A Hybrid Access Control System for Easy Sharing of Organizational Data in Cloud Environment

Reetu Gupta*, Dr. Priyesh Kanungo** and Dr. Nirmal Dagdee***
*Asst. Professor, Department of CSE, S. D. Bansal College of Technology, Indore, India
**Professor & Head , Department of CSE/IT, MPSTME, NMIMS Shirpur, Maharashtra, India
***Director, S. D. Bansal College of Technology, Indore, India

Abstract: The development of cloud technology has enabled the present organizations to put their data 24X7 online. The requirement of easy sharing and exchange of data has now become prevalent. Organizations are outsourcing their shared data on cloud storage systems and that too in encrypted form for security reasons. There are a large number of users with different privileges and authorities for data access according to their roles and cadre in the organization. When the organization shares its data, the user can be from the closed domain (i.e. from the organization itself) or from the open domain (i.e. any user outside the organization). In this paper, we conceptualize a hybrid access control system, which allows the data sharing to closed as well as open domain users depending upon their attributes issued by multiple attribute authorities and the data owner. Such a system will enable easy sharing of useful data with large number of users outside the organization and also provide proper control on access to organization's private data.

Keywords: Cloud storage systems; Closed domain; Open domain; Access control system; Attribute authorities.

Introduction

The technological innovations and advancements of ICT are directing the individuals and organizations to put enormous digital data online. For a variety of reasons data sharing and exchange of data has become a need. Organizations are scattered around the globe and distributed environments like cloud systems can be used to enable data sharing capabilities amongst them. Higher productivity, less time compared to manual exchange of data and retrieval of updated data from anywhere, at any time is the benefits of online shared data [1]. E-health, e-government, e-business, online social networks etc. are major domains requiring data sharing among various entities. For example in e-healthcare environments, the healthcare providers store and share electronic medical records via cloud and hence remove the geographical dependence between multiple entities such as doctors, pharmacy labs, researchers, insurance companies, patients etc. [2]. This type of sharing of medical data allows the remote monitoring and diagnosis of a patient. Also in emergency situations, patient's health records can be accessed for suitable treatment. This example basically dictates 'Need to Share' principle. To benefit a large group of users, there is a need of promoting easy access to all the legitimate users. For example, a professor working in an organization wants to share his research data on cloud to benefit a large group of users. He wants to easily share his data not only to the people of the organization but also to the outside users. This example explains the principle of 'Easy Share'.

Whenever data is shared in distributed environment, it necessitates appropriate access control mechanisms to prevent unauthorized access [3, 7]. Attribute based access control approaches have been proposed for data access control in cloud storage systems [1, 2, 8, 9, 14], where data owner outsources his sharable data on cloud and defines his own access control policies over that. Data owner may or may not be aware of the user's identity to whom he wants to share the data. When data owner knows the users or users are registered to the organization, that type of environment is called closed environment. When he does not know the identity of the users but he recognizes them based on their characteristics, that type of system is called open system. In case of organizational data sharing, a large number of users work under a domain and generally form a hierarchy governed by various administrative levels. There may be users who work in collaboration with the organization or who are not known to the organization, but need the shared data. So there is a need of development of access control methodologies for data sharing, which can be applied in open environment as well as closed environment. Attribute Based Encryption (ABE)[10] is regarded as one of the most promising technologies, where data is kept on cloud in encrypted form and data owner can frame the policies based on various attributes. A user can decrypt the encrypted data only when its attributes satisfy the access policies.

To further illustrate the need of access control system for above mentioned hybrid scenario, we look into our example of research data sharing by a professor. The professor wants to share his data to a large group of users to benefit them. He shares the data by the name of the organization he is working with. The users of the data can be people of the organization itself or can be the outside users. He imposes some access control restrictions on the shared data. The data can be shared with following users:

a) All the PG scholars of the organization who have registered in the year before 2016.
b) The faculty members of the organization who are deputed in the R&D centre of the organization.
c) All the professors who are having IEEE membership.
Here several authorities are responsible for managing attributes and distributing keys to the users. The closed domain authorities are the registration office and the administrative section of the organization. The authorities in the open domain are any university distributing credential of professor and the IEEE membership office. An access control system is needed to implement varied kind of requirements for such a hybrid system. This access control system should provide fine grained, flexible and scalable access in multi-domain environment.
The remaining of this paper is organized as follows: we discussed the related work in Section II. In Section III, we discussed the problems in current system and the proposed system model. In Section IV, we discussed system functionality of the proposed system. In Section V, we have concluded the proposed work by summarizing its advantages.

Related Work

Data Sharing System
In today's world, every organization and individual are maintaining their data online. May it be business organization, healthcare organizations, research institutes or any commercial body; all are putting enormous data online every day. Connectivity of individual to web is making individual to share data for numerous reasons. Fast retrieval and low maintenance are the reason for choosing cloud storage space as data outsourcing media [1]. Data owners share their data for various reasons. Some reasons are higher productivity, flexibility, giving benefit to the user etc. For a strong data sharing system, some requirements are there:

1) Secure and Safe: The data owner wants that the outsourced data should be secure. Even the party managing the data called Cloud Service Provider (CSP) is also not considered as trusted. So the data is stored in encrypted form on the cloud.
2) Selective access: The data owner should be able to specify to whom he wants to share the data. No one other should able to access the data, even the Cloud Service Provider.
3) Scalable and flexible system: The data owner should maintain the criteria of access in such a manner that the eligible users must not be static. New users should be automatically added to the group of users, who are eligible for accessing the data.
4) Automatic access revocation: The users who fail to satisfy the criteria mentioned by data owner, their access rights must be automatically revoked.

Access Control Techniques
Access control is one of the aspects of secure data sharing. Access control restricts the access of data to eligible users who satisfy the access control policy mentioned by the data owner. Considerable work has been done in the field of access control on data storage systems [4, 6, 8, 9, 13, 14]. Access control mechanisms are mainly of three types: User Based Access Control (UBAC), Role Based Access Control (RBAC), and Attribute Based Access Control (ABAC). In UBAC, the access control list (ACL) contains the list of authorized users. When there are many users, it is not easy to maintain ACL. In RBAC [4], users are classified based on their individual roles. Data can be accessed by users who have matching roles, which are defined by the system. RBAC is usable, where users are registered to the system and they are mapped to some roles. The ABAC can be applied in open domain, in which users are identified by their attributes, and the data has attached access policy. Only users with valid set of attributes, satisfying the access policy, can access the data [6]. For instance, in e-healthcare system, medical records of a patient are accessed by only the treating doctor in the hospital but no others. Most of the work of access control in cloud [9, 13, 14, 16] makes use of a cryptographic primitive of ABAC known as Attribute Based Encryption (ABE). It is the technique to provide fine grained access control over encrypted data by using access policies and attributes. It was proposed by Sahai and Waters [10].
There are two main variants of ABE: Key-policy ABE (KP-ABE) and Ciphertext-policy ABE (CP-ABE). In the KP-ABE [12], a ciphertext is associated with a set of attributes, and a private key is associated with a monotonic access structure like a tree, which describes the user's identity (e.g. Doctor AND (Physician OR Orthopedist)). A user can decrypt the ciphertext if and only if the access tree in his private key is satisfied by the attributes in the ciphertext. When a re-encryption occurs, all of the users in the same system must have their private keys re-issued so as to gain access to the re-encrypted files. In the CP-ABE[10], ciphertexts are created with an access structure, which specifies the encryption policy, and private keys are generated according to users' attributes. A user can decrypt the ciphertext if and only if his attributes in the private key satisfy the access tree specified in the ciphertext. By doing so, the encrypter or data owner holds the ultimate authority about the encryption policy.
In all above approaches, single Trusted Authority (TA) was used, but a single TA cannot maintain the large number of users in an open distributed environment. For example, a medical student of a university needs to access patient and therapy data in

one hospital, where she is doing internship. To grant proper permissions to that student, hospital checks the organizational policies and finds that senior medical student from recognized university can access the insensitive patient and therapy data. In this case, hospital asks the student to provide the proof of being senior medical student. To handle the attributes from multiple domains, multiple attribute authorities are required. In multi-authority ABE, several authorities (coordinated by a central authority) distribute attributes and secret keys to users. A solution proposed in [5] allows data owner to specify a number of attributes issued by attribute authority to be presented by data user for decryption. In this scheme, a central authority still exists but with less functionality. It is fully trusted but handles no attributes. A number of multi-authority cloud storage systems have been
proposed in [9, 11, 15, 17].
Another challenging issue in multi-authority cloud storage systems is user-level and attribute level revocation to administer dynamic addition and deletion of users. When a user does not persist the hold of certain attributes, her attributes must be revoked to maintain the secure access right management. There are a number of works about revocation in literature [9, 14, 15].

Problem Statement

Need of hybrid system

Organizations share their data to various users for various reasons. E-healthcare organizations can share the data with other organization or individual for patient's treatment. Research institutes can share the data to promote the use of new findings and to further advance the research. Business organizations can share the data to their collaborators to provide fast service to the consumers. The organization's data owner can frame the access control policy by using the attributes of the closed domain users as well as the open domain users. This hybrid nature will expand the scope of data sharing. The closed domain users can be authenticated by the organization or data owner itself. The open domain users get their attributes for their characteristics from various domain authorities.

System Model

In this paper, we consider data sharing service which is hosted in the cloud environment. There are four entities which are involved in this system.

- Central Authority- The CA sets up the system and assigns unique aid to attribute authorities, uid to users and oid to data owner. The CA does not perform any attribute management.
- Multiple Attribute Authorities (AA) - AAs are responsible for key management tasks which include generating keys to users according to attribute possessed by them, publishing public parameters needed in various operations etc.
- Data Owner- This entity outsources the data with access control policies at cloud servers so as to enable access to eligible users only. This also authenticates the closed domain users by issuing them suitable attributes according to their role or identity in the organization.

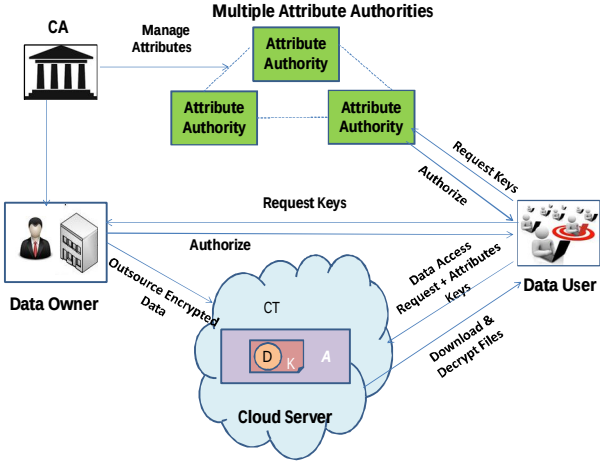

Figure 1: Architecture of hybrid data sharing system

- Cloud Server- This entity is responsible for storing the encrypted data and performing appropriate searches when required.

- Data user- This entity actually submits request to retrieve the file stored at cloud server. The users can be from closed domain or open domain. They are called closed domain users and open domain users. Closed domain users are identified and authenticated by data owner and open domain users are issued attributes from various attribute authorities from their domain.

Access Control Policy Structure

In our example, an organization's professor wants to share his research data to benefit a large group of users. He outsources the data in encrypted form to cloud storage system but with some access constraints. One ciphertext may be decrypted by several keys issued to different eligible users. The access control policy structure can be *And-Or* structure of attributes issued by data owner and attribute authorities. The access control policy can be made using combination of open domain attributes and closed domain attributes.

In figure 2 , we have shown policy structure of our example stated in Section 1.

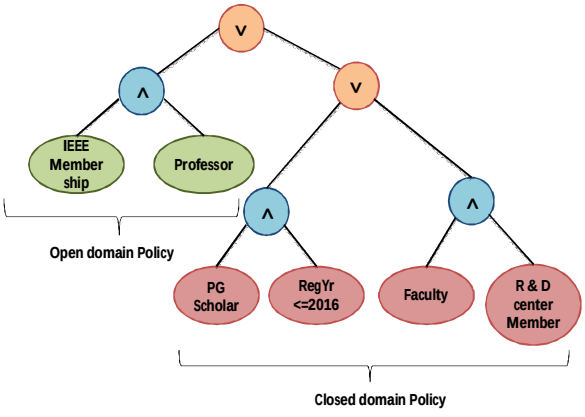

Figure 2: Example Access Control Policy

System Functionalities

In order to provide a hybrid access control system, we propose a scheme that is based on multi-authority ABE[5,11]. We combine it with the scheme where CP-ABE[10] is used by data owner to assign secret key to organization's user based on his attributes and identity. Here we assume that the CA is fully trusted party. The attribute authorities are also trusted. They never collude with any of the users. The data owner will also act as an attribute authority for closed domain.

Let U_o be the set of attributes managed by various attribute authorities and U_c be the set of attributes managed by data owner. The system consists of following steps:

CA Setup: CA runs the algorithm for set up of the system. It takes input parameter λ. The CA chooses two multiplicative groups G and G_T of prime order p. The generator of G is g and $e: G \times G \rightarrow G_T$ is a bilinear map. Let H :$\{0,1\}^* \rightarrow$G be a collision resistant hash function, which maps an attribute to a random group element. The global parameters of system are {p, g, G, G_T, e, H}.

CA also registers all the attribute authorities with unique ids aid and also assigns an unique oid to data owner/organization.

AA Setup: Each AA takes global parameters and the attribute set U_{aid} as input to setup algorithm. The AA chooses a random variable $x_{aid} \in Z_p^*$ and computes $e(g,g)^{x_{aid}}$. Then it chooses a random number $y_{aid_{i,j}} \in Z_p^*$ for each attribute and computes $g^{y_{aid_{i,j}}}$. The public key of AA is now $\{e(g,g)^{x_{aid}}, g^{y_{aid_{i,j}}}\}$ and secret key is $\{x_{aid}, y_{aid_{i,j}}\}$.

DO Setup: Data owner with identifier oid works same as one of the attribute authority. It does have a set of attributes U_c. The public key and secret key for data owner are generated as: $\{e(g,g)^{\alpha_{oid}}, g^{\beta_{oid_j}}\}$ and $\{\alpha_{oid}, \beta_{oid_j}\}$.

User Key Generation: Each user gets a global unique identifier uid from the CA. The user gets various attribute keys issued from AAs after authentication. The user's secret key is in the form $\{g^{x_{aid_i}}.H(uid)^{y_{aid_{i,j}}}\}$. The closed domain users get the secret keys issued from data owner oid in the form $\{g^{\alpha_{oid}}.H(uid)^{\beta_{oid_j}}\}$.

Data Encryption: The data owner encrypts the data m under the access policy $\mathbb{A}$. The inputs to the algorithm are the public keys of AA and the data owner. Let n_o be the number of attributes managed by AA and n_c be the number of attributes managed by data owner. The data owner randomly chooses $s \in Z_p^*$ and creates ciphertext $CT_{\mathbb{A}} = (\mathbb{A}, C_1, C_2, C_3)$, where

$C_1 = m \cdot (\prod_{t=1}^{no} e(g,g)^{x_{aid}\,t} \cdot \prod_{p=1}^{nc} e(g,g)^{\alpha_{oid}\,p})^s$

$C_2 = g^s$

$C_3=(\prod_{t=1}^{no} g^{y_{aid_t}} \cdot \prod_{p=1}^{nc} g^{\beta_{oid_p}})^s$

***Data Decryption*:** At the receiver side, the user runs the decryption algorithm with his unique uid, the attribute secret keys from either the closed or open domain to decrypt the data m. The secret keys are

$SK_{OD} = \prod_{t=1}^{no} SK_{aid}$

$SK_{CD} = \prod_{p=1}^{nc} SK_{oid}$

The data m can be decrypted by:

$$m=\frac{C1\cdot e(H(uid),C3)}{e(C2,SK_{OD})e(C2,SK_{CD})}$$

Conclusion

In this paper, we have conceptualized a hybrid access control system, which allows sharing of organizational data not only to the organizational users but also with the users who would be interested in that data in open domain. Access to the data is controlled based on the attributes issued by multiple attribute authorities as well as the data owner. Under the assumption that the CA and the AAs are fully trusted parties, we have developed the entire scheme that includes set-up of the CA and the AAs, key generation of users in closed and open domains, and the encryption and decryption algorithms. We conclude that the proposed ABE scheme will enable an organization to realize proper control of access to its data by the users internal to the organization and at the same time allow easy access to the useful data selectively to the users outside the organization based on the attributes they own.

References

[1] D. Thilakanathan, S. Chen, S. Nepal, and R. A. Calvo, "Secure data sharing in the cloud," in Security, Privacy and Trust in Cloud Systems. Springer Science + Business Media, 2013, pp. 45–72.

[2] R. Wu, G. J. Ahn and H. Hu, "Secure sharing of electronic health records in clouds," *8th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom)*, Pittsburgh, PA, 2012, pp. 711-718.

[3] A. Gholami and E. Laure, "Security and privacy of sensitive data in cloud computing: a survey of recent developments," Seventh International Conference on Network & Communications Security (NCS 2015), 2015, pp. 131–150.

[4] R. S. Sandhu, E. J. Coyne, H. L. Feinstein and C. E. Youman, "Role-based access control models," in *Computer*, vol. 29, no. 2, pp. 38-47, Feb 1996.

[5] M. Chase, "Multi-authority Attribute Based Encryption," in Proceedings of the 4th Conference on Theory of Cryptography, 2007, pp. 515–534.

[6] V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, K. Scarfone, Guide to attribute based access control (ABAC) definition and considerations, available online on http://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf.

[7] X. Dong, J. Yu, Y. Luo, Y. Chen, G. Xue, and M. Li, "Achieving an effective, scalable and privacy-preserving data sharing service in cloud computing," Comput. Secur., vol. 42, pp. 151–164, 2014.

[8] S. Ruj, M. Stojmenovic and A. Nayak, "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 384-394, Feb. 2014.

[9] K. Yang, X. Jia, K. Ren and B. Zhang, "DAC-MACS: Effective data access control for multi-authority cloud storage systems," *2013 Proceedings IEEE INFOCOM*, Turin, 2013, pp. 2895-2903.

[10] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," in Proceedings of the 2007 IEEE Symposium on Security and Privacy, 2007, pp. 321–334.

[11] M. Chase and S. S. M. Chow, "Improving Privacy and Security in Multi-authority Attribute-based Encryption," in Proceedings of the 16th ACM Conference on Computer and Communications Security, 2009, pp. 121–130.

[12] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based Encryption for Fine-grained Access Control of Encrypted Data," in Proceedings of the 13th ACM Conference on Computer and Communications Security, 2006, pp. 89–98.

[13] M. Decat, D. V. Landuyt, B. Lagaisse, and W. Joosen, "On the need for federated authorization in cross-organizational e-health platforms," in Proceedings of the International Conference on Health Informatics (BIOSTEC 2015) , pp. 540-545, 2015.

[14] S. Ruj, A. Nayak and I. Stojmenovic, "DACC: Distributed Access Control in Clouds," *2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications*, Changsha, 2011, pp. 91-98.

[15] K. Yang and X. Jia, "Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 7, pp. 1735-1744, July 2014.

[16] M. Li, S. Yu, Y. Zheng, K. Ren and W. Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 1, pp. 131-143, Jan. 2013.

[17] Li, Qi, et al. "Secure, efficient and revocable multi-Authority access control system in cloud storage." Computers & Security, vol. 59, 2016, pp. 45–59., doi:10.1016/j.cose.2016.02.002.