6th International Conference on Multidisciplinary Research (ICMR-2019)
Osmania University Campus, Hyderabad (India)
30th-31st May 2019 www.conferenceworld.in
Conference World
ISBN : 978-93-87793-89-7

Implementation of Efficient RABE Technique with Constant Ciphertext in Dynamic Groups

Sonal S. Gulkari[1](PG Scholar)**, Prof. R.V. Mante**[2](Assistant Professor)

[1]*Department of Computer Science and Engineering, Government College of Engineering, Amaravati*

[2]*Department of Computer Science and Engineering, Government College of Engineering, Amaravati*

***Abstract*—*The secure cloud-based application to improve revocable attribute-based encryption technique is our new innovation regarding the field of cloud computing. Together with it for improving security of document we propose AES algorithm with modification. 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 safer and adept. In our paper first off all, there is outline for the making of a revocable attribute-based encryption (RABE) scheme having some modification in existing RABE algorithm in conjunction with the characteristics of ciphertext relegation by few efforts and exclusively combining some techniques to roll back the computation overhead. There is comparison between existing and our proposed methodology in our proposed technique. Particularly, in this paper the main focused on modified AES regarding privacy issue of document that plays a valuable role in cloud-based application. Furthermore, in this user revocation there is new concept of adding and deleting of users. We make our system not user specific but document specific. 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 alternatives for 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 there so 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, not the 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 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 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 other users need not to change and update even if new user unites 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 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. We designed 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 selecting even 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. In Identity 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 confirmed that 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 [21] 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

1. 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. If new user get registered then each time attribute key get changed It is very time-consuming job to update cipher text for large size files time to time. 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.

2. 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 keep the the document key for user verification along with subscription key and attribute key. 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: -

- Cloud Admin panel
- Institute
- Trainer
- Student
- Encryption
- Decryption
- Attributes Revocation/Addition
- Revocable Attributes-Based Encryption

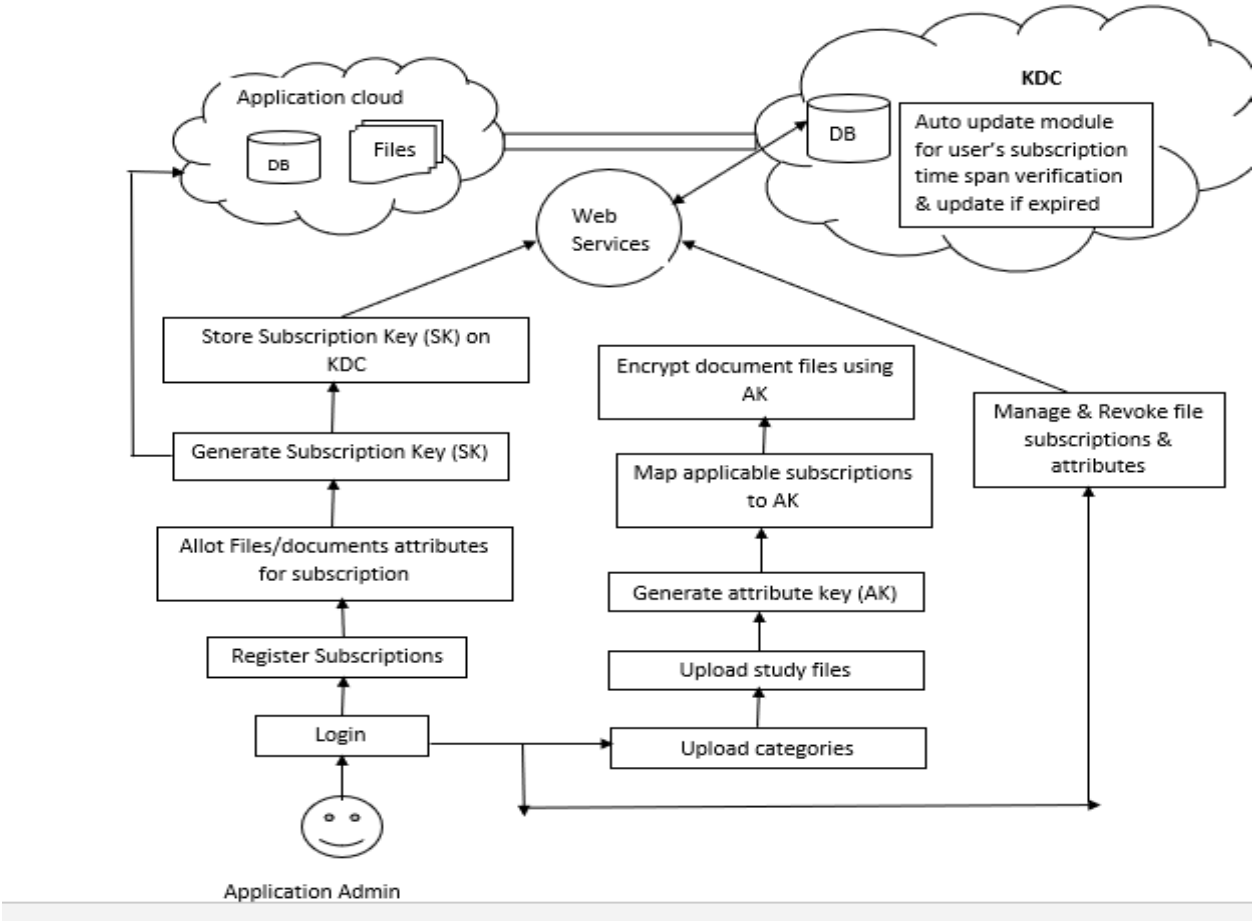

Fig 2.1: Working of Admin

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.

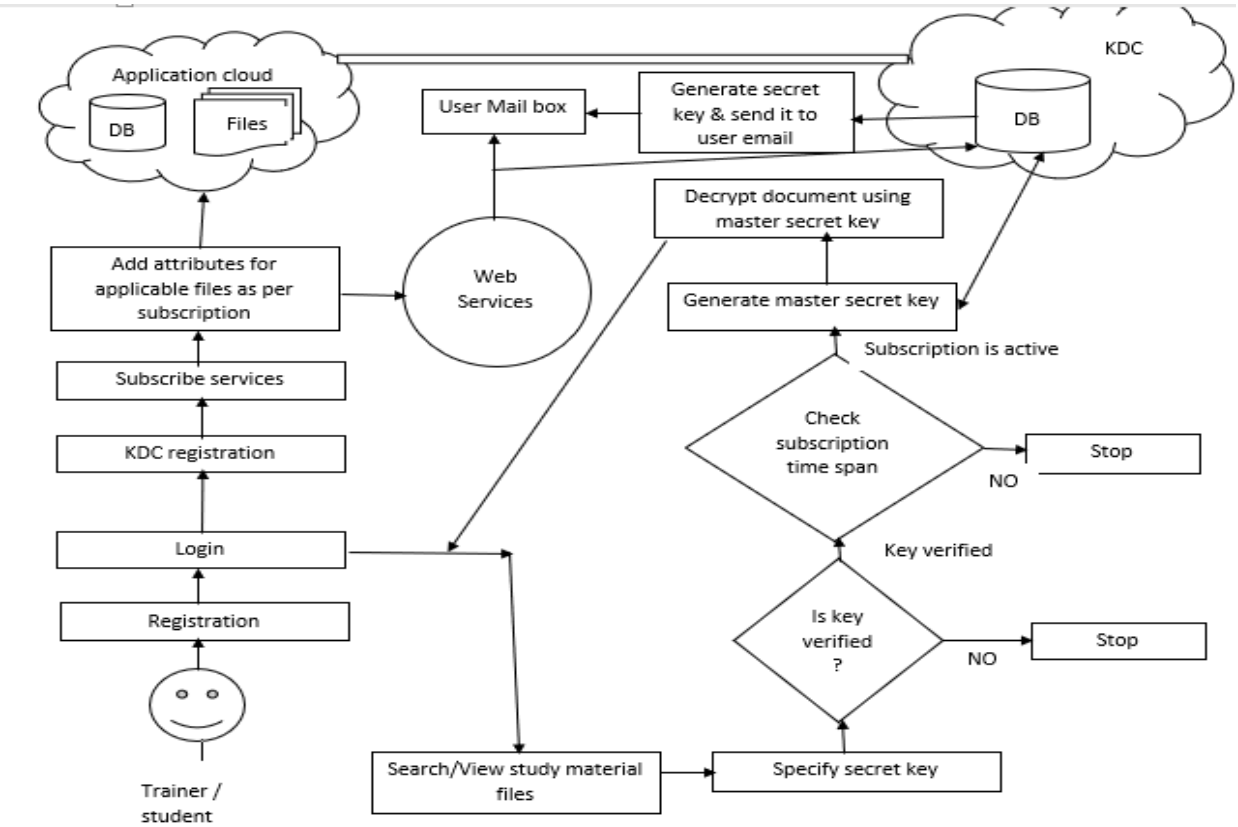

Figure 2.2: Working of User

Whenever student get login then he/she is able to see different 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.EXPERIMENTAL ANALYSIS

In case of existing system, if we are uploading my test upload file it takes 10739471ns for encrypting by using AES but in our proposed system as we are using modified AES it takes 395109037ns.If admin uploads database queries it takes 26574000ns for encryption it but modified AES takes 66256000ns for encryption. Similarly, for project synopsis of length 255104 takes 37582800ns for encryption in existing one but now it takes 63728300ns for encryption. While uploading documents like project presentation and text it takes 32345000ns and 29714500ns for encryption in case of existing whereas in case of our proposed it takes 33152500ns and 67574300ns for encryption. On the basis of all of the above performance, modified AES takes

more time for encryption as compared to existing AES. So, we can conclude from these that our system is more secured than previous one and efficient one also.

For existing system, attribute key is separate for each user so it needs to update if new user add but in case of our proposed system there only one attribute key user upto end and document key is provided for accessing document. So, if there are 2 users subscribing same service then it takes 12068400ns for attribute key and in our proposed work it takes 6034200ns.Proposed system 33.33% time while existing takes 66.67% for attribute key time. This reduces the computation overhead.

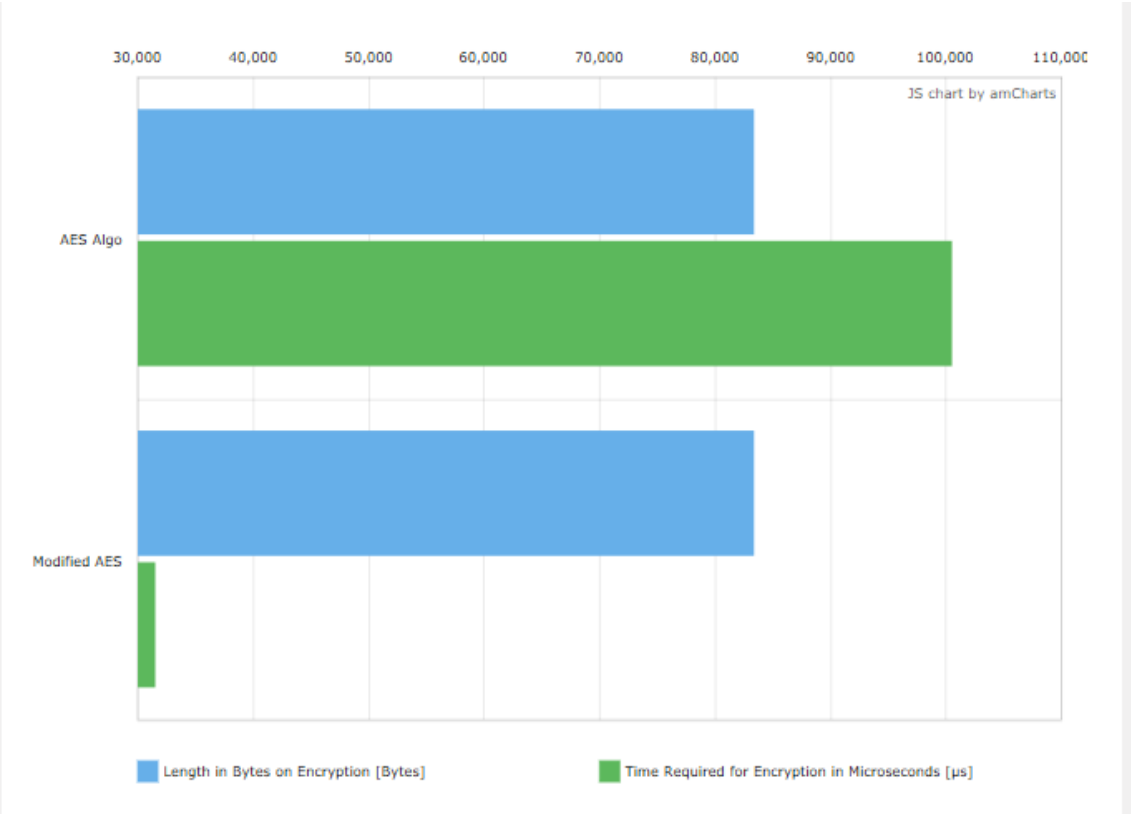

Fig 3.1: Comparison of Existing and Proposed System in Case of Average Time for Encryption

Criteria	Encryption Time	Encrypted Length
AES Algorithm	31520.13 µs	83368.0 Bytes
Modified AES Algorithm	100472.44 µs	83368.0 Bytes

Fig 3.2: Overall Result

If there are 6 documents encrypted which is of length 83368 bytes then AES takes average time of 31520.13 microsecond for encrypting those 6 documents. Whereas if we are using our proposed modified AES which is

of same length then it takes average time of 100472.44 microseconds for encrypting those 6 documents. It concludes our proposed algorithm is efficient and secure regarding document privacy.

V.RESULT

In our proposed system, we proposed two modified algorithms. First is modified algorithm with some pre encryption which improves the security of document. As we are developed system which is document specific not user specific so computation overhead get reduced. We make the system which reduces the time required for updating the secrete key in case of new member addition/ revocation. Our proposed system takes average 100472.44 microseconds to encrypt six documents and existing takes 31520.13 microsecond. Our system takes more times therefore we can conclude that our system is more efficient than existing system regarding privacy of document.

REFERENCES

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

[2] NuttapongAttrapadung and Hideki Imai," Attribute-Based Encryption Supporting Direct/Indirect Revocation Modes"pp. 278–300, 2009. c Springer-Verlag Berlin Heidelberg 2009

[3] NuttapongAttrapadunga, Javier Herranzb,FabienLaguillaumiec,BenoîtLibertd,, Elie de Panafieue, Carla Ràfolsf ," Attribute-based encryption schemes with constant-size ciphertexts",Elsevier,2011.

[4] VA Patil ,PratikshaKute,PritamPardeshi,SmrutigandhaPathare ," Efficient user revocation for dynamic groups using cloud "International Journal of Research in Advanced Engineering and Technology. Volume 3; Issue 2; May 2017; Page No. 48-50

[5] Amit Sahai, and Brent Waters," Fuzzy Identity-Based Encryption", 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

[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, 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., vol. 2139, pp. 41–62. Springer, Heidelberg (2001)

[12] R. Canetti, S. Halevi, J. Katz, A forward-secure public-key encryption scheme,, 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.