ISSN 2320 2610
Volume 3, No.5, September- October 2014
International Journal of Multidisciplinary in Cryptology and Information Security
Available Online at http://warse.org/pdfs/2014/ijmcis01352014.pdf

Enhancing the secure data transfer under private cloud by using an proposed architecture of Orthogonal Handshaking Authentication Protocol (OHSAP)

M.Mohamed Sirajudeen[#1], Dr.K.Subramanian[#2]

[#1] Department of Computer Science, J.J College of Arts and Science, Pudukottai.{mdsirajudeen1@gmail.com}
[#2] Department of Computer Science, J.J College of Arts and Science, Pudukottai.{subjjcit@gmail.com}

ABSTRACT

Cloud computing technology is the modern trend in the information technology era. In general, the word computing gives a meaning of evolution of an existing IT infrastructure that provides a long-dreamed vision of computing as a utility for the existing resources. The rapid development of the cloud services and its technology to play an inevitable role in the profit centric organizations. Now-a-days more number of business firms utilizes the cloud services in an effective and efficient manner. Due to the more concern on the data transaction conducted by the business organizations as well as more number of government organizations bring an question mark for the security. The way of data transaction for cloud computing under different cloud models (such as Private, Public, Hybrid, Community …).There will be a mechanism to protect the data under each cloud by different security as well as authentication algorithm. In this paper, mainly focus on the security mechanism data transaction under the private cloud by applying a special kind of cryptographic authentication algorithm named as Orthogonal Handshaking Authentication Protocol (OHSAP). After the careful investigation reported by different private and government sector [1], the architecture for OHSAP will be proposed and discussed in this research architecture.

Key words: Cloud, security, orthogonal and authentication.

1. INTRODUCTION

The utilization of existing services or recourses usually an agreement between the service provider and the consumer.

A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models. The importance of cloud computing and its adoption can be best described in terms of its underlying characteristics, delivery and deployment models, how customers can use these services, and how to provide them securely. Cloud computing consists of three delivery models, four deployment models and five characteristics [1].

These models and characteristics lie on the top of each other, thereby forming a stack of a cloud. The three delivery models of cloud computing environment are: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) [1]. Infrastructure-as-a-Service [IaaS] can be defined as virtual machines on demand, where users benefit from networking infrastructure facilities, computing services, and data storage. Amazon and Rackspace are leading vendors for IaaS platforms. PaaS is built on the top of IaaS, from where end-users can run their custom applications using their service providers' resources. Examples of PaaS are App Fog, Google App etc. SaaS is build on the top of PaaS which provides delivery of business applications designed for a specific purpose. SaaS comes in two distinct modes named simple multi-tenancy and fine grained multi-tenancy. An example of SaaS is the SalesForce.com CRM application. These delivery models reside at the second layer of cloud stack. In terms of deployment models, cloud computing platform includes public cloud, private cloud, community cloud, and hybrid cloud. Public clouds are predominantly owned by large scale organizations and services owned by this cloud are made available to the general public or a broad industry group.

Private cloud is owned solely by one organization and is available for a particular group, while community cloud is shared and managed by the particular organization and supported by the specific community that has shared concern. Hybrid cloud is composed of two or more clouds (private, public, and community). These deployment models reside at the third layer of a cloud stack. The five characteristics of each cloud are: location-independent resource, pooling, on-demand self-service. The above discussion of the delivery and deployment models is depicted by the following figure 1.

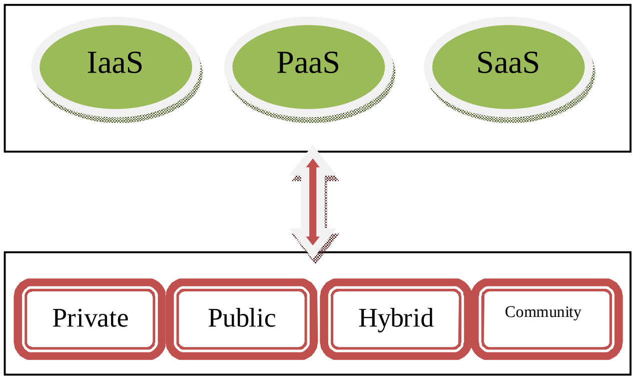


Figure 1. Delivery and Deployment models of cloud

2. RELATED WORK

Cloud Computing helps the service provider to switch over from the traditional data center infrastructure to the modern data datacenters in order to ensure more secure transaction between the service provider and the consumer. Despite its advantages, like on demand service, pay-as-you-go, resource allocation, etc, there exist critical security related vulnerabilities within the cloud computing platform. Some of them are listed below: [12][13][17].

2.1 Data Privacy and Reliability

In a cloud environment the same data center may contain information belonging to different customers in an identical computer. In such cases information belonging to different customers is needed to be isolated, which further raises the issue of reliability. As system platforms of CSP (Cloud Service Providers) are shared among different customers, reliability may be an issue. For example, malicious software or viruses may penetrate services and further affect user environment.

2.2 Data Integrity

Data integrity is important concern and it has been argued that should be strengthened in every cloud computing environment, as it is susceptible to both internal and external attacks. The lack of trust between CSP and cloud user may also raise the issue of data integrity. Unlike traditional database systems, all of its tenant's information is stored on typical data center [14][15].

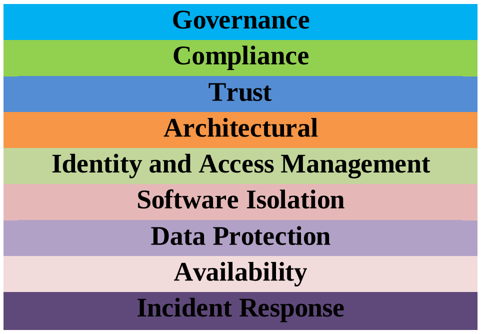
2.3 Authentication and Authorization

Web GUIs have become one of the most sophisticated technologies for delivering cloud services to both user's and administrators. However, they lack certain fundamental aspects of security for what is available on the front-end GUI. Some of its limitation in terms of authentication and authorization are: Front-end GUIs are generally designed to ease the communication between cloud services and its backend components through API calls. These GUIs represent different functions of a basic management console.

However, the whole architecture is designed and implemented using the corresponding structure as traditional web server with Internet access. Thus, it is vulnerable to potential attacks, unless certain countermeasures are applied. Standard OpenStack front-end GUI uses username and password login method in order to access to the user dashboard.

This approach has certain disadvantages as compared to other authentication frameworks, like OpenID, SAML, or Shibboleth [16]. Front-end GUI, being a separate OpenStack entity, requires maintaining separately the different user's credentials. General concept of web services discusses this requirement; however, OpenStack still lacks federated authentication architecture.

The National Institute of Standards and Technology (NIST) is one of the governmental funded organization, is listed the security issues will be repented by the table 1.



Governance
Compliance
Trust
Architectural
Identity and Access Management
Software Isolation
Data Protection
Availability
Incident Response

Table 1. Security Issues identified by NIST

3. PROPOSED WORK

From the base paper entitled as *“Security Architecture for cloud computing Platform”* written by the author *“shanjaya Dahal”*, I have to choose two of the security issues: Identity and Access Management and Data protection.

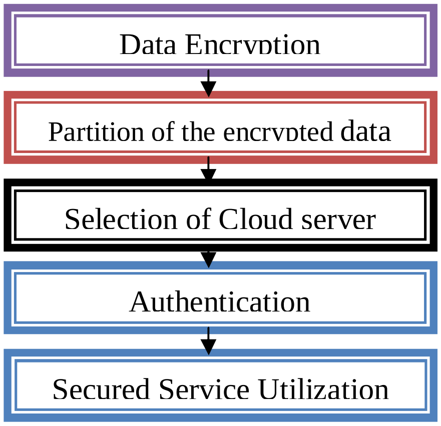

Data Encryption
Partition of the encrypted data
Selection of Cloud server
Authentication
Secured Service Utilization

Figure 2. Component of OHSAP

It is the problem statement of include my research work under the private cloud data transaction. The entire work will be categorized into five modules: It will be illustrated by the figure 2.

The components of the proposed architecture for the orthogonal handshaking authentication protocol (OHSAP) will be represented by the following figure 3.

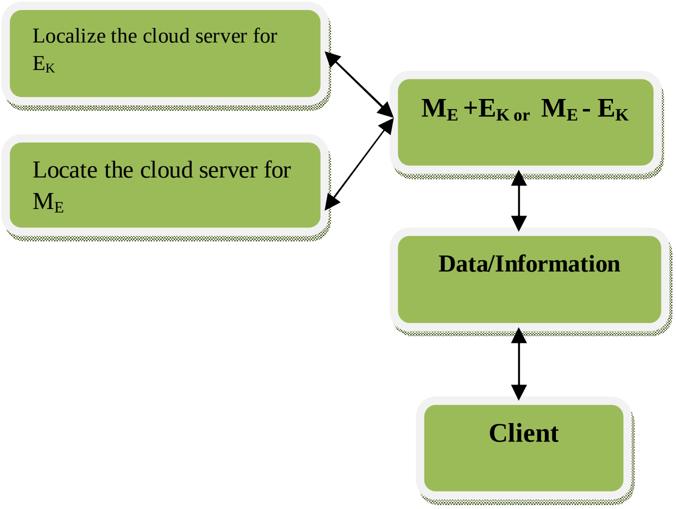

Localize the cloud server for E_K
Locate the cloud server for M_E
M_E +E_K or M_E - E_K
Data/Information
Client

Figure 3. Block diagram for the proposed architecture for the OHSAP

The procedure for the client information either to store in the cloud server or the stored information to be accessed by the client as a utilization will be follow the mechanism of Orthogonal encryption. The basic principle or the algorithm will be discussed in detail under the proposed algorithm component for the continuation of research work. Actually the algorithm to be implemented on the perpendicular with each data store individual location. As per the above architectural representation, the encrypted message will be partitioned into the message part and the key part. Thereafter, the encrypted message and the key will be stored into different cloud server/cloud service provider. In the way of retrieval/access the existing information need to get combination of both the encrypted message as well as the key in order to utilize the required service by the client. The way of data protection, authentication /Identity and method of locate the cloud server/cloud service provider will be descried under features of OHSAP algorithm section.

4. RECOMMENDATIONS AND CONCLUSIONS

The way for the proposed architecture implementation to solve the security issues for the identity and authentication management as well as the data protection. The remaining components of the proposed architecture will be explained and extended by the author to the continuity of this work in order to develop an algorithm to ensure the data protection. For better performance, the private cloud to be taken in the empirical part.

REFERENCES

1. Ren, Kui, Cong Wang, and Qian Wang. "Security challenges for the public cloud." Internet Computing, IEEE 16.1 (2012): 69-73.
2. S. Subashini and V. Kavitha, "A Survey on Security Minimal issues in service delivery models of cloud computing” Journal of Network and Computer Applications, 34(1), 2011, pp 1-11
3. Sosinsky B, Cloud Computing Bible. 1st ed. Wiley; 2011.
4 .Kaufman, Lori M. "Can public-cloud security meet its unique challenges?"Security & Privacy, IEEE 8.4 (2010): 55-57.
5. Guidelines on Security and Privacy in Public Cloud Computing, NIST Special Publication 800-144
6.http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf
7.Catteddu, Daniele. "Cloud Computing: benefits, risks and recommendations for information security." 2009
8.http://www.microsoft.com/presspass/press/2010/jan10/1-20BrookingsPR.mspx
9 .D. Talbot. Security in the Ether. Technology Review, pages 36–42
10. Hassan Takabi and James B.D.Joshi, Security and Privacy Challenges in Cloud Computing Environments,

University of Pittsburgh, Gail-Joon Ahn,Arizona State University.

11. S. Kamara and K. Lauter, "Cryptographic Cloud Storage", FC'10: Proc. 14 Intl.Conf. On Financial, cryptography and data security, 2010, pp. 136-149.

12 .Okuhara, Masayuki, Tetsuo Shiozaki, and Takuya Suzuki. "Security Architecture for Cloud Computing." FUJITSU Sci. Tech. J 46.4 (2010): 397-402.

13. C. Cachin, I. Keidar and A. Shraer, "Trusting the Cloud", ACM SIGACT News, 40, 2009, pp. 81-86.

14.Snjaya dahal," Security architecture for cloud computing".

15 .Sun, http://blogs.sun.com /gbrunett/entry/ amazon_s3_silent_data_corruption.

16. RedHat, //rhn.redhat.com/errata/RHSA-2008-0855.html.

17 .OpenID Foundation, http://openid.net/get-an-openid/individuals/, last accessed September 13 2012.