International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 11 – No. 10, February 2017 – www.ijais.org

Verified Message Exchange in Providing Security for Cloud Computing in Heterogeneous and Dynamic Environment

Atul Verma
Assistant Professor,
Dept. of Computer Science
Babu Banarasi Das University
Lucknow

Gaurav Kant Shankhdhar
Assistant Professor,
Dept. of Computer Science
Babu Banarasi Das University
Lucknow

Manuj Darbari
Associate Professor,
BBDNITM,
Lucknow

ABSTRACT
Providers to cloud computing including Amazon, Google, Microsoft, Rachspace and Terremark have all contributed at a high end for this bulk storage technology. As goes with all the software packages including CRMs and ERPs the need for security has to be redefined, restructured and its domain adjusted because as the development progresses the vulnerabilities are exposed. To deal with the security issues in cloud computing this paper discusses some concepts like ontology, web semantics, and message passing within or between cloud components. This paper introduces a Context Sensitivity Policy approach for the Cloud Security Paradigm.

Keywords
Cloud computing, Distributed computing, Grid computing, Concurrent computing, Computer science,High performance computing, Parallel processing, Platform virtualization, Computer industry, Network servers

1. INTRODUCTION
In this section we made a study about security methods. A. Encryption Outsourced cloud data will stored in the third party storage, the problem is we stored our original data. So the Better way to secure our outsourced data is Encryption [6]. Providing the Confidentiality is the main theme of the Encryption. Encryption is the best way to hide our information from service provider. We can use either symmetric encryption or asymmetric encryption i.e. Public Key Cryptography [9]. If the data is very sensitive means we need to provide more level of security for the outsourced data. Personal Health Information is the most sensitive information. So Attribute based encryption [4] [5] is a good way to protect the outsourced data. So we need to provide separate authentication and confidentiality for both public and private domain. Increasing security level we can also use the Digital Signature for protecting the sensitive information like Personal Health Records.

B. Auditing Third Party Auditor [7] [8] is the very good solution for protecting the outsourced cloud data. For reducing the infrastructure cost we moving to the third party cloud storage. The security issue is the service provider can distribute to the information to other distributor. So we need the help of auditor. Auditor always audits the operations on our data. Example if we are the seller of the amazing pictures. We using cloud storage we sell our pictures. In the sense by using auditor we can audit the operations on our pictures. If any kind of error log means auditor will monitor and restrict the unauthorized operations as well as the details send to us.

C. Identity Monitoring and confidentiality is the needed for the cloud security. But we also concentrate on the authentication also. So identity [10] is the good approach to make sure the authentication. Identity in the sense we can use the biometrics. Biometrics is the excellent identity for authentication. We suggest the IRIS is the best identity for authentication. We also integrate identity with the encryption. That is identity with encryption. IRIS based encryption. We can check IRIS for authentication. For Confidentiality we can use the encryption algorithm. So we provide the multiple level of security. These methods are used for efficiently in private cloud.

The Generation of Policies evolved for the verification of Message Exchanges is described below. The evolution of approaches given under, tend to culminate on Context Sensitive Management of Policies. These Policies take care of unambiguous, less error prone and accurate message exchange within the cloud environment.

2. XACML ("eXtensible Access Control Markup Language"): No Semantic Support [1]
There have been two parallel themes in access control re-search in recent years. On the one hand there are efforts to develop new access control models to meet the policy needs of real world application domains. In parallel, and almost separately, researchers have developed policy languages for access control. This paper is motivated by the consideration that these two parallel efforts need to develop synergy.

A policy language in the abstract without ties to a model gives the designer little guidance. Conversely a model may not have the machinery to express all the policy details of a given system or may deliberately leave important aspects unspecified. Our vision for the future is a world where advanced access control concepts are embodied in models that are supported by policy languages in a natural intuitive manner, while allowing for details beyond the models to be further specified in the policy language.

This paper studies the relationship between the Web Ontology Language (OWL) and the Role Based Access Control (RBAC) model. Although OWL is a web ontology language and not specifically designed for expressing authorization policies, it has been used successfully for this purpose in previous work. OWL is a leading specification language for the Semantic Web, making it a natural vehicle for providing access control in the CLOUD ONTOLOGY. In this paper we

show two different ways to support the NIST Standard RBAC model in OWL and then discuss how the OWL constructions can be extended to model attribute-based RBAC or more generally attribute-based access control. We further examine and assess OWL's suitability for two other access control problems:

supporting attribute based access control and performing security analysis in a trust-management framework for Cloud Computing. These include industry standards such as XACML [23]

3. RBAC (ROLE BASED ACCESS CONTROL)

This was the major transition. This was used to build Policies. It was totally static and the policies for agents were framed at design time. No dynamic alterations in Policy Rules were possible. There have been two prominent themes in access control research in recent years.

One has focused on efforts to develop new access control models to meet the policy needs of real world application domains. These have led to several successful, and now well established, models such as the RBAC96 model [1], the NIST Standard RBAC model [2] and the RT model [3]. This line of research continues with recent innovations such as Usage Control models [4, 5]. In a parallel, and almost separate thread, researchers have developed policy languages for access

control. These include industry standards such as XACML [6], but also academic efforts ranging from more practical implemented languages such as Ponder [7] to theoretical languages such as [8] and finally to Semantic Web based languages such as Rei [9] and KAoS [10]. Policy languages grounded in Semantic Web technologies allow policies to be described over heterogeneous domain data and promote common understanding among participants who might not use the same information model. This paper is motivated by the consideration that these two parallel efforts - access control models and Semantic Web based policy languages- need to develop synergy to enable the development of security infrastructures for emerging, open, and dynamic environments. [2]

4. ABAC (ATTRIBUTE BASED ACCESS CONTROL)

Removed shortcomings of RBAC. First ABACα, ABACβ were introduced. ABAC introduced the concept of Dynamic Population of attributes that store changing values such as Location, Business Hours (time, day), etc. Here Policies are implemented in OWL as OWL supports Description Language. [3] Most organizations have policies that control their behavior. The ability to capture these policies, which are normally expressed in some natural language, in a machine understandable format has been an active thread of research (see for instance [3], [8], [10], [11]). The Web Ontology Language (OWL) [9] provides an efficient way to represent policies formally. Access control models when combined with formal policy specification language like OWL give the ability to write policies that describe entities and relationships in the system, how they affect access control, and how they are grounded out in models that are well understood in the security community. This combination further helps by using the power of reasoning to make access control decisions. A

key contribution of our paper is to create an ontology and rules that capture the Attribute Based Access Control model, thus allowing for policies that are grounded out in ABAC. The specific model we capture is ABAC_ [4]. We have used the EYE [1] reasoner to infer more facts from the specified access control model, data and policies for implementing security in Cloud Computing Resources.

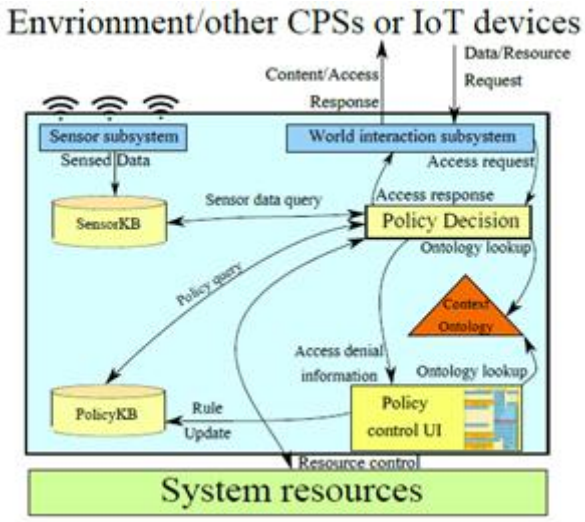

Fig. 1 IoT (Internet of Things) model for security in Cloud Computing

5. A COMBINATION OF RBAC AND ABAC

The concept of **Context Sensitive Policy** used for **verification of message flow between cloud components** is guided by the IoT as shown in Fig. 2. The IoT field is exploding with novel smart systems and applications in multiple domains. Most of these systems and applications leverage the computation and communication capability of such systems that allows information sharing and collaboration. Information leakage from CPSs or behavior

modification of such systems can have dangerous real life impacts. Upon doing a survey of the literature we found a number of attacks have already been mounted on CPSs and how they affected human lives. Hence in this paper, we have proposed the design of a system that allows context-sensitive policy based security to control and protect information sharing operations among CPSs. Our system design creates a **middle-ware** that is capable of executing such policies and thus protect security and privacy of user and his data. We use Semantic Web technologies to represent our policies and to reason over contextual attributes and user role attributes to determine outcomes of access control requests. We use a context ontology to allow easy policy refinement. Due to dynamic and open environments that IoT systems are deployed in, their access control policies maybe highly complex and we are able to capture that by using Attribute Based Access Control (ABAC) model represented in OWL. We also describe few use case scenarios that shows how access control decisions can be made in such a system. As part of future work, we would like to evaluate performance of CPS systems when a reasoning system executes access control policies. Detecting suspicious events at run-time could be another interesting area of research. The introduction of Proximity Beacon API from Google, have made sharing of information like policies, capabilities, services etc. easier for CPSs. However, self-organization and interoperability between a diverse group of CPSs is still a challenging goal

6. IMPLEMENTATION

The implementation has been planned for the Context Sensitive Cloud Security Model. Python will be used for the projection and construction of this Model. DotNet, Java or OWL API can be used along with SPARQL, a recursive acronym for **SPARQL** Protocol and RDF Query Language) is an RDF query language, that is, a semantic query language for databases, able to retrieve and manipulate data stored in Resource Description Framework (RDF) format. for developing a Security Framework for the Cloud.

7. CONCLUSION AND FUTURE SCOPE

In this paper the authors have discussed a solution for providing by far a concrete approach by proposing a technique to quash the discrepancies encountered in the security of messages exchanged within the Cloud Components. This is done through the use of Context Sensitive Policies that devise the rules for proper communication within the Cloud Environment. This Research will continue in the implementation of this concept for Cloud Security Paradigm. Work is also being done for security of Message Exchange within Multi Agent Systems which is already started [32].

8. REFERENCES

[1] R*OWL*BAC - Representing Role Based Access Control in *OWL, T. Finin, A. Joshi Univ. of Maryland, Baltimore County finin,joshi@cs.umbc.edu, 2008.*

[2] Role Based Access Control and OWL, T. Finin, A. Joshi Univ. of Maryland, Baltimore County finin,joshi@cs.umbc.edu, 2016.

[3] Context-Sensitive Policy Based Security in Internet of Things, Context-Sensitive Policy Based Security in Internet of Things, 2016.

[4] V. G. Cerf, "Prospects for the internet of things," XRDS, vol. 22, no. 2, pp. 28–31, Dec. 2015. [Online]. Available: http://doi.acm.org/10.1145/ 2845145

[5] N. Eddy, "Stress-free parking," November 2015. [Online]. Available: http://www.informationweek.com/mobile/mobile-devices/ gartner-21-billion-iot-devices-to-invade-by-2020/d/d-id/1323081.

[6] S. Karnouskos, "Stuxnet worm impact on industrial cyber-physical system security," in IECON 2011 - 37th Annual Conference on IEEE Industrial Electronics Society, Nov 2011, pp. 4490–4494.

[7] K. Kochetkova, "Shock at the wheel: your jeep can be hacked while driving down the road," July 2015. [Online]. Available: https://blog.kaspersky.com/remote-car-hack/9395/

[8] S. Khandelwal, "100,000 refrigerators and other home appliances hacked to perform cyber attack," January 2014. [Online]. Available: http:// thehackernews.com/2014/01/100000-refrigerators-and-other-home.html

[9] I. Gartner, "Gartner's 2015 hype cycle for emerging technologies identifies the computing innovations that organizations should monitor," August 2015. [Online]. Available: http://www.gartner.com/newsroom/ id/3114217

[10] H. Chen, F. Perich, T. Finin, and A. Joshi, "Soupa: standard ontology for ubiquitous and pervasive applications," in Mobile and Ubiquitous Systems: Networking and Services, 2004. MOBIQUITOUS 2004. The First Annual International Conference on, Aug 2004, pp. 258–267.

[11] L. Kagal, T. Finin, M. Paolucci, N. Srinivasan, K. Sycara, and G. Denker, "Authorization and privacy for semantic web services," IEEE Intelligent Systems, vol. 19, no. 4, pp. 50–56, Jul 2004.

[12] S. Bechhofer, "Owl: Web ontology language," in Encyclopedia of Database Systems. Springer, 2009, pp. 2008–2009.

[13] J. Slay and M. Miller, Lessons learned from the maroochy water breach. Springer, 2007.

[14] J. Leyden, "Polish teen derails tram after hacking train network," The Register, vol. 11, 2008.

[15] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in Security and Privacy, 2008. SP 2008. IEEE Symposium on. IEEE, 2008, pp. 129–142.

[16] M. Abomhara and G. M. Koien, "Security and privacy in the internet of things: Current status and open issues," in Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on. IEEE, 2014, pp. 1–8.

[17] K. Zhao and L. Ge, "A survey on the internet of things security," in Computational Intelligence and Security (CIS), 2013 9th International Conference on. IEEE, 2013, pp. 663–667.

[18] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, vol. 57, no. 10, pp. 2266–2279, 2013.

[19] S. N. Narayanan, S. Mittal, and A. Joshi, "Using data analytics to detect anomalous states in vehicles," arXiv preprint arXiv:1512.08048, 2015.

[20] S. Godik, A. Anderson, B. Parducci, P. Humenn, and S. Vajjhala, "Oasis extensible access control 2 markup language (xacml) 3," Tech. rep., OASIS, Tech. Rep., 2002.

[21] K. Lalana, "Rei: A policy language for the me-centric project," TechReport, HP Labs, 2002.

[22] J. M. Bradshaw, A. Uszok, M. Breedy, L. Bunch, T. Eskridge, P. Feltovich, M. Johnson, J. Lott, and M. Vignati, "The kaos policy services framework," in Proc. 8th Cyber Security and Information Intelligence Research Workshop, 2013.

[23] T. Finin, A. Joshi, L. Kagal, J. Niu, R. Sandhu, W. Winsborough, and B. Thuraisingham, "R owl bac: representing role based access control in owl," in Proceedings of the 13th ACM symposium on Access control models and technologies. ACM, 2008, pp. 73–82.

[24] NIST, NIST CPS, 2016 (accessed February 1, 2016). [Online]. Available: http://www.nist.gov/cps/

[25] X. Jin, R. Krishnan, and R. Sandhu, "A unified attribute-based access control model covering dac, mac and rbac," in Proceedings of 26th Annual IFIP WG 11.3 Working Conference on Data and Applications Security and Privacy (DBSec 2012), Paris, France, July 2012.

[26] X. Jin, "Attribute-based access control models and implementation in cloud infrastructure as a service," Ph.D. dissertation, The University of Texas, San Antonio, May 2014.

[27] M. Dean and G. Schreiber, "Owl web ontology language guide," W3C Recommendation, http://www.w3.org/TR/owl-guide/, 2004.

[28] N. K. Sharma and A. Joshi, "Representing attribute based access control policies in owl," in 2016 IEEE Tenth International Conference on Semantic Computing (ICSC), California, USA, Feb 2016, pp. 333–336.

[29] C. Seitz and R. Sch¨onfelder, The Semantic Web – ISWC 2011:10th International Semantic Web Conference, Bonn, Germany, October 23-27, 2011, Proceedings, Part II. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, ch. Rule-Based OWL Reasoning for Specific Embedded Devices, pp. 237–252. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-25093-4 16

[30] L. Zavala, P. K. Murukannaiah, N. Poosamani, T. Finin, A. Joshi, I. Rhee, and M. P. Singh, "Platys: From position to place-oriented mobile computing," AI Magazine, vol. 36, no. 2, 2015.

[31] Google, "Mark up the world using beacons," March 2016. [Online]. Available: https://developers.google.com/beacons/

[32] IEEE Explore, 2016, Building Custom, Adaptive and Heterogeneous Multi-Agent Systems for Semantic Information Retrieval Using Organizational-Multi-Agent Systems Engineering, O-MaSE, Gaurav Kant Shankhdhar