

Conclusion

In our proposed system, we proposed two modified algorithms to improve security of the existing system as well to reduce the time required for updating the secrete key if any there is new member addition/ Revocation/Deletion. As we are using attribute id to encrypt the documents using ABE instead of complete attributes, there is not essential to update the cipher text of documents. We have to update the KGC database only. Therefore, we can conclude that our system is more efficient than existing system.

REFERENCES

Aiello, W., Lodha, S., Ostrovsky, R. Fast digital identity revocation (extended abstract). In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 137–152.Springer, Heidelberg (1998).

Amit Sahai, and Brent Waters, 2005. "Fuzzy Identity-Based Encryption", R. Cramer (Ed.): EUROCRYPT 2005, LNCS 3494, pp. 457–473, 2005. *International Association for Cryptologic Research.*

Ankita Nandgaonkar, Prof. Pallavi Kulkarni, 2016. "Encryption Algorithm for Cloud Computing", *International Journal of Computer Science and Information Technologies,* Vol. 7 (2), 983-989.

Attrapadung N., B. Libert, E. De Panfieu, 2011. Expressive key-policy attribute-based encryption with constant-size ciphertexts, in: PKC'11, in: LNCS, vol. 6571, Springer, pp. 90–108.

Attrapadung N., H. Imai, Dual-policy attribute based encryption, in: ACNS'09, in: LNCS, vol. 5536, 2009, pp. 168–185.

Bethencourt, J., Sahai, A., Waters, B.2007. Ciphertext-policy attribute-based encryption. In: IEEE Symposium on Security and Privacy 2007, pp. 321– 334.

Bindu K. Madhavi, C. Sudarsana Reddy, 2014. Data Sharing For Dynamic Groups In The Cloud," *International Journal of Advances in Electronics and Computer Science,* ISSN: 2393-2835 Volume-1, Issue-2.

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

Boneh D. and M. K. Franklin, 2001. Identity-based encryption from the Weil pairing. In CRYPTO, pages 213–229.

Boneh D., X. Boyen, E.J. Goh, 2005. Hierarchical identity-based encryption with constant size ciphertext, in: Eurocrypt'05, in: LNCS, vol. 3494, 440–456.

Canetti R., S. Halevi, J. Katz, 2003. A forward-secure public-key encryption scheme, in: Eurocrypt'03, in: LNCS, vol. 2656, pp. 254–271.

Cheung L., C. Newport, 2007. Provably secure ciphertext policy ABE, in: ACM- CCS'07, pp. 456–465.

Craig Gentry, 2003. Certificate-based encryption and the certificate revocation problem. In EUROCRYPT, pages 272–293.

Emura K., A. Miyaji, A. Nomura, K. Omote, M. Soshi, 2009. A ciphertext-policy attribute-based encryption scheme with constant ciphertext length, in: ISPEC '09, in: LNCS, vol. 5451, pp. 13–23.

Goyal V., O. Pandey, A. Sahai, B. Waters, Attribute-based encryption for fine-grained access control of encrypted data, in: ACM CCS'06, 2006, pp.89–98.

Hanaoka Y., G. Hanaoka, J. Shikata, and H. Imai, 2005. Identity -based hierarchical strongly key-insulated encryption and its application. In ASIACRYPT, pages 495–514.

Libert B. and J.J. Quisquater, 2003. Efficient revocation and threshold pairing based cryptosystems. In PODC, pages 163–171.

Matthew Pirretti, Patrick Traynor, and Brent Waters, 2006. "Secure Attribute-Based Systems" CCS'06, October 30–November 3, 2006, Alexandria, Virginia, USA. Copyright 2006 ACM 1-59593-518-5/06/0010

Nabeel M., N. Shang, and E. Bertino, 2013. "Privacy preserving policybased content sharing in public clouds,"IEEE Trans. on Know. *And Data Eng.,* vol. 25, no. 11, pp. 2602-2614.

Naor M. and K. Nissim, 1998. Certificate revocation and certificate update. In USENIX Security Symposium.

Naor, D., Naor, M., Lotspiech, J. 2001. Revocation and tracing schemes for stateless receivers. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, 41–62. Springer, Heidelberg.

Nuttapong Attrapadung and Hideki Imai," Attribute-Based Encryption Supporting Direct/Indirect Revocation Modes" M.G. Parker (Ed.): Cryptography and Coding 2009, LNCS 5921, pp. 278–300, 2009. Springer-Verlag Berlin Heidelberg 2009.

Nuttapong Attrapadunga, Javier Herranzb, Fabien Laguillaumiec Benoît Libe rtd, Eliede Panafieue, Carla Ràfolsf,"Attribute- Based encryption schemes with constant-sizeciphertexts"© 2011 Elsevier B.V. Allrightsreserved

Patil, V.A., Pratiksha Kute, Pritam Pardeshi, mrutigandha Pathare," Efficient user revocation for dynamic groups using cloud" *International Journal of Research in Advanced Engineering and Technology,* ISSN: 2455-0876; Impact Factor: RJIF 5.44 www.newengineeringjournal.in Volume 3; Issue 2; May 2017; Page No. 48-50

Shucheng Yu, Cong Wang, Kui Ren, and Weijing Lou, 2010. "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292.

Varshini B.V., M. Vigilson Prem, J. Geethapriya, 2017. "A Review on Secure Data Sharing in Cloud Computing Environment," *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET),* Volume 6, Issue 3, ISSN: 2278 – 1323.

Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yang, 2013. "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 6, pp. 1182-1191.

Zhongma Zhu, Rui Jiang (Corresponding author)," A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud "1045-9219 (c) 2013 IEEE.

Zhongma Zhu, Zemin Jiang, Rui Jiang, "The Attack on Mona: Secure Multi-Owner Data Sharing for DynamicGroupsin the Cloud," Proceedings of 2013 International Conference on Information Science and Cloud Computing (ISCC 2013), Guangzhou,Dec.7,2013,pp. 185-189.

****