A Novel Multi-Attribute Authority Based Encryption for Controlling Access to Cloud Data

Asst. Lect. Saif Khalid Musluh
Saifalkhaldi1982@gmail.com

Asst. Lect. Riyadh Rahef Nuiaa
riyadh@uowasit.edu.iq

Abstract:-Cloud computing has changed the way IT department are working with respect to outsourcing data and having controlled access to the data. In the new computing paradigm that supports on-demand services, the storage service became an attractive service for many cloud users. When data is outsourced to cloud, there is an issue of giving controlled access to the cloud data. Many schemes came into existence. Some of the schemes focus on auditing, provable data possession and proof of irretrievability. Some other schemes threw light into the access control on the cloud data. While giving privileges to accessing data attribute based encryption has achieved significant fine-grained control over the data. In this paper we propose a methodology that can allow controlled access to cloud data with multi-attribute authority based encryption. The multi-attribute based approach is used to make the scheme robust. Moreover the proposed approach is aimed at prevention of identity leakage and also achieves anonymity as well. We built a prototype application that demonstrates the proof of concept. The empirical results revealed that the proposed method improves access control significantly.

Index Terms–*Cloud computing, attribute based encryption, multi-authority, anonymity*

*****

I. INTRODUCTION

Cloud computing has changed the way computations take place in the computing world. It provides many services with a pool of centralized resources that can be accessed from any corner of the world. With cloud computing users of the cloud can outsource their data to cloud. The rationale behind this is that cloud can handle huge amount of data with the help of data centres. Since cloud has no limits in providing storage space and has no time and geographical restrictions, it has become an important service. Many users in the world are outsourcing their data to cloud. The cloud based storage become popular due to the benifits provided by the cloud such as global access, cheaper and affordable. In spite of benifits, there are many issues pertaining to data security, privacy and identity disclosure. Not only securing data, but also it is important to ensure that the data can be given access to other users in a controlled fashion. The data access given to others are subjected to the privileges they have. Towards this end many schemes came into existence. They are role based access control (BBAC), Attribute Based Encryption (ABC), Predicate Based Access Control (PBAC) and so on.

Of late identify based encryption came into existence. Privacy and non disclosure of identity became important expectations of the users of cloud. In this context, it is essential to have mechanisms to fulfil all these requirements. In the process of providing such security to the cloud based data, ABE, Key-Policy ABE and Cipher text-Policy ABE provided the required security to great extent. Now the need of the hour is non only access control bust also privacy, non disclosure of identity and also the anonymity are required. There was no existing system to provide all these features. In this paper we address all these issues by defining mechanism that can achieve the desired level of security to outsourced data. Preventing disclosure of users' identities is very important for security reasons. The contributions of this paper are as follows.

- We proposed and implemented a mechanism that provides privacy, access control, non-disclosure of identity and anonymity.
- We built a prototype to demonstrate the proof of concept. The empirical results revealed that the scheme is useful.

The remainder of the data is structured as follows. Section II provides review of literature. Section III presents the proposed system in detail. Section IV presents experimental results while section V concludes the paper.

II. RELATED WORKS

The section provides review of literature relevant to the research area. There were many researches based on attribute based encryption. In [2] and [1] pseudonym concept is used in order to provide multi-authority system for secure communications. One user can have different pseudonyms and they are tied to private key. However, the aggregators in the scheme are not aware of the private keys and therefore they cannot map the pseudonyms to same user. More over the set of attributes is divided into many N disjoint groups and they are maintained by N attributes and authorities. Therefore each authority is aware of only certain attributes of users thus improving security of applications. These attributes are not sufficient to find out the identity of users. The scheme presented in [2] is threshold-based KP-ABE. This scheme has drawback as it lacks generality with respect to policy expression of encryption. There are many schemes that are using attribute based encryption with multiple authorities as explored in [5], [4] and [3]. However they are using either ABE with threshold-based [3] or making use of a semi-honest approach with central authority [5], [4]. In [3] the scheme cannot tolerate collusion attack [3].

The work present in this paper is related to the work of [7] and [6] where the researchers tried to use decentralized approach for CP-ABE scheme. LSSS matrix is used as access structure but the scheme is able to convert the OR and gates only to the LSSS matrix. Thus it has limitations to make a robust encryption policy with Boolean formula. However, there is flexibility inherited from access tree with threshold gates. The approach also supports Disjunctive Normal Form (DNF) as part of the encryption policy. Besides it can also be used to express a general encryption policy. The system can also have the ability to tolerate the compromise attacks that are targeted on the attribute authorities which is missing in the literature in many works.

Of late there was traceable multi-authority ABE scheme explored in [9] and [8] which is not similar to that of ours in this paper. These schemes are able introduce accountability in such a way that it is possible to trace the keys of the malicious users. The similar approach to us is found in [11] and [10]. In the approach the encryption policy is hidden in the cipher texts and the solution is not able to prevent attribute disclose issue in the process of key generation. However, these works and our work are able to complement each other in terms of combination of protection and thus complete the anonymous ABE.

III. PROPOSED SYSTEM AND IMPLEMENTATION

The proposed system is implemented with four different modules. The aim of the system is to simulate the cloud outsourcing process in order to ensure data privacy, user-identity privacy, privilege control and anonymity. The proposed mechanism has different algorithms such as Setup, KeyGenerate, Encrypt, and Decrypt. There are many actors in the sytem namely data owner who outsources data to cloud, cloud server which holds the data and the data consumer who make use of data as per the privileges.

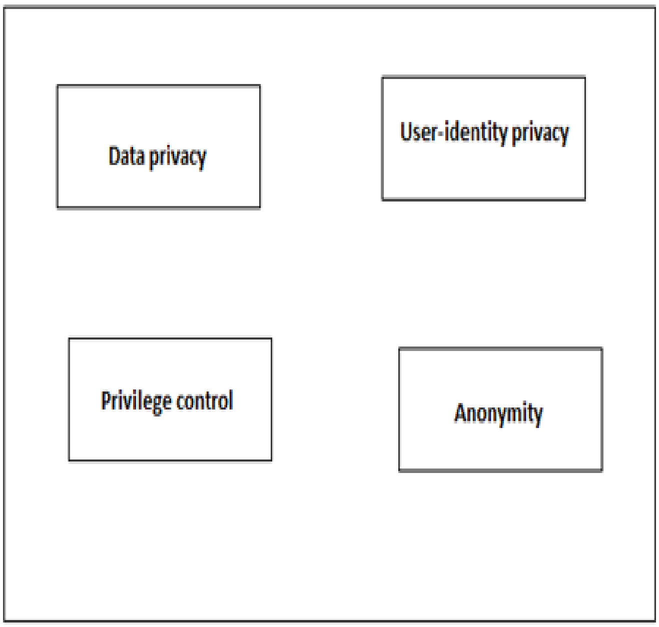


Figure 1 –Shows the important modules implemented in the system

The data owner outsources data to cloud. The authorities are assumed to have abilities to provide access rights to users based on the attributes. The Setup algorithm takes care of producing public parameters that are later used by the system. This is executed by attribute authorities. The KeyGenerate algorithm is used to interact with attribute authorities in order to gain access to private key. The Encrypt algorithm takes a message, set of privileges and public key and complete encryption process. The Decrypt algorithm takes public key, private key and cipher text as input and performs decryption process. It is involved from the cloud data consumer.

Data Privacy

Data privacy refers to the protection of data contents and ensuring that the privacy of the data is not lost. The data access is controlled based on the access privileges given by the data owner to the data consumer.

User Identity Privacy

User identity privacy refers to the fact that the users' actual identity should not be disclosed. The cloud operations should not reveal the actual data owner. Instead it can have mechanisms to ensure that the user identity is not leaked.

Privilege Control

Multiple authorities are used to give access to attributes based on the privileges. The multi-attribte authorities can provide high level of security to data with respect to access privileges.

Anonymity

Anonymity is important as the user identies are to be reserved. The multi-attribute authorities, user-identity privacy, data privacy can complement each other and finally the anonymity is achieved.

Implementation

The implementation is done as part of the prototype application we built. The prototype supports three types of users with different activities. The cloud user, user, and guest user. The three users have common authentication use case. The activities of cloud server include viewing of registered users, uploading files, and view anonymity of users. The user is able to register, login, search for file, download file, and update file. The guest user is responsible for getting access code, search for file, and download files.

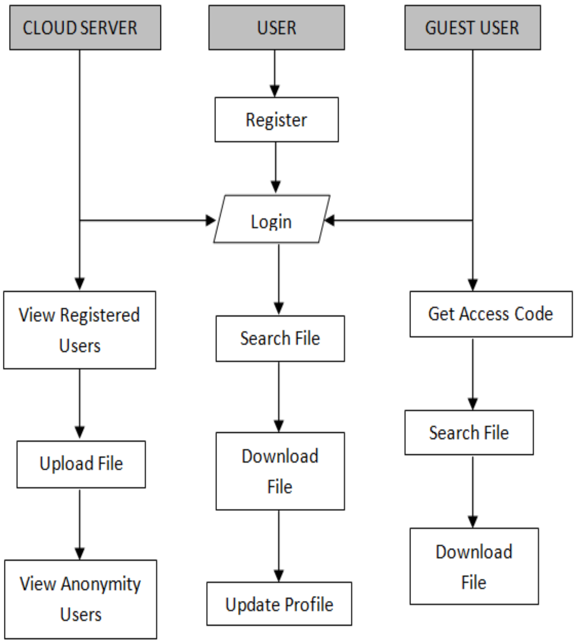
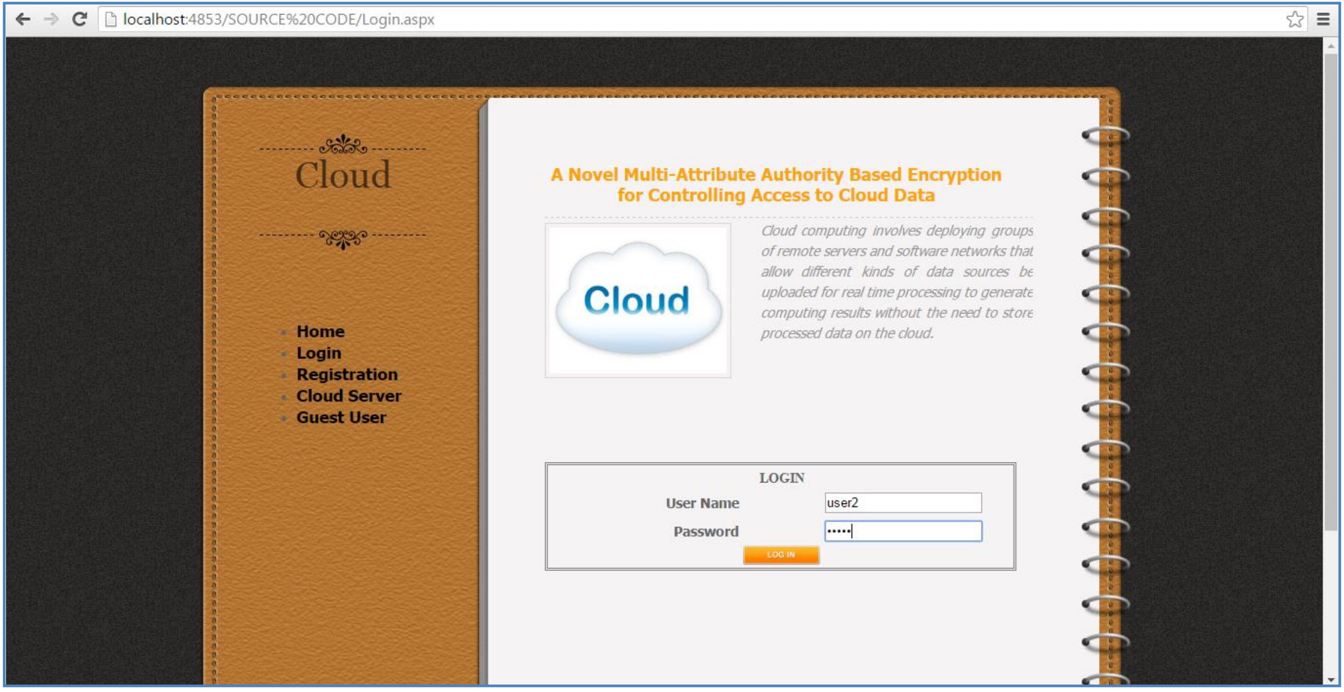


Figure 2 –The users of the implemented system and their activities

The activities of the users are implemented using Microsoft .NET platform. The main user interface of the prototype application is follows. The main UI reflects the home page having links to access functionalities of different users after due authentication.


localhost:4853/SOURCE%20CODE/Login.aspx

A Novel Multi-Attribute Authority Based Encryption for Controlling Access to Cloud Data

Cloud computing involves deploying groups of remote servers and software networks that allow different kinds of data sources be uploaded for real time processing to generate computing results without the need to store processed data on the cloud.

LOGIN

User Name: user2

Password: •••••

Figure 3 –Main UI facilitating all users to start their functionalities

As can be seen in Figure 3, it is evident that the functionalities of all users are provided thorough this application. As mentioned above the functionlaities of the sytem are implemented with web based interface. The implementation is carried out uing ASP.NET and C#. Particularly ASP.NET is used to design dynamic web pages while the functionality is implemented using C# programming language.

IV. EXPERIMENTAL RESULTS

This section provides experimental results with respect to the security and access control in terms of number of attributes and the number of attribute authorities. The experiments are made in terms of setup time and key generation time as part of the proposed mechanism.

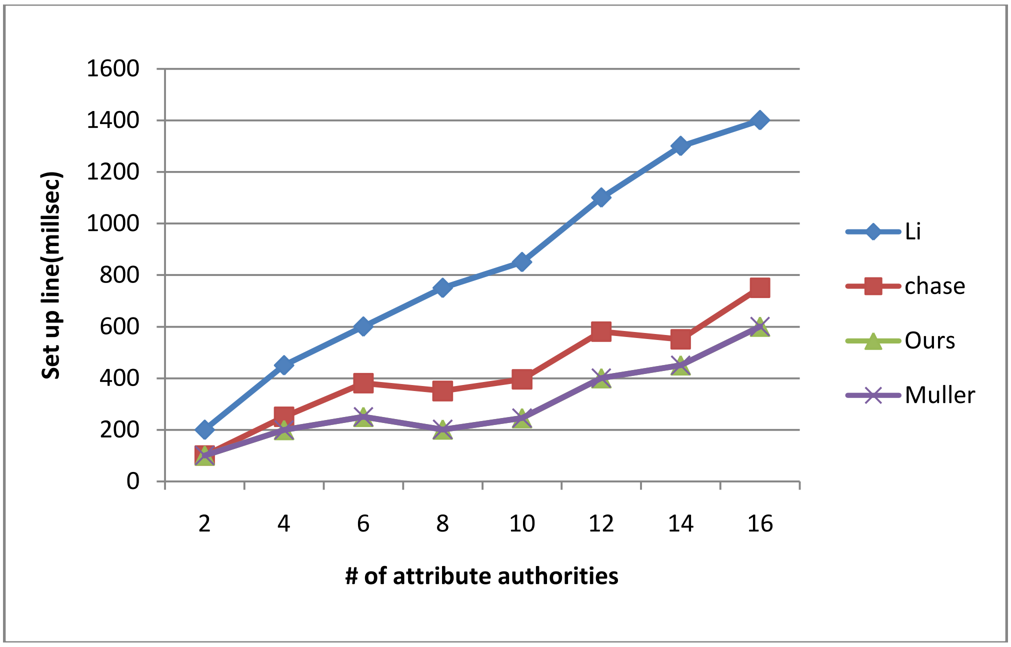


Figure 4 - # of attribute authorities and setup time

As can be seen in Figure 4, it is evident that the performance is presented for different approaches in terms of setup time with the presence of different number of attribute authorities. As the number of attributes is increased, it resulted in the increase of the key gen time for the proposed mechanism. However the proposed scheme took less time when compared with other schemes.

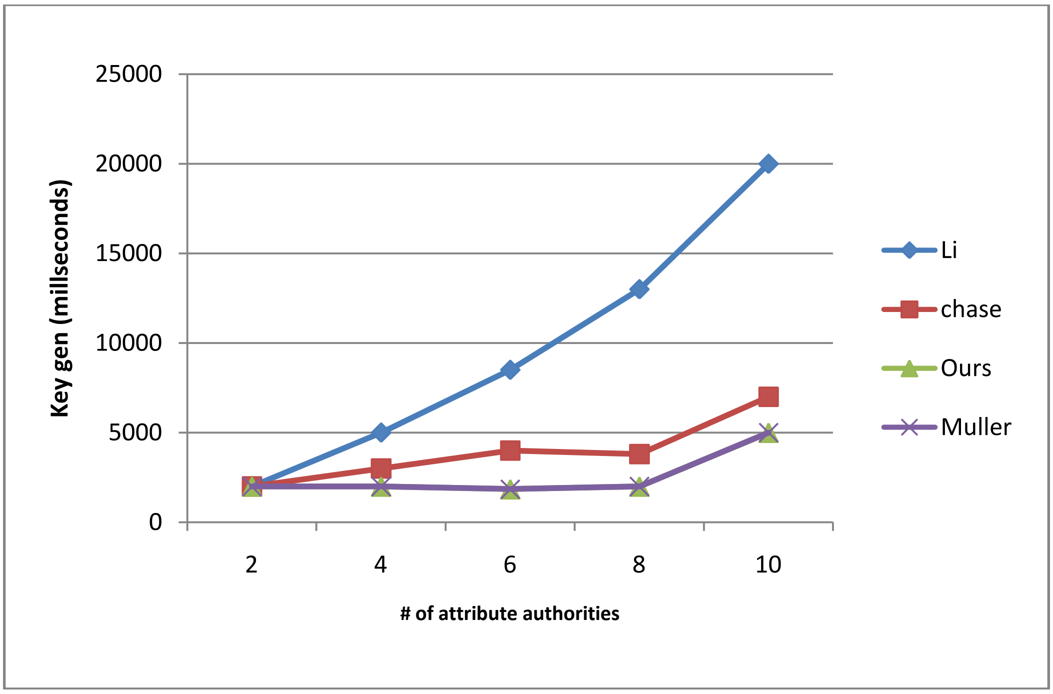


Figure 5 - # of attribute authorities vs. key gen time

As can be seen in Figure 5, it is evident that the performance is presented for different approaches in terms of key generation time with the presence of different number of attribute authorities. As the number of attributes is increased, it resulted in the increase of the key gen time for the proposed mechanism. However the proposed approach took less time when compared with other schemes.

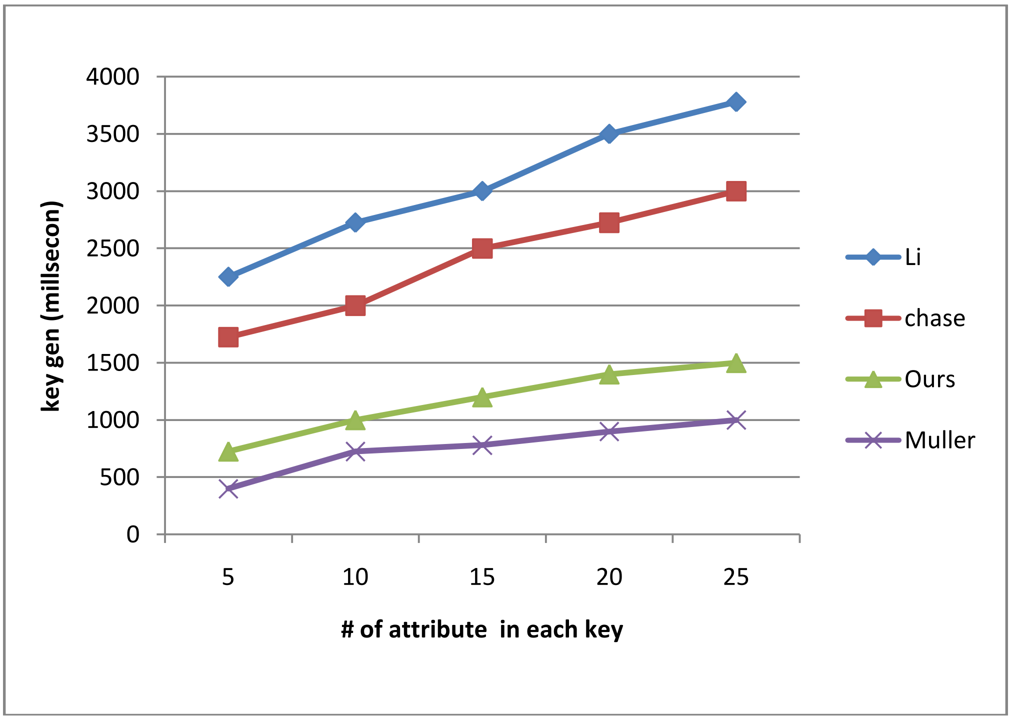


Figure 6–# of attribute in each key and key gen time

As can be seen in Figure 6, it is evident that the performance is presented for different approaches in terms of key generation time with the presence of different number of attributes. As the number of attributes is increased, it resulted in the increase of the key gen time for the proposed mechanism. However the proposed system showed comparable performance improvement over many other schemes.

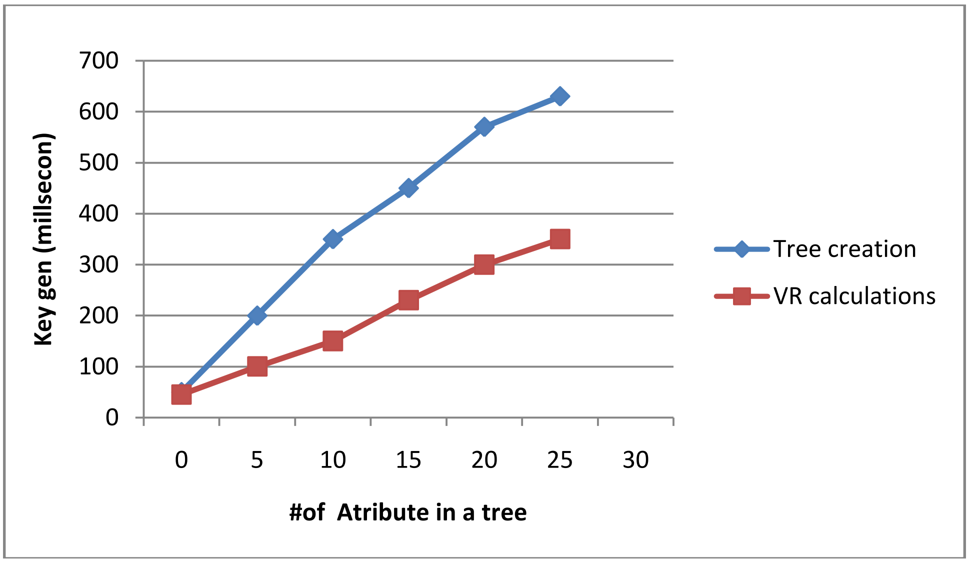


Figure 7 - # of attributes v. key gen time for tree creation and VR calculations

As can be seen in Figure 7, it is evident that the performance is presented for tree creation and VR calculations in terms of key generation time with the presence of different number of attributes. As the number of attributes is increased, it resulted in the increase of the key gen time for the proposed mechanism. However the VR calculations took less time when compared with tree creation time.

V. CONCLUSIONS AND FUTURE WORK

In this paper we studied the controlled access to cloud data. Cloud data control has been around for many years. Many schemes came into existence. Some of the schemes focus on auditing, provable data possession and proof of irretrievability. Some other schemes threw light into the access control on the cloud data. While giving privileges to accessing data attribute based encryption has achieved significant fine-grained control over the data. In this paper we propose a methodology that can allow controlled access to cloud data with multi-attribute authority based encryption. The multi-attribute based approach is used to make the scheme robust. Moreover the proposed approach is aimed at prevention of identity leakage and also achieves anonymity as well. We built a prototype application that demonstrates the proof of concept. The empirical results revealed that the proposed method improves access control significantly. This research can be extended further by using combining our approach with predicate based approach in order to provide more flexibility.

VI. REFERENCES

[1] M. Chase, “Multi-authority attribute based encryption,” in Theory of Cryptography. Berlin, Germany: Springer-Verlag, 2007, pp. 515–534.

[2] M. Chase and S. S. M. Chow, “Improving privacy and security in multi-authority attribute-based encryption,” in Proc. 16th CCS, 2009, pp. 121–130.

[3] H. Lin, Z. Cao, X. Liang, and J. Shao, “Secure threshold multi authority attribute based encryption without a central authority,” Inf. Sci., vol. 180, no. 13, pp. 2618–2632, 2010.

[4] V. Božovi´c, D. Socek, R. Steinwandt, and V. I. Villányi, “Multi-authority attribute-based encryption with honest-but-curious central authority,” Int. J. Comput. Math., vol. 89, no. 3, pp. 268–283, 2012.

[5] K. Yang, X. Jia, K. Ren, and B. Zhang, “DAC-MACS: Effective data access control for multi-authority cloud storage systems,” in Proc. IEEE INFOCOM, Apr. 2013, pp. 2895–2903. JUNG et al.: CONTROL CLOUD DATA ACCESS PRIVILEGE AND ANONYMITY 199

[6] A. Lewko and B. Waters, “Decentralizing attribute-based encryption,” in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2011, pp. 568–588.

[7] S. Müller, S. Katzenbeisser, and C. Eckert, “On multi-authority ciphertext-policy attribute-based encryption,” Bull. Korean Math. Soc., vol. 46, no. 4, pp. 803–819, 2009.

[8] J. Li, Q. Huang, X. Chen, S. S. Chow, D. S. Wong, and D. Xie, “Multiauthorityciphertext-policy attribute-based encryption with accountability,” in Proc. 6th ASIACCS, 2011, pp. 386–390.

[9] H. Ma, G. Zeng, Z. Wang, and J. Xu, “Fully secure multi-authority attribute-based traitor tracing,” J. Comput. Inf. Syst., vol. 9, no. 7, pp. 2793–2800, 2013.

[10] S. Hohenberger and B. Waters, “Attribute-based encryption with fast decryption,” in Public-Key Cryptography. Berlin, Germany: Springer-Verlag, 2013, pp. 162–179.

[11] Y. Zhang, X. Chen, J. Li, D. S. Wong, and H. Li, “Anonymous attributebased encryption supporting efficient decryption test,” in Proc. 8th ASIACCS, 2013, pp. 511–516.