An Efficient Architecture and Enhanced Security to Cloud Services for Users

B.Vijay
Department of Computer Engineering
MITS College, Madanapalle, India
Bunnyvijay1@gmail.com

Dr.V.C.Bharathi
Senior Assistant Professor
Computer Science and Engineering,
MITS college
bharathivc@mits.ac.in

Abstract
The idea of a Cloud Service Broker(CSB) is quickly developing. The general part of the CSB is to transitional cloud Administrations. Where it has certain disadvantage. It is not customizable the way you want, no privacy, doesn't support large amounts of data transfer. To understand this, we have to distinguish the essential partners, characterize key prerequisites, and characterize the general structure of the CSB. It is these structural worries on which the present project is engaged. We propose a CSB we allude to as the virtual cloud bank. It intermediates inhabitant driven cloud benefits that satisfy the prerequisites of inhabitants. We additionally characterize the partners, their prerequisites, and the design of VCB. We present re-encrypted cloud data by using AES 256 bit provides privacy of data, keywords and trapdoors novel dynamic secret key generation protocol is used to prevent attackers from secret key thefting and acting as valid user

Key words: Virtual cloud bank; Third party; Trap doors; Dynamic secret key; Key words; Re-encryption

1. Introduction

Since twenty years cloud computing brought drastic change in hardware and software. During these years, it changed in terms of principles, protocols, and different designs. Now worldwide there are millions of tenants are there using the services of cloud computing. Cloud computing offers various benefits such as ease of utilization, elasticity, scalability, quality of service etc. Today many companies are providing services to the tenants to make more efficient and effective

Cloud computing has unique features. Even though it has many benefits cloud computing cannot do well in all applications. In cloud computing it is insecure to transfer large amounts of data transfer. As far as it is concerned about privacy and security are particular areas in where problem arises. Though virtualization and firewall provide security in the cloud, it cannot provide security outside of the cloud. Encryption is conventional way to secure the data but it has many challenges to use the encryption when it comes to the proxy server. Proxy server is intermediary between the one computer and another server. To make cloud computing services more effective the cloud service brokerage is introduced which send services with certain agreement and accurately to all the consumers. Here as far as we concern about the security it has challenges. Encryption cannot be used because it involves with the third party. Encryption makes to be depended on the proxy server.

More privacy is needed when it comes to the proxy server. When the plain text is transferring the trusted third party cannot learn the plaintext. And other intruders also cannot affect the data. It means more secure transfer of data is necessary. One should determine what security mechanism is suitable for the services in the cloud. The earliest encryption is not suitable for these services. However, the encryption in different aspect can be used to secure transfer of services. We cannot provide security unless you enhance the encryption. In fact most of the computers were depended on trusted third parties proxy server by decrypting the data by the server.

This paper focus on how to secure transfer of data from service provider to tenant where CSB acts as a third party doesn't read the plain text. So we should implement another move in cryptography that is Re-encrypt which doesn't depend on trusted third parties. This doesn't allow the third party member either to read or learn the plain text. Re-encryption is efficient and effective than the primitive encryption. Re-encryption provide services more accurately to the tenant than the primitive encryption by determining the exact key words. There is a separate key in the re-encryption. This key allows the third party to re-encrypt from one key to another so

the proxy serve either read the data or learn the plain text. This method is more reliability, secure both for the service provider and tenant. Based on this re-encrypt we will provide the services more accurately. To provide service more efficiently a Secure Re-encrypted search protocol Algorithm is used. By adopting this algorithm one can realize the objective of this re-encrypt search protocol algorithm

2. Related Work

At beginning many of the researchers make an attempt to provide the services more precisely that's where the cloud service brokerage was initiated. It made the tenants access the services more precisely. Even though cloud computing paradigm providing service to provide more precisely they begin with this new approach cloud service brokerage. The cloud service brokerage acts as a third party between the tenant and service provider. In cloud computing the client cannot approach the provider it means there is no communication between the service provider and client. By the cloud service brokerage although the client cannot interact directly with the service provider but client can interact through the intermediary that is cloud service brokerage interpreted as Virtual Cloud Bank (VCB)

In cloud service brokerage the researchers have modified many of the aspect in the CSB. They have modified to make more precise. In cloud computing there are many service among all these services SaaS, PaaS, IaaS are vital. In SaaS the tenant responsibility starts and terminated by managing the applications. In PaaS the tenant is responsible for installing and managing the applications. In IaaS Tenant is responsible for all the aspects of applications.

Badidi[10] stated that and proposed that providing SLA on the service of SaaS Provisioning. Only it limited to the certain services. The SLA is negotiated only based on the services provided to the tenant. It has certain contracts, policies. Badidi performed several operations on this approach. Service provision is significant task in this approach.

Ventincinque[11] stated and proposed that to optimize the SLA negotiation and management. This approach is to manage several resources and service. The main objective of the ventincinque approach was to provide optimize services between the service provider acts as the vendor and tenant acts as a consumer.

Ngan[12] stated and came up with a different proposing approach it depends on OWL-based semantic cloud discovery. The intermediary consists of semantic service repository. This approach focuses to seek the matched service using semantic technologies. This approach is entirely depended on the semantic technologies

2.1 *Challenges of the Existing system*

- There is no security.
- Lack of identification of stakeholders.
- When you use an application or service in the cloud, you are using something that isn't necessarily as customizable as you might want

3. Proposed Approach

In this approach using the secure Re-encrypted search protocol algorithm the services are provided. The cloud server provides access to the authenticated tenant by providing the specific key words. By authorization only specific owner and specific user can receive and access the data. In authorization not only the passwords were used but also the smart cards, hardware keys, and biometrics. Where cloud server which acts like a third party is intermediary between service providers and consumers as shown in Fig 1. Proxy server is cloud server which is responsible for linking the set of file and set of keywords. Whenever the tenant request service with particular secret keyword, the proxy server should provide that set of files to the tenant where these files are sent to cloud server by the service provider. If there is invalid secret keyword entered by the tenant then probably server cannot send the requested files to the proxy server

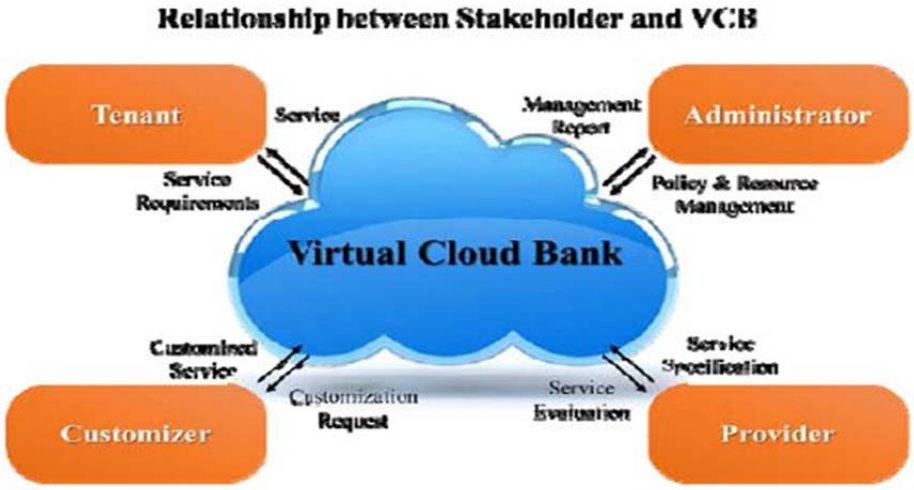

Fig1: Architecture showing how stake holders interact with VCB

3.1 *Algorithm*

Notations:

***F* means collection of files uploaded by owner.**

***C* means cipher text derived from plaintext.**

***T* means trapdoor generated by user.**

***D* means decrypting the file content by user.**

***K* means keywords forwarded to cloud.**

Secure re-encrypted search protocol Algorithm:

INPUT: *F, C, T, D, K*

OUTPUT: RETRIVED RELEVENT DOCUMENTS

STEP1: Owner re-encrypts the file send to cloud.

STEP2: Extracting keywords related to file is send to administration server.

STEP3: Admin server Re-encrypt the keywords and send to cloud.

STEP4: User behalf of data owner generates trapdoor forwarded to admin server.

STEP5: Admin server Re-encrypt keywords and send it to cloud.

STEP6: Cloud server matches the user search request with data owner encrypted keyword.

STEP6: if matching is success returns relevant document list.

STEP7: Otherwise returns unsuccessful result.

Here there is a re-encryption of files $C\ (F_1, C_1, T_1, D_1)$ are stored in the proxy server uploaded by the service provider. There are specific keywords defined $k\ (k_1, k_2, k_3, k_4)$ for these files. By entering the keyword the files sent to the administration server. Administration server Re-encrypt the key words and sent to cloud which is proxy server. The tenant generates the trapdoor and sent to admin server. Admin re-encrypt the keywords and send it the cloud. Cloud server matches the user search request with data owner encrypted keyword. If matching

is success returns relevant document list. Otherwise returns unsuccessful result. According to the secure re-encrypted search protocol algorithm it works.

Here re-encryption is used to give more privacy to files by re-encrypt the cipher text from one secret key to another without depending on the third party like proxy server. The re-encryption protocol algorithm explores new aspect in providing security to the files that are transferred between provider and user

It provides more privacy and security when compared to the other formats of encryption for secure transfer of files. To realize this concept we should implement it practically. It is more effective and efficient than the other approaches. Reliability can be achieved through the re-encryption algorithm. One thing the stakeholders must notice that when entering the keyword taken utmost care so that no loss of data will be done. By this either tenant or service provider are not depended on the third party which makes secure transfer of data

4. Conclusion

No intruder can modify or hack the services between the tenant and the cloud service provider. In addition to that it provides the Quality of Service (QoS) to the tenants. This system has the reliable transfer of the data between consumer and provider. By adopting this system it makes ease for tenant and service provider

The primary focus of our proposed VCB is its use for intermediation and its provision of tenant-centric cloud services. A primary difference between related works and ours is our clear definition and description of architectural concerns. We have identified the key stakeholders that interact with VCB. In addition, we explicitly defined the key functions relating key stakeholders. Finally, we proposed a layered VCB architecture that consists of an access interface layer, a service brokerage layer, an operation support layer, and an evolution management layer.

References

[1] B. Wadhwa, A. Jaitly and B. Suri, “Cloud Service Brokers An emerging trend in cloud adoption and migration”, Asia-Pacific Software Engineering Conference, pp. 140-145, Dec. 2013
[2] S. Somashekar, “Opportunities for the Cloud in the Enterprise”, Product Startegy White Paper, 2010
[3] Gartner, http://www.gartner.com/it-glossary/cloud-services-brokeragecsb
[4] R. Bohn, J. Messina, F. Liu, J. Tong, and J. Mao, “NIST CloudComputing Reference Architecture”, NIST Special Publication, Jul.2011
[5] L. Bass, P. Clements and R. Kazman, “Software Architecture in Practice”, Addison-Wesley, 1998
[6] NIST Cloud Computing Program, http://www.nist.gov/itl/cloud/
[7] SPI model, http://searchcloudcomputing.techtarget.com/definition/SPImodel, Feb. 2012
[8] L. Badger, R. Bohn, S. Chu, M. Hogan, F. Liu, V. Kaufmann, J. Mao, J. Messina, K. Mills, A. Sokol, J. Tong, F. Whiteside and D. Leaf, “US Government Cloud Computing Technology Roadmap Volume IIRelease 1.0”, NIST, Nov. 2011
[9] D. Morrison, “The evolution of cloud service brokerage”http://www.huawei.com/en/static/HW-193390.pdf, Sep. 2012
[10] E. Badidi, “A Cloud Service Broker for SLA-based SaaS Provisioning”, International Conference on Information Society, pp. 61-66, Jun. 2013
[11] S. Venticinque, R. Aversa, B. Martino, M. Rak, and D. Petcu, “A Cloud Agency for SLA Negotiation and Management”, Euro-Par 2010 Parallel Processing Workshops Lecture Notes in Computer Science, Vol. 6586, pp. 587-594, 2011
[12] L. Ngan and R. Kanagasabai, “OWL-S Based Semantic Cloud Service Broker”, International Conference on Web Services, pp. 560-567, Jun. 2012[13]Barrie Sosinsky, “cloud computing”, Copyright 2011 by Wiley publishing, Inc. , Indianapolis, indiana