Efficient Revocable Attribute Based Encryption Technique with Constant Ciphertext to Reduce Computation Overhead

Sonal S. Gulkari
PG Scholar
Department of Computer Science and Engineering
Government college of engineering
Amravati-444 604, Maharashtra, India

R. V. Mante
Assistant Professor
Department of Computer Science and Engineering
Government college of engineering
Amravati-444 604, Maharashtra, India

***Abstract*—We recommend a secure cloud-based application forenhancing revocable attribute-based encryption technique. In addition to this to rise the security of the document we designed a modified AES algorithm along with some pre-encryption modifications in document to make system more safe and adept. In our paper firstoff all,there is outline for the makingof a revocable attribute-based encryption (RABE) schemehaving some modification in existing RABE algorithmin conjunction with the characteristics of ciphertext relegation by fewefforts and exclusively combining some techniques to roll back the computation overhead. Then there is not only the presentation of fine-grained access control but thedata sharing mechanism for on-demand services along with dynamic user groups in the cloud. There is comparison between existing and our proposed methodology in our proposedtechnique. Particularly, in this paper the main focused on upgraded RABE scheme that plays avaluable role in cloud-basedapplication. Furthermore, in thisuser revocation there is new concept of adding and deleting of users. The comparative data proves that our proposed innovation is more effective and scalable than existing one.**

Keywords—cloud computing, access control, dynamic groups, revocation, security

I.INTRODUCTION

Cloud systems can be used to authorize data sharing capabilities and this can support several benefits to the user as well as organization when the data shared in cloud. Since many users from various organization's commit 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. One of the techniques where users can store their document and share them with others easily is nothing but cloud computing. To maintain the customer's trust, the privacy of document is important.There is need to design encryption technique to keep privacy of those documents which are of any types.

For that many more researchers are doing research on ABE technique. In our base paper, there are many alternativesfor ABE technique regarding access permission and revocation. Revocable attribute-based encryption technique is used in this paper. RABE is capable to manage access permissions. In RABE technique, the management of attributes are performed inside the master secret key just like ABE technique and the timestamp (Service subscription time period) is managed separately. On taking the support of that master secrete key, the document gets encrypted and stored on cloud. In case of decryption of any document, user has to submit his allotted key containing attribute key. Then the KDC will responsible for checking service time span and update attribute key to create master secrete key. Using master secrete key, the document will be decrypted and likely given to the user. To share data in cloud computing applications, the security requirements are data security, privacy, data confidentiality, fine-grained access control, user revocation, scalable and efficient, public cloud, dynamic user groups.

Some security measures must be thereso that the data on cloud remains protected in data security. In case of privacy, only authorized data can access data and all the details of customers must be safe. The information of any customer not access by any illegal one from the cloud, this is data confidentiality. The data owner grants different access rights to a group of users for accessing the data, while others not allowed to access without permissions. The access permission must be controlled with the help of owner in an un-trusted cloud environment, this. is the concept of fine-grained access control. 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. In case of dynamicuser groups, joining and leaving of users from the cloud at any time is happened.

As per base paper, the evaluation is limited for maximum 30 attributes to scale down computation overload. And also the base paper only explains the revocation problem, notthe addition problem. If any new user registered and subscribed the service, the cipher text needs to update with new attributes. It is very time-exhaustingtask to update cipher text for large size files. Therefore, to overwhelmed this issue we proposed an efficient RABE technique with small change in the algorithms which was described in base paper. In addition to this we proposed modified AES algorithmfor 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 other users need not to change and update even if new user unitesthe 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 cooperate with the untrusted cloud.

For enabling secure data sharing via a third-party storage service provider such as cloud storage,Revocable attribute-based encryption (RABE) supporting ciphertext delegation is a

useful primitive. Wedesigned the most advanced level of RABE scheme which supports ciphertext delegation and proposed a new construction paradigm that gives more efficient system compared with the existing solution. We provided formal security evidence for our proposed schemes and performed experiments to demonstrate that our new schemes are indeedmore helpful 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 occursfrequently in many large-scale applications.Protecting encrypted media for example Videos in thecloud has been studied in the literature. In, a multimessage attribute-based encryption remain proposed for 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 concept, we focus on enabling efficient user revocation for attribute-based cloud media systems.

II.LITERATURE REVIEW

In [1] Zhongma Zhu'sscheme, users are able to obtain certificate authorities from group manager as well as secure communication media.In [2], NuttapongAttrapadung allows senders for selectingeven if to use either director in direct revocation mode when any message get encrypted. 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 [3][6], 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 [4], proposed a scheme to realize efficient and secure data integrity to audit for sharing dynamic data with multiple users modification. In [5], 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 [7] which is in the favor of trusted party. The concept which is reviewedin
[7] is an alternative for public key encryption. This scheme creates binary tree data structure hence it is more secure.

In [8], 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 [9], certificate revocation component includes certificate authority (CA) which is trusted and useful for authentication of public keys. The problem with thistechnique is that the probably certificate is not revoked and certificate updation in not valid for long term period. InIdentity based encryption scheme [10],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. In this system, surety is not confirmedthat identitymust belongs to intended user, also user revocation is not in this proposed concept. Scalability issues is also in this technique.

NaorD. [12] defines subset cover algorithm through which the disjoint subset, all the non-revoked users are managed. Thisalgorithm is not fully efficient in terms of complexity. Certificate-Based Encryption [13] and Revocation helps to remove third party queries on the certificate status. The [14] review the way of revocation with RSA keys. Revocation is done by the mediators and this mediator has givenan instruction to stop supporting to the user for signing or decrypting message. In Hierarchical identity-based encryption according to Boneh, X. Boyen, E.-J. Goh [15], the size of ciphertext and cost of decryption are not relay on hierarchy depth. Security is not efficient over here. HIBE is only for limited delegation.

The [17] develops the advance form of attribute-based encryption and its application. Goyal [17] uses Key-Policy attribute-based encryption for private keys which creates the problem of key escrow. Attrapadung [20] propose the Dual Policyattribute-based encryption permits simultaneously CPABE and KPABE.These both are the access control schemes. In [24] Xuefeng Liu presents the new concept of MONA which is data sharing concept having cost effective and powerful solution to share group systembetween cloud users. There is no identity privacy in this system. This creates system with less efficient.

III.METHODOLOGY

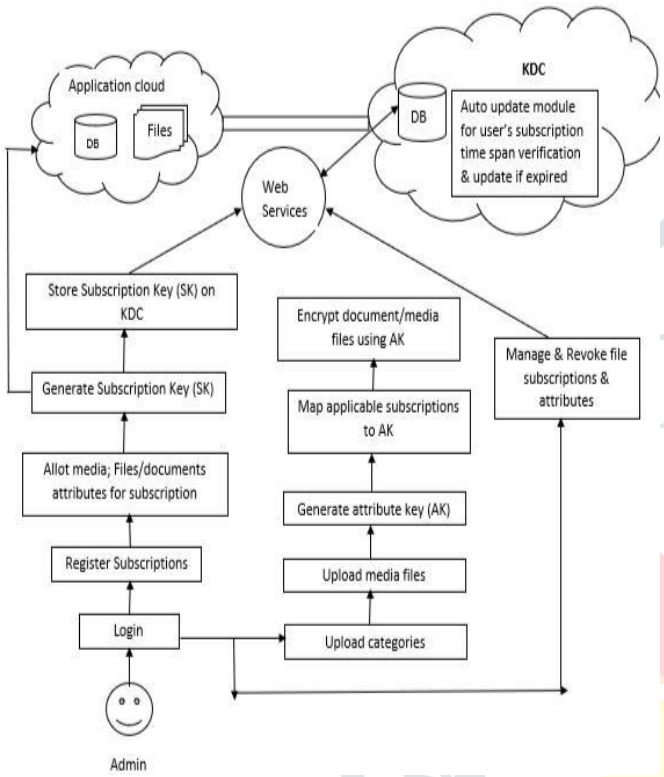
A. Existing Methodology

In existing methodology,the evaluation is shown for maximum 30 attributes to reduce computation overload. The existing system is only for 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-consuming job to update cipher text for large size files.The existing system may slow down for large files.Therefore, to overcome this problem we proposed an efficient RABE technique with slightly changes in the algorithms described in existing technique.

B. Proposed Methodology

We proposed a secure cloud-based application. In our proposed system, to improve the security of existing system we proposed two modified algorithms. One is AES algorithm with some pre-encryption defined by us. And second is revocation attribute-based encryption algorithm to reduce the time required for updating the secrete key in case of new member addition/ Revocation. As we are using attribute id to encrypt the documents using ABE instead of complete attributes, there is no need to update the cipher text of documents. We have to update the KDC database only. We are developing an elearning application For that purpose, we are designing following modules to implement our new technology: -

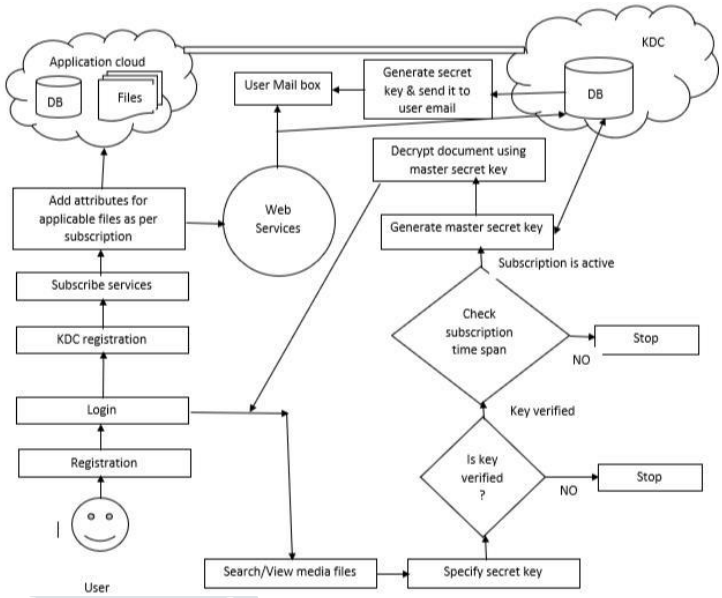
- Admin panel
- Trainer
- Student
- Encryption
- Decryption
- Attributes Revocation/Addition
- Revocable attributes-based encryption



Working of Admin

There is one cloud administrator in admin module which has responsibility to accept or reject the institute. It also manages client institute. Cloud rent, cloud service usage and tracking of cloud payments are noticed under this cloud administrator. When institute get login under admin there is registration of trainers under institutes. The trainer uploads the documents having different categories. When the document gets uploaded it generates attribute key. Here the document gets uploaded by modified AES algorithm.

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.



Working of User

Whenever student get login then he/she is able to seedifferent course wise subscriptions which is design under trainer. After this student can see various subscriptions plans, courses under the trainer. When any student subscribes any course, he/she allotted the subscription key. And the student decrypt/download by using master secret key. At the time of decryption, user will submit his key, our system will send request to KGC for verification. KGC will verify the key as well as service timestamp. If the user has access permission, he will get security token to recheck the user's identity on his email. User will specify that token, if the token is verified, the master secrete key will be generated to decrypt the document. The master secrete key will be made up of attribute key as well as owner's identity information.

IV. Conclusions

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. We are maintaining the theme of the base paper (ie ABE + IDE) as it is by using efficient algorithm.

.

References

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

[2] NuttapongAttrapadung 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. c Springer-Verlag Berlin Heidelberg 2009

[3] NuttapongAttrapadunga,JavierHerranzb,FabienLaguillaumiec,BenoîtLibe ec, EliedePanafieue,CarlaRàfolsf ," Attribute-basedencryptionschemeswithconstant-sizeciphertexts"

© 2011ElsevierB.V.Allrightsreserved

[4] 1 VA Patil, 2 PratikshaKute, 3 Pritam Pardeshi, 4 SmrutigandhaPathare ," 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

[5] Amit Sahai1, and Brent Waters2," Fuzzy Identity-Based Encryption", R. Cramer (Ed.): EUROCRYPT 2005, LNCS 3494, pp. 457–473, 2005. c International Association for Cryptologic Research 2005

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

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

[8] 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).

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

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

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

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

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

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

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

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

[17] V. Goyal, 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.

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

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

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

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

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

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

[24] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yang, "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, June 2013.

[25] Zhongma Zhu, Zemin Jiang, Rui Jiang, "The Attack on Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud,"Proceedings of2013 International Conference on Information Science and Cloud Computing (ISCC 2013), Guangzhou,Dec.7,2013,pp. 185-189.

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

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

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

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