ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 9(23), DOI: 10.17485/ijst/2016/v9i23/95148, June 2016* ISSN (Online) : 0974-5645

Ontology Centric Access Control Mechanism for Enabling Data Protection in Cloud

M. Auxilia[1*] and K. Raja[2]

[1]Faculty of Computer Science and Engineering, Department of Computer Science and Engineering, Sathyabama University, Chennai - 600 119, Tamilnadu, India; auxilia.michael@gmail.com
[2]Alpha College of Engineering, Chennai, Tamilnadu, India; raja_koth@yahoo.com

Abstract

Background: Cloud computing provides access to a large scale of resources. Access control is the indispensable requirement for protecting cloud resource. A cloud service provider is responsible for enforcing access control and they normally rely upon conventional access control mechanisms. **Methods:** These access control policies, consider the access control primitives in separation which may lead to abuse of access control. These aforesaid problems motivated our research to center around the provision of access control by considering the association among the three access control primitives namely the user making access request, resource upon which access is requested and operation performed by the user on the resource. Hence Ontology Centric Access Control (OCAC) is being proposed in this paper. **Findings:** This OCAC circulates authorization rules among the primitives of access control say subject, object and action by reducing the various associations among the associations among the access control elements; it is observed that there is less chance for security violation. Ontology is used since it reduces the times of agreement while exchanging the authorization policies across the security domains. For reducing the number of statements and rules in policy base, subsumption property is used. This reduces the space and time complexity. **Applications/Improvements:** We are applying our work to protect bank data as banks are embracing clouds to store huge data by cutting their IT costs.

Keywords: Access Control, Ontology, Cloud Computing, User Ontology, Resource Ontology, Activity Ontology Introduction

1. Introduction

Access control is a process of allowing each attempt of a genuine user for accessing a resource in an organization. Controlling access to a resource is one of the vital security requirements. Three primitives of access control are subject, object and operation. Subject is an entity in the form of a person or a process requesting access. Object is an entity to which access is being requested. Operation determines the action applied to the object. Practically all applications and organizations incorporate their own form of access control. Implementing access control requires three concepts, namely policy, model and mechanism. These concepts are normally interchanged thus leading readers to misunderstand their part in achieving access control. Policy is the set of rules identifying who can access what resource and how they can access it. It is a high level prerequisite. Policies are expressed using languages and can be exchanged among organizations. Models are mathematical representations of policies to prove the performance of the system. Mechanism transforms access request of a user to a format that the system provides. Programs or protocol accomplishes this transformation; hence it is high level enforcement of access control.

Transition to cloud provides usage of large scales of assets through Internet at anytime and anywhere [1]. The consumers can pay for what they have used. These features magnetize small and medium size enterprises as well as large scale enterprises towards the cloud. But the migration is still dawdling. In 2013, CSA reports that the topmost threats hindering the adoption of cloud are data infringement, thrashing, self-doubting API, DoS spasms[2]. Prominent among them is data security. Access control is the fundamental requirement for protecting cloud resources as different users make an access request for the resources in the cloud[3]. A Cloud service provider is

* *Author for correspondence*

responsible for enforcing access control and they normally rely upon conventional access control mechanisms.

Mandatory, discretionary, non discretionary and role based access controls are some of the well known conventional access control policies[4-7]. These access control policies, consider the access control primitives in separation which may lead to abuse of access control. For instance role based access control policy focus on the roles played by the subject. If a loophole is created in role configuration, then definitely access violation can take place. And they are static. They hardly ever meet the access control requirements of cloud since the cloud environment is dynamic and has diverse users with diverse access requirements. RBAC is used widely by organizations owning data center as they control the access of users on the basis of the activities they perform. But the dispute is the conflict among tough protection and simpler administration. For tougher protection, it is healthier that all roles be coarser, and so having many roles for every user. For simpler administration, it is better to deal with fewer roles. Cloud has plenty of consumers for which role assignment is too tough and no of roles and hierarchy will explode [8-11].

These aforesaid problems motivated our research to center around the provision of access control by considering the association among the three access control primitives namely subject, object and operation. Association, among the primitives can be well studied by means of ontology. It is verified that ontology lessens the times of contract once information must be exchanged from one security domain to the other. Ontology also develops possibilities for interoperability and heterogeneity. Hence Ontology Centric Access Control (OCAC) is being proposed in this paper. This OCAC circulates authorization rules among the subject, object and operation by reducing the various meaningful associations among them into a subsumption problem. This reduces the space and time complexity of the access control mechanism based on the OCAC.

The need for controlling access to resources in cloud system is addressed by several researchers. Antonios Gouglidis verified security policy for multi domain cloud systems. They followed the NIST standard model improved with RBAC. The work also has proper definition of the suggested method and security properties to be validated in multi domain cloud systems. In addition, an assessment of the method through a series of performance tests is presented[12].

A work by Chang Choi suggests that traditional RBAC and extensions to it does not provide complete solution. RBAC lacks in considering security levels amongst objects. In addition, they do not signify a variety of dynamic relationship amongst objects[13-14].

Ontology created for role assignment by Hong Sun et al., simplifies role assignment[15]. But they lack in handling the concept explosion problem since cloud users are enormous.

TrBAC was recommended [16] as another work. This work uses assurance index for measuring trust level. The con is that focusing on trust alone is not adequate for making access decisions.

Semantic access control language suggested by Hu, affords efficient access control and interoperability for cloud data[17]. MTACM for securing applications in public Cloud was proposed by Li et al by combining MAC and DAC models. Instead of using IP address for framing security rules, they use user identification. The subjects and objects are categorized into fine grained user level, and application level. But the work doesn't resolve policy conflicts and is more platform dependent, hence complex modification for different environment[18].

An ARBAC mechanism for Multi-tenancy Cloud Environment was proposed by Nai Wei Lo et al. They combine attribute and role based access control mechanisms for finding which tenant the user can access. They also use simple matrix calculation to fine-tune the access decision. This reduces compile time of XACML and even if the access information leaks out, the attacker could not identify it easily. But ABAC is not yet standardized[19].

Zhenji Zhou et al., propose a new access control model called Context Aware Access Control model which ensures privacy and data security [20].

Sanka et al[21] proposed access control model by means of capability lists, determining who uses what. They revised Diffie-Hellman exchange protocol to exchange keys between providers and consumers. But the cons are that the model fails to manage policy conflicts, not dynamic and could not be implemented in heterogeneous platforms.

All these works follow different mechanisms to control access to cloud resources. Yet they have not considered the association among the access control primitives which lead to security violations. And most of the work does not find any mechanism for resolving policy conflict and do not follow any common policy format. Moreover the cloud service consumers could not manage their own policies. Hence our research objectives are: To frame

Common Access Control policy format, to resolve policy conflicts and also Enabling Cloud Service Consumers to manage their own policies.

Our paper is arranged as follows: Section II explains the OCAC Framework, Section III expresses the formal definitions to prove the performance of our work, Section IV describes the implementation of our proposed work . Section V discusses about the access control metrics suggested by NIST and how our OCAC abide them. Section VI concludes our work.

2. Proposed Work

Our framework in Figure 1 contains Ontology database, Policy database, Ontology handler, and Policy Decision Point. Each component performs its work efficiently.

Ontology Database contains User Ontology (UserOnt), Resource Ontology (ResourceOnt), and Activity Ontology (ActivityOnt).User Ontology consists of concepts or individuals concerning the users and properties relating them. Resource Ontology consists of concepts or individuals concerning the data and properties relating them. Activity Ontology consists of concepts or individuals regarding the user actions and properties relating them.

Policy Database is a repository of rules. A rule is given by (u, r, ±a), where u is in User Ontology, r is in Resource Ontology, a in Activity Ontology. Ontology Handler makes an inference request to ontology base and receives inference response.

A policy decision point gets the access request of the user and equals it with the rules stored in Policy database. If equal, the user is granted access right otherwise not.

3. Formal Definition

The A triplet (OntDB, PolDB, Oprs) decides whether to delegate access or not. Repository of all ontologies is OntDB Repository of rules is PolDB. The actions done on PolDB are Oprs.

$$OCA = (OntDB, PolDB, Oprs)$$

OntDB is designated as

{Ontology|Ontology = UserOnt ∨ Ontology = ResrouceOnt ∨ Ontolgy =ActivityOnt ∨ Ontology}

Ontology is a set of *UserOnt*, *ResrouceOnt* and *ActivityOnt*.

PolDB is given as

PolDB = {(u, r, ±a)| u∈UserOnt ∧ r∈ResourceOnt ∧ a ∈ ActivityOnt}

Rules PolDB are given as

$$PolDB \subseteq u \times r \times a$$

Oprs is given as

$$Oprs = (Decision, true, false)$$

Decision function results in either grant or deny. If the result is yes then the access control rue is inserted into PolBase else it is deleted from PolBase.

Decision is designated as

$$Decision\ (u, r, a)$$

And given as function of decision making by

$$Decision: u \times r \times a(\{true, false\})$$

If the decision function yields true, then access is granted or else denied.

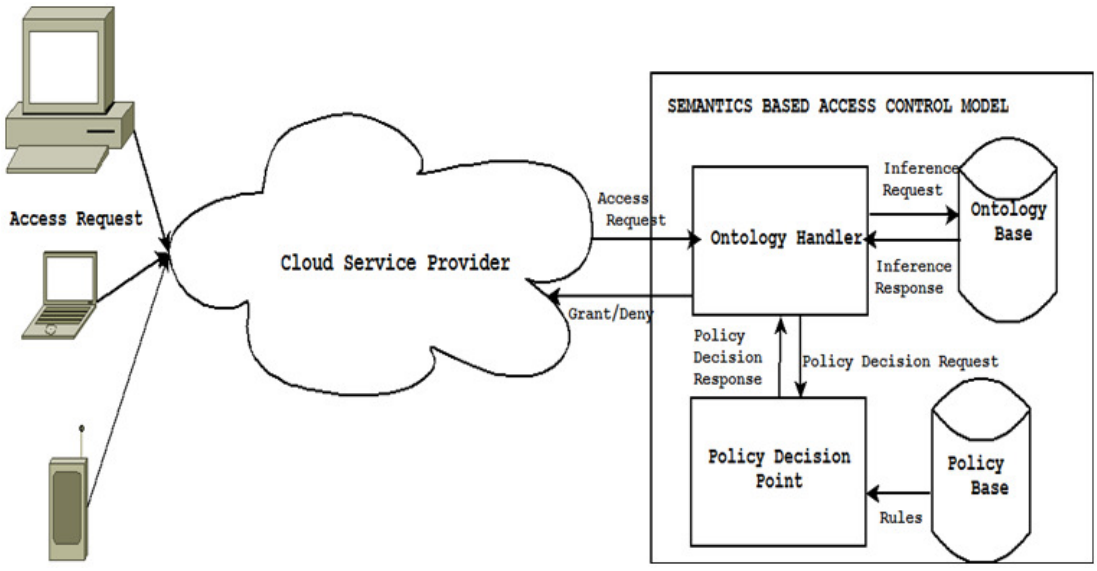

Figure 1. Ontology Centric Authorization Framework.

4. Implementation

This section describes how our framework is implemented. To implement our work we used the protégé tool for creating ontologies and Gena for extracting the details and Fact++ reasoner for deriving inferences[22]. For cloud implementation, we used Jelastic public cloud. The domain we have chosen is banking. The reason for choosing banking as domain is that banks handle massive sum of secret data 24×7. Thus investment must be put in a lot IT resources for handling large volume and velocity of data. Because of financial problems, banks are in a position to minimize their IT cost by minimizing their resources. This should be realized without compromising the basic security requirements. The ultimate solution to this problem is cloud computing. But only few applications of banks are realized through the cloud. Multifarious security issues of cloud hinder the migration of bank data to the cloud. Our proposed system OCAC will accomplish security to bank data effectively. Based on this, the subject ontology is created in terms of user credentials and is represented in Figure 2. User credential is a union of smart card, ID card and virtual fingerprint. Through the subsumption property, the access rules inflicted on smart card will also be enforced on the other two subjects. The object ontology is created in terms of account details and is given in Figure 3. Action Ontology is created in terms of activities performed by the user over the account and is given in Figure 4.

Figure 2. Subject Ontology.

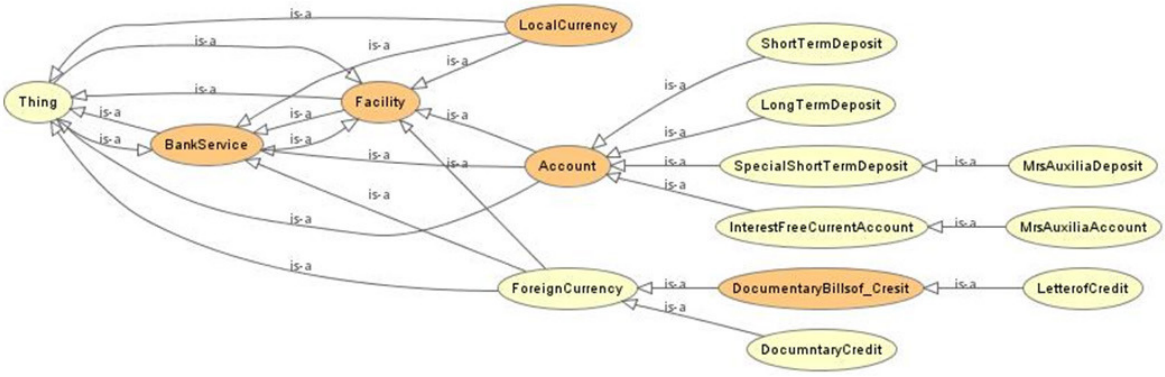

Figure 3. Object Ontology.

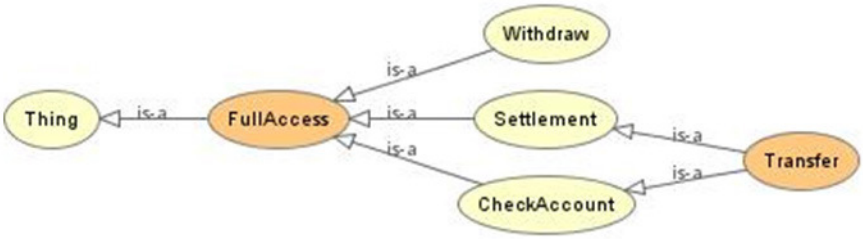

Figure 4. Action Ontology.

Table 1. Comparison of related works and proposed work against NIST Access Control Metrics

Metrics/Related work	Rw1	Rw2	Rw3	Rw4	Rw5	Rw6	Rw7	Rw8	Rw9	PW
Steps to assign and dis-assign user capabilities	Difficult	Difficult	Moderate	Difficult	Moderate	Difficult	Moderate	Easy	Moderate	Easy
Steps to assign and dis-assign object Access control	Difficult	Difficult	Moderate	Difficult	Moderate	Difficult	Moderate	Moderate	Moderate	Easy
Support for least privilege	High	High	High	Low	Low	Low	Low	Medium	Medium	High
Support for Separation of duty	High	High	High	High	High	Low	High	High	High	High
Adaptability	Low	Low	Low	Medium	High	Low	High	Medium	Medium	High
Horizontal Scope	High	Low	High	High	Medium	Low	Low	Low	Medium	High
Support for safety	Medium	Medium	Low	Medium	Medium	Low	Medium	Medium	Medium	High
Degree of freedom for AC management	Low	Low	Medium	Low	High	Low	Low	Medium	Low	High
Resolving Policy conflicts	No	No	No	No	yes	Yes	Yes	No	No	Yes
Resolving Policy conflicts	No	No	No	No	yes	Yes	Yes	No	No	Yes
Flexibility	High	Low	Low	High	High	low	High	Low	medium	High

Scenario 1: For preventing master cards supported by some bank to clear up money in a special account, a rule can be framed as follows:

(SomeBankMasterCards,$Account_x$,–settlement)

This can be framed using two properties namely 'IssuedIn' and 'RegisteredIn'. These two properties results in a new property called 'SupportedBy'.

RegisteredIn(Bankx,SomeBank) ∧ IssuedIn(MasterCard,$Bank_x$) → SupportedBy(MasterCard,SomeBank)

Scenario 2: A property can be declared as symmetric, reflexive, and transitive. When a property is defined as symmetric, say 'SupportOf' and $Account_x$, $Account_y$ are individuals, then we can infer that

SupportOf($Account_x$,$Account_y$) → SupportOf($Account_y$,$Account_x$)

Scenario 3: Three rules are usually framed namely positive rules, negative rules and exception rules. Exception rules lead to conflicts in access decision. To resolve conflicts, our proposed work gives preference to exception rules first than explicit rules. An exception rule is framed if the bank authority would like to proscribe the credit cards given by some bank from settling funds to any account in *Bankx* whereas there is a further clear rule that allows all credit cards clear up funds in any account. Example is given in scenario 1. This is possible when there is a possibility to compare the rules that are conflicting. If they cannot be compared, then the negative rules are given more preference than positive rules. Thus conflicts are handled efficiently and successfully in our work.

5. Evaluation of Our Work Based on Access Control Metrics Afforded By NIST

National Institute of Standards and Technology [NIST] had proposed some metrics to assess the efficacy of an access control of an organization in 2006. To mention a few are steps to assign and dis-assign user capabilities, Steps to assign and dis-assign object Access control, Support for least privilege, Support for Separation of duty, Adaptability, Horizontal Scope, Support for safety, Degree of freedom for AC management, Resolving policy conflicts and Flexibility. The related works and our proposed works are compared against these metrics and a comparison chart is also provided. Refer Table 1 and Figure 5. To implement our work we used the protégé tool for creating ontologies and gena for extracting the details and Fact++ reasoner for deriving inferences. For cloud implementation we used Jelastic public cloud.

Here we have used the quantitative measures as high, low, medium, moderate, difficult, easy, yes and no. All these measures are given values 0(low, difficult, no), 1(high, easy, yes), 0.5(medium, moderate). Taking summation of these values we have plotted the comparison chart.

$$\sum_{i=1}^{n} M_i$$ Where M indicates the above mentioned metrics and i ranges from 1 to number of metrics

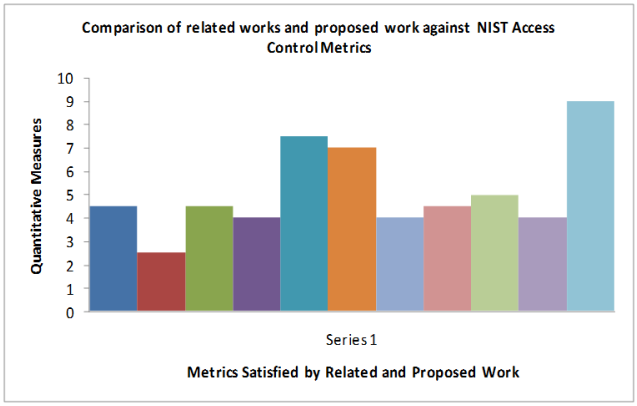

Figure 5. Comparison of related works and proposed work against NIST Access Control Metrics.

6. Conclusion

Our work focuses exclusively on access control concerns related to cloud and prospective solutions. A comprehensive scrutiny of various access control models is made. We compared our work with other related works based upon the metrics given by NIST report. Based on these, we analysed that contemporary access control solutions are vague and do not satiate the required features appropriately. Thus we proposed Ontology Centric access control mechanism for protecting data in the cloud. This proves to be a standard resolution for the access control problems identified.

Our future work is extending XACML a well known access control specification language to accommodate our mechanism. Thriving implementation of the proposed work will significantly eliminates access control concerns in the Cloud and help reassure users that their information on Cloud is protected effectively.

7. References

1. Mell P, Grance T. The NIST Definition of Cloud Computing. ver. 15. Information Technology Laboratory, US Nat'l Institute of Standards and Technology. Oct. 2009.
2. CSA: The Notorious Nine Cloud Computing Top Threats in 2013. https://downloads. cloudsecurityalliance.org/initiatives/topthreats/The_Notorious_Nine_Cloud_Computing Top_Threats_in_2013.pdf (2013). Accessed Jul. 2013
3. Chunming Rong, Son.T.Nguyen, Martin Gilje Jaatun. Beyond Lightning: A Survey on Security Challenges in Cloud Computing. Journal of Computers and Electrical Engineering, 2012.
4. Diogo A. B. Fernandes, Liliana F. B. Soares, Jo˜ao V. Gomes, M´ario M. Freire, Pedro R. M. In´acio. Security Issues in Cloud Environments — A Survey. International Journal of Information Security. 2014 April,13(2), 113-170.
5. Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez. An analysis of security issues for cloud computing. Springer Open Journal of Internet Services and Applications. 2013, 4(5).
6. Nelson Gonzalez, Charles Miers, Fernando Red´ıgolo, Marcos Simpl´ıcio, Tereza Carvalho, Mats N¨aslund and Makan Pourzandi. A quantitative analysis of current security concerns and solutions for cloud computing. Journal of cloud computing, SpringerOpen Journal. 2012,1.
7. Takabi, H., Joshi, J.B.D, Ahn, G.J. Security and privacy challenges in cloud computing environments. IEEE Security and Privacy. 2010, 8(6),25–31.
8. Hong Sun, Xueqin Zhang, Chunhua G. Role-based Access Control Using Ontology in Cloud Storage. International Journal of Grid and Distribution Computing. 2014 7(3), 1-12.
9. Lin G, He S, Huang H et al. Access Control Security Model Based on Behavior in Cloud Computing. Journal on Communications. 2012, 33(3), 59-66.
10. Luokai Hu, Shi Ying, Xiangyang Jia, and Kai Zhao. Towards an Approach of Semantic Access Control for Cloud Computing. LNCS. Springer-Verlag Berlin Heidelberg. 2009, 5931, 145–156.

11. Yuh-Jong Hu and Win-Nan Wu and Jiun-Jan Yang. Semantics-enabled Policies for Super-Peer Data Integration and Protection. International Journal of Computer Science and Applications. 2012, 9(1), 23 – 49.
12. Antonios Gouglidis, Ioannis Mavridis, Vincent C. Hu. Security policy verification for multi-domains in cloud systems. International Journal of Information Security. Springer. 2014 Volume 13, 97-111
13. Chang Choi, Junho Choi, Byeongkyu Ko, Kunseok Oh, Pankoo Kim. A Design of Onto-ACM(Ontology based Access Control Model) in Cloud Computing Environments. Journal of Internet Services and Information Security (JISIS). 2012, volume: 2, 54-64.
14. Chang Choi, Junho Choi, Byeongkyu Ko, Kunseok Oh, Pankoo Kim. Ontology-based access control model for security policy reasoning in cloud computing. Journal of SuperComputing. 2014, 67(3), 711-722.
15. Hong Sun, Xueqin Zhang, Chunhua G. Role-based Access Control Using Ontology in Cloud Storage. International Journal of Grid and Distribution Computing. 2014 7(3), 1-12.
16. Jingwei Huang, David M Nicol. Trust mechanisms for cloud computing. Springer Open Journal of Cloud Computing. August 2012, 2(9).
17. Hongxin Hu, Gail-Joon Ahn, Ketan Kulkarni. Discovery and Resolution of Anomalies in Web Access Control Policies. Transactions on Dependable and Secure Computing. 2013 November-December, 10(6),341-354.
18. Li X, Shi Y, Guo Y, Ma W. Multi-tenancy based access control in cloud. In: Proceedings of the International Conference on Computational Intelligence and Software Engineering (CiSE). 2010, 1–4
19. Nai Wei Lo, Ta Chih Yang Ming Huang Guo. An Attribute-Role Based Access Control Mechanism for Multi-tenancy Cloud Environment. Wireless Pers Commun, Springer Science+Business Media, New York. 2015
20. Zhenji Zhou, Lifa Wu, Zheng Hong. Context-Aware Access Control Model for Cloud Computing. International Journal of Grid and Distribution Computing. 2013 6(6), 1-12.
21. Sanka S, Hota C, Rajarajan M. Secure Data Access in Cloud Computing. In: Proceedings of the IEEE 4th International Conference on Internet Multimedia Services Architecture and Applications (IMSAA), 2010.
22. S. Vigneshwari, M. Aramudhan. Social Information Retrieval Based on Semantic Annotation and Hashing upon the Multiple Ontologies. Indian Journal of Science and Technology, 2015 Jan, 8(2), Doi no: 10.17485/ijst/2015/v8i2/57771.