DOI: http://dx.doi.org/10.26483/ijarcs.v9i2.5848

Volume 9, No. 2, March-April 2018

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

PROTECTION OF PRIVATE CLOUD DATA TRANSACTION BY AN PROPOSED ARCHITECTURE OF ORTHOGONAL HANDSHAKING AUTHENTICATION MECHANISM (OHSAM)

Prof. K. Subramanian
Assistant Professor, H.H Raja's Govt. Arts College
Department of Computer Science
Pudukottai, Tamil Nadu, India

M. Mohamed Sirajudeen
J.J College of Arts and Science
Department of Computer Science
Pudukottai, Tamil Nadu, India

Abstract: In general, the either the private or public concerns those are mainly focus on the profitable orientation organization, much more concentrate on the security because to protect the sensitive data transaction or utilization. This paper especially focuses on the security issues raised in the data transaction under private cloud. The security for the data transaction between the cloud service provider (CSP) and the end users is always ensures the secure transaction. There is any conflict in the mutual authentication between these pairs to bring the issue on Security over the data transmission. In most of the occurrences, the intruders to break the data chain during the transmission period or the data residence portion in the CSP storage. For this reason, there is a necessity to analyze the level of secure transaction between the CSP and the service utilization end users. It will be depicted in this research article in a clear manner and named as Orthogonal Handshaking Authentication Mechanism (OHSAM).

Keywords: Cloud, Security, Authentication, Orthogonal and Utilization.

I. INTRODUCTION

The effective utilization of existing resources will be taken by a mutual authentication between the cloud service provider and the end users/clients. In general, the service utilization taken place on-demand access in the required occurrences. The literature survey of the cloud computing clearly specify the cloud deployment model in to four major categories: Private, public, Hybrid and Community [4][5]. The following table listed the categories of cloud computing deployment models with its description,

TABLE 1: Deployment models in cloud computing

Private cloud	Cloud infrastructure and computational resources are made available to the general public over public network.
Public cloud	The one customer has the exclusive access and usage of the infrastructure and computational resources; hosted on the organizations within the campus or provided by a provider outside of the campus.
Hybrid cloud	The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability.
Community cloud	Group of users sharing the same infrastructure and computational resources.

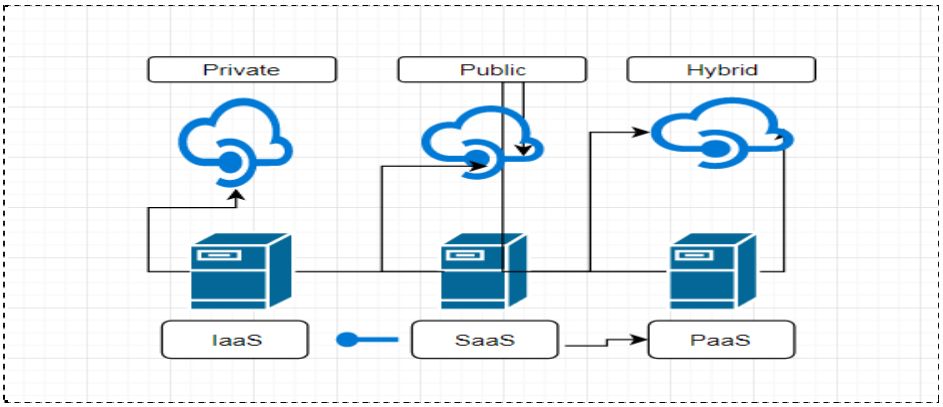

FIGURE 1: The Deployment models for Cloud Computing with its services

The deployment model for the cloud computing is illustrated by the figure 1. It explicitly specifies the service accessed by the deployment models such as IaaS (Infrastructure as a Service), PaaS (Platform as a Service) and SaaS (Software as a Service)[3]. In most of the occurrences, the private cloud utilizes the service for IaaS. 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 2.

TABLE 2: Security issues listed by the NIST

Governance	The general rules and policies for the organization to provide services or act as cloud service provider(CSP)
Compliance	The mode of agreement with the consumer/end user.
Trust	The expectation for secure data transaction.
Architectural	The establishment for the platform or hardware setup to utilize the recourses.
Identity and Access Management	A method of Authentication.
Software Isolation	Feature extraction for the suitable software to provide services.
Data Protection	Protection of sensitive data.
Availability	A form of reliability.
Incident Response	Quick response for the authenticated users regarding to utilize the services.

From the list of issues, this research paper focus on the Identity for Access management and the data protection for the continuation work with an empirical study.

2. RELATED WORK

The European Union Agency for Network and Information Security (ENISA) conducted different level of security risk assessment in the cloud service utilizations. Thereafter, they listed different level of issues along with a solution to avoid such kind of circumstances while sharing the existing resources. It also provides cooperative studies with various stakeholders to identify the critical cloud services and analyze the impact of the cloud service failure in several circumstances. In the following subsections, we present the state-of-the-art general tools that are individually and collectively used to countermeasure cloud security attacks. They were listed and discussed more on rest of the private cloud. In many occurrences, the cloud service utilization for the private cloud or data transaction under the private will not be discussed in depth manner and not addressed any issues. The level of security and privacy issues to be listed in a clear picture in case of extended usage for the PaaS/ SaaS [1][3]. Before to start the utilization/sharing the access is better to find the secure way of transaction in spite of different algorithms are exiting in the resource pool. The Identity and access management [2] will include the following components listed in the table 3,

TABLE 3: Components of the Identity and Access Management

Authorization	To provide the privilege for creation of an account after verify the credentials
Identity Provisioning	The exchange of key
Management Personal Data	To maintain the privacy of the stored data especially for the personal information
Key Management	The way of managing the encryption key for the authentication
Encryption	To encrypt the data during period of transaction
Authentication	To ensure the correct user with the help different authentication protocols

FIGURE 2. User Identity Management protocol Layers

In the figure 2, represents the user's identity management protocol architecture. This architecture will be replaced by the proposed architecture in this research work and named as "Orthogonal Handshaking Authentication Protocol (OHSAP)".

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. It is the problem statement for the research work under the private cloud data transaction. The entire work will be categorized into five modules: It will be illustrated by the fig 4.

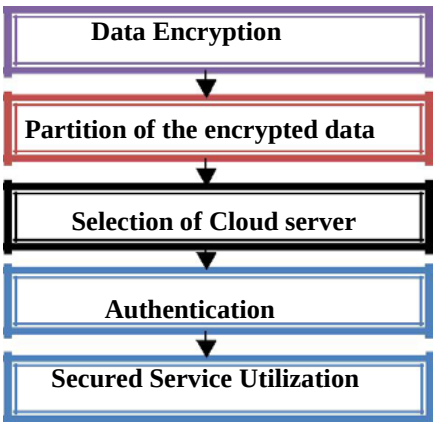

FIGURE 4: Components for the OHSAM

In order to conduct a secure data transaction between the CSP and the end user /Client to start from the storage portion for the cloud server. In the first step, the data get encrypted before the transmission by using a proposed orthogonal Encryption algorithm. In the next stage, the encrypted text/data will be partitioned into Orthogonal Encryption Text (OE_T) and Orthogonal Encryption Key (OE_K). After the partition, these two components will be stored into different cloud servers that will be identified by the Orthogonal Handshaking Authentication Mechanism (OHSAM) algorithm. For this purpose, the segments for the "selection of cloud server" are combined with the authentication to ensure the secure data transaction. In the authentication part, will be confirmed using an OHSAM along with the secure certification. Finally, the data transaction will be taken place between the cloud service provider and the end user/client.

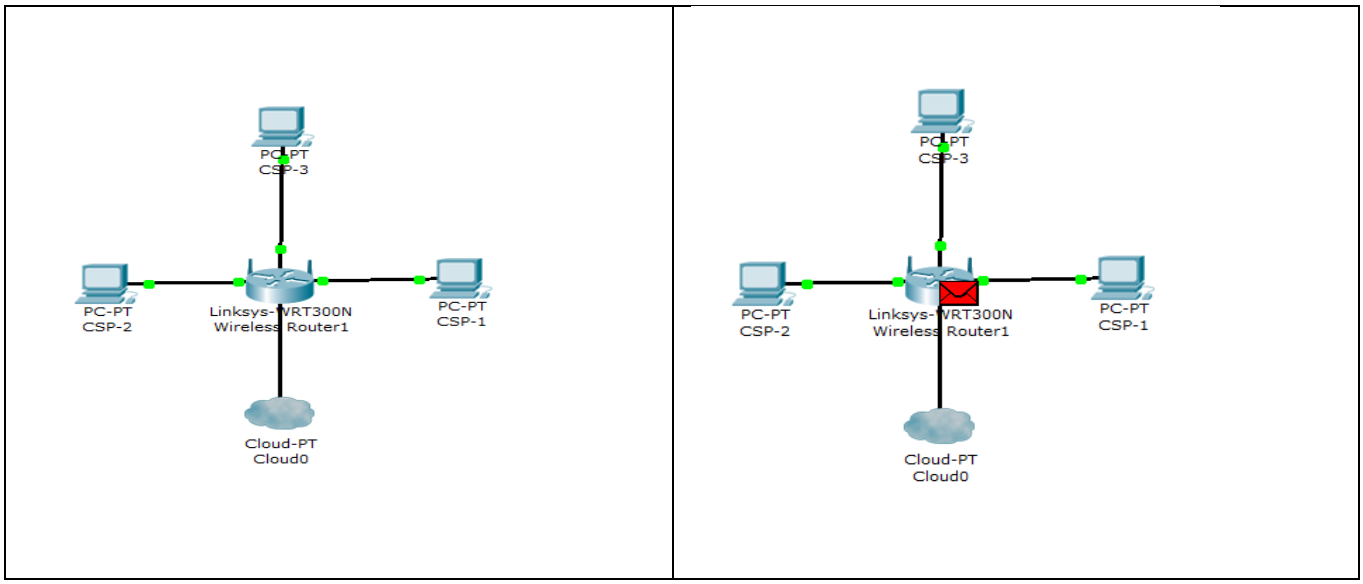

FIGURE 5: Identity for Cloud service provider (ICSP)

The data to be involved in the transaction or utilization will be stored in the cloud service storage in the split for two components and the location of the storage to be finalized in the orthogonal constraints. It will be illustrated by the figure 5. The logic behind the authentication is a selection of the cloud server /service provider on the basis of orthogonal constraint (perpendicular with each other) and to ensure the authorized user/client. The proposed OHSAP logic behind as follows,

Begin procedure AUTH ()

1: S_{Req} → CSP
2: CSP→ A_K from CSP (A_K)
3: A_K → S_{Req}
4: if (S_{Req} (K) ==A_K) then

5: Fetch the data /information from CSP (D) CSP (A_K)

6: end if

End AUTH;

Step 1: From the specification, initially the service request (S_{Req}) will be initiated by the end user/client towards the cloud service provider (CSP).

Step 2: If the CSP receive a service request, then it will send the authentication encryption key (A_K) from the Cloud server storage of the encrypted key portion.

Step 3: Then the authentication key will be forwarded to the service request initiation end user /client.

Step 4: The key confirmation with the service request client and the CSP.

Step 5: Then the client/end user to utilize the required service from the appropriate CSP. (The information retrieval taken place the CSP perpendicular with each other).

The authentication handshaking taken place under the private cloud clients and the CSP and the transaction will be secured by the proposed architecture for OHSAP.

4. CONCLUSION

In this research article, to discuss the secure data communication under the private cloud by using the proposed OHSAM architecture for secure data transaction under the private cloud. The outline of OHSAM algorithm components are specified in this section clearly with functional steps. In the continuation of this research work to describe the detailed functional procedure as well as the experimental result along with the algorithm description for each and every component.

5. REFERENCES

[1]. Final Version of NIST Cloud Computing Definition Published. Available online: http://www.nist.gov/itl/csd/cloud-102511.cfm (accessed on 25 August 2013).

[2] . Wang, C.; Wang, Q.; Ren, K.; Lou, W. Towards secure and dependable storage services in cloud computing. *IEEE Trans. Serv. Comput.* **2012**, *5*, 220–232.

[3] . Wang, J.-J.; Mu, S. Security issues and countermeasures in cloud computing. In Proceedings of the 2011 IEEE International Conference on Grey Systems and Intelligent Services (GSIS), Nanjing, China, 15–18 September 2011; pp. 843–846.

[4]. Sabahi, F. Virtualization-level security in cloud computing. In Proceedings of the 2011 IEEE 3rd International Conference on Communication Software and Networks (ICCSN), Xi'an, China, 27–29 May 2011; pp. 250–254.

[5]. Lingfeng, C.; Hoang, D.B. Towards scalable, fine-grained, intrusion-tolerant data protection models for healthcare cloud. In Proceedings of the 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Changsha, China, 16–18 November 2011; pp. 126–133.

[6]. Sanjaya Dahal, "Security architecture for cloud computing platform", Master thesis, Stockholm, Sweeden, 2012.