Role Based Access Control Design for Indonesian E-Health Cloud

Moh. Kresna Widyahanto[1], Sri Chusri Haryanti[2], Sri Puji Utami Atmoko[3], Rosini[4]
[1]moh.kresna@student.yarsi.ac.id, [2]sri.chusri@yarsi.ac.id, [3]puji.atmoko@yarsi.ac.id, [4]rosini@yarsi.ac.id
Informatics Department, Faculty of Information Technology, Universitas YARSI

Abstract

Access control is a critical issue in cloud provisioned multi-tenant healthcare systems in order to protect information against unauthorized access. Indonesian e-Health community cloud is a multi-tenant cloud consist of hospitals in Indonesia. Hospitals that have better human resources, equipment, and infrastructures are responsible for providing and managing cloud resources. Meanwhile, other hospitals with a lack of resources commit as users in the cloud. In this research, we design policy and access control for Indonesian e-Health community cloud based on hospital type and roles. Finally, we implement the design in the Amazon cloud.

Keywords: access control, e-health cloud, role based

Implementation

We applied the access control design in Amazon Web Services (AWS). Type A hospitals serve as root administrator.

Indonesian e-health cloud model

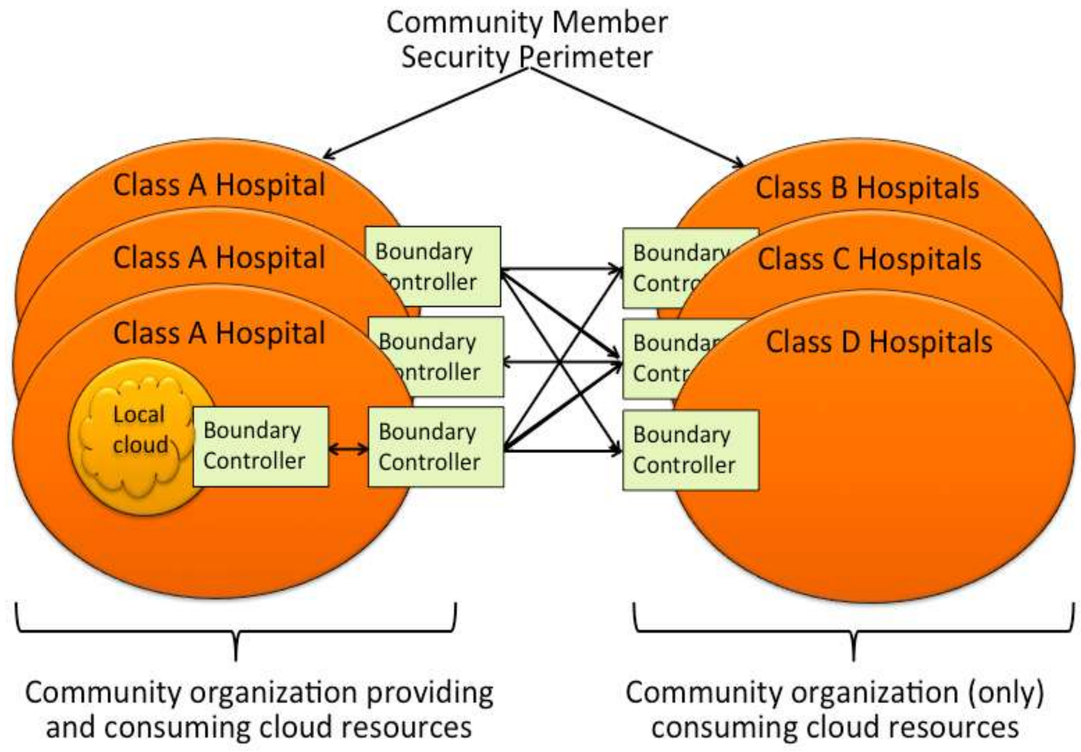

Figure 1. Indonesian e-Health Community Cloud Model

The e-Health Cloud Model for Indonesia is seen in Figure 1. The type A hospitals provide and consuming cloud resources, because they have adequate infrastructure and better human resources compare to type B, C and D.

Access Control Design

Table 1. Policy of access control based on hospital type and role

Hospital Type	Policy								
	Image files Bucket			Medical Record Bucket			Administrative Bucket 3		
	Get	Put	Del	Get	Put	Del	Get	Put	Del
Type A	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed
Type B	Allowed	Allowed		Allowed	Allowed		Allowed	Allowed	Allowed
Type C	Allowed			Allowed			Allowed	Allowed	
Type D	Allowed			Allowed			Allowed	Allowed	

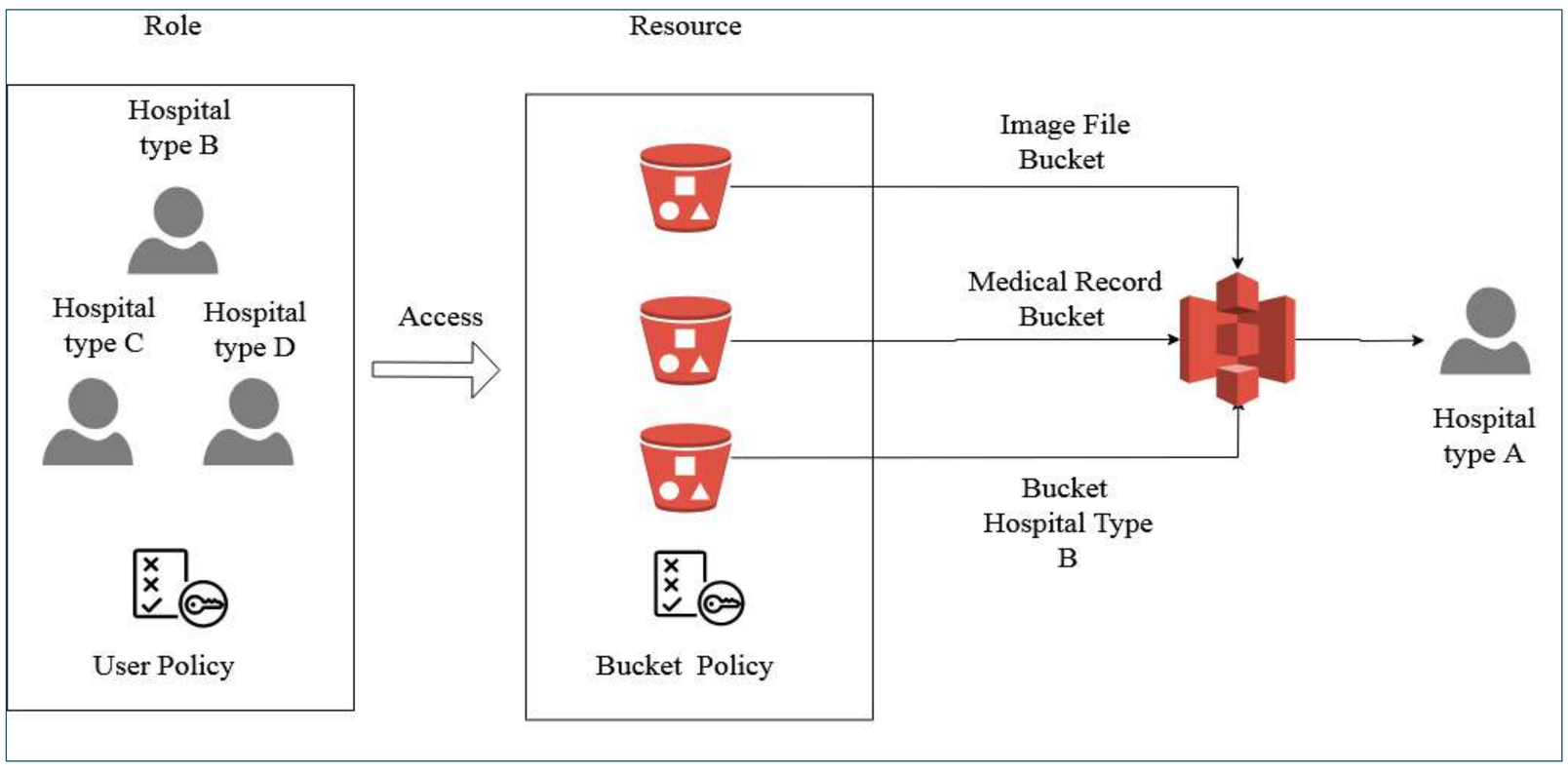

Figure 2. Role based access control architecture

Future Works

Role-based access control design for Indonesian e-Health Community Cloud Model in this research is still very modest design.

For further research, the design will take into consideration of hierarchical access of users and more detail roles of each type of hospitals.

It also needs performance testing to prove the security of the proposed design.

References

1. Haryanti, S. C., Pradipta, A., Atmoko, S. P. U., Rachmawati, U. A., Suhartanto, H. (2017). Indonesian E-Health Community Cloud. Poster, SEAIP 4-8 December 2017, Taiwan.
2. Wu, R., Zhang, X., Ahn, G. J., Sharifi, H., & Xie, H. (2013). Design and Implementation of Access Control as a Service for IaaS Cloud. Science, 2(3), 115–130.
3. Younis, Y. A., Kifayat, K., & Merabti, M. (2014). An access control model for cloud computing. Journal of Information Security and Applications, 19(1), 45–60. https://doi.org/10.1016/j.jisa.2014.04.003
4. Dašić, P., Dašić, J., & Crvenković, B. (2016). Applications of access control as a service for software security. International Journal of Industrial Engineering and Management, 7(3), 111–116.
5. Chen, D., & Zhao, H. (2012). Data security and privacy protection issues in cloud computing. Proceedings - 2012 International Conference on Computer Science and Electronics Engineering, ICCSEE 2012, 1(973), 647–651.

Acknowledgment

Funded through a grant from the Indonesian Ministry of Research, Technology and Higher Education, No. SP DIPA-042.06.1.40156/2018-contract No. 014/INT/UM/WRII/UY/V/2018.