International Journal of Innovative Research in Information Security (IJIRIS) ISSN: 2349-7017(O)
Issue 2, Volume 5 (May 2015) ISSN: 2349-7009(P)
www.ijiris.com

A Modified Things Role Based Access Control Model for Securing Utilities in Cloud Computing

Oyeyinka, F.I.(Mrs)*
Centre for Information Technology and Management,
Yaba College of Technology, Lagos, Nigeria

Prof. Omotosho O.J.
Department of Computer Science
Babcock University, Ilishan,
Ogun State, Nigeria,

Oyeyinka I.K. (Ph.D)
Gateway Polytechnic
Saapade, Ogun State, Nigeria

Abstract— Cloud computing introduces a radical change in Computer resources services that may become the best service provider at a reduced cost to the users. In spite of all the advantages of cloud computing, there are a lots of security challenges that come with its implementation. In overcoming these challenges, there are many access control models proposed in literature; these include Discretionary Access Control, Mandatory Access Control and Role Based Access Control. Role Based Access Control models use role hierarchies and constraints. Administrative roles can be designated to manage other roles. Authorisation constraints may be enforced to protect information misuse and fraud. In this paper, a Modified Things Role Based Access Control model (T-RBAC) is proposed that extend security in the cloud to other concepts of internet of things in which different objects are networked in such a way that a thing may obtain permission to use or modify other objects. In T-RBAC, in addition to normal role assignment and permissions in RBAC, alerts are generated to object owner before permission to access or operate the object is granted.

Keywords— T-RBAC, Cloud Computing, Access Control, SaaS, PaaS, IaaS, HaaS, RBAC, MAC, DAC

I. INTRODUCTION

Cloud is seen in different perspectives by different group of people; it is an on-demand model which enables access to computer resources over a network [1]. The cloud in this case refers to the internet. Hence cloud computing means a real time internet based information technology services that certify users' needs without the users having to pay maintenance and infrastructures cost. Cloud computing offers a wide range of services to organisations and businesses in a transparent manner over a large network like the internet [2]. Despites the advantages of cloud computing, it has brought up a new set of security challenges which includes the problems of trust and access control. The problem of trust in cloud computing include trusting the data warehoused in the cloud, the cloud computing technology and the providers themselves.

There are three categories of cloud computing: Software as a service, platform as a service and infrastructure as a service. Software as a Service (SaaS) is a model that allows software applications to be hosted by cloud provider and accessible to customers over the internet. This require broadband network to be available to support access from different locations all over the world. SaaS may also be referred to as on-demand software delivery model. Benefits of SaaS model include: Easier administration, automatic updates and patch management, compatibility, easier collaboration and global accessibility [3]. Platform as a Service (PaaS) refers to hiring of storage, operating system, hardware and bandwidth on the internet. There are cloud platform technologies that have been built that allow large number of businesses and employees to run their computing job online [4] and [5]. Customers may rent server and services for organisational used. The benefit of PaaS includes include Access to most recent software technology tools, software teams in different locations can work together on a project, services may be obtained across international boundaries and project cost may be reduced and overall expenses may be minimised. Infrastructure as a Service (IaaS) is sometimes referred to as Hardware as a Service (HaaS). Equipment like hardware, network storage may be outsourced. In this case the organisation pay per use.

The remaining of this paper is organised as follows: section 2 reviews some literatures on challenges of cloud computing, security issues in cloud computing and types of cloud computing access control models, section 3 focuses on the Role Based access Control Model (RBAC), section 4 discuses a modification to RBAC while section 5 concludes the paper.

II. REVIEW OF RELATED LITERATURES

A. Challenges of Cloud Computing

The disadvantage of cloud computing includes amongst others, the fact that customers do not have control over the clouds' server, software, security, the customer data is in the cloud providers' custody. Hence, the issue of trust becomes difficult.

It may be difficult to change provider if there is need for change because it will be impossible for large data to be successfully moved from one provider to another. Network unreliability may prevent the cloud services effectively most especially in a third world country like Nigeria. Security is topmost challenge in the adoption of cloud computing. [6].

B. Security Issues in Cloud Computing

Cloud computing is an unsecured platform due to the fact that the client do not have control over data integrity and confidentiality, because the cloud provider has complete control over the computing infrastructure that render the services [7]. There have been many security models proposed for the cloud computing in order to minimise the shortfall. This includes:- Trust certificate models, Access control models.

C. Types of Access Control Model

For improvement of data integrity and reliability, and to secure customers right on the cloud, the following different access control models are available: Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role Based Access Control (RBAC), Attribute-Based Access Control (ABAC), History-Based Access Control (HBAC), Relationship-Based Access Control (ReBAC), Usage Control (UCON), Access Control Models for Workflow (WFMs), Tasks Based Access Control (TBAC), Agent-Based Approach (AgBAC), Certificate-Based Approach (CBAC), Hypertext-Based Authorizations (HyBAC), Intranet- Based Access Control (I-RBAC) and Provenance-Based Access Control (PBAC).

The first three of these models are the most popular in literature. In DAC, the subjects and objects in the system are listed and the access authorization rules for each of the subject and object are specified. The examples of subject are users, groups or processes that act on behalf of other subjects. If a subject is the owner of an object, the subject is authorized to grant or revoke access rights on the object to other subjects at his discretion. DAC policies are flexible but the policies do not possess high security assurance [8]. All subject and object in a MAC model are classified based on predefined sensitivity levels that are used in the process of access decision. MAC model control information flow to ensure confidentiality and integrity, this did not feature in DAC model. By rule MAC model ensures that information does not flow from higher sensitivity level to a lower sensitivity level to achieve information integrity [9]. For a cloud based applications multilevel classification of information is required by the service provider to differentiate between the users and the information being accessed. MAC model are more robust than DAC model for data protection, however enforcement of MAC policies is difficult for cloud based application. These entire shortcomings are addressed by RBAC.

III. ROLE BASED ACCESS CONTROL MODEL

One of the most challenging problems in managing large networks is the complexity of security administration. Role Based Access Control (also called Role Based Security), as formalized by [10], has become the predominant model for advanced access control because it reduces this cost. A variety of IT vendors, including IBM, Sybase, Secure Computing, and Siemens began developing products based on this model in 1994. In 2000, the Ferraiolo-Kuhn model was integrated with the framework of Sandhu et al. to create a unified model for RBAC, published as the NIST RBAC model [11] and adopted as an ANSI/INCITS standard in 2004. Today, most information technology vendors have incorporated RBAC into their product lines, and the technology is finding applications in areas ranging from health care to defense, in addition to the mainstream commerce systems for which it was designed. As of 2010, the majority of users in enterprises of 500 or more are now using RBAC, according to the Research Triangle Institute. [12]

This model has been described as a generalised access control model because they provide well recognised advantages. RBAC model are policy neutral [13]. They used role hierarchies and constraints. Administrative roles can be designated to manage other roles. Authorisation constraints may be enforced to protect information misuse and fraud. An example of the authorisation constraints is the separation of duties which reduces fraud by not allowing any individual to have authority within the system to perpetrate fraud. RBAC model is good for the security requirement of cloud applications. However, in literature the challenge has been how to develop a robust RBAC framework that will handle the complex security needs of cloud computing. [14] Reported the implementation of a RBAC system for the web. Other RBAC implementation has been developed which include TrustedWeb, getAccess and SESAME. I-RBAC (Intranet Role Based Access Control). [15], used software agent to differentiate between local role and global role hierarchy on the intranet. The shortcoming of I-RBAC is the difficulty of maintaining information about the roles as numbers of role increases.

In figure 1, three primary rules are defined for RBAC: Role assignment, Role authorization and Permission authorization. A subject can exercise permission only if the subject has selected or been assigned a role. A subject's active role must be authorized for the subject. With role assignment, this rule ensures that users can take on only roles for which they are authorized. A subject can exercise permission only if the permission is authorized for the subject's active role. [16].

Figure 1 defined five elements of RBAC: User, Role, Permissions, Operation and Object. User is defined as human being. The concept of user can be extended to include machines, networks and so on. Role is a job function within the contest of an organization with some associated semantics regarding the authority and responsibility conferred on the user assigned to that role. Permissions are an approval to perform an operation on one or more RBAC protected objects. Operation is an executable image of the program, which upon invocation executes some function for the user or a specific function that depends on object while Object is anything that contains information that a user may need to access or an application that a user may need to employ.

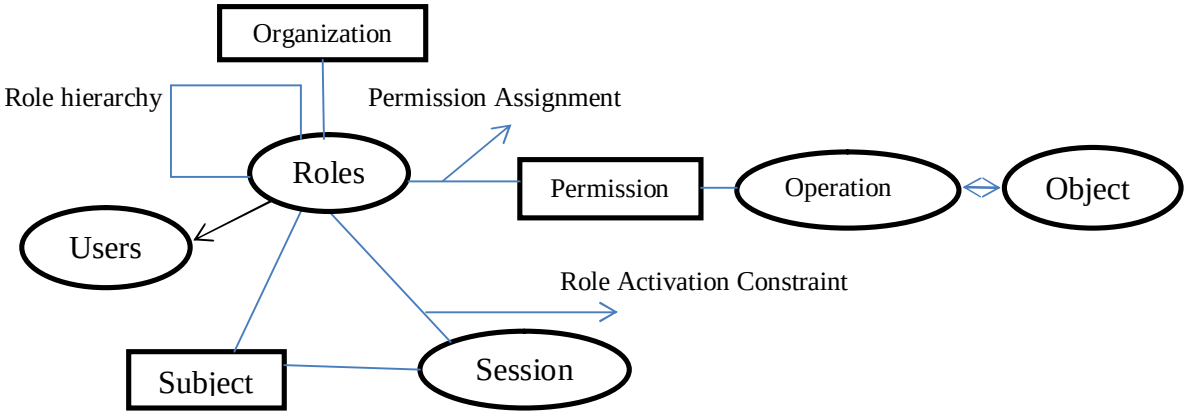

Fig 1: RBAC Model

Other related works in literature include [17] in their paper cloud computing security and challenges introduces a detailed analysis of the cloud computing security issues and challenges focusing on the cloud computing types and the service delivery types. They identified the following challenges which is associated with the current cloud computing. These challenges include security issues like data loss, phishing, and botnet. Other challenges include cost modelling, charging modelling, service level agreement, what to migrate and cloud interoperability. However most of these security issues raised in this paper have been addressed adequately. For instance the issues of data loss is now minimised with the advent of different cloud storage technologies. [18], in his work "A fine grain Role Based Access Control Framework" was able to include a feature that can securely handle large number of users, able to provide a secured authorization and authentication to users and also managed database easily with Eucalyptus paradigm of role and access management.

[19], in the dissertation Decentralizing Trust: New Security Paradigms for Cloud computing stated that, data computation integrity and security are the major challenges to be combated by for cloud users. The study enables us to see the high level of data mistrust which has cause loss of confidence in today's cloud centralisation and universal trust in all cloud's nodes rendering the clouds vulnerable to attacks. In order to resolve this anomaly the dissertation used five new paradigm (Hatman, Hadoop, Anonymous Cloud, Penny and Cloud cover) for decentralizing cloud trust relationship to ensure a robust cloud security, computation integrity, confidentiality labelling of data, ownership privacy, efficient validation, enforcement of security policy and data integrity. [16], in their paper Cross Bread Role based Access Control For Extended Security, introduced "A New Advanced RBAC Architecture" system that is a kind of ontology which can keep a backup of the data send to the cloud server and to put a restriction on the user per role. The ordinary RBAC do not place any restriction on the number of users per role, the existing system send data directly to the cloud without any backup which can lead to data security threat in case the data lost. But the new ontology based RBAC is a conceptualisation of structure in terms of relationship among the domain which is used to generate an agreed simple and understandable language for information exchange and role specification. The challenge here is that space required and utilization may double and challenges of maintaining generations of backed up data may be overwhelming.

IV. Design of a Modified Things Role Based Access Control

Things Role Based Access Control (T-RBAC) modifies RBAC in such a way that roles are assigned to both users and things on the cloud. Unlike the Cross Bread RBAC, T-RBAC does not put restriction on users per role. Roles can be assigned to things or users on request, however, permission needed to be obtained from the object owner before operation on the object is granted.

From fig 2, Things can be any device, procedure or human (with some biochip). Roles can be assigned to a user or things on the internet. Hence, a user or thing may be assigned a role. In addition permission shall be obtained from an object owner before such object is operated. This is in addition to other role activation constraints that may have been introduced. It only when these conditions are satisfied that a user or thing may be allowed to operate an object. For instance, the robotic circuit at home may need permission from the house owner to switch on the Air conditioner by 5.20pm in anticipation of his coming home by 6.pm. This permission may be in the form of an alert on the owners mobile or computer before the role is activated and the action completed. Different other scenario may involve a thing obtaining permission from other thing, a thing obtaining permission from a human user/ owner and a human user obtaining permission from a thing on the cloud.

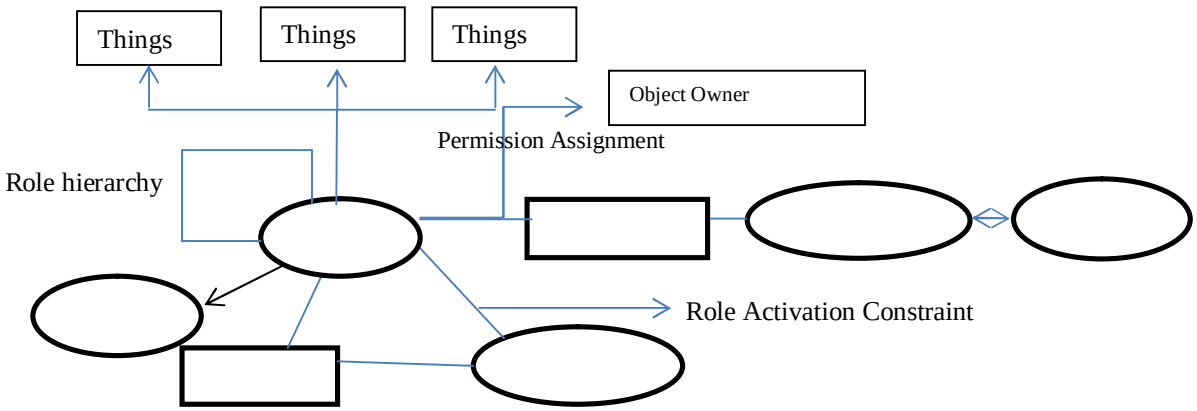

Fig 2: Design of T-RBAC

V. Conclusions

The importance of developments in cloud computing cannot be overemphasized. It is the future of internet applications. Utility computing will advance and become a common place infrastructure while internet of things will become a household concept with all equipment utilities in the offices, houses and cars are connected and controllable via internet and other devices. The implication of these on security on the internet and on these utilities is very high. Traditional security models fail at this juncture and this is why a new robust and intelligent security model like modified T-RBAC that will ensure that resources and utilities on such network are secured is needed. This is work in progress, T-RBAC shall be implemented and tested in both simulated environment and in real time.

References

[1] Zhenji Zhou1, Lifa Wu2 and Zheng Hong, Institute of Command Information System, PLA University of Science and Technology Nanjing, Jiangsu, China 1zhou_zhenji@163.com, 2wulifa@vip.163.com, 3hongzhengjs@139.com, International Journal of Grid and Distributed Computing, Vol.6, No.6 (2013).

[2] Habib, S.M. Ries and S. Muhlhauser,"Cloud Computing Landscape and Research Challenges Regarding Trust and Reputation" in Ubiquitous Intelligence & Computing and 7th International Conference on Autonomic & Trusted Computing (UIC/ATC), Oct. 2010, pp. 410-444.

[3] (Software as a Service (SaaS), 2006). [Accessed 04-25-2015]

[4] Halton G., Deepak S., (2009), "Cloud Computing Essay", [Accessed 12-04-2010]: http://www.scribd.com/doc/23743963/Cloud-Computing-Essay.

[5] Gil V., Redero M., and Vaquero L. (2010), "Infrastructure Delivery to Service Management in Clouds Future Gener Comput Syst 26(8):1226-1240.

[6] Dans E., (2011), "Benefits and Disadvantages of Cloud Computing", [Accessed 03-14-2011]:http://algramrandomramblings.blogspot.com/2011/01/benefits-and-disadvantages-of- cloud.html .

[7] Ali Asghary Karahroudy, Security Analysis and Framework of Cloud Computing with Parity-Based Partially Distributed File System, July 2011.
[8] James B. D. Joshi, Walid G. Aref, and Eugene H. Spafford, Security Models Web-Based Application. Proceeding of Communication of ACN, February 2001/Vol. 44 no.2. Kuhn D.R, Coyne E.J.,. Weil T.R, "Adding Attributes to Role Based Access Control", *IEEE Computer*, vol. 43, no. 6 (June, 2010), pp. 79-81.
[9] Sandhu, R. Lattice-based Access Control models. IEEE Computer 26. 11 (1993).Proceeding of the Fifth ACM Workshop on Role-based Access Control, Berlin, Germany, July, 2000.
[10] Ferraiolo D.F. and Kuhn D.R. (1992) "Role Based Access Control" 15th National Computer Security Conference, Oct 13-16, 1992, pp. 554-563.
[11] Sandhu R., Ferraiolo D.F., and Kuhn, R. (2000), "The NIST Model for Role Based Access Control: Toward a Unified Standard," Proceedings, 5th ACM Workshop on Role Based Access Control, July 26-27, 2000, Berlin, pp.47-63 – first public draft of the NIST RBAC model and proposal for an RBAC standard.] rbac-info@nist.gov Proceeding of 5th ACM workshop on RBAC, 2000).
[12] Ferraiolo, D.F., Barkley, J.F., and Kuhn, D.R., A role-based Access Control model and reference implementation within a corporate intranet. ACM Trans. Info Syst. Security 2, 1(Feb. 1999), 34-64Gil P., (2010), "What is Cloud Computing", [Accessed 01-22-2011]: http://netforbeginners.about.com/od/c/f/cloudcomputing.htm
[13] Tari, Z., and Chan, S. A role-based access control for intranet security. IEEE Internet Computing (Sept-Oct. 1997), 24-34.
[14] Parminder Singh1, Sarpreet Singh2, Cross Bread Role based Access Control for Extended Security At Azure in Cloud Computing, International Journal of Application or Innovation in Engineering & Management (IJAIEM) Web Site: www.ijaiem.org Email: editor@ijaiem.org, editorijaiem@gmail.com Volume 2, Issue 2, February 2013 ISSN 2319 - 4847 Volume 2, Issue 2, February 2013 Page 206.
[15] Kuyoro S. O., Ibikunle F., & Awodele O., Cloud Computing Security Issues and Challenges International Journal of Computer Networks (IJCN), Volume (3): Issue (5): 2011.
[16] Shefali Modi., Design A Fine Grain Role Based Access Control Framework For Cloud Computing, submitted to B.S. Punjab Technical University, 2005.
[17] Khan 2013, "Decentralizing Trust: New Security Paradigms for Cloud Computing", University of Texas at Dallas Richardson, TX, USA, ISBN: 978-1-303-63341-6.

