An Integrative Access Control with an Attributes-based Event Handler for Data Protection in Cloud Storage

Phyo Wah Wah Myint, Swe Zin Hlaing
University of Information Technology, Yangon, Myanmar
phyowahwah@uit.edu.mm, swezin@uit.edu.mm

Abstract

For many enterprises, cost savings and reducing the security risk are very important for data exchanging between all the involved parties. Cloud computing allows users to use different services which save storage and maintenance costs. The personal data has to be protected against unauthorized accesses in cloud storage. This paper shows an integrative access control with an attributes-based event handler for data protection. This access control is also an improvement of ciphertext policy attribute-based encryption (CP-ABE). In this access control scheme, a data owner firstly chooses an attribute-based access policy before he encrypts his data, and then encrypts the data. Moreover, an attributes-based event handler is integrated in this scheme before decryption phase. Every authorized/unauthorized user has to be checked by this handler. If and only if a user can pass this handler, he/she can decrypt the data. This handler checks every user by four cases. All of the four cases in this handler depend on both attributes-based policy and session timer of user during his/her requests for ciphertext. This integrative access control intends to give a full right on data owner to define access policy and to get a fine-grained access control for data protection in cloud storage.

Keywords- cloud storage, attribute-based access control (ABAC), attribute-based encryption (ABE), ciphertext policy ABE (CP-ABE)

1. Introduction

Modern societies and organizations are more and more complex, dynamic and flexible. The management of private and confidential information is a major problem for dynamic organizations. Data owners and organizations are motivated to outsource more and more sensitive information into the cloud servers. Protecting cloud from unauthorized users and other threats is a very important task for security providers who are in charge of the cloud. The secure cloud is always a reliable source of information. Access control is one of the most fundamental requirements in cloud computing. Access control has the paramount responsibility of providing smooth and easy access to authorized users as well as, at the same time, preventing access to any unauthorized users. It is also a mechanism by which services know whether to honor or deny requests. There are some existing systems on access control in cloud which are centralized in nature. For securing data storage in cloud, it needs to use decentralized access control scheme that supports user authentication, key generation and management as well as multi authority data storage and retrieval. This paper focuses on the integration of access control and an attributes-based event handler for data protection in cloud storage. Moreover, it refers to the improvement of ABE schemes such as Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE) for cloud computing. Section 2 describes the related work including the ABE, literature review and their problem statements. Section 3 describes proposed integrative access control with an attribute-based event handler for data protection in cloud storage. Section 4 describes analysis on access control techniques over CP-ABE and proposed system. Section 5 includes conclusion. Section 6 describes limitation and further extensions and finally describes the references.

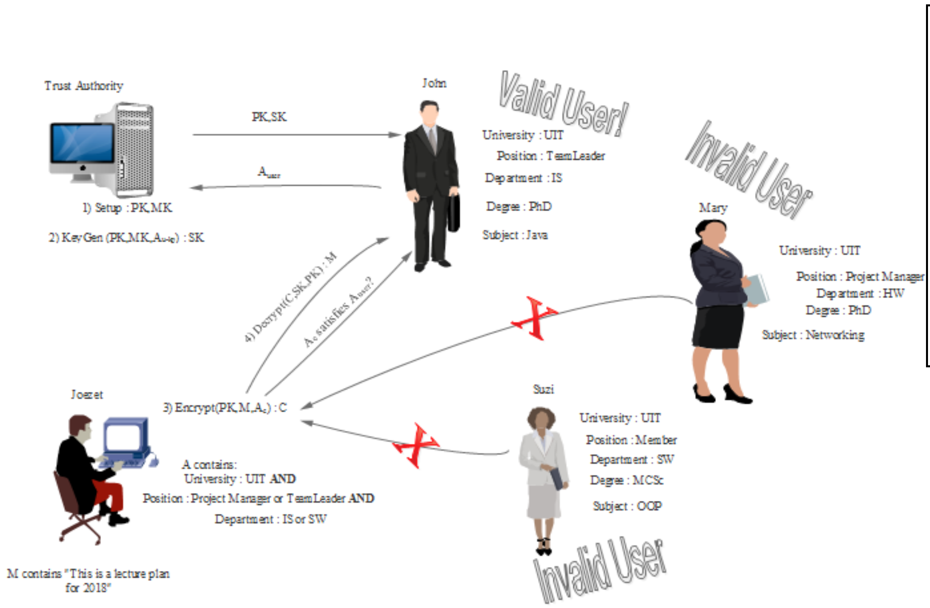
2. Related Work

2.1. Attribute-based Encryption (ABE)

Attribute-based encryption (ABE) is a public-key based one-to-many encryption that allows users to encrypt and decrypt data based on user attributes [1] in which the secret key of a user and the ciphertext are dependent upon attributes. The decryption of a ciphertext is possible only if the set of attributes of the user key matches the attributes of the ciphertext. Decryption is only possible when the number of matching is at least a threshold value. Collusion-resistance is crucial security feature of Attribute-Based Encryption. An adversary that holds multiple keys should only be able to access data if at least one individual key grants access. Another modified form of classical model of ABE is Key-Policy ABE (KP-ABE) as in Figure.1. The KP-ABE scheme can achieve fine-grained access control and more flexibility to control users than ABE scheme. Another modified form of ABE is called Ciphertext Policy ABE (CP-ABE) as in Figure. 2. CP-ABE improves the disadvantage of KP-ABE that the encrypted data cannot choose the decryptor who can decrypt it. It can support the access control in the real environment. [1] [3].

2.2. Literature Review of Ciphertext Policy Attribute-based Encryption

Researchers have described the problems occurred in ABE schemes in various ways. Shucheng Yu, Cong Wang, KuiRen, and Wenjing Lou proposed a combining technique of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption technique to achieve a fine-grained data access control in cloud computing [5]. Tengfei Li, Liang Hu, Yan Li, Jianfeng Chu, Hongtu Li, and Hongying Hanstudied ABE schemes of data access control in cloud storage environment. They listed some unsolved issues of existing access control schemes for cloud storage to provide some future developed direction about the further improvement [2]. Pradnya P. Shelar and Prof. Manisha M. Naoghare surveyed on efficient CP-ABE and secure data access control for multi authority cloude storage with data mirroring. They proposed a revocable multi-authority CP-ABE scheme to design the data access control scheme [4]. John Bethencourt, Amit Sahai, Brent Waters proposed ciphertext policy attribute based encryption (CPABE) by additional consideration for a delegation on an essential attribute structure [6]. Luan Ibraimi, Muhammad Asim, Milan Petkovic, Brent Waters proposed An Encryption Scheme For A Secure Policy Updating [7]. But, it could not be efficient to be enough secure. G. Wungpornpaiboon1 and S. Vasupongayya proposed Two-layer Ciphertext-Policy Attribute-Based Proxy Re-encryption for Supporting PHR Delegation [8]. In [8], the encryption layer is divided into two layers such as inner and outer layer. The inner layer is possessed by data owner and outer layer is to satisfy the access structure for delegator. Jianwei Chen and Huadong Ma proposed Efficient Decentralized Attribute-based Access Control for Cloud Storage with User Revocation[9]. The authors proposed to consider the user revocation associated attributes set [9]. Le Qun Mo and Fu Yong Lin proposed a dynamic re-encrypted ciphertext-policy attributed-based encryption scheme for cloud storage [10]. The authors proposed to consider for re-encryption the ciphertext by using re-key in case of attribute revocation or delegation by delegator. Jiguo Li, Wei Yao, Yichen Zhang,Huiling Qian and Jinguang Han proposed Flexible and Fine-Grained Attribute-Based Data Storage in Cloud Computing [11]. In [11], the authors proposed a fine- grained access control (ABE) scheme with efficient user revocation for cloud storage system. The issue of user revocation can be solved efficiently by introducing the concept of user group. When any user leaves, the group manager will update users' private keys except for those who have been revoked [11].



PK = Public Key
MK = Master Key
SK = Secret Key
A_c = Attributes policy for cipher
A_{user} = User's attributes
A_{u-kp} = Key policy attributes of user
A_{u-cp} = Ciphertext policy attributes of user
M = Plain text message
C = Ciphertext

Figure 1. Key policy attribute-based encryption (KP-ABE) Illustration

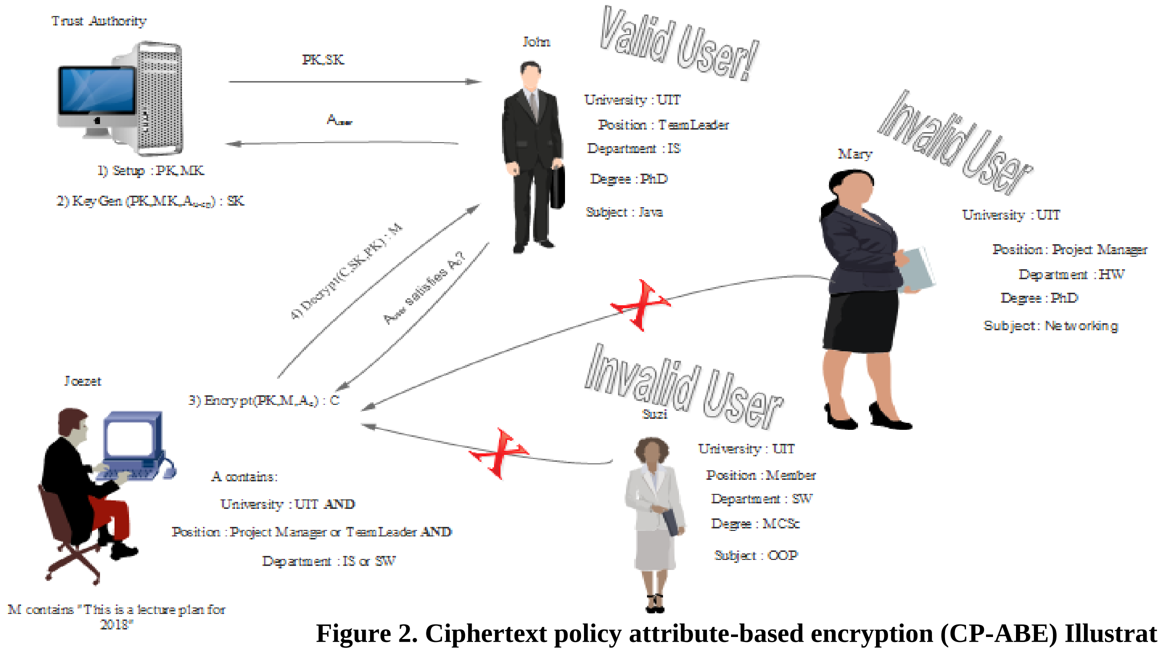


Figure 2. Ciphertext policy attribute-based encryption (CP-ABE) Illustration

2.3. Problem Statement

The problem with attribute based encryption (ABE) scheme is that data owner needs to use every authorized user's public key to encrypt data. The application of this scheme is restricted in the real environment because it uses the access of monotonic attributes to control user's access in the system [1]. The problem with KP-ABE scheme is that data owner cannot decide a user who can decrypt the encrypted data. It can only choose descriptive attributes for the data, it is unsuitable in some application because a data owner has to trust the key issuer [1] [3]. CP-ABE has still limitations in terms of specifying policies and managing user attributes [1] [2]. CP-ABE is one of the ongoing works in security research areas for data protection in cloud storage.

3. Proposed Integrative Access Control with an Attributes-based Event Handler for Data Protection in Cloud Storage

3.1. System Structure

In proposed system structure, there are four entities as follows [12]:

- Trusted Authority (TA): An entity which is trusted by all other participating entities in this system. It is trusted in the sense that it securely generates and stores master key and users' secret keys. It securely transmits those secret keys to the users upon valid requests.
- Data Owner (DO): The entity who owns data and encrypts those data.
- Data User (DU): The entity who would like to access encrypted data with proper authorization.
- Cloud Storage Provider: The entity that will provide storage service to store encrypted data.

3.2. System Design

In proposed integrative access control scheme, it emphasizes on defining access policies by the data owner's right. It assumes that a data owner can also update his access policy to grant/deny users who access the data. To check the access ability to the stored data, an attributes-based event handler is used to grant/deny the ciphertext. If user can pass this handler during his session for requesting the ciphertext, he can decrypt the ciphertext and can access data. So, any adversary has to challenge this access control with handler. This handler strongly filters any adversary. The detailed work of this handler will be explained in section 4.2. A workflow of this system design is shown in Figure.3 and Figure.4.

command lines, susu is not an invalid user so she cannot decrypt the filename.pdf.cpabe file and zarzar is a valid user because of her owned attributes so she can decrypt the ciphertext and read the plaintext filename.pdf successfully. In this toolkit, CP-ABE has still limitation in updating policy cases and revoking attributes/users cases.

4.2. Proposed Integrative access control with an Attributes-based Event Handler

In proposed access control scheme, it is written by C# language. In this system design, there are two sites such as data owner and data user sites. For a data owner, he needs to choose attributes access policy as he likes to encrypt the plaintext message. He can also update the attributes access policy for the cipher. For data user site, he firstly requests the ciphertext to access data. So, he needs to give his credentials including attributes for authorization. Here, an attributes-based event handler checks any authorized/unauthorized user before decryption phase. In this handler, each attribute filling is limited by each timer (milliseconds) control and what result he types (right/wrong) control. There are four cases to check the adversary. The first one case 'Session Timeout & Policy Fail' occurs where an adversary fails the session timer control for each attribute filling step and types the wrong result for attributes-based policy in ciphertext. The second one case 'Session Timeout & Policy Pass' occurs where an adversary fails the session timer control for each attribute filling step and types the right result for attributes-based policy in ciphertext. The third one case 'Session Gain & Policy Fail' occurs where an adversary gains the session timer control for each attribute filling step and types the wrong result for attributes-based policy in ciphertext. The last one case 'Session Gain & Policy Pass' occurs where an adversary gains the session timer control for each attribute filling step and types the right result for attributes-based policy in ciphertext. Among these four cases of handler, only the last case 'Session Gain & Policy Pass' can pass the handler and download the ciphertext and can decrypt it. If and only if the user who can pass the handler, he can access the plaintext message. The system architecture is shown in Figure 5.

In Figure 5, the notations are as follows:

DO = Data owner
DU = Data user
TA = Trust authority
CSP = Cloud storage provider
PK = Public Key
MK = Master Key
SK = Secret Key
C = Ciphertext
M = Plaintext message
A = User's attributes

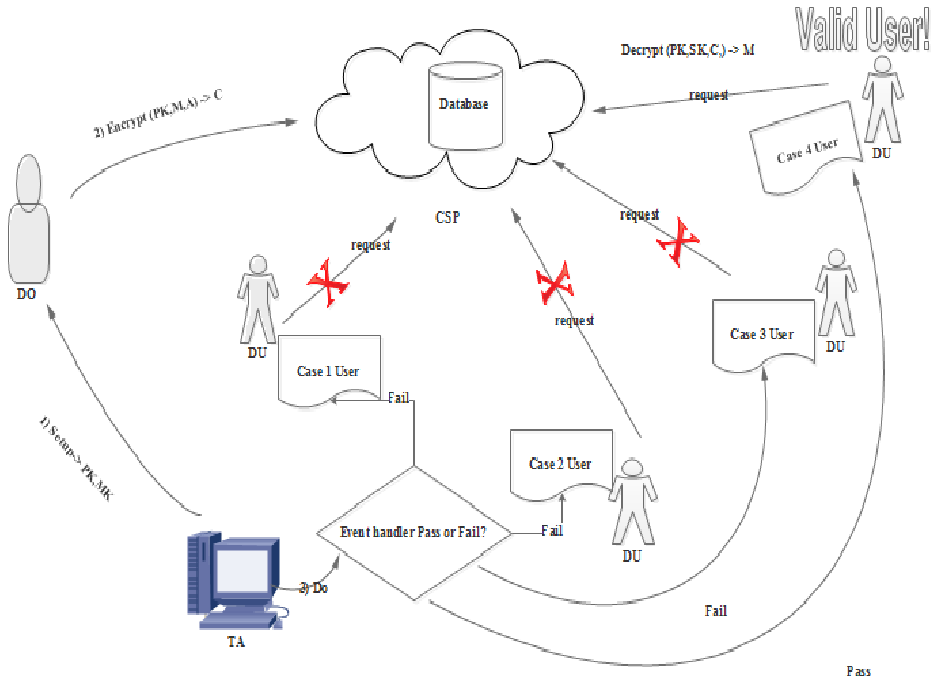


Figure 5. Proposed system architecture

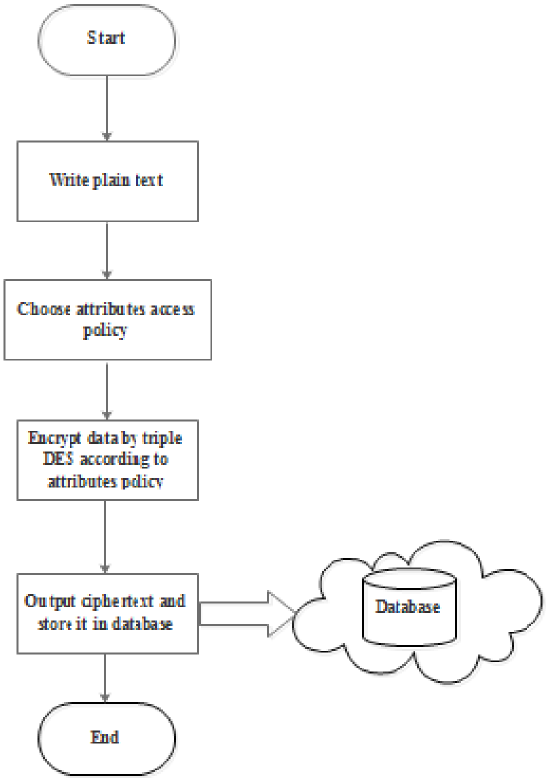

Start
Write plain text
Choose attributes access policy
Encrypt data by triple DES according to attributes policy
Output ciphertext and store it in database
Database
End

Figure 3. System flow for data owner site

4. Analysis on access control techniques over CP-ABE and proposed system

4.1. Access Control by CPABE Technique

In the CP-ABE toolkit testing, it can only use for available attributes access structure in toolkit [6]. This tool is written by C language and tested on OpenSUSE Linux OS. In CP-ABE, there are four basic functions such as setup, key generation, encryption and decryption. The command lines are cpabe-setup, cpabe-keygen, cpabe-enc and cpabe-dec respectively.

The example of cpabe-setup command line is below.

- srv1:~/Desktop/cpabe-0.11/test # cpabe-setup

In setup phase, the system starts up and outputs public key and master key.

In the following keygen command lines, the attributes of user susu are ‘research_field is Crypto, department is HW, qualification is MCTech, age is 28, office is 205 and position is tutor’. The attributes of user zarzar are ‘research_field is DataMining, department is SW, qualification is MCSc, age is 32, office is 105 and position is tutor’ respectively.

- srv1:~/Desktop/cpabe-0.11/test # cpabe-keygen –o susu_priv_key pub_key maser_key research_field Crypto department HW qualification MCTech ‘age = 28’ ‘office = 205’ position tutor
- srv1:~/Desktop/cpabe-0.11/test # cpabe-keygen –o zarzar_priv_key pub_key maser_key research_field DataMining department SW qualification MCSc ‘age = 32’ ‘office = 105’ position tutor

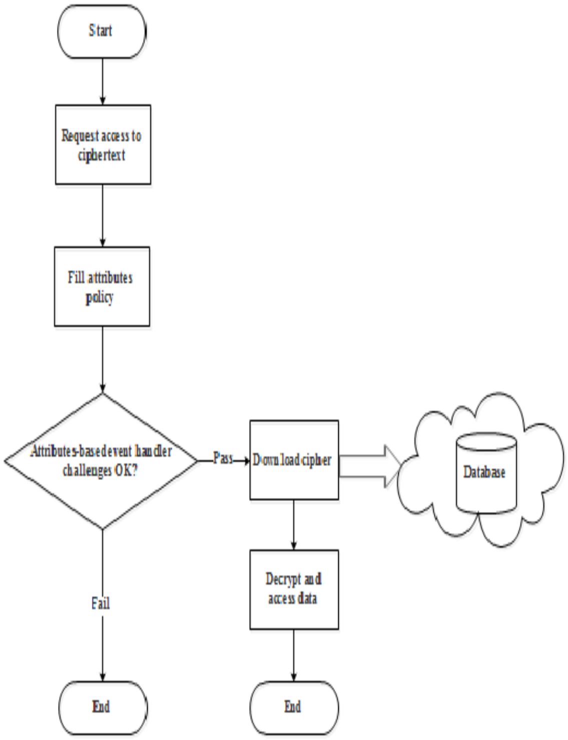


Figure 4. System flow for data user site

In key generation phase, a secret key is generated for each user according to attributes policy.

The example of cpabe-enc command line is below.

- srv1:~/Desktop/cpabe-0.11/test # cpabe-enc pub_key filename.pdf ‘department and 2 of (‘age=32’, SW,IS)’

In encryption phase, the plaintext file filename.pdf is encrypted according to attributes policy ‘(department is SW or IS) and age is 32’ and then plaintext is overwritten as filename.pdf.cpabe file extension. It cannot be read without decryption.

The examples of cpabe-dec command lines are below.

- srv1:~/Desktop/cpabe-0.11/test # cpabe-dec pub_key susu_priv_key filename.pdf.cpabe
- srv1:~/Desktop/cpabe-0.11/test # cpabe-dec pub_key zarzar_priv_key filename.pdf.cpabe

In decryption phase, any authorized user can decrypt the ciphertext and read the plaintext by using a secret key according to attributes policy. In the above two cpabe-dec

4.3. Comparison between CP-ABE and proposed integrative access control with an attributes-based event handler scheme

In CP-ABE access control technique, the keys are generated by attributes access policy. It uses an advanced encryption standard (AES) for encryption. It is suitable for projects in real environment because data owner has a full access control. It has still limitations for attributes management and user revocation problems for multiple domain authority in cloud storage. It is still now in many research areas for data protection in cloud storage.

In proposed integrative access control scheme, the keys are also generated by attributes access policy. It uses triple data encryption standard (triple DES) for encryption. An attribute-based access control is used to define authorized/unauthorized user before both encryption and decryption phases as in the existing CP-ABE methodologies. An attributes-based event handler is also used to check any users. It is more secure and strong detection for user before decryption phase.

5. Conclusion

In this paper, the proposed integrative access control scheme uses an attribute-based access control with an event handler for detection of user credentials. It refers to help the CP-ABE over existing methodologies for data protection in cloud storage. It also focuses on the full control of data owner according to his/her access policy. An attribute-based event handler is also a good supporter for data confidentiality before decryption phase. This proposed integrative access control can give data confidentiality and availability.

6. Limitation and Further Extension

At this moment, only a text message is tested by proposed technique. It will be extended to test another messages (files). As a future work, it is going on to analyze the encryption techniques among CP-ABE researches for data protection in cloud storage.

7. References

[1] Minu George, Dr. C.Suresh Gnanadhas, Saranya.K, “A Survey on Attribute Based Encryption Scheme in Cloud Computing”, International Journal of Advanced Research in Computer and Communication Vol. 2, Issue 11, November 2013.

[2] Tengfei Li, Liang Hu, Yan Li, Jianfeng Chu, Hongtu Li, and Hongying Han, “The Research and Prospect of Secure Data Access Control in Cloud Storage Environment”, Journal of Communications Vol. 10, No. 10, October 2015.

[3] C. Vinoth, G.R.Anantha Raman, “A Survey on Attribute Based Encryption Techniques in Cloud Computing”, International Journal of Engineering Sciences & Research Technology, January 2015.

[4] Pradnya P. Shelar, Prof. Manisha M. Naoghare, “A Survey on Efficient CP-ABE and Secure Data Access Control for Multi Authority Cloud Storage with Data Mirroring”, International Journalof Innovative Research in Computerand Communication Engineering Vol. 3, Issue 10, October 2015.

[5] Shucheng Yu, Cong Wang, KuiRen, and Wenjing Lou, “Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing”, in Proc. of INFOCOM’10, 2010.

[6] John Bethencourt, Amit Sahai, Brent Waters, “Ciphertext-Policy Attribute-Based Encryption”, www.cs.utexas.edu/~bwaters/publications/papers.

[7] Luan Ibraimi, Muhammad Asim, Milan Petkovic, Brent Waters, “An Encryption Scheme For A Secure Policy Updating”, in Proc. of the Security and Cryptography(SECRYPT) International Conference, 2010.

[8] G. Wungpornpaiboon, S. Vasupongayya, “Two-layer Ciphertext-Policy Attribute-Based Proxy Re-encryption for Supporting PHR Delegation”, 978-1-4673-7825-3/15/$31.00 ©2015 IEEE.

[9] Jianwei Chen and Huadong Ma, “Efficient Decentralized Attribute-based Access Control for Cloud Storage with User Revocation”, IEEE ICC - Selected Areas in Communications Symposium, 2014.

[10] Le Qun Mo, FuYong Lin, “A dynamic re-encrypted ciphertext-policy attributed-based encryption scheme for cloud storage”, IEEE Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, 2014.

[11] Jiguo Li, Wei Yao, Yichen Zhang, Huiling Qian and Jinguang Han, Member, IEEE , “Flexible and Fine-Grained Attribute-Based Data Storage in Cloud Computing”, DOI 10.1109/TSC.2016.2520932, IEEE Transactions on Services Computing.

[12] Phyo Wah Wah Myint, Swe Zin Hlaing, Ei Chaw Htoon, “An Encryption Access Control Scheme for Flexible Policy Updating in Cloud Storage”, in Proc. of 14th International Conference on Computer Applications’ Feb, 2017, pp-28-33.