International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)
Impact Factor: 3.45 (SJIF-2015), e-ISSN: 2455-2585
Volume 4, Issue 5, May-2018

Secure Cloud Storage Data Transaction by using an Orthogonal Handshaking Authentication Mechanism

Prof.K.Subramanian[1], M.Mohamed Sirajudeen[2]
Assistant Professor, H.H Raja's Govt. Arts College[1],
J.J College of Arts and Science[2]
Department of Computer Science
Pudukottai, Tamil Nadu, India.
subjjcit@gmail.com[1], mdsirajudeen1@gmail.com[2]

Abstract: ***In general, the Cloud computing is a model for enabling the current demands in the effective resource utilizations. The cloud computing technological approach gives out a road map to fulfill the rift between service and demand in the information technology sector with efficient manner. The cloud data storage architectural mechanism is projected by different researchers in the aspect of secure cloud data transaction over the communication channel. Each and every cloud service provider represents different storage architectural in order to provide security in different cloud services. The platform of architectural make a clear picture in order to conduct secure data transaction under cloud either it may be a private, public or hybrid. This research paper focus on how to conduct a secure data transaction under private cloud related with healthcare domain based on Orthogonal Hand Shaking Authentication Mechanism (OHSAM).***
Key words: Secure, Cloud, Data, heath care and Orthogonal.

I. INTRODUCTION

In the healthcare industry are having significant impact on the data transaction under the cloud service utilizations. There is a substantial growth, in demand for healthcare services because of the demand for huge data maintenance as well as the necessity for distributes the records to the different geographical locations over the communication channel. Expectations for better outcomes, higher quality treatment and more value from the healthcare services provided increase the need for point-of-care access to medical data and the parallel evolution and adoption of mobile devices, both for medical staff and for patients, are forcing the need for IT systems to adapt under the categorization for the impact on software as a service (SaaS). Also the significant increase in digitization of medical records – including the accelerating increase in adoption of electronic medical records, electronic health records and personal health records.

Medical systems built using cloud services can provide web access to data, avoiding the need to store information on client devices. The need for scarce IT security skills within the healthcare organization also is minimized. Cloud service providers typically operate on such a scale that they have all the necessary IT skills, with the costs of those skills spread across many customers. Healthcare functionality can be enhanced by cloud-based healthcare IT systems that offer the potential for broad interoperability and integration. Healthcare cloud services are Internet-based and generally use standard protocols. Also, cloud services offer access to a much larger ecosystem of healthcare provider, payer, life sciences and IT solution partners; all of which increase the potential for a wide range of services to healthcare provider organizations. These services offer the opportunity to extend the capabilities available to health organization staff, in order to implement better ways of working and to offer new services to patients. The capabilities offered by health cloud services can be expected to facilitate personal health maintenance, improve diagnoses, obtain better case outcomes, optimize healthcare delivery operations and facilitate the transformation from volume to value based care.

Cloud computing is a one of the effective computing methods as compared to the conventional form of desktop computing. Today, this new technology has received great attention by researchers and organizations. The Remote Data Auditing (RDA) method is introduced to provide remote data storage in single cloud server domain with aim of improving the retrievable rate. Cloud data transaction was performed in a capable manner by different users at various access levels, but it fails to provide optimal security framework. Shield was designed with the objective of improving security using Merkle Hash Tree without the need of modifying the file system.

However, the cloud data storage technique in Shield has not concentrated on maximizing the security on performing the multiple data owners are considered in which the entire system is divided into numerous domains. The data is encrypted using AES technique and then for the purpose of broadcasting, the AES key is encrypted using Attribute Based Broadcast Encryption (ABBE) technique which uses the limitless size on attributes. But it creates complexity in providing immediate revocation in case of multiple authorities being online. An architecture based on cloud computing is used to secure the data and retain the sensitive information regarding the location of user data. The information regarding the location of data is identified using Global Positioning System (GPS). The limitation of this technique is that it works only in GPS enabled systems.

Optimal Integrity Policy method is used for data security in which private keys are generated based on AND, EXOR and hashing operations and then integrity of data is verified by using MAC process. Even though, the security is enhanced in this process, the decryption is very slow for the devices. The confidentiality is provided the detailed structure of Conditional Source Encryption based Data Transactional Security (CSEDTS) framework is constructed. The framework provides high secure transactions across different conditional attributes. Figure 1 shows data transactional security mechanism in cloud. The client sends requests to the cloud data storage system for the purpose of transactional processing. The proposed framework is concentrated on encrypting the conditional attribute from the source root systems, to improve the security level measure.

The client system sent request to cloud data storage for transactional processing. At first, the conditional attribute is evaluated by Bilinear Mapping Transformation function. Bilinear function performs one to one mapping to improve the transaction processing security. Finally, the conditional requests are updated to the decrypted conditional attribute from cloud data storage using CSEDTS framework. The concept used in CSEDTS framework increases the stochastic nature of the particle and attain maximum result with better solution.

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,

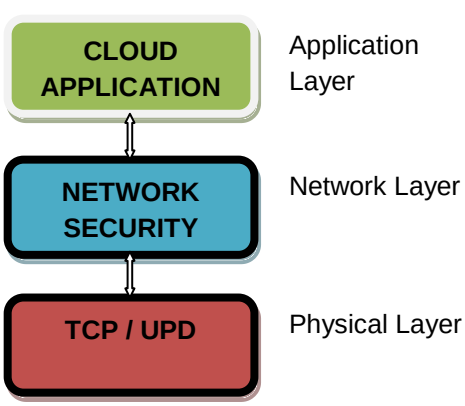

TABLE 3: Components of the Identity and Access Management

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.

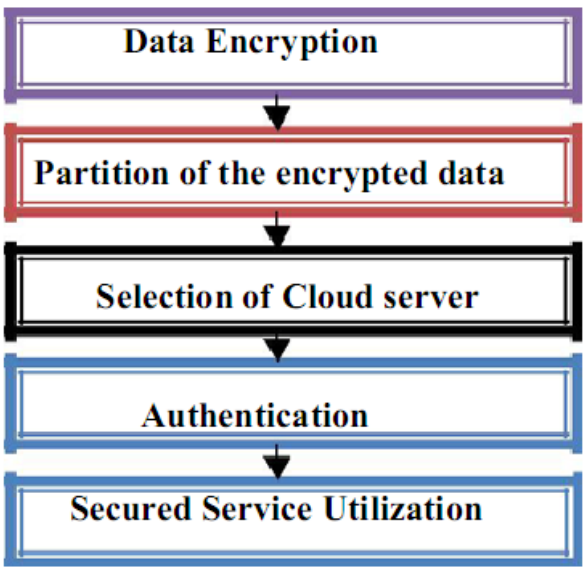

Figure 4 Components for OHSAM

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). $\perp$

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.

P1={(c1+k1),(c2+k2),(c3+k4),..,(cm+kn)}
P2={(c1+k1),(c2+k2),(c3+k4),..,(cm+kn)}
P3={(c1+k1),(c2+k2),(c3+k4),..,(cm+kn)}
P1,{(c1+k1),(c2+k2),(c3+k4),..,(cm+kn)}=0
P2,{(c1+k1),(c2+k2),(c3+k4),..,(cm+kn)}=0
P3,{(c1+k1),(c2+k2),(c3+k4),..,(cm+kn)}=0

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.