Enhancement of the Private Cloud Data Transaction by using an Orthogonal Handshaking Authentication Protocol (OHSAP)

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

K.Subramanian, PhD
Department of Computer Science
J.J College of Arts and Science, Pudukottai
Tamil Nadu, India

ABSTRACT
Now a day, "Cloud Computing" is an inevitable trend in the field of information technology due to the reason for information sharing as well as the resource utilization. In most of the organizations either it may be a profitable or non profitable category must focus on the resource sharing due to minimization of its infrastructure development cost. In spite of its tremendous growth, there will be a great question mark for the security on the data transaction between the cloud service providers (CSP) and the end user or client. The privacy information stored in the cloud service provider data bases will be utilized by the authorized end users in many occasions as well as it will be shared by communication channel with highly secured authentication protocols. Even though existence of several cryptographic algorithms, the intruders breaks the cipher text for the authentication protocol and create a road map for data loss. In this research paper especially focus on the security issues of data transaction under private cloud with the help of the proposed protocol named as "Orthogonal Handshaking Authentication Protocol (OHSAP)".

Keywords: Cloud, Private, Security, Data and Authentication.

1. INTRODUCTION

Security for the data storage as well as the utilization is a challenging task either in the public /private cloud environments for the reason of the service consumer/clients attempt themselves to do the data transactions. In the category of private cloud service providers are always ensure themselves a secure data storage management or service allocation for the clients. Anyhow, there will be numerous possibilities for the intruders attack on the data transaction by the third party agents/intruders. The possibility for the data loss due to the interruption for unauthorized users is clearly depicted by the fig 1.1. The major issues are the security for the existing /stored data in the cloud server. Usually, the required user utilize the service via the cloud may cause the problem of data loss or intruder inject his own message. In this, case there is a question mark for the security on the private data transmission between the cloud server and the service consumer. In this paper address this issue and propose the solution to protect it.

The data transaction over the common communication channel always needs an advanced security mechanism to ensure the secure transaction especially in the privacy information for clients or end users. In most of the occurrences, the privacy information's or confidential documents will be modified by the intruders on the communication channel with the help of malicious authentication protocols.

The orthogonal handshaking authentication protocol (OHSAP) mechanism is a proposed security solution; it allows data to be protected in storage and transit in private clouds in a specialized form of an Encryption. The information sharing between the end users with the help of cloud service provider (CSP) is usually carried out by the web based tools or applications [1].

In general, the functional components of the cloud service providers will be categorized as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) [4], and Software as a Service (SaaS) and other different services are also to offer [2][3][4].

2. RELATED WORK

In the contemporary trends in information technology provide a root cause for simplify the task of the resource sharing and utilization .In the meantime, the cloud service provider must ensure the communication will be a secure one especially in the sensitive data transactions under the private cloud . In few circumstances, the unauthorized users try to break the encrypted key exchange or to find the physical address for the CSP by the way to create an unauthenticated effective server in the path of data communication and indulged in the information theft [5].

The data on cloud will be intersected by the intruders either in the data at rest in the data store or in the transaction. For this reason, the researchers focus these above two aspect whenever try to propose or implement a security algorithms. The attempt of a security attack in the data store usually prevent by using an encryption mechanism for ensuring the data confidentiality and to secure the data during transaction by using an authentication protocols. In the way of ensuring the data encryption will be based on the encrypted text (Cipher Text) and the Encryption Key (E_K) [6].

In general the "cloud computing" data storage and access to be entertain huge volume of data storage as well as data transaction. In this perspective, the researchers also concentrate on the time delay for the response. The end user or clients submits their request in order to access the data to be stored on the cloud storage, it will give a quick response.

If the processing time for the proposed algorithms by the researchers takes long time to run the application, abruptly

affect the performance of entire data traction between the clients and the CSP. Thereafter, another issue is arises in this critical circumstances; it will be the key management. The related work base paper [7] categorized the cloud data into three groups: data in the transmission, data at rest in the cloud storage and the data to be processed by the client machine.

In most of the occurrences the encryption mechanism plays an important role in order to ensure the secure data transaction. It will be the basic tool to overcome the security issues addressed by the cloud computing environment.

By applying the encryption mechanism of "Symmetric key" involving a single key for both encryption and decryption. In other hand, another mechanism of encryption algorithm by using "asymmetric" involving two different key for both encryption and decryption [8].

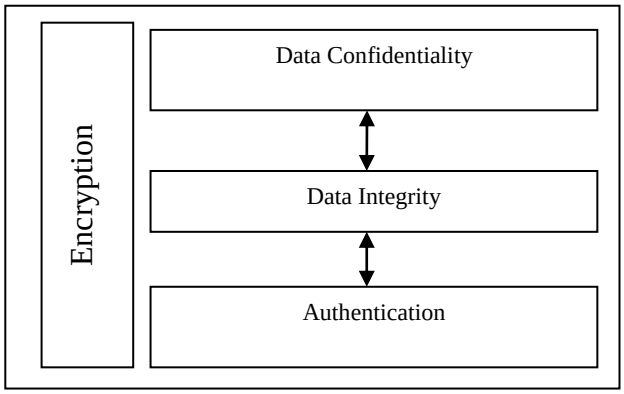


Fig 1.0 Layered Architecture for secure communication

The transmission data will be ensured in the secure way with the help of Encryption and Authentication. In the proposed work, constitute two major components regarding to perform the encryption and authentication based on the Orthogonal Encryption Algorithm.

3. PROPOSED WORK

3.1 Secure data at Rest

In this research article mainly discuss, the proposed algorithm for data at rest in the cloud storage. Usually, the encrypted message will be stored in the cloud server data storage along with the key in the identical server. It creates an opportunity for the malicious users attack. For this reason, in this proposed work, the encryption message (Ciphertext) and the Encryption key (E_K) in two different server and the selection of the cloud service provider will be finalized by using an orthogonal (perpendicular with each other) mechanism.

The way to introduce the method of encryption on the stored data and the key will be stored on another server. Whenever the service is required by the client to ensure the authentication on the basis of symmetric encryption algorithm.

In the initial stage to be considered the data (plain text) for the cloud storage (M) along with the key position (i.e. the number of bits for the key construction-K_P) . Thereafter, the plain Text will be encrypted by using the Orthogonal Encryption Algorithm as well as divided into the encryption message (M_E) and the Encryption Key (K_E). The encrypted message will be transformed during the transmission (M_{E+1}) .

Thereafter, the message will be stored in the cloud server data storage. At the same moment, the Key for the encrypted text will be stored along with the reference link into cloud service provider data storage by using the orthogonal mechanism. It will be depicted by the figure 1.1 in clear manner.

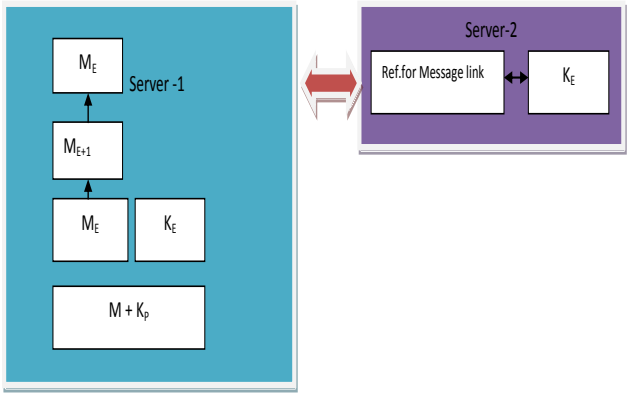


Fig 1.1 Data Storage Mechanism in CSP

The general problem will be faced by the client whenever try to store or access the resided information the privacy data in the cloud server will be depicted by the figure 1.2. The message storage or access via cloud will be intersected by the unauthorized users either in the active (copy the content and modified it) or passive(only copy the content). In this aspect , if the message and the key will be stored in different location to avoid the risk of data loss or to secure the original message from the malicious attack.

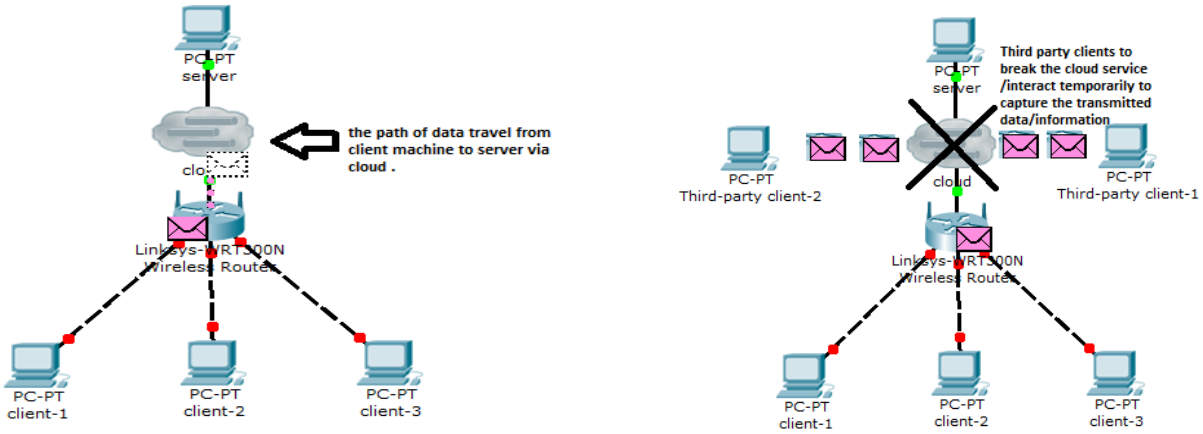


Fig 1.2 Security Attack on data at rest and transmission

3.2 OHSAP Encryption algorithm

Step 1: To assign the numeric value for the English alphabets as shown by the below table (NV*- Numeric Value]

Alphabet	NV*	Alphabet	NV*	Alphabet	NV*
A or a	1	J or j	10	S or s	19
B or b	2	K or k	11	T or t	20
C or c	3	L or l	12	U or u	21
D or d	4	M or m	13	V or v	22
E or e	5	N or n	14	W or w	23
F or f	6	O or o	15	X or x	24
G or g	7	P or p	16	Y or y	25
H or h	8	Q or q	17	Z or z	26
I or i	9	R or r	18	Blank ( )	27

Step 2: The encryption bit position for the message as well as the key generation will be considered as 128-bit binary format and the numeric value conversion for the required encryption to be considered as 4 bit position.

128	64	32	16	8	4	2	1

Step 3: To encrypt the message before to store into the cloud service provider. For example consider the message as "HELLO". The equivalent numeric value for the given message is "00080005001200120015"

Step4: Then the numeric value will be converted into the equivalent binary value. [4 bit input string will be considered for the conversion of 128bit position]

0000 1000	0000 0101	0000 1100	0000 1100	0000 1111

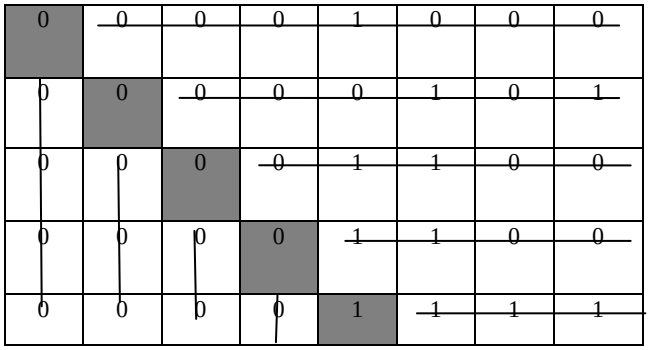
Step 5:

i. The Orthogonal encryption key will be generated from the storage that initiates to store the binary values for individual character in row for individual position (M x N).

M= 5 rows and N=8 columns

[1,1]	[1,2]	[1,3]	[1,4]	[1,5]	[1,6]	[1,7]	[1,8]
[2,1]	[2,2]	[2,3]	[2,4]	[2,5]	[2,6]	[2,7]	[2,8]
[3,1]	[3,2]	[3,3]	[3,4]	[3,5]	[3,6]	[3,7]	[3,8]
[4,1]	[4,2]	[4,3]	[4,4]	[4,5]	[4,6]	[4,7]	[4,8]
[5,1]	[5,2]	[5,3]	[5,4]	[5,5]	[5,6]	[5,7]	[5,8]

The actual binary values storage for the information,



ii. From the stored value , the orthogonal position (perpendicular with each other) to be considered for the key generation, [1,1],[2,2],[3,3],[4,4] and [5,5]. Such as ,

O_K = 00001……..[1]
"O_K" is the orthogonal key. The Encrypted orthogonal key will be represented as follows,

OE_K=H + $(O_K)_{128}$ ----------[2]

iii. From the equation [2], " OE_K "is the encryption key, "H" is the header for the table representation (in this example H=5x8) and the orthogonal key value will be represented as 128 bit position as well as the header bit position will be considered as 4-bit information . From the given example, the orthogonal Encryption key (OE_K) is,

OE_K = 01011000000000001……[3]

4. CONCLUSION AND FUTURE WORK

In this research paper, the proposed algorithm to cover a portion of the encrypt the message to be stored in the cloud server along with the key (E_K). The continuation of this work to include the identification for the cloud server to where the data to be stored, to encrypt the service request , to decrypt the ciphertext and implement the handshaking protocol for the way to enhancing and ensuring the data transaction as well as the authentication between the end user and the cloud service provider(CSP) .

5. REFERENCES

[1] Joshi Ashay Mukundrao , Galande Prakash Vikram "Enhancing Security in Cloud Computing" in Information and Knowledge Management www.iiste.org ISSN 2224-5758 (Paper) ISSN 2224-896X (Online), Vol 1, No.1, 2011

[2] Junjie Peng, Xuejun Zhang, Zhou Lei, Bofeng Zhang, Wu Zhang, Qing Li, "Comparison of Several Cloud Computing Platforms," in Second International Symposium on Information Science and Engineering, 2009.

[3] 3tera, http://www.3tera.com, April 2009, "Cloud Computing For Web Applications.".

[4] http://www.sales.com, April 2009, "Platform as a Service (Paas) - Powering On-Demand SaaS Development."

[5] N. Mead, et ai, "Security quality requirements engineering (SQUARE) methodology," Carnegie Mellon Software Engineering Institute.

[6] Deyan Chen and Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," International Conference on Computer Science and Electronics Engineering, 2012

[7] Navia Jose and Clara Kanmani .A, "Data Security Model Enhancement In Cloud Environment"IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 10, Issue 2 (Mar. - Apr. 2013), PP 01-06

[8] M. Vijayapriya, "International Journal of Computer Science & Engineering Technology (IJCSET)", ISSN: 2229-3345 Vol. 4 No. 09 Sep 2013, Page no: 1209 - 1211.