IJCSN - International Journal of Computer Science and Network, Volume 8, Issue 5, October 2019
ISSN (Online) : 2277-5420
www.IJCSN.org
Impact Factor: 1.5

Improved Hierarchical Role Based Access Control Model for Cloud

Navod Thilakarathne

Department of Industrial Management, Faculty of science
University of Kelaniya
Srilanka

Abstract - Cloud computing is considered as the one of the most dominant paradigm in the field of information technology which offers on demand cost effective services such as Software as a service (SAAS), Infrastructure as a service (IAAS) and Platform as a service (PAAS).Provisioning all these services as it is, this cloud computing associates with number of challenges such as data security, abuse of cloud services, malicious insider and cyber-attacks. Among all these security requirements of cloud, access control is the one of the prominent requirement in order to avoid unauthorized access to data stored in the cloud. Main objective of this research is to review the existing methods of cloud access control models and their variants pros and cons and to identify further related research directions for developing an improved access control model for cloud data storage. We have presented detailed access control requirement analysis for cloud computing and have identified important gaps, which are not fulfilled by conventional access control models. As the final outcome of the study we have come up with an improved access control model with hybrid cryptographic schema and hybrid cloud architecture and practical implementation of it. Finally we have tested our proposed model for security implications, performance, functionality and data integrity to prove the validity. We have used advanced encryption standard (AES) which is a private key algorithm and Rivest–Shamir–Adleman (RSA) public key algorithm to implement the cryptographic schema and used public and private cloud to enforce our access control security and reliability. By validating and testing we have proved that our model can withstand against most of the cyber-attacks in real cloud environment. Thus it has improved capabilities compared with other previous access control models that we have reviewed through the literature.

Keywords *– Public cloud data storage, Hybrid cloud, Hybrid cryptographic schema*

1. Introduction

Cloud computing is one of the major and dominate technology that paves the way for digital transformation across the globe. It is a model for providing convenient on demand network access for computing resources such as applications, services, servers and storages that can be rapidly provisioned and released with minimal management effort or service provider interaction [2].Cloud has a lot of advantages mainly in ubiquitous services where everybody can access computing services through the internet. This cloud model composed of three service delivery models mainly Software as a service, Platform as a service and Infrastructure as a service. Depending on the type of the data that you are working with, cloud computing come in three forms. Public cloud, Private cloud and the Hybrid cloud. Along with the rapid steady development of the cloud applications cloud computing cyberattacks are also increased and cloud itself create a good attacking surface for hackers. [3] Denial of Service attacks (DOS attacks), Authentication attacks, Side channel attacks, Cryptographic attacks and Malicious insider attacks are best attack vectors for those hackers and due to these generalized attacks we need a better security reinforcement for cloud computing as it can lead to a major breach. Due to this reason there are number of security challenges associated with utilizing cloud computing such as data security, abuse of cloud services, malicious insider and cyber-attacks. [1]

In conclusion cloud access control is one of the fundamental requirements in order to avoid unauthorized access to system [7] and organizational assets and cloud access control models can be categorized into Discretionary access control (MAC), Mandatory access control (DAC) and Role Based Access Control (RBAC).In the Discretionary access model ,the administrator of the objects who is the owner of the data decides its access permissions for users based on an access control list and in the Mandatory access control model access permissions are decided by the administrator of the system. In the Role-based access control model, a user has access to a resource based on his/her assigned role in the system [5] Roles are defined based on job functions and permissions are defined on authority and responsibilities of the job. Operations on the resources are invoked based on the permissions. [8] Role Based Access Control model is more scalable than the Discretionary and Mandatory access control models, and more suitable for use in cloud computing environments [4].In summary Role based

Copyright (c) 2019 International Journal of Computer Science and Network. All Rights Reserved.

access control has many advantageous compared MAC and DAC yet it has own difficulties when it's deployed in real cloud environment that can be further enhanced. [6] Based on the literature review we have identified what are the potential loopholes in existing methods and identified Role based access control model can be further improved with cryptographic schema and a hybrid cloud architecture [9] where we can provide resilient layered security to protect the cloud data.

2. Methodology

A thorough Literature Survey has been done to find out the potential gaps and the features that are not available in the existing access control mechanisms. Based on the literature we have identified Hierarchical RBAC access control model to be improved with hybrid cloud architecture *(combination of public and the private cloud)* and hybrid encryption schema (*AES -128 bit symmetric key algorithm and RAS 1024 bit public key encryption*).Our proposed model uses AES for encrypting and decrypting public cloud data and RSA public key encryption algorithm is used to encrypt the secret key generated by the AES cryptographic algorithm.

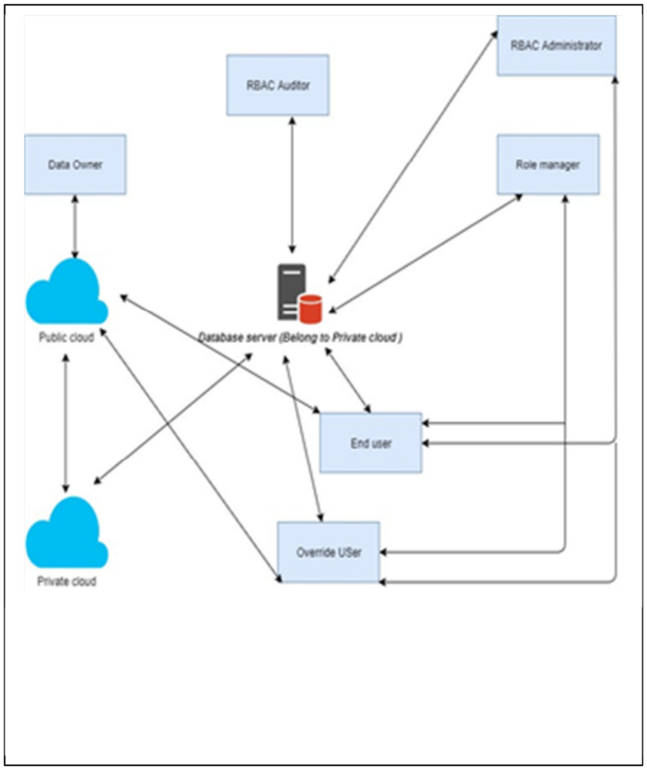


Fig 1 Architecture of our proposed access control model

As depicted in figure 1, proposed architecture of the access control model comprised of Public Cloud, Private Cloud, System Administrator, Role Manager, Data Owner, End User, and Override User.

Public information are encrypted using symmetric AES algorithm which will be saved in the public cloud. The organizations stores only critical and confidential information in the private cloud. Private cloud is built on an internal data center that is hosted and operated inside the organization. The amount of information stored in private cloud is relatively smaller when compared to public cloud. Administrator of role based system provides authentication to end users. End users are just to access data from cloud. They cannot do any modifications or updates the original data. They cannot communicate directly with the private cloud as they do not possess access permission and don't have a direct affiliation with the private cloud. Administrators generate the system parameters. System parameters represent the position of the role and finally they are getting stored in the private cloud. Also administrators manages role hierarchy. Role manager will be there for manage roles for users. According to the role and authorization from the role manager, user gets access permission to cloud data. The access policies related to user authorization and roles are stored in private cloud.

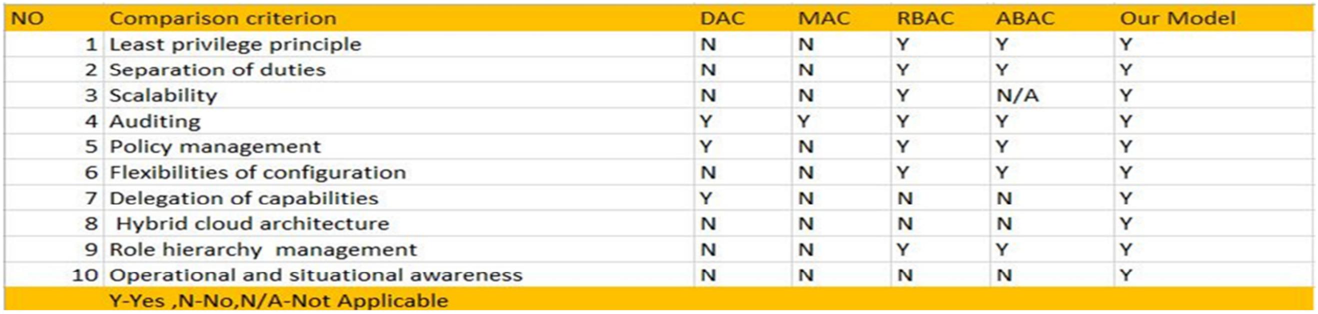
3. Results

We have implemented the proposed model in C#, ASP.NET web development language, using Visual Studio 2017 IDE and for the public cloud we have taken an instance from Microsoft azure. Testing and validation done on Microsoft Azure instance that has a single core, 1.75G Ram with a 10 GB storage. For the implementation on the private cloud we have chosen a SQL server instance from the Microsoft Azure with inbuilt firewall with 50 MB storage. (SQL Server database as a service). For the public cloud we have deployed our developed model on to the Microsoft Azure as an App service.

After successful implementation, we have tested our model for performance, data integrity, security implications and functional analysis. From the performance testing we conclude that encryption time took more time than decryption time and we can see when the file size increases both the encryption and decryption time are gradually increasing. For the Data integrity testing we have compared and verified MD5, SHA-1, SHA-256 and SHA-512 values for both original file and the decrypted downloaded file and both types of files have the same values when testing for data integrity. Thus we conclude that the file integrity of resources was preserved during encrypting and decrypting which enforce the reliability and the integrity of our access control model.

Copyright (c) 2019 International Journal of Computer Science and Network. All Rights Reserved.

We have performed three vulnerability assessment phases to compare and validate our model in real cloud environment followed by initial reconnaissance, port and service scanning and vulnerability analysis. Results from these three tests have showcased that our access control model withstand against most of the cyber-attacks. Further for functional testing we have compared our access control model with conventional access control models for cloud, based upon the functionality that our model and those models can offer as depicted in figure 2.



NO	Comparison criterion	DAC	MAC	RBAC	ABAC	Our Model
1	Least privilege principle	N	N	Y	Y	Y
2	Separation of duties	N	N	Y	Y	Y
3	Scalability	N	N	Y	N/A	Y
4	Auditing	Y	Y	Y	Y	Y
5	Policy management	Y	N	Y	Y	Y
6	Flexibilities of configuration	N	N	Y	Y	Y
7	Delegation of capabilities	Y	N	N	N	Y
8	Hybrid cloud architecture	N	N	N	N	Y
9	Role hierarchy management	N	N	Y	Y	Y
10	Operational and situational awareness	N	N	N	N	Y
	Y-Yes ,N-No,N/A-Not Applicable					

Fig 2 Functional analysis and testing

4. Conclusion

The main objective of this research was to come up with an improved access control model, that can be utilize in cloud and also that can be utilize for secure cloud data storage. Before proposing our model we have reviewed almost every access control model in cloud and none of the researches were targeted about the security implications of access control in real cloud computing environment. We have showed the experimental results of our implemented access control model through the perspective of performance, data integrity and security in real cloud environment. We observed that time taken for encryption and decryption is efficient on public cloud and maintaining data storage in public cloud is efficient as it is highly scalable, cost effective and provides redundancy for the organization data. Further we observed that original and decrypted data after encryption was same, while checking for data integrity thus it will enhance the reliability and assurance of our model. From the security perspective we have observed that it’s not vulnerable to exploit and hence it provide the reliability and security for our access control model.

We believe that the proposed model is useful in various commercial and non – commercial situations as it implements the hierarchical cryptographic role based access control policies based on the job functionality and user requests in an organization for providing secure data storage in the real cloud environment which enforces hybrid cryptographic techniques for providing security for underlying data along with hybrid cloud architecture.

References

[1] Aditya, k., & Ashish, D. (2013). Cryptographic Role-Based Access Control for Secure Cloud Data Storage.

[2] Bibin, K. (2013). Access Control in Cloud Computing International Journal of Scientific and Research Publications Volume 3, Issue 9, September 2013.

[3] Faisal, M., & Aranganathan, S. (2015) Secure Access Control Requirement Analysis in Cloud Computing “Volume 3, Issue 3, March 2015.

[4] Natarajan, M. (2011) Review of Access control models for cloud computing Jackson State University, 1400 Lynch St, Jackson, MS, USA 2011.

[5] Younis,A ., Kashif, Kifayat., & Madjid , M.(2014) An access control model for cloud computing journal of information security and applications 2014.

[6] Lan Zhou,Vijay Varadharajan,, Michael Hitchens “Trust Enhanced Cryptographic Role-based Access Control for Secure Cloud Data Storage” 2015.

[7] Punithasurya K , Jeba Priya S “Analysis of Different Access Control Mechanism in Cloud ” International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868Foundation of Computer Science FCS, New York, USA Volume 4– No.2, September 2012.

[8] Parminder Singh , Sarpreet Singh “ A New Advance Efficient RBAC to Enhance the Securit in Cloud Computing “ International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 6, June 2013.

[9] Bokefode Jayant D ,Ubale Swapnaja A,Pingale Subhash V,Karande Kailash J,Apate Sulabha S “ Developing Secure Cloud Storage System by Applying AES and RSA Cryptography Algorithms with Role based Access Control Model” Volume 118– No.12, May 2015

Copyright (c) 2019 International Journal of Computer Science and Network. All Rights Reserved.