IJRD International Journal of Research & Development Organisation

ISSN: 2455-6653

Journal of Applied Science

A Proposed Architectural Framework of Orthogonal Handshaking Authentication Protocol (OHSAP) for Secure Private Cloud Data Transactions on Client based Access mechanism

M.Mohamed Sirajudeen [#1] and M.Abubacker Siddiq[#2]

[#1] Lecturer, Department of Information Technology, University of Gondar, Ethiopia
[#2] Asst.professor, Department of Industrial Engineering, P.S.N Institute of Technology and Science, Palayankottai, Tamil Nadu, India.

Abstract: In the emerging trends in cloud computing help to reduce the operating cost for required resources irrespective of the geographical barriers. Simultaneously, the data/information access by various clients arises too many security issues in the existing cloud deployment models. Especially, profitable oriented transactions give more attention for secure data transmission between the clients and cloud service providers (CSP). Usually, the programmers /researchers follow a method of encryption /decryption to protect the data from intruders. In this proposed approach faintly different from the existing one with some additional features for the cloud service provider's location in order to store the encrypted data (ED) and the Encryption key. The security related protocols are usually run over the untrusted networks regarding to ensure the secure data transactions. Private Clouds play an important role to access confidential /privacy information's for an individuals or an organization. It will be composed into two major issues: client based access mechanism and server based access mechanism. In this proposed architectural framework to describe the client based access mechanisms with all required features.

Key words: Client, Secure, Cloud, Encryption, Decryption and Key

1. INTRODUCTION

In Cloud Computing enabled resource sharing or resource utilization highly concentrates on the area of Security, consistency, privacy and legal responsibility for the cloud service providers. Among the existing issues, the privacy of the clients acquires highest priority in cloud computing technique and the hit the highest point concern is security [3]. The secure communication or data transformation based on the cloud service provider (CSP). The CSP mainly focused on the following concerns: Problem Related to passive At-tacks, Data location, Privacy, Data Integrity and Recovery [3]. Even though different researchers proposed variety of security algorithm as well as security protocol for reliable data transformation, still the security concerns in question mark for most of the commercial applications related with financial /confidentiality concerns [3]. Different types security based protocols will be discussed by most of the researchers mentioned in the specified references [4] [5] [6].

In the internet based transactions the services are processed through the web browser using http's protocols such as HTTP, HTTPS & S-HTTP. However these protocols have some security issues which are discussed in HTTP is an application layer protocol which helps in sending and receiving the information. HTTP is not suitable for sensitive information transaction because it is not a secure protocol [4]. HTTPS

is another protocol designed to provide security. This protocol works in presentation layer in encrypting the sensitive transaction. HTTPS is not effective because, along with message body it also encrypts the message header [5]. S-HTTP is designed in such a way that it encrypts only a message body [6]. These protocols do not help the security challenges such as man- in- middle attack, data integrity, strict authentication and authorized techniques and intruder detection [4][5][6][7].

2. RELATED WORK

In the junction of the information exchange technology make roadmap for the cloud scheme for resource sharing and address different threats under the cloud data transfer. Many researchers addressing the threats will be addressed in the data transfer under the private cloud. An inappropriately secured Cloud environment can be a point from which various inter/intra system attacks can be launched to either co-tenants or external systems, thereby causing a potential cascading failure of multiple systems that are co-tenants. Threat amplification means that a problem propagates faster and farther through a Cloud environment than it would under alternate circumstances (i.e., in a non-Cloud environment) [1]. This also has the effect of potentially reducing a timely response to and recovery from the threat. This challenge can be addressed by ensuring that comprehensive and well managed security and governance processes are in place to detect, manage and correct threats before they go viral and spread [1]. As a part of this security issues, a major component is an authentication to ensure the secure data communication between the client and the cloud service providers. At present, most of the organizations apply the authentication mechanism in their wireless network deployments. In the private cloud data aspects, the organizations create a private cloud intranet access or other services to the employees, which are authenticated separately by using any one the authentication mechanism. Application of a single authentication mechanism is more convenient for the user and decreases the number of possible security threats [2]. Sometimes, there will be a problem to encounter in the handshaking process, and it cannot be continued because of a detected problem, such as unsuccessful authorization or unacceptable cipher suites, it must close the network connection associated with the established session and release all the resources of this session [2]. In the existing architecture to describe the authentication between the client and single server CSP (Cloud Service Provider). The encrypted message from the client transferred to the CSP storage area along with the key.

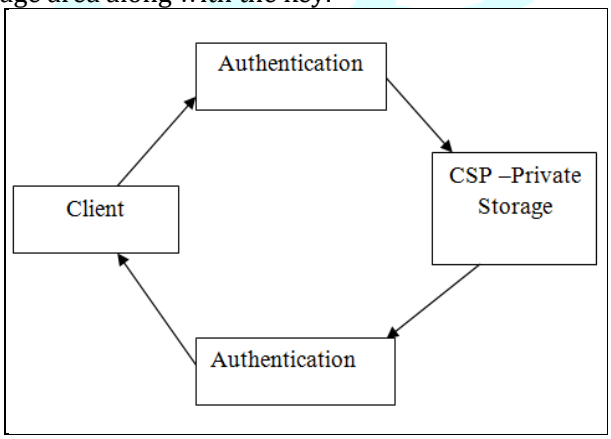

Fig 1.1 Client and Server Authentication framework

If there will be any intruders attack in the handshaking authentication mechanism, the level of security risk is high. Either the stored information the Private Cloud storage will be altered or completely modified by the intruders. In order to avoid such kind of security risk , in this research paper proposed an the Orthogonal handshaking authentication Protocol (OHSAP) comprised two major issues for the data storage in the private cloud such as : Encrypted message(E_M) will be stored in one CSP and the

Encryption Key (E_K) will be stored into the another CSP. In this mechanism, the client is required for both to get the required information access. In this way, the secure data transaction is enhanced by using this proposed architectural framework of OHSAP).

3. PROPOSED ARCHITECTURE FRAMEWORK FOR OHSAP

The proposed authentication algorithm (OHSAP) on client based access to ensure the secure private data transaction comprised into three major components: Encryption/Decryption, Protocol stack, and Authentication. The general outline for the proposed OHSAP architecture is depicted in the following fig 1.2. It shown the message transmission though the router (it maintains the address for the nearer cloud service providers [CSP]- Server) . From the existing CSP –servers, the OHSAP algorithm choose the service providers for its Encryption Text as well as the Encryption Key storage in the orthogonal manner.

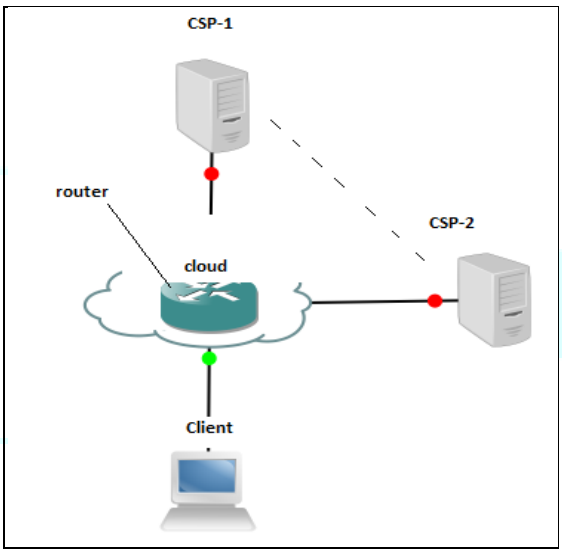

Fig 1.2 Proposed Architecture for OHSAP client centric access

Step1: Encryption/Decryption:

The privacy or confidential information's relayed out of the client machine will be encrypted by using the proposed orthogonal Encryption Algorithm (OEA) and portioned into two parts: Encrypted Text (E_T) and Encryption Key (E_K). It will be shown by the following fig 1.3.

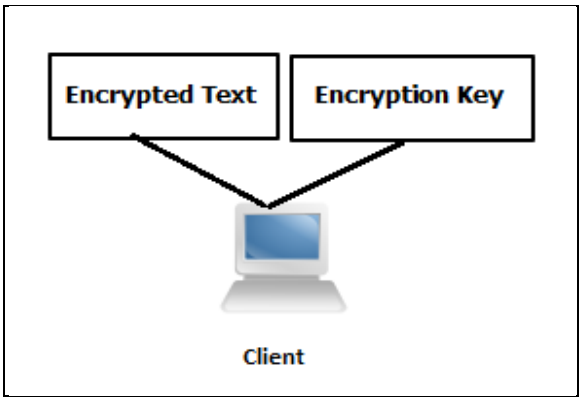

Fig 1.3 Transmitted message from client

Step 2: Protocol Stack:

The communication protocol for the security measures OHSAP algorithm is 256 bits protocol stack specifications: Such as the bits from 0-4(5 bits) is used to represent the Header(H) , 5th bit is used to indicate the synchronization(SYN) for the communication channel , the bits from 6-23(18 bits) are used to specify the source address (SA), the bits from 24- 39(16 bits) is used to specify the Encrypted message stored cloud service provider address (CSPAET) and the bits from 40- 55(16 bits) is used to indicate the Encryption Key stored cloud service provider address(CSPAEK) .The Bits from 56-119(64 bits) is used to indicate the Encryption /Decryption message content , the bits from 120-247(128 bits) is used to specify the encryption key and the bits from 248-255(8 bits) is used to ensure the error free service(EF). It will be shown by the following fig 1.4.

H (5)	SYN (1)	SA (18)	CSPAET (16)	CSPAEK (16)	ED (64)	EK (128)	EF (8)

Fig 1.4 Protocol Stack format

Step 3: Authentication

The authentication play a vital role to ensure the appropriate client to perform either retrieval or information access with the private cloud data storage portion in the data base. The method of data storage for Encrypted Text (E_T) as well as the Encryption Key (E_K) via to open the connection with cloud servers. The method of Cloud server selection will be clearly specified by the continuation of this work in the consecutive publications. At the end of connection establishment, the Cloud service providers issue the token (T) to the appropriate clients for future communication regarding to perform the retrieval operation. It will be illustrated by the fig 1.5, fig 1.6 and fig 1.7. The service requested clients are required to use the token in order to access the private cloud transactions.

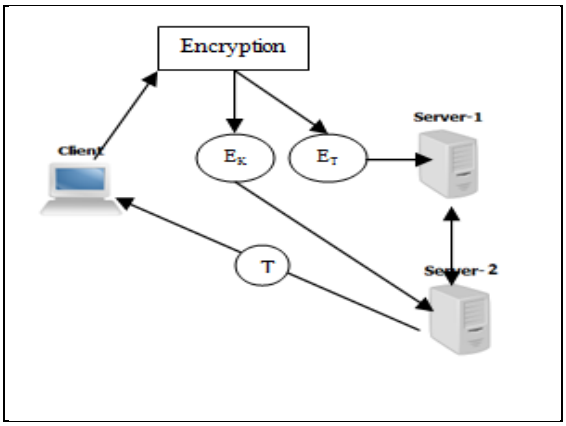

Fig 1.5 Message Storage Mechanism on client centric

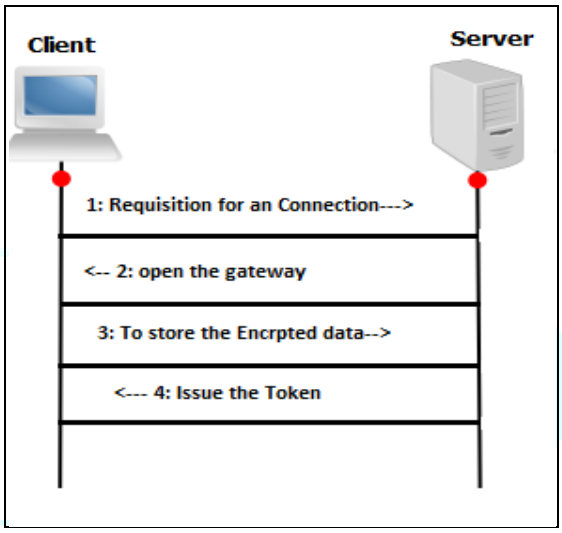

Fig 1.6 Handshaking mechanism of storage

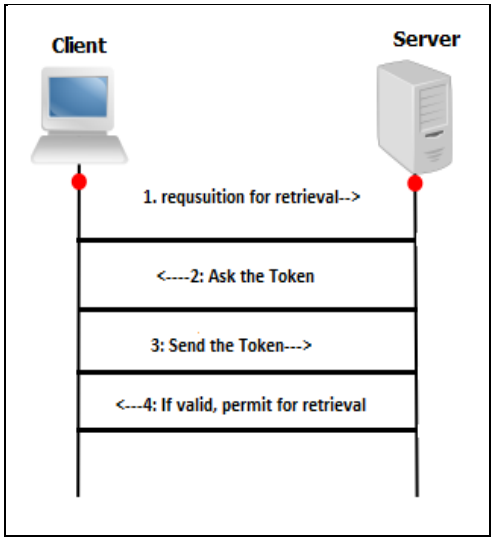

Fig 1.7 Handshaking mechanism of Retrieval

4. CONCLUSION AND FUTURE WORK

In Clouds, the storage of client's privacy information's in cloud service providers (CSP) for the sharing access will be carried by secure manner under the private cloud using the proposed client based OHSAP. This architectural framework provides the solutions related confidential data transformations between the appropriate client and the CSP. In point of fact, it needs some additional consideration based on the identification of the cloud storage from the CSP and the way to share the token among the approved clients. It will be carried out to the continuation of this work.

References

[1]. "Security in Private Database Clouds", Whitepaper, Published by an Oracle Corporation, July 2012.
[2]. Krzysztof Grochla and Piotr Stolarz, "Extending the TLS protocol by EAP handshake to build a security architecture for heterogeneous Wireless network", Grid Air Sync - The Network Management System for Intelligent Grid" project subsidized by Polish Agency of Enterprise Development by the grant no POIG.01.04.00-24-022/11.
[3]. Kartik Sharma, Renuka Sharma, Gitesh Dalal ," A Secure Protocol for Data storage Security in cloud computing International Journal of Scientific & Engineering Research", Volume 4, Issue 6, June-2013 2348 ISSN 2229-5518.
[4]. Hyper Text Transmission Protocol: Communication Technology Proceedings-2003. ICCT 2003. International Conference on Study on conformance testing of hypertext transfer protocol by Xiaoli Yu; Jianping Wu; Xia Yin; Dept. of Comput. Sci., Tsinghua Univ., Beijing, China
[5]. hyper text transmission protocol with security: A Performance Analysis of Secure HTTP Protocol by Xubin He, Member, and IEEE.http://en.wikipedia.org/wiki/HTTP_Secure.http://www.technolozy.net/difference-between-http-and-https-protocols.html.
[6]. S-HTTP: Secure Hypertext Transfer Protocol:http://www.javvin.com/protocolHTTPS.html.http://en.wikipedia.org/wiki/Secure_Hypertext_Transfer_Protocol.
[7]. Dinesha H A, Prof.V.K Agrawal, "Framework Design of Secure Cloud Transmission Protocol", International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, January 2013
ISSN (Print): 1694-0784 | ISSN (Online): 1694-0814.