International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 2 436 - 439

A Review on Identity and Access Management for Multitier Cloud Infrastructure by using Kerberos

Mr. Merajul Haque Farooqui
Department of Computer Science & Engineering
J D College of Engineering and Management
Nagpur, India
merajcomp@gmail.com

Prof. Kemal U. Koche
Department of Computer Science & Engineering
J D College of Engineering and Management
Nagpur, India
kemalkoche@yahoo.com

Abstract- In this paper presents a novel architecture to manage identity and access (IAM) in a Multi-tier cloud infrastructure, over the Internet the most services are supported by massive-scale data centres. To provide resources in different tire, Multi-tier cloud infrastructure uses tier-based model from Software Engineering. In this paper we focus on authentication and security of centralized identity and access management system for the multitier cloud infrastructure. By using the Kerberos algorithm we provide the authentication to the identity and access (IAM) in a Multi-tier cloud infrastructure.

Keywords-*cloud computing,Identitity and access management,Secure Authentication for multi-tier cloud.*

*****

I. INTRODUCTION

Cloud computing has promoted the hosting and delivery of services over the Internet and the movement of computation and data from terminal devices and local servers to core data centers due to advantages in flexibility, scalability, and economics of savings [1]. Most services have been supported by massive-scale distant datacenters located at sites. However, some services will require low latency (e.g. alarms in smart grids, safety applications in transportation, monitoring in remote health, fire or emergency alarms in smart cities), the processing of large volumes of local information (e.g. In lecture rooms a video capturing), or intelligent converged network provides high security and at the edge of the network computing, for example in the premises of traditional telecom service providers.

The Smart Applications on Virtual Infrastructure (SAVI) project has been established with a focus on future application platforms designed for applications enablement [2]. As shown in Figure 1, SAVI considers a multi-tier cloud infrastructure to include Smart Edges where local players work together with remote massive-scale data centers to provide better Quality of Service (QoS) for sensitive the application. The hypothesis is investigated by the SAVI that all computing and networking resources can be virtualized and managed using Infrastructure-as-a-Service (IaaS). The Smart Edge should go beyond conventional cloud resources to address QoS demanding applications such as video distribution, wireless access controls, secure and fast communication etc. In other words, the Smart Edge will be heterogeneous data centres including line rate processors, graphical processors, reconfigurable hardware, and crucially future highly programmable networking equipment, specialized hardware accelerators.

The Global Environment for Network Innovations (GENI) [3], which provides a virtual laboratory for networking and distributed systems research and education, is another multitier cloud and networking infrastructure but with a different view. Unlike SAVI which is looking for a unified management layer,

GENI intends to federate a variety of testbeds or resource providers with different control and management planes. GENI provides a wrapper in front of a set of testbed suits or resource aggregators to provide unified APIs for users, while maintaining their independence. Users can allocate slices in different testbeds by joining to one of the organizations in GENI. GENI can be considered as a community cloud.

While the benefits of cloud computing is clear, security is a severe concern in these infrastructures. Kandukari et a.[4] considers five cloud security issues that should be included in a Service Level Agreement. There are the following: privileged user access, data location, data segregation, data disposal and investigation and protective monitoring. Privileged user access ensures only authorized users have access to an organization data and resources. Therefore, identity and access management is considered as a security concern in cloud computing. Various models have been proposed to address identity management in clouds, such as central IAM, trusted third party, federation solutions, etc. Most of solutions are mainly focused on federation of cloud providers, and pay less or no attention to access management.

II. RELATED WORK

The A. Jøsang and S. Pope, was proposed User centric identity management [5]. in this this paper describes an appearing approach, known as user-centric identity management, that focuses on usability and cost effectiveness from the users' perspective, and this is also compatible with conventional identity management models.

For being SP centric, traditional identity management systems have largely ignored that it is often equally important for the users to be able to recognize service providers, as it is for service providers too many authenticate user. In case of online service provision through the web, user authentication typically takes place on an application layer; SP authentication occurs on the transport layer through SSL protocol.

However, the common scam called password phishing illustrates the difficulty of service provider authentication with SSL. The practice is committed by attackers posing, for example, as online banks and sending out spam email to people asking them to log on to false, but genuine looking web sites, which allows the attackers to "phish" identifiers and passwords from unsuspecting users. The problem is not to due to weak authentication techniques; however it is due to poor usability of current SSL security model. Although strong cryptographic mechanisms are being used, it can be difficult for users to know which SP identity has been authenticated. In Improved usability, not build up cryptography is needed in order to strengthen users' ability to authenticate service providers in Web interactions.

Gunjan et al. [7] compiled a list of available technologies and solutions for cloud computing, including Primary and Identity Management for Europe (PRIME), Windows CardSpace, OpenID, Higgins, and Liberty Alliance. Academic research has concentrated on cloud-based IAM security issues entity's identity, which helps the SP to decide whether to permit the entity to use a service or not provided for the developers to write programs or build applications on it rather than doing it using their own infrastructure. For ex- Google App Engine and Microsoft Azure services. In IaaS model, users can provision servers, storage and other computing resources on demand without bothering about their maintenance, security etc which is being taken care of by the service providers. For ex- Amazon Elastic Compute Cloud (EC2) and Amazon Simple Storage Service (S3).It is attractive because of its perceived economic and operational benefits. In spite of the fact that it offers great value and opportunity for organizations, several surveys of potential cloud adopters indicate security and privacy as the number one concern delaying its adoption [8]. Various approaches and models have been proposed for addressing identity management in cloud computing. The approaches include user centric IDM in place of traditional application centric model, use of trusted third parties in identifying users, identity federation solutions, protection of Identity information without Trusted Third Party etc.

The Mohammad Faraji, Alberto Leon-Garcia, Joon-Myung Kang, and Hadi Bannazadeh were proposed a new architecture to manage identity and control access to resources in a multi-tier cloud infrastructure [9]. First, we discuss system requirements, and then we propose architecture to address these requirements. Our architecture comprises two major components: middleware and central IAM to manage user and infrastructure related data. Middleware sits in front of a resource provider and handles time-consuming decision making such as authentication and authorization, while the repository handles data manipulation. We deploy performance enhancing techniques to boost middleware and repository performance while using load balancing to make it scalable.

ExoGENI IAM leverages Shibboleth to be federated with other infrastructure and cloud provider they presents a trust framework for federated community clouds, combining these common elements with a general trust management system incorporating logic-based authorization and inference[15]. Their solution is suited to the needs of federated multi-provider systems that serve user communities spanning multiple organizations. One example of such a system is NSF's GENI initiative (Global Environment for Network Innovation), a suite of infrastructure to support research in network science and engineering. Their approach was developed with support from GENI and NSF's Trustworthy Computing program, and has been adopted in the GENI architecture. GENI contributes multiple providers offering diverse virtual infrastructure services or other virtual resources. They illustrate the trust system by describing a prototype implementation developed for initial use within the ExoGENI testbed [3] was being deployed for GENI. ExoGENI is a network of cloud provider sites privately administered clouds based on OpenStack software on multiple campuses, linked using network circuit fabrics and the ORCA control framework [2].

III. PROPOSED WORK

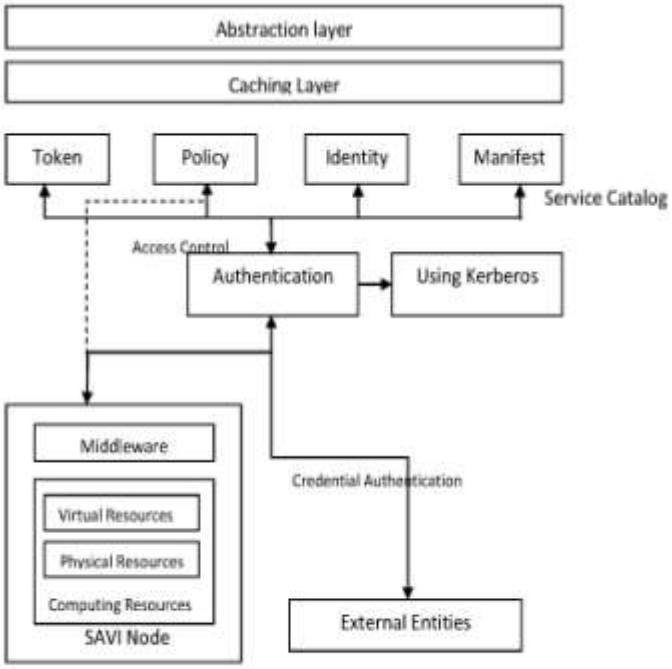

Fig. IAM Architecture

We have developed an IAM solution for the multi-tier infrastructure such as SAVI testbed. SAVI Testbed main entities include a SAVI TB Control Centre, Core Nodes, Edge Nodes, and a SAVI network. Core and Edge nodes contain resources that are used for creating applications. The SAVI TB Control Centre hosts SAVI control and management functions including resource allocation, clearing house, monitoring and measurement, and so on. The SAVI IAM system located in the SAVI Control Centre, and asserts identities about users, applications, and threads of execution that can be called an entity.

We have designed and implemented SAVI IAM to address the requirements in the previous section. The SAVI IAM is a central identity manager with distributed middleware based on IdP/SP model and comprised of 6 basic components: Manifesting Management, Identity Management, Token Management, Policy Management, Middleware and Authentication Management. Figure illustrates the architecture.

IV. CONCLUSION

In this paper, we have introduced security to a novel architecture for a cloud-based IAM by using Kerberos. The architecture uses a central IAM and decentralized middleware to carry out IAM duties. The main features of this architecture are scalability, adaptability. In the future, we plan to study federation to enable bursting in other cloud providers.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," Commun. ACM, vol. 53, no. 4, pp. 50–58, Apr. 2010. [Online]. Available: http://doi.acm.org/10.1145/1721654.1721672

[2] J.-M. Kang, H. Bannazadeh, and A. Leon-Garcia, "Savi testbed: Control and management of converged virtual ict resources," in Integrated Network Management (IM 2013), 2013 IFIP/IEEE International Symposium on. IEEE, 2013, pp. 664–667.

[3] T. Anderson and M. K. Reiter, "Geni: Global environment for network innovations distributed services working group," 2006.

[4] B. Kandukuri, V. Paturi, and A. Rakshit, "Cloud security issues," in Services Computing, 2009. SCC '09. IEEE International Conference on, 2009, pp. 517–520.

[5] A. Jøsang and S. Pope, "User centric identity management," in AusCERT Asia Pacific Information Technology Security Conference. Citeseer, 2005, p. 77.

[6] P. Angin, B. Bhargava, R. Ranchal, N. Singh, L. B. Othmane, L. Lilien, and M. Linderman, "An entity-centric approach for privacy and identity management in cloud computing."

[7] K. Gunjan, G. Sahoo, and R. Tiwari, "Identity management in cloud computing–a review," International Journal of Engineering, vol. 1, no. 4, 2012.

[8] R. Gellman;Privacy in the Clouds:Risks to Privacy and Confidentiality from Cloud;World Privacy Forum;2009.

[9] M. Faraji, Joon-Myung Kang, Hadi Bannazadeh, and Alberto Leon-Garcia," Identity Access Management for Multi-tier Cloud Infrastructures", 2014 IEEE

[10] Daniele Catteddu, Giles Hogben, (ENIS report) "Cloud Computing: Benefits,risks and recommendationsfor information security". (http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-riskassessment/ at_download/fullReport)

[11] X. Huang, T. Zhang, and Y. Hou, "Id management among clouds," in Future Information Networks, 2009. ICFIN 2009. First International Conference on. IEEE, 2009, pp. 237–241.

[12] H. Y. Huang, B. Wang, X. X. Liu, and J. M. Xu, "Identity federation broker for service cloud," in Service Sciences (ICSS), 2010 International Conference on, 2010, pp. 115–120.

[13] H. Koshutanski, M. Ion, and L. Telesca, "Distributed identity management model for digital ecosystems," in Emerging Security Information, Systems, and Technologies, 2007. SecureWare 2007. The International Conference on. IEEE, 2007, pp. 132–138.

[14] J. Chase, L. Grit, D. Irwin, V. Marupadi, P. Shivam, andA. Yumerefendi, "Beyond virtual data centers: Toward an open resource

[15] T. F. Steve Schwab, "Managing identity and authorization for community clouds," Duke University, Tech. Rep., 2012. [Online].

[16] Available: www.exogeni.net/ [13] P. Liu, S. Jajodia, and C. D. McCollum, "Intrusion confinement by isolation in information systems," Journal of Computer Security, vol. 8, 2000.

[17] N. Gunti, W. Sun, and M. Niamat, "I-rbac: Isolation enabled role-based access control," in Privacy, Security and Trust (PST),

2011 Ninth Annual International Conference on, 2011, pp. 79–86.

[18] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Rolebased access control models," Computer, vol. 29, no. 2, pp. 38–47, Feb. 1996. [Online]. Available: http://dx.doi.org/10.1109/2.485845

[19] G.-J. Ahn and R. Sandhu, "Role-based authorization constraints specification," ACM Trans. Inf. Syst. Secur., vol. 3, no. 4, pp. 207–226, Nov. 2000. [Online]. Available: http://doi.acm.org/10.1145/382912. 382913

[20] A. H. Karp, H. Haury, and M. H. Davis, "From abac to zbac: the evolution of access control models," Hewlett-Packard Development Company, LP, vol. 21, 2009.

[21] N. Dan, S. Hua-Ji, C. Yuan, and G. Jia-Hu, "Attribute based access control (abac)-based cross-domain access control in service-oriented architecture (soa)," in Computer Science Service System (CSSS), 2012 International Conference on, 2012, pp. 1405–1408.

[22] S. Hai-Bo, "A semantic- and attribute-based framework for web services access control," in Intelligent Systems and Applications (ISA), 2010 2nd International Workshop on, 2010, pp. 1–4.

[23] X. Zhang, S. Oh, and R. Sandhu, "Pbdm: a flexible delegation model in rbac," in Proceedings of the eighth ACM symposium on

[24] Access control models and technologies, ser. SACMAT '03. New York, NY, USA: ACM, 2003, pp. 149–157. [Online]. Available: http://doi.acm.org/10.1145/775412.775431

[25] J.-M. Kang, H. Bannazadeh, and A. Leon-Garcia, "SAVI testbed: Control and management of converged virtual ICT resources," in IFIP/IEEE International Symposium on Integrated Network Management (IM 2013), Ghent, Belgium, 2013, pp. 664–667.

[26] O.Foundation,"Openstack keystone architecture, "http://docs.openstack. org /developer/keystone/.