EFFICIENT AND SECURE ATTRIBUTE REVOCATION OF DATA IN MULTI-AUTHORITY CLOUD STORAGE

Reshma Mary Abraham and P. Sriramya
Computer Science Engineering, Saveetha University, Chennai, India
E-Mail: reshmamaryabraham@gmail.com

ABSTRACT

One method which is effective and also ensures security in cloud storage is data access control. Now-a-days this method faces lot of challenges from data out sourcing as well as un-trusted cloud servers. In this case data owners should get direct controls on access policies, which is provided by Cipher text-Policy Attribute-based Encryption (CP-ABE).Due to attribute revocation it is not easy for applying existing CP-ABE schemes to data in cloud storage. This design gives an efficient, expressive and revocation in data access control scheme in multi-authority storage cloud systems, in which there is co-existence of multiple authorities and each will be able to issue independently attributes. Specifically, this implemented system has a revocable multi-authority CP-ABE scheme, which gives the underlying techniques that helps to design schemes in data access control. This efficient revocation method achieves forward security as well as backward security. The screenshots show results in the data access control scheme which is secure and efficient.

Keywords: cloud storage, data access control, cloud servers, multi-authority, attribute revocation, CP-ABE scheme.

1. INTRODUCTION

An important feature of cloud computing is cloud storage [1], this offers many services for the data owners in hosting their data in cloud computing. This method of data hosting and data access services leads to great challenges to data access control. This is why cloud server is not fully trusted by data owners, they are not reliable on servers to do access control. Cipher text-Policy Attribute-based Encryption (CP-ABE) [2], [3] is mentioned as one of the most suitable technologies for data access control. In CP-ABE scheme, there is an authority which is takes the responsibility for key distribution and management of attributes. The data owner will define these access policies also encrypts data in regards to these policies. The user will be provided with a secret key for its attributes. The user can only decrypt data as the attributes satisfies these access policies.

Cloud computing consists of number of resources and services that is offered through Internet. The delivery of cloud services are from the data centers that are located throughout the world. Cloud computing facilitates its consumers by providing virtual resources via internet. One of the cloud services is Google apps, which is provided by Google and also the Microsoft SharePoint. The field of "cloud computing" shows a fast growth which in turn increases severe security issues. Security issues is the only challenge in this broad world of cloud computing. Cloud computing security issues are securing data, and the utilization of cloud by the computing vendors. The www has raised security risks along with the many benefits, same in the case of cloud computing.

There are two different types of CP-ABE systems, they are single authority CP-ABE [2], [3] [4], [5] in which all attributes are managed by a single authority, and multi-authority [6], [7], [8] in which the attributes are managed by different authorities and the attributes are from varied domains. Cloud computing enables users to get the computing power and many varieties of information services from the internet. The types of services are distributed computing, parallel computing and grid computational evolution. In this cloud computing, all these users' data will be stored in these cloud resources Nodes. The result in the computing is distributed to the user through the network whenever the user needs. Although cloud computing has become an effective service model, and has large demand, cloud computing is still faces problems. Three major challenges are:

- Safety
- Stability
- Performance issue

It is not easy to directly use the multi-authority CP-ABE schemes to the multi-authority cloud storage systems due to attribute revocation problem. The significance of multi-authority in cloud storage systems, is that users' attributes can change dynamically. The user will be given new attributes or revoke current attributes. And permission of data access should also accordingly changed. All the existing revocation methods [9], [10], [11], [12] mostly rely on a trusted server or may be lack of efficiency; thus makes it not suitable for dealing with the attribute revocation issues in data access control in the multi-authority in cloud storage. This revocable multi-authority CP-ABE scheme is in which an efficient and also secure revocation method is implemented to remove the attribute revocation problem in the system.

The attribute revocation method is efficient that it takes only less communication cost and also less computation cost, and is secure as it shows that it can achieve both backward security and forward security.

This scheme do not require server to be totally trusted, because the key updating is done by each attribute authority and not by the server. If in case the server is not semi-trusted in certain scenarios, this scheme still shows guarantee regarding the backward security. This revocable multi-authority CP-ABE scheme is applies as the underlying technique to construct an efficient and secure attribute revocation of data in multi-authority cloud storage.

2. SYSTEM MODEL AND SECURITY MODEL

This data access control system in multi-authority cloud storage, as mentioned in Fig.1. There are five main entities in this system and they are: certificate authority (CA), attribute authorities (AAs), data owners (owners), the cloud server and data consumers. CA is a globally trusted certified authority in system. CA sets up the system and accepts the registration for all users and attribute authorities in system. For every legal user in system, CA assigns a unique user identity and then generates a public key for the same user. But, CA is not involved in attribute management and also creation of secret keys which are associated with the attributes. In this scheme, each of the attribute is associated with a single AA, but then each AA can only manage an arbitrary number of attributes. Each AA has full control on the structure and of its attributes. These AA is also responsible for generating public attribute key for the attribute it manages and also secret key for every user reflecting its attributes.

Each and every user is given a global identity in this system. The user may be entitled to a set of attributes which may come from multiple attribute authorities. The user will receive a secret key associated with its attributes corresponding # attribute authorities. Each owner divides the data into several components according to the logic. They encrypt data components using different content keys by using the symmetric encryption techniques. The owner also defines the access policies from multiple attribute authorities and then encrypts content keys under these policies. Then, owner sends encrypted data to cloud server with the cipher texts. This does not rely on server to do data access control. The access control happens in within the cryptography. That is only when the user's attributes satisfies the access policy given in cipher text, the user decrypts the cipher text. The users' with different attributes decrypts different number of content keys and obtains different granularities of information from same data.

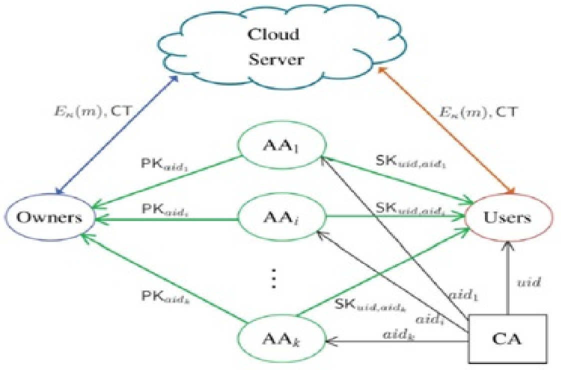


Figure-1. System model.

3. DESIGN DATA ACCESS CONTROL SCHEME

To design the data access control scheme initially for the multi authority cloud storage systems, the underlying Revocable Multi authority CP-ABE protocol is constructed. There are five phases: System Initialization, Key Generation, Data Encryption, Data Decryption and Attribute Revocation.

In [6], Chase has proposed a multi-authority CP-ABE protocol, still it cannot be applied directly as the underlying techniques because of these two reasons: 1) Security Issue:

2) Revocation Issue:

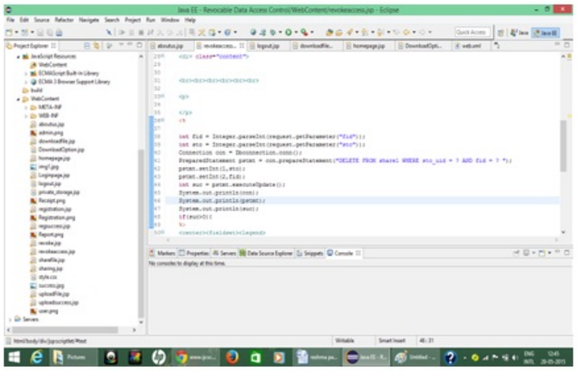
The protocol in [6] do not support attribute revocation. This, new revocable multi-authority CP-ABE protocol which is based on single-authority CP-ABE proposed by Lewko and Waters in [16] is extended it to multi authority scenario and make it revocable. Also the techniques in Chase's multi-authority CP-ABE protocol [6] applied together with secret keys generated by different authorities for the same user to prevent collusion attack. The functionality of the authority divided into global certificate authority (CA) and multiple attribute authorities (AAs). CA sets up the system and also accepts registration of users and AAs in system. It assigns a global user identity to each user and a global authority identity to each attribute authority in the system. The ID is globally unique in system, secret keys issued by different AAs for same ID together for decryption. Also, each attribute is distinguished but also some AAs may issue same attribute. This scheme requires attribute authorities to generate own public keys and then uses them to encrypt data with the global public parameters. This prevents the certificate authority in the scheme from decrypting the cipher texts. When an attribute revocation occurs, cipher texts are updated only for those components associated with revoked attribute in secret keys. When an attribute of a user is revoked there generates a new version key for the revoked attribute and also generates an update key. The updated key, users, except revoked user, who has revoked attributes can update its secret key. Using updated key, components associated with the revoked attribute in the cipher text are also updated to latest version. To improve the efficiency re-encryption method, that the new joined user can decrypt the previous published data, which was encrypted with previous public keys, if they got enough attributes (Forward Security). When updating these cipher texts, the users need to have only current secret key, no need to keep records of previous secret keys.

4. SECURITY ANALYSIS

In this multi-authority cloud storage systems, the following assumptions are made: CA is totally trusted in system. It does not collude with any user, but it prevents from self decrypting any cipher texts. CA executes correctly the task that is assigned by each attribute authority. Each user may be dishonest and may collude to obtain the unauthorized access to the data.

5. IMPLEMENTATION

Here the software used is eclipse Java EE, the programs are called into the software in Figure-2.



```
<div class="content">


<br><br><br><br><br><br>

<p>

</p>
<%

int fid = Integer.parseInt(request.getParameter("fid"));
int eto = Integer.parseInt(request.getParameter("eto"));
Connection con = Dbconnection.conn();
PreparedStatement pstmt = con.prepareStatement("DELETE FROM share1 WHERE eto_uid = ? AND fid = ? ");
pstmt.setInt(1,eto);
pstmt.setInt(2,fid);
int suc = pstmt.executeUpdate();
System.out.println(con);
System.out.println(pstmt);
System.out.println(suc);
if(suc>0){
%>
<center><fieldset><legend>
```

No consoles to display at this time.

Figure-2. Programs in software eclipse.

After connecting the LAN run the programs to get the required output in system 1 and system 2. The internet explorer is used to get the home page as designed in the java program. The home page shows the tab to login to the web page and it also has button which give some details about the organization.

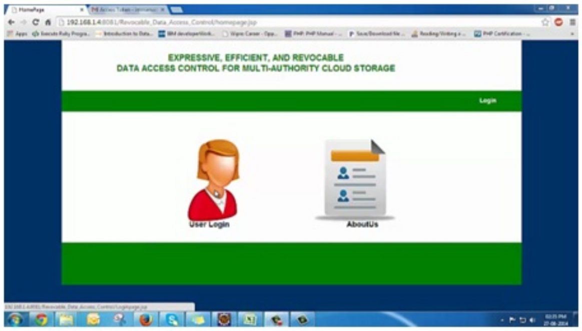

192.168.1.4:8081/Revocable_Data_Access_Control/homepage.jsp
EXPRESSIVE, EFFICIENT, AND REVOCABLE
DATA ACCESS CONTROL FOR MULTI-AUTHORITY CLOUD STORAGE
Login
User Login
AboutUs

Figure-3. Home page.

The next page shows the text boxes to type in the user ID and the password and login to the user account.

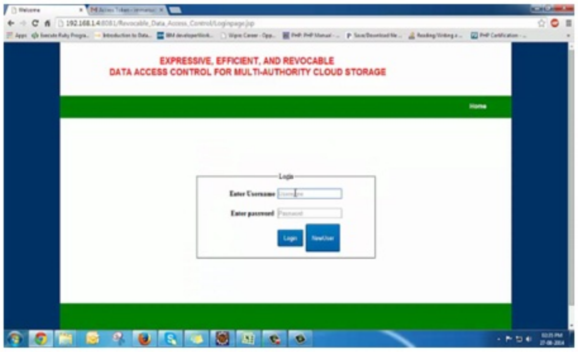

192.168.1.4:8081/Revocable_Data_Access_Control/Loginpage.jsp
EXPRESSIVE, EFFICIENT, AND REVOCABLE
DATA ACCESS CONTROL FOR MULTI-AUTHORITY CLOUD STORAGE
Home
Login
Enter Username
Enter password
Login
NewUser

Figure-4. Login page.

When logged into the system it gives three options which are revoke access, download file and share file. First we upload a file which needs to be shared.

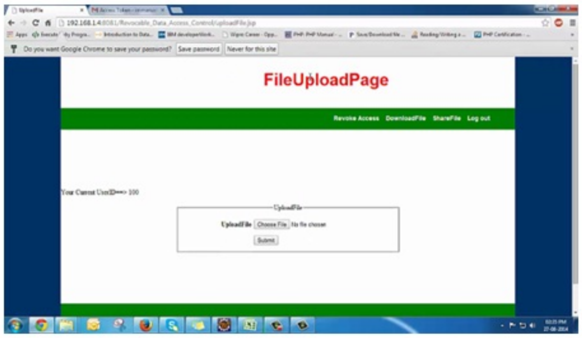


Figure-5. File upload page.

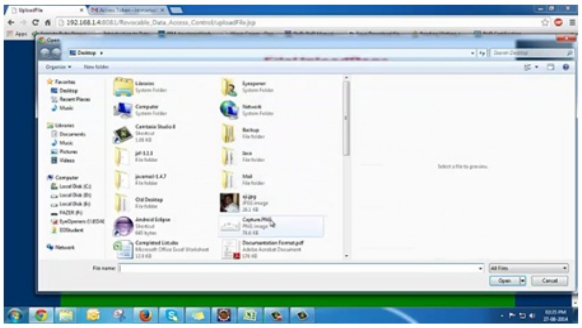


Figure-6. Choosing File.

Thus the desired file has been chosen to share.

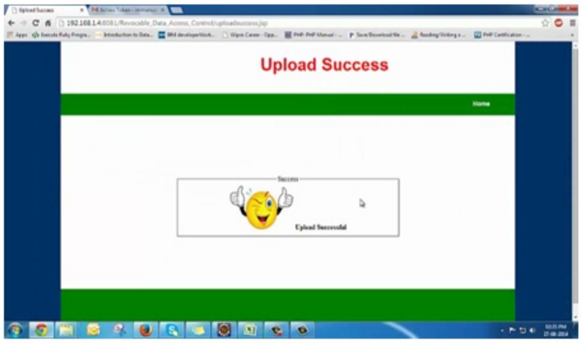
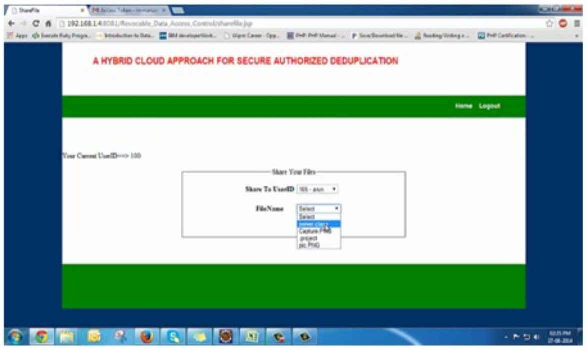

192.168.1.4:8081/Revocable_Data_Access_Control/uploadsuccess.jsp
Upload Success
Home
Success
Upload Successful

Figure-7. Upload success page.

This page shows that the file has been uploaded successfully. In the next step, the desired user, in the desired group is selected to whom the uploaded file has to be shared.



A HYBRID CLOUD APPROACH FOR SECURE AUTHORIZED DEDUPLICATION

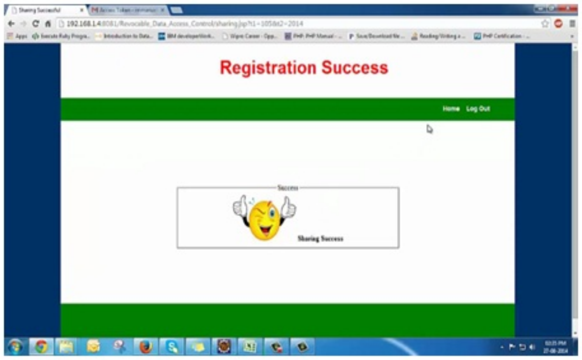
Your Current UserID==> 100

Share Your Files

Share To UserID: 105 - arun

FileName: Select

Figure-8. Choosing user to share.



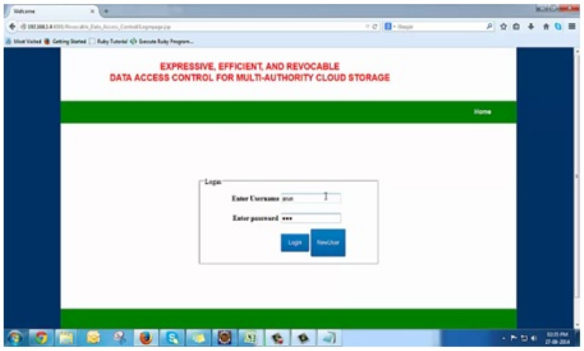
Registration Success

Success

Sharing Success

Figure-9. Successfully shared file.

Now the user is logged into his account and finds the shared file in his account.



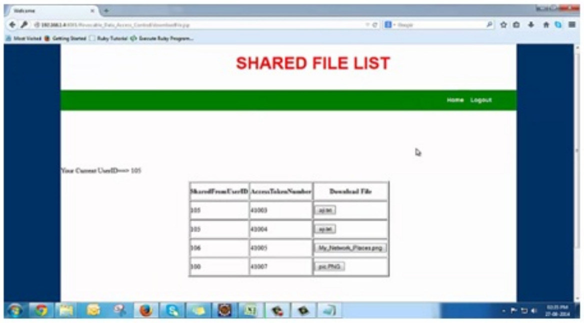
EXPRESSIVE, EFFICIENT, AND REVOCABLE
DATA ACCESS CONTROL FOR MULTI-AUTHORITY CLOUD STORAGE

Login

Enter Username: arun

Enter password: ●●●

Figure-10. User page login.



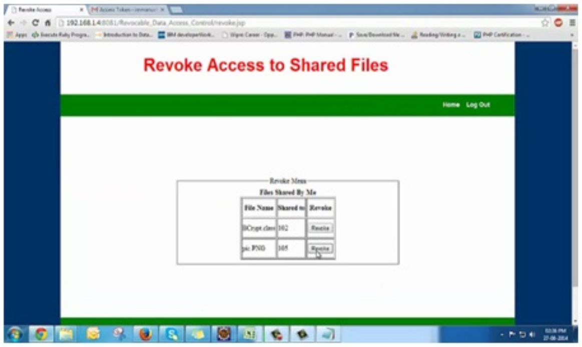
SHARED FILE LIST

Your Current UserID==> 105

SharedFromUserID	AccessTokenNumber	Download File
105	43003	aj.txt
105	43004	aj.txt
106	43005	My_Network_Places.png
100	43007	pic.PNG

Figure-11. User page files inbox.

The next page shows the authority's account in which they can revoke the file which was shared to the particular user.



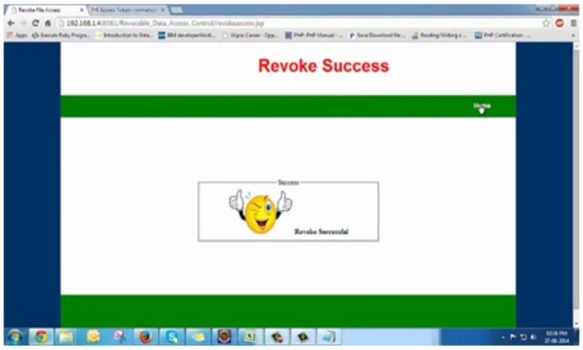
Revoke Access to Shared Files

Revoke Menu

Files Shared By Me

File Name	Shared to	Revoke
BCrypt.class	102	Revoke
pic.PNG	105	Revoke

Figure-12. User account revoke option.



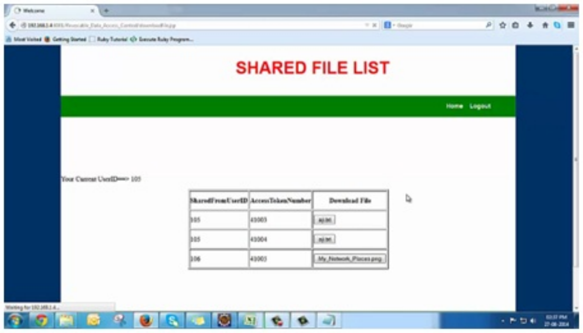
Revoke Success

Success

Revoke Successful

Figure-13. Successfully revoked.

After this process, if the user logs into his account he no longer finds the previously shared file in his shared file list.



SHARED FILE LIST

Your Current UserID==> 105

SharedFromUserID	AccessTokenNumber	Download File
105	43003	aj.txt
105	43004	aj.txt
106	43005	My_Network_Places.png

Figure-14. User account no longer has revoked file.

The attribute revocation was successful.

6. EFFICIENCY

This scheme improves the efficiency of the attribute revocation. In this attribute revocation method, only cipher texts that associates with revoked attribute has to be updated, but in [14], all cipher texts that associated with any attribute from the authority has to be updated.

Also this key and the cipher text updated by using same update key, instead of requiring the owner to generate an update information for each cipher text, such that owners do not required to store each number generated during encryption.

7. CONCLUSIONS

Thus the proposed system is successfully implemented for a revocable multi-authority CP-ABE scheme that shows support efficiency in attribute revocation. Also, then constructed an effective data access control scheme for multi-authority cloud storage systems. Thus scheme is proved by the help of the software. Thus this scheme of revocable multi-authority CPABE is a effective technique, which should be applied in remote storage systems, also online social networks and so on.

REFERENCES

[1] P. Mell and T. Grance. 2009. ‘‘The NIST Definition of Cloud Computing,’’ National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep.

[2] J. Bethencourt, A. Sahai and B. Waters. 2007. ‘‘Ciphertext-Policy Attribute-Based Encryption,’’ in: Proc. IEEE Symp. Security and privacy (S&P’07), pp. 321-334.

[3] B. Waters. 2011. ‘‘Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization,’’ in: Proc. 4th Int’l Conf. Practice and Theory in Public Key Cryptography (PKC’11), pp. 53-70.

[4] V. Goyal, A. Jain, O. Pandey and A. Sahai. 2008. ‘‘Bounded Ciphertext Policy Attribute Based Encryption,’’ in: Proc. 35th Int’l Colloquium on Automata, Languages, and Programming (ICALP’08), pp. 579-591.

[5] A.B. Lewko, T. Okamoto, A. Sahai, K. Takashima and B. Waters. 2010. ‘‘Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption,’’ in: Proc. Advances in Cryptology- EUROCRYPT’10 , pp. 62-91.

[6] M. Chase. 2007. ‘‘Multi-Authority Attribute Based Encryption,’’ in: Proc. 4th Theory of Cryptography Conf. Theory of Cryptography (TCC’07), pp. 515-534.

[7] M. Chase and S.S.M. Chow. 2009. ‘‘Improving Privacy and Security in Multi-Authority Attribute-Based Encryption,’’ in: Proc. 16th ACM Conf. Computer and Comm. Security (CCS’09), pp. 121-130.

[8] A.B. Lewko and B. Waters. 2011. ‘‘Decentralizing Attribute-Based Encryption,’’ in: Proc. Advances in Cryptology-EUROCRYPT’11, pp. 568-588.

[9] S. Yu, C. Wang, K. Ren and W. Lou. 2010. ‘‘Attribute Based Data Sharing with Attribute Revocation,’’ in: Proc. 5th ACM Symp. Information, Computer and Comm. Security (ASIACCS’10), pp. 261-270.

[10] M. Li, S. Yu, Y. Zheng, K. Ren and W. Lou. 2013. ‘‘Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption,’’ IEEE Trans. Parallel Distributed Systems , Vol. 24, No. 1, pp. 131-143, January.

[11] J. Hur and D.K. Noh. 2011. ‘‘Attribute-Based Access Control with Efficient Revocation in Data Outsourcing systems,’’ IEEE Trans. Parallel Distributed Systems, Vol. 22, No. 7, pp. 1214-1221, July.

[12] S. Jahid, P. Mittal and N. Borisov. 2011. ‘‘Easier: Encryption-Based Access Control in Social Networks with Efficient Revocation,’’ in: Proc. 6th ACM Symp. Information, Computer and Comm. Security (ASIACCS’11), pp. 411-415.

[13] S. Ruj, A. Nayak and I. Stojmenovic. 2011. ‘‘DACC: Distributed Access Control in Clouds,’’ in: Proc. 10th IEEE Int’l Conf. TrustCom, pp. 91-98.

[14] K. Yang and X. Jia. 2012. ‘‘Attribute-Based Access Control for Multi-Authority Systems in Cloud Storage,’’ in: Proc. 32nd IEEE Int’l Conf. Distributed Computing Systems (ICDCS’12), pp. 1-10.

[15] D. Boneh and M.K. Franklin. 2001. ‘‘Identity-Based Encryption from the Weil Pairing,’’ in: Proc. 21st Ann. Int’l Cryptology Conf.: Advances in Cryptology - CRYPTO’01 , pp. 213-229.

[16] A.B. Lewko and B. Waters. 2012. ‘‘New Proof Methods for Attribute-Based Encryption: Achieving Full Security through Selective Techniques,’’ in: Proc. 32nd Ann. Int’l Cryptology Conf.: Advances in Cryptology - CRYPTO’12, pp. 180-198.