 JCS, vol.1, no.1, pp.43-50, 2019

Review of Access Control Model

Zhengtao Liu[1, *], Wen Gu[1] and Jinyue Xia[2]

Abstract: Access control is one of the core problems in data management system. In this paper, the system requirements were described in three aspects: the traditional access control model, the access control model in the Internet era and the access control model in the cloud computing environment. Meanwhile, the corresponding major models were listed and their characteristics and problems were analyzed. Finally, the development trend of the corresponding model was proposed.

Keywords: Access control, RBAC, ABAC, cloud computing.

1 Introduction

Access control refers to that subject regulates access capacity of objects through the authorization policy. It is to prevent unauthorized use of system resources by illegal users and protect legal use of system resources. Authorization policy is one of the core problems in studies on access control. Model judges the access capability of one subject to an object by the authorization strategy.

2 Traditional access control model

Discretionary access control (DAC) [Sandhu, Samarati (1994); LaPadula, Bell and LaPadula (1973)]. DAC is a kind of access control method that offers restricted access of subject by identity and the affiliated group of the subject. DAC allows subject with access rights to transfer the access rights to other subjects. The DAC model allows users to adjust the access strategy conveniently. However, it still has some disadvantages, such as security hole of Trojan horse.

Mandatory access control (MAC) [LaPadula, Bell and LaPadula (1973); Wang and Ding (2003)]. MAC is a mandatory access control of the system uniformly to all objects constructed by users. It decides what kind of users can access to the certain type of objects according to the system design rules. MAC is a multi-level security (MLS) mechanism or known as the multi-level security model. MAC was applied by American government and military part and it was safer and stricter than DAC. This mode includes Lattice model, Bell-LaPadula model and Biba model. Among them, the Bell-LaPadula model is applied more widely than the rest two models. It is mainly used in military development systems. The model solves the security issues of Trojan horse in the DAC model successfully. As a multi-level security model based on the Bell-LaPadula model,

[1] School of Computer Science and Engineering, Sanjiang University, Nanjing, 210012, China.

[2] International Business Machines Corporation (IBM), New York, USA.

[*] Corresponding Author: Zhengtao Liu. Email: lzt_jh_cn@163.com.

Chinese wall [Brewer and Nash (1989)] can offer automatic control and mandatory control, so it is extensively used in business field to prevent benefit conflict of competitive enterprises caused by information flow. In a strong MAC, the establishers of objects also have to gain authorization to access to the object. This determines the poor flexibility of the authorization mechanism.

Role-based access control (RBAC) [Sandhu, Coyne, Feinstein et al. (1996)]. RBAC model introduces the concept of role and sets the role of users, which simplifies the management problem in the authorization process. It overcomes the problem that automatic access control distributes the access rights to subjects. In the RBAC model, firstly, the authorization is associated with roles and then the role of users is defined. The user's authorization is obtained through the roles of users, and resources (objects) are accessed. Sandhu et al. [Sandhu, Coyne, Feinstein et al. (1996)] proposed the formalized expression of RBAC model in 1996, which was called the RBAC96 model.

Based on the RBAC96 model, researchers proposed the ARBAC97 model [Sandhu, Bhamidipati and Munawer (1999)] and ANSI RBAC model [Ferraiolo, Sandhu and Gavrila (2001)]. Currently, these models have been widely used in different application systems.

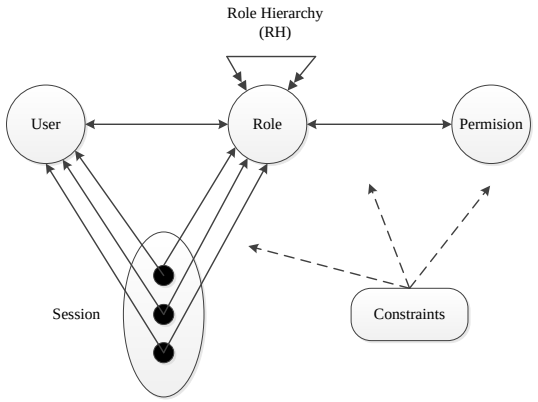

Figure 1: RBAC96 model

3 Access control models of the internet era

Internet has characteristics of high open, heterogeneousness and dynamics, which is inappropriate to use the traditional MAC model, DAC model and RBAC model based on identities.

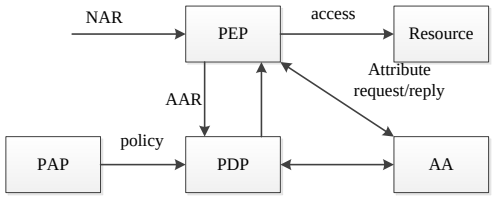

Figure 2: ABAC model

Attribute-based access model (ABAC). ABAC model [Sandhu (2015); Hu, Kuhn and Ferraiolo (2015); Yang and Jia (2014)] solves the problems of traditional control model in large-scaled dynamic increase of users and excessive coarse granularity of access control model. It adapts to the open and dynamic features of Internet, and shows remarkable expansibility and flexibility. Researches on ABAC model mainly focus on solid attributes of ABAC, description and semantic interoperability of ABAC strategies, synthesis and conflict offset of ABAC strategies, which formalized model of ABAC model, interaction between ABAC attribute and strategic security, and so on.

Usage control (UCON) model [Park and Sandhu (2004); Sandhu and Park (2003); Zhang, Parisi-Presicce, Sandhu et. al. (2005)]. Park et al. proposed the usage control (UCON) model which was called the next generation of access control model with respect to the demands for security and privacy in modern application platform and information system. The UCON model covers three basic elements (e.g., subject, object and permission) and three process elements (authorized rules, conditions and obligations). Which covers the conditions and obligations that the subject has to be fulfilled during the model authorization. This model contains not only four typical access control models (e.g., MAC mode, DAC model, RBAC model ad ABAC model), but also the contents related with digital rights management and trust management as well. UCON model provides a new method for researchers to study the next generation of access control. However, it still has some disadvantages. For example, the UCON model is difficult to be used and realized. Moreover, the theoretical UCON model has to be further explicated and formalized.

Semantic access control model. In semantic related access control mode, Sacco et al. [Sacco and Passant (2011)] proposed a lightweight vocabulary set by using the Web access control vocabularies, and defined the RDF data privacy protection method of fine granularity according to category and attribute of vocabularies. A method to describe the access control strategy by using the RDF original data was proposed in Hollenbach et al. [Hollenbach, Presbrey and Berners-Lee (2009)], which the RDF document is stored in the Web server, aiming to protect the social semantics Web network. An attribute-based on authorization framework was put forward in Costabello et al. [Costabello, Villata and Rocha (2013)] which could be transformed to access control of SPARQL inquiry results operated by HTTP on RDF. Kayes et al. [Kayes, Han and Colman (2012)] proposed an access control framework based on context perception which strategy combines the system context in this framework, which allows one user sends a request of resource access, and the access control can make decisions according to current relevant status. Costabello et al. [Costabello, Villata and Delaforge (2012)] proposed the access control model for data web based on context perception. This model can define the fine granular access control strategy by the lightweight ontology to protect RDF DATA. A fine granular context perception access model for Linked data was proposed by Liu et al. [Liu and Wang (2016)]. Based on the semantic network technology, this model allows the association data managers or developers to define the data access conditions. Moreover, this model extended the XACML by considering semantics of association data. In this model, the definition strategy of XACML rule was applied and semantic relation and reasoning problems were expressed by the SWRL rules. Managers or publishers of association data can use the facts deduced by the reasoning machine in defining the XACML rules. Access strategies can be reproduced in FCAC, thus reducing the number

of access strategies for definition.

Table 1: Contrast analysis of semantic access control models

Related Work	CRUD	Context awareness	Semantic Rule Reason	Conflicts verification	Granularity
Sacco and Passant (2011)	Read/Write	N/A	N/A	N/A	RDF document
Hollenbach, Presbrey and Berners-Lee (2009)	Read/Write/Control	N/A	N/A	N/A	RDF document
Costabello, Villata and Rocha (2013)	CRUD	N/A	N/A	N/A	Resources
Kayes, Han and Colman (2012)	Read/Write	YES	N/A	N/A	Resources
Costabello, Villata and Delaforge (2012)	CRUD	YES	N/A	N/A	Name Graphs
Liu and Wang (2016)	User define	YES	YES	YES	Name Graphs

4 Access control model in the cloud computing environment

Cloud computing is a new business computing mode of sharing fundamental resources which is developed to adapt to the rapid developments of computing, storage, communication and network technologies. It has the characteristic of service for demands, network access at any moment, sharing of the resource pool, elastic configuration and measurable services. In cloud computing, users lose control over the data and computing in the cloud server. It is hard to be sure whether data are protected and computing task is implemented accurately. Therefore, the corresponding safety mechanism has to be designed to protect confidentiality, integrity and applicability of user data. In addition, the implementation of the cloud server should be reliable or the position of problem should be recognized quickly upon the attack through accountability. In public cloud, many users can rent resources from the cloud and lend infrastructures to other users. Hence, these users will certainly share communication or data. A safety access control mechanism needs to be designed among users in the cloud [Hao, Lakshman and Mukherjee (2010); Oberheide, Cooke and Jahanian (2008)].

Existing access control models oriented to cloud computing environment mainly focus on the improvement and expansion of traditional models based on role and attempt to

expand the traditional role access control model to adapt to the cloud computing environment. The cloud computing environment was analyzed in Zhao et al. [Zhao and Yao (2012)], and an access control model based on the cloud computing was proposed which disclosed the virtualization and elasticity. Researches on key technologies of access control oriented to cloud computing environment mainly introduce the dynamic changing mechanism and subjective and objective safety into the access control strategy, thus improving safety, reliability and flexibility of access control. The UCON model was used to solve the access control of cloud federal [Anastasi, Carlini and Coppola (2014)]. Based on the semantic integration nature of XML data, Wang et al. [Wang, Wang, Guo et al. (2018)] proposes a data access control model for individual users, through which the global visual range of inverted XML structure is realized by the semantic dependency between data and the integration process from bottom to top. Container virtual technology aims to provide program independence and resource sharing. The container enables flexible cloud service. Within container-based cloud environment, services can adopt multi-target nodes. Xie et al. [Xie, Yuan, Zhou et al. (2018)] proposes a method to improve the traditional trust model with consideration of cooperation effects. Which ensures the nodes are in a cooperation state when multiple target nodes work for one service at the same time. When multi-target nodes were cooperated to complete the service, the target nodes can evaluate each other. The calculation of cooperation trust evaluation is used to update the degree of comprehensive trust. This method shows that the cooperation trust evaluation can help solving the trust problem in the container-based cloud environment and improve the success rate of following cooperation.

In the unreliable cloud environment, data owners often upload data onto the cloud server after encryption, which brings certain difficulties to the data sharing. Firstly, data sharing of abundant users require many secret keys which are difficult to be produced, distributed and kept. Secondly, fine granular access control may double secret keys when flexible and controllable access strategies are formulated. Thirdly, new secrete keys have to be produced again upon updating or revoking of users' access rights, which definitely cause heavy computation load. Another important problem is that the traditional access control method depends on a reliable server, which is impossible in unreliable cloud computing environment. In order to solve the problems mentioned above, researchers proposed the attribute based encryption (ABE) [Su, Cao and Wang (2011)]. ABE uses the attribute of users as the public keys, and connects ciphertext or private keys of users with attribute by introducing in the access structure. Meanwhile, ABE can express the access control strategy flexibly and realize fine access authorization of data and good system expansibility. It is the ideal scheme of access control to cloud data. ABE method can be divided into Ciphertext-Policy ABE (CP-ABE) [Bethencourt, Sahai and Waters (2007)] and key-policy ABE (KP-ABE) [Goyal, Pandey and Sahai (2010); Tang, Lian, Zhao et al. (2018)]. In CP-ABE, private key is related with the attribute set and the cipher text is related with the access structural tree. If the attribute set meets the needs of the access structural tree, the secret key gained by the user can be used in decryption. In KP-ABE, secrete key is related with the access structural tree and the cipher text is related with the attribute set. Due to the frequent updating of cipher text and the big user quantity in the cloud storage system, CP-ABE is believed to be more applicable under cloud storage.

The content-based image retrieval (CBIR) has been widely studied and become increasing

important in our daily life. Compared with the text documents, images consume much more storage and thus are very suitable to be stored on the cloud servers. The outsourcing of CBIR to the cloud servers can be a very typical service in cloud computing in the area of the privacy-preserving purposes, sensitive images such as medical and personal images, which needs to be encrypted before being outsourced will cause the CBIR technologies in plaintext domain unusable. Xia et al. [Xia, Xiong, Vasilakos et al. (2017)] proposes a scheme that supports CBIR over the encrypted images without revealing the sensitive information to the cloud server. Firstly, the feature vectors are extracted to represent the corresponding images. Secondly, the pre-filter tables are constructed with the locality-sensitive hashing to increase the search efficiency. Thirdly, the feature vectors are protected by the secure k-nearest neighbor (kNN) algorithm. The security analysis and experiments show the security and efficiency of the proposed scheme. Xia et al. [Xia, Lu, Qiu et al. (2019)] presents a secure retrieval scheme for encrypted images in the YUV color space. First of all, the discrete cosine transform (DCT) is performed on Y component. The resulting DC coefficients are encrypted with stream cipher technology and AC coefficients are encrypted by using value permutation and position scrambling. In addition, U and V components encrypted use the same encryption method as the AC coefficients. After that, the image owner transmits the encrypted images to the server. Second, the server extracts AC-coefficients histogram from encrypted Y component and two colors histograms from encrypted U and V components, and combines these three histograms as image feature. After receiving a query trapdoor from one query user, the cloud server extracts query feature and computes Manhattan distance between query feature and database image feature. Last, the encrypted images that most similar to the query image are selected to return to the query user.

5 Future trends

As a traditional information security technology, access control is vital to data protection in various information systems and network systems. It is an effective way to protect legal users for accessing to resources and preventing resource from stealing and misusing of illegal users. With the continuous development of computer technology, access control is going to occupy an increasing important role in safety. On the one hand, access control has to construct a stronger and simpler model to protect security of information data. On the other hand, according to different application demands, access control should propose higher and more updating demands on the basis of traditional model. Furthermore, the traditional model requires further reconstruction for the sake of adapting to the application development. Last but not the least, access control combines with encryption technology and semantic technology can provide stronger and safer information supports in the near future.

Acknowledgement: This work was sponsored by Qing Lan Project of Jiangsu Province. The authors are grateful for the anonymous reviewers who made constructive comments and improvements.

References

Anastasi, G. F.; Carlini, E.; Coppola, M. (2014): Usage control in cloud federations. *IEEE International Conference on Cloud Engineering*, pp. 141-146.

Su, J. S.; Cao, D.; Wang, X. F. (2011): Attribute-based encryption schemes. *Journal of Software*, vol. 22, no. 6, pp. 1299-1315.

Bethencourt, J.; Sahai, A.; Waters, B. (2007): Ciphertext-policy attribute-based encryption. *Proceedings of IEEE Symposium on Security and Privacy*, pp. 321-334.

Brewer, D. C.; Nash, M. J. (1989): The Chinese wa11 security policy. *Processing of IEEE Symposium Security and Privacy*, pp. 215-228.

Costabello, L.; Villata, S.; Delaforge, N. (2012): Linked data access goes mobile: Context-aware authorization for graph stores. *LDOW-5th WWW Workshop on Linked Data on the Web*, vol. 21, no. 2, pp.14-16.

Costabello, L.; Villata, S.; Rocha, O. R. (2013): Access control for HTTP operations on linked data. *The Semantic Web: Semantics and Big Data*, pp. 185-199.

Ferraiolo, D. F.; Sandhu, R.; Gavrila, S. (2001): Proposed NIST standard for role-based access control. *ACM Transactions on Information and System Security*, vol. 4, no. 3, pp. 224-274.

Goyal, V.; Pandey, O.; Sahai, A. (2010): Attribute-based encryption for fine grained access control of encrypted data. *Proceedings of the 13th ACM Conference on Computer and Communications Security*, pp. 89-98.

Hao, F.; Lakshman, T. V.; Mukherjee, S.; Song, H. (2010): Secure cloud computing with a virtualized network infrastructure. *HotCloud*.

Hollenbach, J.; Presbrey, J.; Berners-Lee, T. (2009); Using RDF metadata to enable access control on the social semantic web. *Proceedings of the Workshop on Collaborative Construction, Management and Linking of Structured Knowledge*, vol. 6644, no. 2, pp. 405-420.

Hu, V. C.; Kuhn, D. R.; Ferraiolo, D. F. (2015): Attribute-based access control. *Computer*, vol. 48, no. 2, pp. 85-88.

Kayes, A. S. M.; Han, J.; Colman, A. (2012): ICAF: a context-aware framework for access control. *Australasian Conference on Information Security and Privacy*, pp. 442-449.

LaPadula, L.; Bell, D. E.; LaPadula, L. J. (1973): Secure computer systems: mathematical foundations. *Draft MTR-2574*, vol. 1.

LaPadula, L.; Bell, D. E.; LaPadula, L. J. (1973): Secure computer systems: a mathematical model. *Draft MTR-2574*, vol. 2.

Liu, Z.; Wang, J. (2016): A fine-grained context-aware access control model for health care and life science linked data. *Multimedia Tools and Applications*, vol. 75, no. 22, pp. 14263-14280.

Oberheide, J.; Cooke, E.; Jahanian, F. (2008): CloudAV: N-version antivirus in the network cloud. *USENIX Security Symposium*, pp. 91-106.

Park, J.; Sandhu, R. (2004): The UCON ABC usage control model. *ACM Transactions on Information and System Security*, vol. 7, no. 1, pp. 128-174.

Sacco, O.; Passant, A. (2011): A privacy preference ontology (PPO) for linked data. *Linked Data on the Web Workshop at the World Wide Web Conference*.

Sandhu, R. (2015): Attribute-based access control models and beyond. *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*, pp. 677-677.

Sandhu, R.; Bhamidipati, V.; Munawer, Q. (1999): The ARBAC97 model for role-based administration of roles. *ACM Transactions on Information and System Security*, vol. 2, no. 1, pp. 105-135.

Sandhu, R.; Coyne E.; Feinstein, H.; Youman C. (1996): Role-Based access control models. *IEEE Computer*, vol. 29, no. 2, pp. 38-47.

Sandhu, R.; Park, J. (2003): Usage control: a vision for next generation access control. *In International Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security*, pp. 17-31.

Sandhu, R.; Samarati, P. (1994): Access control: principle and practice. *IEEE communications magazine*, vol. 32, no. 9, pp. 40-48.

Tang, Y.; Lian, H.; Zhao, Z.; Yan, X. (2018): A proxy re-encryption with keyword search scheme in cloud computing. *Computers, Materials and Continua*, vol. 56, no. 2, pp. 339-352.

Wang, L. S.; Ding, Q. L. (2003): Study and improvement of MLS relational data model. *Transactions of Nanjing University of Aeronautics & Astronautics*, vol. 20, no. 2, pp. 236-242.

Wang, M.; Wang, J.; Guo, L.; Harn, L. (2018): Inverted XML access control model based on ontology semantic dependency. *Computers, Materials & Continua*, vol. 55, no. 3, pp. 465-482.

Xia, Z.; Lu, L.; Qiu, T. Shim, H. J.; Chen, X. et al. (2019). A privacy-preserving image retrieval based on AC-coefficients and color histograms in cloud environment. *Computers, Materials & Continua*, vo. 58, no.1, pp. 27-44.

Xia, Z.; Xiong, N. N.; Vasilakos, A. V.; Sun, X. (2017). EPCBIR: an efficient and privacy-preserving content-based image retrieval scheme in cloud computing. *Information Sciences*, no. 387, pp. 195-204.

Xie, X.; Yuan, T.; Zhou, X.; Cheng, X. (2018): Research on trust model in container-based cloud service. *Computers, Materials & Continua*, vol. 56, no. 2, pp. 273-283.

Yang, K; Jia, X. (2014): ABAC: attribute-based access control. *Security for cloud storage systems*, pp. 39-58.

Zhang, X.; Parisi-Presicce, F.; Sandhu, R.; Park, J. (2005): Formal model and policy specification of usage control. *ACM Transactions on Information and System Security*, vol. 8, no. 4, pp. 351-387.

Zhao, M. B.; Yao, Z. Q. (2012): Access control model based on RBAC in cloud computing. *Journal of Computer Applications*, vol. 32, no. S2, pp. 267-270.