FP-International Journal of Computer Science Research (IJCSR)
Volume 2, Issue 1, Pages 32-36, March 2015

Review on the Models of Access Control For Cloud Computing

Gagandeep Kaur
Department of Computer Science
Chandigarh University,
Gharuan Punjab, India
Geetkhangura10@gmail.com

Arvinder Kaur
Department of Computer Science
Chandigarh University,
Gharuan Punjab, India
Arvindercse.cgc@gmail.com

ABSTRACT
Cloud computing is an dominant paradigm which provides a number of resources and cost effective software services to their clients on demand such as Software as a Service, Platform as a Service, Infrastructure as a Service. However these services provides a lot of benefits for their clients, but still there is a need of data security against unauthorized access of data. So enhancement in security can be done by using access control mechanism for authorized access. So access control is an important aspect of cloud computing. This paper focus on various access control mechanisms used in the environment of cloud computing. This paper gives an insight into, how access control model enhances the data security. With this aim, this paper presents a review on the background of access control for security.

General Terms
Cloud Computing, Access Control Models.

Keywords
Cloud Computing, Access Control, Discretionary Access Control, Mandatory Access Control, Other Access Control Models,

1. INTRODUCTION

In modern era cloud computing is an important paradigm in industry and academia, which provide ubiquitous computing and offers a on-demand access. The definition of cloud computing provided by NIST [1]:Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Cloud computing has becoming the exciting prospected which is not only brought the opportunities but also create challenges to secure the data. Access control is the process that prevents the illegal access of data by granting the permissions to the data stored in cloud. System security relies on the access control.

There are the five essential features according to the cloud security alliance [2]: on-demand self service, resource pooling, broad network access, rapid elasticity and measured service. Service and deployment models provided by cloud computing environment as shown in fig 1:

In SaaS (Software as a Service) cloud provider provides the applications over the network which can be use by the cloud users, PaaS (Platform as a Service): In this provider provide the environment in which users create and deploy their applications, IaaS (Infrastructure as a Service) provides the storage, network capacity to their customers on demand.

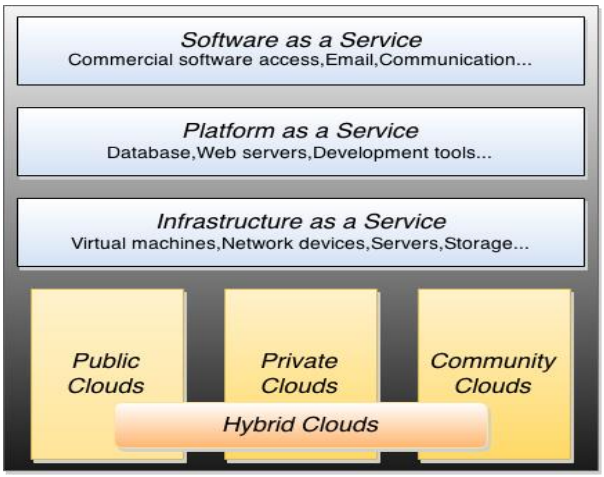

Fig 1. Cloud Computing Model [3].

Deployment model can be categorized as: Public cloud: provides a cloud environment that is publically accessible and referred to as off-premise cloud. Private cloud referred to as on-premise cloud which is owned and maintained by an organization. Community cloud is the composition of public and private cloud according to the target set of users. In hybrid cloud two or more clouds (private, public, and community) are involved that makes a hybrid cloud.

The rest of the paper is organized as follows. Section II discusses the access control models, section III discusses the related work. Finally discusses the conclusion of the paper.

2. ACCESS CONTROL MECHANISM

Access control is any mechanism or policy that grants and denies the access of any system and always identifies the illegal access performed by unauthorized users [4]. Identity based access control model are mostly used access control models [4].

Access control was initiate in 1960's to manage the shared information access. Access control is an important aspect of data security in which primary features such as confidentiality, integrity and availability is directly bind (tied). From the perspective view of access control cloud provider provide the following: i) control the access to the services based on the same policies and purchased customer service level. ii) Control the access of users' data from other users. iii) Control the access of both admin function based on privilege and consumer functions. iv) Update and maintain policies of access control. So access control ensures the legal access of data resource by limit the user privilege to access the data or file.

Cloud storage access control has becoming a challenging subject or issue in area of research and many scholars have done lots of researches on access control methods.

3. RELATED WORK

Traditional access control methods can be categorized as DAC (discretionary access control) [5], MAC (mandatory access control) [6], RBAC (role based access control) [7]. These models are based on centralized control model which are applied to the environment of static single domain.

DAC (discretionary access control) the object owner decides and set the permission to access the data for other users. DAC provides the access of data based on identity of user and authorization that define the permission (write/read/execute) for same group member and other group members. User has the total control over the programs. DAC contains the access attributes and rules. Access attribute provides the distinct authorization level and access rules describe the methods to prevent the sensitive data from unauthorized access. DAC deals with the i) system auditing event ii) permission inheritance iii) user-based authorization iv) admin privileges.

In MAC (mandatory access control) used by the multi level security system where admin decide the access permissions of the system not by any other subject.MAC model is based on level of security and number of subjects for accessing the objects. Traditional MAC security consideration is [8]: read down (current security level of user must control the object access being read), write up (current security level of user must control the object access being write). MAC follow the hierarchical approach to control the cloud data access which is depend on level of security and widely used in government and military applications.

A. Role Based Access Control Model

Role based access control RBAC model was first time develop by the American National Standardization Technical Committee in 90's. RBAC method defines the role concepts and reduce the defect of management that arises by assigning the permission for access directly to user in standard matrix model [9]. Roles in RBAC acts as a bridge between the permission and user access [10] which logically separate the permission and user access. The procedure of access control: mapping of permissions and role and role and user. R Sandhu et al of George proposed RBAC96 mechanism in 1996 [11] having systemic introduction. After that ARBAC97 (administrative RBAC) [12] was proposed by R Sandhu which describe the concepts of management roles and right also modified the centralized management of role assignment and definition.

M. B. Zhao et al. [13] proposed CCRBAC (cloud computing RBAC) model having three constraints environment, tense and limitation. To enhance the flexibility of access control mechanism attribute of subjects and objects were modified and also provided the subject role. Subject and object security level and attribute were also imported into this model.

Bertino et al [14] proposed the temporal-RBAC (TRBAC) model which considers the run-time role enables and disables according to user requests. In [15], the authors discussed that sometimes roles need to be enabled all the time. In the context of this they presented a generalized TRBAC (GTRBAC) model that support the activation of roles instead role enabling. When any user assumes a role this role known as role activation. GTRBAC proposed the enabling and disabling of constraints on the duration of activation assigned to any user. The greater number of role activation within a specific interval of time by a single user.

L. L. Wei [16] proposed a risk based dynamic multi domain access control model. They focused on the concepts of risk into access control. The level of risk and length visit both were linked together. Thereby they realized the fine grain access control.

Q. N. Shen et al. [17] presented a flexible access control mechanism for storage of cloud. This mechanism was RBAC model based and label of organization and grouping of many security attributes logically were combined. They ensure the strong isolation of data for the different enterprises and provide proper isolation for

internal data of enterprise. They realized the sharing of data between the enterprises by importing the concept of virtual organization at the same time and restrict the sharing of data between the competitive enterprises by importing the concept of interest conflict.

Y. P. Zhu and J. Zhang [18] proposed an extension of RBAC in SaaS (Software as a Service) in multitenant environment by considering the roles particularity. This model contains a tenement role. Another variant of access control models for cloud computing proposed based on the RBAC named as Attribute role based access control model (ARBAC) [19], where certain attributes and values are assigned to the data objects, a appropriate value for attributes need to be submitted by the user with a particular role and service provider provides the access to the objects after the completion of proper validation.

T. Ristenpart et al. [20] presented fine grain ARBAC key based mechanism where symmetric or private keys are assigned to user to encrypt or decrypt the attribute values that are defined for data objects and privacy of these objects need to be protected.

Distributed RBAC model was proposed in dynamic alliance environment named as DRBAC (Distributed Role based Access Control for Dynamic Coalition Environments) by Freudenthal et al. [21]. This model has three features which makes it different from RBAC model named as: numerical attributes, third part appointment and certificate reservation. DRBAC merge the advantages of trust management system and RBAC. The user of this model needed to manage the identity information because data and services were stored in the cloud of same type which made the identity authentication requests of cross-domain complex.

In [22], the author proposed the cloud-RBAC model which serves on platform of cloud computing. The features of RBAC and DRBAC inherited by this model and contain one role of admin. Each user had an different cloud-RBAC identity. The supplied resources without the information included in identity that was a certificate. Each role in this model had a information of domain and each domain had a specific admin role for the management of internal RBAC. Redundancy of data due to the superabundant identity information management has been reduced by Cloud-RBAC and also improve the performance of access control system.

B. Trust Based Access Control Model

Z. J. Tan [23] proposed the TBDAC (Trust Based Dynamic Access Control) model which is the combination of RBAC and trust management. The light weight certificate provided by the model by which user certify the validity of identity and the access rights via information of roles and trust rank in the certificate. The trust model based on vector mechanism [24], the literature present the entity of trust rank in two ways: recommended and direct trust. The attack to recommended and direct trust were resisted by the strategies given by this model.
In [25], discussed the idea of trust rank into model of access control and they analyzed the features of cloud computing security and proposed a trust based multi domain access control model based on the management of trust and RBAC model. This model built the relation between the user and platform of cloud computing by analyzing the action of users.

C. Access Control Model Based on Attribute-Based Encryption

Elisa Bertino, Mohamed Nabeel [26] proposed fine grained access control system based on attribute among users group each identified by attributes set. Attribute based systems needed by a collaborative application for the distribution and management of group keys. Monotonic access control policy over the attributes set supported by this system. This system reduce the requirement of establishing private communication channels which were expensive.

J. Bethencour [27] proposed a CP-ABE (ciphertext-policy attribute-based encryption) [28] and AB-ACCS (Attributes Based Access Control for Cloud Storage) access control method. The user was associated to attributes group and data was associated to condition of attributes group. The decryption of data could be done if the user satisfied the conditions of attribute. By controlling the ciphertext attributes of data the access authority could managed by the owner of data thus this model reduced the cost of management of access authority.

C. Hong et al. [29] presented ciphertext access control method based on the algorithm of secret sharing scheme. This method moved the secret key re-encryption [30] caused by access control strategy change, thereby this mechanism reduced the re-encryption cost of data owner and also reduced the complexity of authority management.

Jingxin K. W. et al [31], presented a model for data security and authentication for hybrid cloud. They discussed different techniques to protect the data of users from illegal access. This security model contains authentication interface, multilevel virtualization and single encryption. The main focus of this idea was authentication which is based on CA and PKI model.

In [32], the author proposed a distributed access control model based on attributes by using the KP-ABE (Key policy attribute based encryption) characteristics [33] and CP-ABE. The author analyzed that the model could satisfy the requirement of users of constituting multiple access control strategies. The architecture of authorization of unified authorization party adopted in

this model and certified the identity of users by using PKI (Public key infrastructure) to provide the roles public and private key certificate.
S. Yu et al. [34] presented the strategies of access control on the theoretical basis of KP-ABE, PRE (Proxy Re-encryption) and LRE (Lazy Re-encryption) [35,36]. This method used the KP-ABE to manage the information of secret keys that were interchangeable between the owner and user of data. The method of LRE utilized to reduce the cloud computational pressure.

4. CONCLUSION

In cloud computing access control is major area of research to enhance the users data security which is stored in cloud computing environment. Various access control methods are discussed that are widely used previously and presently. To ensure security of users data DAC, MAC and RBAC provide the access control methods. The traditional access control model is DAC, MAC and RBAC and some other related access control models are discussed. The main focus of this paper is to understand the different access control methods in cloud computing. In access control models always conflicts exists between the resource consumption and security. For the higher security in access control with less computation cost and communication and storage will be the main focus for researcher for ongoing exploration.

5. REFERENCES

[1] P. Mell and T. Grance, ”Draft nist working definition of cloud computing” ,vol.15, Aug 2009.

[2] Cloud Security Alliance. (2009, Apr. 1). Security Guidance for Critical Areas of Focus in Cloud Computing [R/OL]. http://www.cloudsecurityalliance.org/guidance/csaguide.v1.0.pdf.Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[3] Jansen W. and Grance T. (2011). Guidelines on security and privacy in public cloud computing. NIST Special Publication 800-144.

[4] Yingjie Xia, Li Kuang and Mingzhe Zhu “A Hierarchical Access Control Scheme in Cloud using HHECC” Information Technology Journal 9 (8): 1598-1606 , 2010.

[5] R. Sandhu and Q. Munawer. (1998). How to do Discretionary Access Control Using Roles[C]// ACM. Proceedings of the 1998 3rd ACM Workshop on Role-Based Access Control, Fairfax, VA, 1998. NYUSA: ACM, 47-54.

[6] J. H. Saltzer and M. D. (1975). Schroeder. “ The Protection of Information in Computer Systems.” Proceedings of the IEEE, 63(9), pp. 1278-1308.

[7] M. Z. Chen. (2007). “Research on The Application of Role-based Access Control Model.” Journal of Engineering in Tianjin Normal University, 17(2), pp. 35-37.

[8] Ravi S. Sandhu and Pierangela Samarati “Access Control: Principles and Practice” IEEE Communications Magazine, September 1994.

[9] W. P. Zhou and S. N. Lu. (2007). Research on RBAC Access Control. computer security, 2, pp.11-16.

[10] J. B. D. JOSHI, E. BERTINO, U. LATIF, et al. (2005). A Generalized Temporal Role-Based Access Control Model. IEEE Trans on Knowledge and Data Engineering, 17(1), pp. 4-23.

[11] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, et al. (1996). Role-Based Access Control Models. IEEE Computer, 29(2), pp. 38-47.

[12] R. S. Sandhu, V. Bhamidipati and Q. Munawer. (1999). The ARBAC97 model for role-based administration of roles. ACM Transaction on Information and System Security, 1, pp. 105-135.

[13] M. B. Zhao and Z. Q. Yao. (2011). RBAC-based Access Control Model in Cloud Computing. Computer Application, 32(S2), pp. 267-270.

[14] D. Nurmi, R. Wolski, C. Grzegorczyk, S. Soman, L. Youseff and D. Zagorodnov, “The Eucalyptus Open-Source Cloud-Computing System,” Proceedings of the International Symposium on Cluster Computing and the Grid, pp. 124-131, 2009.

[15] B. Shafiq, J. B. D. Joshi, E. Bertino and A. Ghafoor, “Secure Interoperation in a Multi-domain Environment Employing RBAC Policies,” IEEE Transactions on Knowledge and Data Engineering, vol. 17, no. 11, pp. 1557-1577, Nov. 2005.

[16] L. L. Wei and J. B. Yuan. (2012). Research on the Risks in crossdomain RBAC model under cloud computing environment. Mini-Micro Computer Systems, 33(12), pp. 2721-2723.

[17] Q. N. Shen, Y. H. Yang, X. Yu, et al. (2011). A multi-tenant cloud storage oriented Access Control Strategy. Mini-Micro Computer Systems, 32(11), pp. 2223-2229.M. B. Zhao and Z. Q. Yao. (2011). RBAC-based Access Control Model in Cloud Computing. Computer Application, 32(S2), pp. 267-270.

[18] Y. P. Zhu and J. Zhang. (2011). Research on Access Control in SaaS.Computer Engineering and Application, 47(24), pp. 12-26.

[19] K. Yang and X. Jia, “Attribute-based Access Control for Multi-Authority Systems in Cloud Storage,” Proceedings of the 32nd IEEE International Conference on Distributed Computing Systems, pp. 536-545, 2012.

[20] T. Ristenpart, E. Tromer, H. Shacham and S. Savage, “Hey, You, Get off my Cloud: Exploring Information Leakage in Third-Party Compute Clouds,” Proceedings of the 16th ACM Conference on Computer and Communications Security, pp. 199-212, 2009.

[21] Eric Freudenthal, Tracy Pesin, Lawrence Port, et al. (2012, July). dRBAC: distributed role-based access control for dynamic coalition environments. In: Proceedings of the 22nd International Conference on Distributed Computing Systems(ICDCS’02), 411-434.

[22] W. L. Deng. (2012). The Application of Access Control System in the Cloud Computing Platform. Bulletin of Science and Technology, 28(12), pp. 214-216.

[23] . J. Tan, “Research on Trust-based Access Control Model in the Cloud Computing Environment,” Ph.D. dissertation, Hunan University, 2011.Q. N. Shen, Y. H. Yang, X. Yu, et al. (2011). A multi-tenant cloud storage oriented Access Control Strategy. Mini-Micro Computer Systems, 32(11), pp. 2223-2229.

[24] H. Jameel, L. X. Hung, U. Kalim, et al. (2005). A Trust Model for Ubiquitous Systems based on Vectors of Trust Values. In: Proc of 7th IEEE International Symposium on Multimedia. Washington: IEEE Computer Society Press, 674-679.

[25] Y. Y. Bie and G. Y. Lin. (2012). Trust-based Multi-domain Access Control Strategy in Cloud Computing. Information Security and Technology, 3(10), pp. 39-52.

[26] M. Nabeel and E. Bertino, "Towards attribute based group key management," in Proceedings of the 18th ACM conference on Computer and communications security, Chicago, Illinois, USA, 2011.

[27] J. Bethencourt, A. Sahai and B. Waters. (2007). Ciphertext-policy attribute-based encryption[C]//Proc of the 2007 IEEE Symp on Security and Privacy. Piscataway, NJ: IEEE, pp. 321-334.

[28] C. Hong, M. Zhang and D. G. Feng. (2010). AB-ACCS: A Ciphertext Access Control Method for Cloud Storage. Computer Research and Development, 47(Suppl.), pp. 259-265.

[29] C. Hong, M. Zhang and D. G. Feng. (2011). A Cloud Storage Oriented Efficient Dynamic Ciphertext Access Control Method. Journal on Communications, 32(7), pp. 125-132.

[30] M. Blaze, G. Bleumer and M. Sreauss. (1998). Divertible Protocols and Atomic Proxy Cryptography. Advances in Cryptology Springer-Verlag, 127-144.

[31] Jingxin K. Wang, XinpeiJia, Data Security and Authentication in Hybrid Cloud Computing Model, IEEE 2012, Page 117-120.

[32] Z. L. Zhang and C. F. Wang. (2012). Attribute-based Distributed Access Control Scheme in the Cloud. Computer Engineering, 38(11), pp. 1-4.

[33] V. Goyal, O. Pandey, A. Sahai, et al. (2006). Attribute-based encryption for fine-grained access control of encrypted data. Proceedings of the 13th ACM Conference on Computer and Communications Security. New York, USA.

[34] S. Yu, C. Wang, K. Ren, et al. (2010). Achieving secure, scalable, and fine-grained data access control in cloud computing. In Proceedings of IEEE infocom, pp. 534-542.

[35] M. Kallahalla, E. Riedel, et al. (2003). Plutus: Scalable secure file sharing on untrusted storage. In Proceedings of the 2nd USENIX Conference on File and Storage Technologies. Berkeley: USENIX Association Press, pp. 29-42.

[36] K. Fu. Group sharing and random access in cryptographic storage file systems. Massachusetts: MIT, 1999.