International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

# COPY RIGHT

ELSEVIER SSRN



IJIEMR Transactions, online available on 30h Nov 2018. Link
:http://www.ijiemr.org/downloads.php?vol=Volume-07&issue=ISSUE-12

Title: **PRIVACY PROTECTION BASED ACCESS CONTROL TECHNIQUES IN CLOUD-BASED SERVICES**

Volume 07, Issue 12, Pages: 685–688.

Paper Authors

**TALARI CHAKKA CHANDRASEKHAR, B.RAMALINGA**
SIR C.V. RAMAN Institute of Technology & Science, AP, India

.
.


USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

# PRIVACY PROTECTION BASED ACCESS CONTROL TECHNIQUES IN CLOUD-BASED SERVICES

**TALARI CHAKKA CHANDRASEKHAR[1], B.RAMALINGA [2]**

[1]PG Scholar, Dept of CSE, SIR C.V. RAMAN Institute of Technology & Science, AP, India
[2] Assistant Professor, Dept of CSE, SIR C.V. RAMAN Institute of Technology & Science, AP, India

**ABSTRACT:** With the rapid development of the computer technology, cloud-based services have become a hot topic. Cloud based services not only provide users with convenience, but also bring many security issues. Therefore, the study of access control scheme to protect users' privacy in cloud environment is of great significance. In this paper, we present an access control system with privilege separation based on privacy protection (PS-ACS). In the PS-ACS scheme, we divide the users into personal domain (PSD) and public domain (PUD) logically. In the PSD, we set read and write access permissions for users respectively. The Key-Aggregate Encryption (KAE) is exploited to implement the read access permission which improves the access efficiency. A high degree of patient privacy is guaranteed simultaneously by exploiting an Improved Attribute-based Signature (IABS) which can determine the users' write access. For the users of PUD, a hierarchical attribute-based encryption (HABE) is applied to avoid the issues of single point of failure and complicated key distribution. Function and performance testing result shows that the PS-ACS scheme can achieve privacy protection in cloud based services.

## I. INTRODUCTION

With the rapid development of cloud computing, big data and public cloud services have been widely used. The user can store his data in the cloud service. Although cloud computing brings great convenience to enterprises and users, the cloud computing security has always been a major hazard. For users, it is necessary to take full advantage of cloud storage service, and also to ensure data privacy. Therefore, we need to develop an effective access control solution. Since the traditional access control strategy [1] cannot effectively solve the security problems that exist in data sharing. Data security issues brought by data sharing have seriously hindered the development of cloud computing, various solutions to achieve encryption and decryption of data sharing have been proposed.In 2007, Bethencourt et al. [2] first proposed the ciphertext policy attribute-based encryption (CP-ABE). However, this scheme does not consider the revocation of access permissions. In 2011, Hur et al. [3] put forward a fine-grained revocation scheme but it can easily cause key escrow issue. Lewko et al. [4] used multi authority ABE (MA-ABE) to solve key escrow issue. But the access policy is not flexible. Li et al [5] presented data sharing scheme based on systemic attribute encryption, which endows different users' different access rights. But it is not efficient from the complexity and efficiency. In 2014, Chen et al. [6] proposed

Key-Aggregate Encryption algorithm, effectively shortening the length of the ciphertext and the key, but only for the situation where the data owner knows the user's identity. These schemes above only focus on one aspect of the research, and do not have a strict uniform standards either. In this paper, we present a more systematic, flexible and efficient access control scheme. To this end, we make the following main contributions:

1. We propose a novel access control system called PSACS, which is privilege separation based on privacy protection. The system uses Key-Aggregate Encryption (KAE) scheme and Hierarchy Attribute-based Encryption (HABE) scheme to implement read access control scheme in the PSD and PUD respectively. The KAE scheme greatly improves access efficiency and the HABE scheme largely reduces the task of a single authority and protects the privacy of user data. 2. Compared with the MAH-ABE scheme which does not refer to the write access control, we exploit an Improved Attribute-based Signature (IABS) [7-9] scheme to enforce write access control in the PSD. In this way, the user can pass the cloud server's signature verification without disclosing the identity, and successfully modify the file. 3. We provide a thorough analysis of security and complexity of our proposed PS-ACS scheme. The functionality and simulation results provide data security in acceptable performance impact, and prove the feasibility of the scheme

## 2. EXISTING SYSTEM:

Data security issues brought by data sharing have seriously hindered the development of cloud computing, various solutions to achieve encryption and decryption of data sharing have been proposed. In 2007, Bethencourt et al. first proposed the ciphertext policy attribute-based encryption (CP-ABE).Li et al presented data sharing scheme based on systemic attribute encryption, which endows different users' different access rights. But it is not efficient from the complexity and efficiency.Chen et al. proposed Key-Aggregate Encryption algorithm, effectively shortening the length of the ciphertext and the key, but only for the situation where the data owner knows the user's identity.The traditional access control strategy cannot effectively solve the security problems that exist in data sharing. This scheme does not consider the revocation of access permissions.It can easily cause key escrow issue. These existing schemes only focus on one aspect of the research, and do not have a strict uniform standards either.

## 3. PROPOSED SYSTEM:

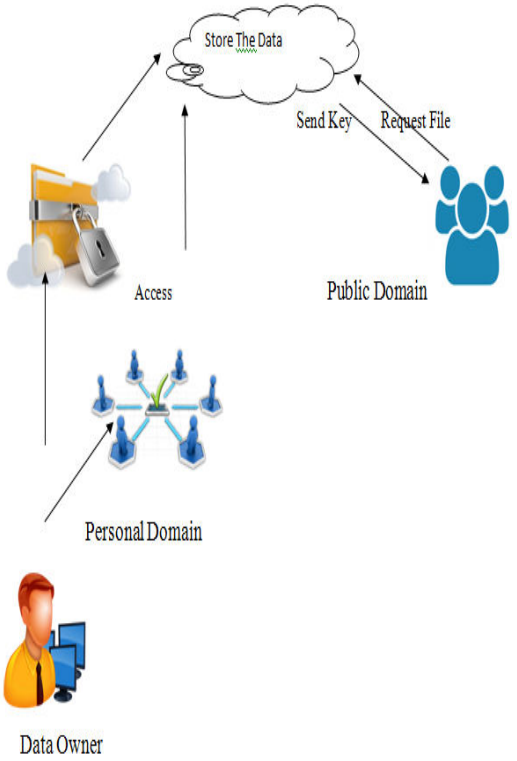
We propose a novel access control system called PSACS, which is privilege separation based on privacy protection. The system uses Key-Aggregate Encryption (KAE) scheme and Hierarchy Attribute-based Encryption (HABE) scheme to implement read access control scheme in the PSD and PUD respectively. The KAE scheme greatly improves access efficiency and the HABE scheme largely reduces the task of a single authority and protects the privacy of user data.Compared with the MAH-ABE scheme which does not refer to the write access control, we exploit an Improved Attribute-based Signature (IABS) scheme to enforce write access control in the PSD. In this way, the user can pass the cloud server's

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

signature verification without disclosing the identity, and successfully modify the file.

In this paper, we present a more systematic, flexible and efficient access control scheme.We provide a thorough analysis of security and complexity of our proposed PS-ACS scheme. The functionality and simulation results provide data security in acceptable performance impact, and prove the feasibility of the scheme. The evaluation results show the high efficiency of our scheme.

## 4. SYSTEM ARCHITECTURE:




## 5. IMPLEMENTATION:

### 1. Cloud Service Provider:

There are two parts of cloud service provider.

1. Data Storage Server
2. Data Service Manager

Data Storage server is responsible for storing confidential data files, and data service management is in charge of controlling external users' access to secret data and returning the corresponding ciphertext.DSS is in charge of controlling the accesses from outside users to the storing data and providing corresponding contents services. All the uploaded data will be stored in Storage service provider. DSS will be in charge of controlling the access to that data from outside users. It will be storing all the data and provides the data only to authorized users.The files which are uploaded by the Data Owner will be stored in the DSS

### 2. CA

In the actual cloud environment, CA manages multiple AA, and AA each manages attributes in their own field. The attributes owned by the user are issued by different authority.

### 3. Data Owner

Data Owner, based on the characteristics of users in public and personal domain to develop different access control strategy, encrypt uploaded files using the corresponding encryption method and then send to the cloud server.

### 4. Users

- **PSD:**

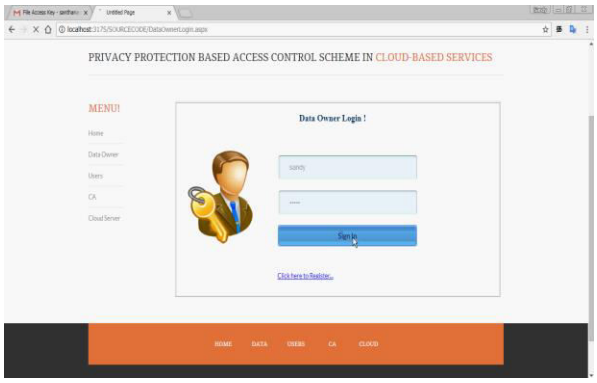
Personal domain (PSD), in which users have special privileges, such as family, personal assistant, close friends and partners. This domain has a small number of users and small scale attributes, and the data owner knows the user's identity, which is easy to manage.

- **PUD**

Public domain (PUD), which owns a huge number of users with unknown identity and a lot of attributes owned by the user.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

## 6. SCREEN SHOTS:




## 7. CONCLUSION

In this paper, we propose access control system (PS-ACS),which is privilege separation based on privacy protection.Through the analysis of cloud environment and thecharacteristics of the user, we divide the users into personaldomain (PSD) and public domain(PUD) logically. In the PSD,the KAE algorithm is applied to implement users read accesspermissions and greatly improved efficiency. The IABSscheme is employed to achieve the write permissions and theseparation of read and write permissions to protect the privacyof the user's identity. In the PUD, we use the HABE scheme toavoid the issues of single point of failure and to achieve datasharing. Furthermore, the paper analyzes the scheme fromsecurity and efficiency, and the simulation results are given. Bycomparing with the MAH-ABE scheme, the proposed schemeshows the feasibility and superiority to protect the privacy ofdata in cloud-based services.

## REFERENCES

[1] S. Yu, C. Wang, K. Ren, "Achieving secure, scalable, and fine-graineddata access control in cloud computing," Proc. IEEE INFOCOM, pp. 1-9,2010.

[2] J. Bethencourt, A. Sahai, B. Waters, "Ciphertext-policy attribute-basedencryption," Proc. Security and Privacy, pp. 321-334, 2007.

[3] J. Hur, D.K. Noh, "Attribute-based access control with efficientrevocation in data outsourcing systems," IEEE Transactions on Paralleland Distributed Systems, vol. 22, no. 7 pp. 1214-1221, 2011.

[4] A. Lewko, B. Waters, "Decentralizing attribute-Based encryption," Proc.Advances in Cryptology-EUROCRYPT, pp. 568-588, 2011.

[5] M. Li, S. Yu, Y. Zheng, "Scalable and secure sharing of personal healthrecords in cloud computing using attribute-Based Encryption," IEEETransactions on Parallel and Distributed System, vol. 24, no. 1, pp. 131-143, 2013.

[6] C.K. Chu, S.S.M. Chow, W.G. Tzeng, "Key-aggregate cryptosystem forscalable data sharing in cloud storage," IEEE Transactions on Paralleland Distributed Systems, vol. 25, no. 2, pp.468-477, 2014.

[7] J. Li, K. Kim, "Hidden attribute-based signatures without anonymityrevocation," Information Sciences, vol. 180, no. 9, pp. 1681-1689, 2010.

[8] H.K. Maji, M. Prabhakaran, M. Rosulek, "Attribute-Based Signatures,"Proc. Topics in Cryptology - CT-RSA, pp. 376-392, 2011.

[9] S. Kumar, S. Agrawal, S. Balaraman, "Attribute based signatures forbounded multi-level threshold circuits," Proc. Public Key Infrastructures,Services and Applications, pp. 141-154, 2011.