 doi:10.20944/preprints201607.0012.v1

Review

Analysis of Access Control Methods in Cloud Computing

Madhura Mulimani * and Rashmi Rachh

Department of Computer Science and Engineering, Visvesvaraya Technological University, Belgaum, India; rashmirachh@gmail.com

* Correspondence: madhurasm@gmail.com

Abstract: Cloud Computing is a promising and emerging technology that is rapidly being adopted by many IT companies due to a number of benefits that it provides, such as large storage space, low investment cost, virtualization, resource sharing, etc. Users are able to store a vast amount of data and information in the cloud and access it from anywhere, anytime on a pay-per-use basis. Since many users are able to share the data and the resources stored in the cloud, there arises a need to provide access to the data to only those users who are authorized to access it. This can be done through access control schemes which allow the authenticated and authorized users to access the data and deny access to unauthorized users. In this paper, a comprehensive review of all the existing access control schemes has been discussed along with analysis.

Keywords: role-based access control; attribute-based access control; attribute-based encryption

1. Introduction

Cloud computing is an emerging technology whose growth is on a rise and is being widely adopted by various IT conglomerate companies such as Google, IBM, Salesforce.com. It combines many technologies such as utility computing, grid computing, virtualization, etc. and leverages the advantages of these technologies and provides many benefits that include low investment cost, large storage, faster computations, virtualization, etc. Users store and share their data and information on the cloud and are able to access it from anywhere, anytime on a pay-per-use basis. Since the cloud service provider uses the multitenancy model [1], the outsourced data in it is accessible to multiple users. Thus, there is a high threat to the security of outsourced data in the cloud. Also, the cloud service providers and the data owners are most likely to be in different domains. Therefore, there is a great need for providing security against these untrusted service providers. Each of these technologies has its own security mechanisms to ensure security and privacy of the user's data. However, security mechanism of one technology cannot be applied to cloud computing as a whole. Protecting the data from the malicious users in the cloud is of utmost importance. Data can be secured and protected by ensuring that only the authenticated and authorized users access it. One of the solutions for providing security and privacy to the data is through the use of access control mechanisms. In this paper, we will provide an analysis of the various access control schemes that have been used earlier.

2. Related Work

This section of the paper lists the various access control methods proposed by many authors for providing security to the data along with the challenges and also, the solution proposed to overcome the challenges.

Kuhn et al. [2] have discussed about providing information security by assigning roles to the users and each role is assigned a collection of permissions. However, it has the disadvantages of difficulty in initial role structure setting, inflexibility as domains cannot change rapidly and no

support for dynamic attributes. If it does support dynamic attributes, it might lead to role expansion resulting in the creation of thousands of roles.

As a solution, attributes and rules in attribute based access control can be used that do not require separate roles for sets of subject attributes. Though it is easy to setup and specify access rules, it is difficult to determine a particular user's permissions as it needs a large set of rules to be executed in exactly the same order as does the system.

Jin Li et al. [3] have addressed the issue of illegal key sharing among the colluding users and defined and enforced access policies based on the attributes.

Ruj et al. [4] have proposed an access control scheme to preserve the privacy of the data providing a trustee's token only to the authenticated users, who will then be able to perform operations on the file (read, write, execute) in the cloud.

According to Goyal et al. [5], encryption of sensitive data stored in the cloud provides just the coarse-grained level access when in fact a fine-grained level access is required. Decryption is possible either when the user acts as an intermediary and decrypts all the entries for the party or gives the party its private decryption key. But, problems arise when setting the audit logs.

To resolve this issue, Sahai and Waters [5] have introduced the concept of Attribute Based Encryption (ABE). Goyal et al. [5] have developed a new cryptosystem, called the Key-Policy Attribute Based Encryption (KP-ABE) to provide a fine grained sharing of the encrypted data.

Ruj et al. [6] have emphasized that preservation of the security of data and privacy of users is of utmost importance. Maintaining an access control list of all the valid users in a dynamic cloud environment becomes difficult. Usage of encryption might lead to the data getting encrypted several times, which incurs huge storage costs.

To resolve this, they have provided a solution of using Attribute Based Encryption (ABE) to achieve access control in clouds. They have also proposed the new distributed access control mechanism, in which the owners decide which attributes users should possess and the users are provided with the decryption keys to access the records for which they have authorization rights.

3. Access Control Methods

Access control is a mechanism in which users may be granted or denied access to the data for the purpose of providing security and privacy to the data and protecting it from the unauthorized and malicious users.

Cloud stores a large amount of sensitive information of users that can be shared by other users of the cloud. Hence, to protect this sensitive information from the malicious users, access control mechanisms are used. Here, each user and each resource is assigned an identity, based on which they may either be granted or denied access to the data. These methods are called the identity-based access control methods. Examples of such methods are the Access Control List (ACL), User Based Access Control (UBAC) system, Role-Based Access Control (RBAC) mechanism and the latest one being, the Attribute-Based Access Control (ABAC) mechanism.

One of the major areas where access control is very extensively used is the medical health care, in which access to the sensitive information about the patients is granted only to the medical professionals, hospital staff, researchers and policy makers. Access control is also gaining lot of importance in online social networking.

Access Control List (ACL): In this mechanism, the names of all the registered users along with their access privileges to a particular system object are maintained in a list [7]. These system objects may be a file directory or an individual file. The access privileges are the ability to read, write and execute a file. The access control list is generally created by the system administrator or the object owner. So, any time a user requested the use of data or the resource from the cloud, the list was checked to verify whether the user was registered or not. If it was on the list, the user was granted the permission to access the data or the resource. Some of the operating systems that use the access control lists are the Windows NT/2000, UNIX-based systems, Novell's Netware. Each of these operating systems uses a different implementation for the access control list.

Disadvantage: It could be used only in a static environment with a limited number of users. The cloud computing environment being a large distributed system could not use the access control list method for access control, mainly because of the huge number of dynamic users, who joined and exited the environment in a dynamic manner, a large number of resources and also, the flexible constructions of the networks.

Mandatory Access Control (MAC): It is a system-wide policy decree who is allowed to have access. This mechanism relies on the system to control the access and therefore, an individual user cannot alter the access [8].

Disadvantage: MAC is not flexible, resulting in user frustration as they cannot dynamically change the underlying access policies. Also, it is difficult and expensive to implement.

Discretionary Access Control (DAC): This method centres on the concept of users having control over the system resources. The access control of the objects (e.g., the files and resources) in the system is left to the discretion of the object's owner who determines the object access privileges and thus, can specify which users are granted access to the resources and which users are restricted from accessing the resources [9].

Disadvantage: Since the users are allowed to control object access permissions, this mechanism makes the system susceptible to Trojan Horse and also, system maintenance and security principles verification are extremely difficult for the DAC systems.

Role Based Access Control (RBAC): In this method, security policies are maintained through granting of access rights to roles rather than to individual users. Here, the system assigned roles to all the users and each role was assigned a set of access privileges. Thus, the roles determined the user's access to the system on the basis of the job role. Roles were assigned to the user based on the concept of least privileges, i.e., the role is assigned with the least amount of permissions required for the job to be done [10]. If, at any time, the privileges for a role changed, then it was possible to add or delete the permissions. Hence, any time a user needed to access the cloud, he would be authenticated by his identity and would be allowed to access the data or the resources on the basis of the assigned privileges to the role assigned to him. This resulted in easier overall system maintenance and also, very effective in the verification of security policies.

Disadvantage: This method is suitable for a system with a limited number of users and roles and also, where the user's roles seldom change. However, when this method was extended across administrative domains, problems arose, as it was difficult to decide a role's privileges. Thus, this method cannot be used in the cloud computing environment due to its dynamic nature.

The identity-based access control methods, namely, ACL, MAC, DAC, and RBAC have sometimes been known as the authentication based control methods and require a tight coupling among domains. These methods provide coarse-grained access control [9] and are effective in unchangeable distributed system where there are only a set of users with a known set of services. Since the growth of the networks as well as the users is always on the rise, identity-based access control was found to lack the strength to support such a large development. Furthermore, IBAC was problematic for the distributed systems due to the difficulty in managing access to the system and the resources and also, due to the vulnerability to errors.

In order to provide fine-grained access control in a large, distributed and dynamic environment such as the cloud, the attribute-based access control (ABAC) was proposed.

Attribute-based Access Control (ABAC): In ABAC, users are assigned attributes and access is granted to those users with a certain set of attributes required to access the data or the resources. Users need to be able to prove that they possess the attributes that they claim to own. For this purpose, the access control method relies on authenticating the user at the site as well as at the time of a request. In a way, the ABAC is an extension of the RBAC with features such as delegation of attribute authority, decentralization of attributes and interference of attributes [9]. This makes the

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 July 2016 doi:10.20944/preprints201607.0012.v1

ABAC more suitable for the cloud environment that consists of an enormous number of dynamic users, massive amount of storage and also, dynamic and flexible constructions of networks.

ABAC consists of four entities, namely, the requestor, the resource, the service and the environment.

Requestor: one who sends requests to the cloud and invokes actions on the service.

Resource: One or more services act upon it

Service: software and hardware with a network-based interface and predefined set of operations.

Environment: contains information that might be useful for taking access decisions.

The access policies are specified based on the attributes of all these four entities. With this approach, the access control will be flexible enough to have multiple policies in multiple domains, which is, otherwise, not the case with the traditional access control models, such as, the ACLs, which have their own security policy. In addition, it also provides scalability essential to large scale distributed system.

Role-based access control (RBAC) and Attribute-based access control (ABAC) use the cryptographic primitive known as Attribute Based Encryption (ABE), which enables the data and the information to be encrypted under some access policy and then stored in the cloud [5]. Here, the users possess a set of attributes and are given the corresponding keys. Only those users having the matching set of attributes will be able to decrypt the data and the information stored in the cloud.

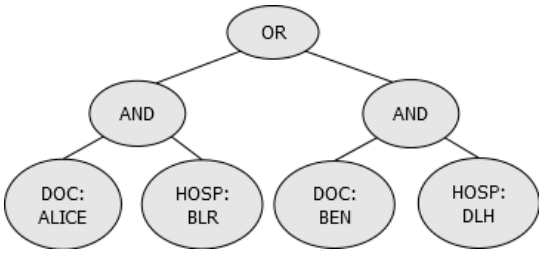

Fig. 1: Example of Access Tree Structure in ABAC

Fig. 1 illustrates an access policy in the form of an access tree in which the leaves represent the attributes and the internal nodes are the logical gates, such as, AND and OR. Suppose Alice is a doctor from the Bangalore hospital or Ben is a doctor from the Delhi hospital. Only they can access a patient's health record.

An access policy can also be represented in the form of a Boolean function as:

$$(DOC=ALICE \wedge HOSP=BLR) \vee (DOC=BEN \wedge HOSP=DLH)$$

The logical gates AND and OR are represented using the symbols $\wedge$ and $\vee$ repectively in the Boolean function. In general, the access policy is of the form :

$$(a1 \wedge a2 \vee a3) \wedge (a1 \vee a2 \vee a3)$$

where a1, a2 and a3 are the attributes and $\wedge$ and $\vee$ are the logical gates that aid in the formation of an access policy in attribute based access control. The access policy indicates that any user possessing the attributes that satisfy the access structure specified is authorized to access the data in the cloud. ABE comes in two flavours [5], Cipher-text Policy Attribute Based Encryption (CP-ABE) and Key Policy Attribute Based Encryption (KP-ABE).

Ciphertext Policy Attribute Based Encryption (CP-ABE): It is a promising cryptographic primitive for fine-grained access control of shared data and has several advantages such as security against ciphertext attacks, applicability to Key Policy Attribute Based Encryption (KP-ABE), size of the public key and the ciphertext being of the same size, etc. [10]. In CP-ABE, the attributes are associated the access structure and the secret key is associated with the ciphertext and it is for this reason, that this scheme is called the Ciphertext-Policy Attribute Based Encryption [5]. This scheme is similar to RBAC and can be used for providing access control in many applications such as medical system. In this scheme, the access policy is determined by the data owner [11]. Therefore, it

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 July 2016 doi:10.20944/preprints201607.0012.v1

is more suitable for access control applications that consist of four probabilistic polynomial time algorithm [12] as Setup, Encryption, Key Generation, and Decryption as shown in Fig. 2.

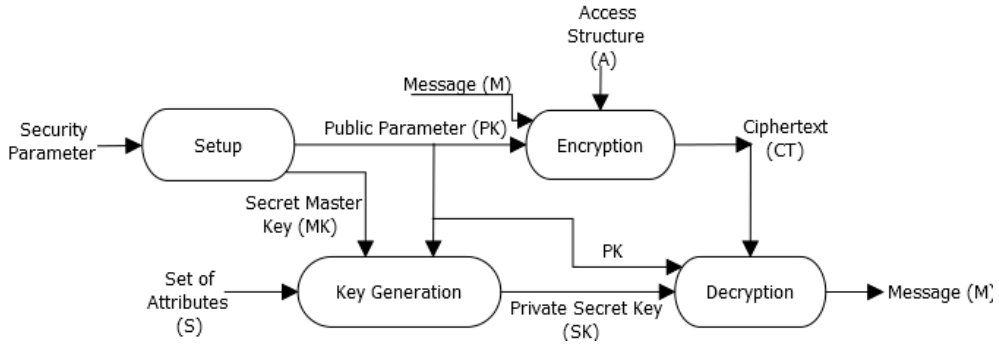

Fig. 2: Ciphertext Policy Attribute Based Encryption (CP-ABE)

Key Policy Attribute Based Encryption (KP-ABE): It is the sister concern of CP-ABE. In this scheme, each ciphertext is labeled by the encryptor with a set of attributes. Each private key is associated with an access structure, which specifies the type of ciphertext the key can decrypt. The KP-ABE is so named because the access structure is specified in the private key [5]. This scheme also consists of four algorithms, namely, Setup, Encryption, Key Generation, and Decryption as shown in Fig. 3. KP-ABE finds its application in secure forensic analysis and pay-per-view TV system. The KP-ABE provides fine-grained data access control and efficient operations such as file creation/deletion and new user grant [5].

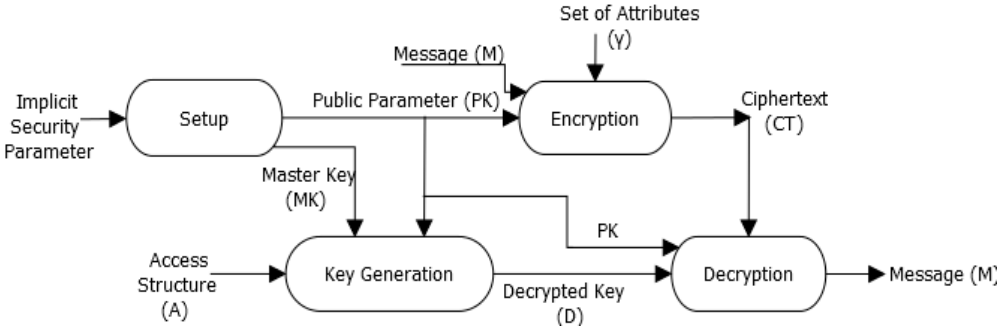

Fig. 3: Key Policy Attribute Based Encryption (KP-ABE)

4. Analysis

Table 1: Access Control Methods and their features.

Methods	Accountability	Disadvantages	Applications
Access Control List (ACL)	System Administrator	Limited number of users, Not scalable, Not flexible	Windows NT/2000, UNIX-based systems, Novell's Netware
Mandatory Access Control (MAC)	System	Limited number of users, Not flexible, Difficulty in implementation	Government and military applications or Mission critical data applications
Discretionary Access Control (DAC)	Data Owner	Susceptibility to Trojan Horse attacks, Difficulty in system maintenance and verification	Data-based Web applications
Role Based Access Control (RBAC)	Roles in the system	Limited number of users and roles, Non-scalability	Medical organizations, Academic institutions

Attribute Based Access Control (ABAC)	Attributes	Not much work has been done yet	Government organizations, Health Care Systems, Airlines, Insurance, Telecommunications Carriers

Table 1 lists the access control methods discussed earlier in the literature survey and provides a comprehensive analysis of them to show who is responsible for providing the access control in each of the methods. It also lists the disadvantages of the methods along with the applications.

5. Conclusion

In this paper, a comprehensive review of the various access control methods has been carried out, from which, we can state that access control plays a very important role in providing security to the data stored in the cloud. In addition, they need to be flexible as well as scalable across multiple domains. Attribute-based access control is the one that provides flexibility and scalability to the sensitive information in the cloud along with confidentiality and authentication of the users. Hence, it is the attribute based encryption (ABE) which has been found to be the most suitable access control mechanism in the cloud computing environment. Also, it is an emerging area of interest in the research field in cloud computing.

Conflicts of Interest: The authors declare no conflict of interest.

References

[1] RajaniKanth Aluvalu, Lakshmi Muddana, "A Survey on Access Control Models in Cloud Computing", Springer International Publishing Switzerland 2015 S.C. Satapathy et al. (eds.), Emerging ICT for Bridging the Future – Vol. 1, Advances in Intelligent Systems and Computing 337, DOI: 10.1007/978-3-319-13728-5_73 pp. 653

[2] D. Richard Kuhn, Edward J. Coyne, Timothy R. Weil, "Adding Attributes to Role-based Access Control", IEEE Computer Society, vol. 43, No. 6, pp. 79 – 81, (June 2010)

[3] Jin Li, Gansen Zhao, Xiaofeng Chen, Dongqing Xie, Chunming Rong, Wenjun Li, Lianzhang Tang, Yong Tang, "Fine-grained Data Access Control Systems with User Accountability in Cloud Computing", Proc. 2nd IEEE International Conference on Cloud Computing Technology and Science, IEEE Computer Society, (2010)

[4] Sushmita Ruj, Milos Stojmenovic, Amiya Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds", 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, 2012, pp. 556 – 563.

[5] Vipul Goyal, Omkant Pandey, Amit Sahai, Brent Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data", ACM CCS'06, Alexandria, Virginia, USA, (October 30 – November 3, 2006)

[6] Sushmita Ruj, Amiya Nayak and Ivan Stojmenovic, "DACC: Distributed Access Control in Clouds", International Joint Conference of IEEE TrustCom – 11, IEEE Computer Society, pp. 91 – 98, (2011)

[7] Abdul Raouf Khan, "Access Control in Cloud Computing Environment"

[8] J. H. Saltzer and M. D. Schroeder, "The Protection of Information in Computer Systems", Proceedings of the IEEE, Vol. 63, No. 9. (1975), pp. 1278-1308

[9] Natarajan Meghanathan, "Review of Access Control Models for Cloud Computing", David C. Wyld (Eds): ICCSEA, SPPR, CSIA, WimoA – 2013, pp. 77–85, 2013

[10] L. Arockiam, S. Monikandan & G. Parthasarathy, "Cloud Computing: A Survey", International Journal of Internet Computing (IJIC), Vol. 1, Issue-2, (2011)

[11] Xiaohui Liang, et al., "Ciphertext Policy Attribute Based Encryption with Efficient Revocation"

[12] Yong Cheng, et al., "Efficient Revocation in Ciphertext-Policy Attribute-based Encryption based Cryptographic Cloud Storage", Journal of Zhejiang University-SCIENCE C (Computers & Electronics) ISSN 1869-1951 (Print); ISSN 1869-196X (Online), Zhejiang University and Springer-Verlag Berlin Heidelberg 2013