International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
www.ijset.com, Volume No.1, Issue No.2 pg:216-221 01 April 2012

# A Conceptual Architecture for Securing public Cloud: **Moving from Trust toward Security**

**Yashpal Kadam**
PG Scholar (M.Tech): Computer Science and Engineering Department
Lakshmi Narain College of Technology, Indore
Yashpal.kadam@rediffmail.com

Abstract— **Cloud computing is next generation era of IT enterprise, which provide services like resource pooling, on demand and metered service. It provides the burden free environment for the consumer, to get rid of resource management. It also shifts all digital assets (data and application) to the centralized large datacentre. These datacentre can be on- premise or off-premise cloud service provider, depending on the nature of cloud service consumer i.e. either general public or small scale enterprise. Such type of cloud consumers need are generally fulfilled by off-premises clouds which are handled by third party cloud service provider, which increases the security threat for identity and access, data privacy and security. Thus cloud consumer has to keep a high level of trust on cloud provider. Thus the conceptual architecture for securing the public cloud is the concept which will help to provide a high level of security in spite of trust for the public cloud. This work proposes a third party "Special Security Agent (SSA)" which will be a government body or certified authority, for maintaining the security and identity of digital asset for both cloud provider and consumer.**

***Keywords***- Cloud Security, security, cloud architecture, computing security agent.

## I. INTRODUCTION

Cloud computing is emerging technology which can be described as the use of a collection of services, applications, information, and infrastructure comprised of pools of network, information and storage resources [1]. These components can be frequently rearranged, delivered, established, removed and scaled up or down providing for an on-demand utility-like model of allocations and consumption [3]. With the ever widening vistas cloud computing has increased the internet- based development, and smart use of underlying resources. The increase in the availability and flexibility of network capabilities has made cloud to be the first choice for any IT enterprise or a developer [2].

The different levels of cloud service model have provided the cheapest and powerful architecture. These three models are software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS) which are transferring data centre in to pools of services. Using the cloud services for storing the data and using it for various other applications such as platform and infrastructure as a service, provides a great convenience to user who now need not to

Manage the resources. With cloud computing the consumer at lower end can use the expensive and emerging technology according to his demand , they do not need to purchase the new costly hardware, software permanently and rapidly but they can rely on Pay as you Go model. There are several mechanisms through which the identity and access management is done, but there is lack of security in terms of data and identity preservation. The cloud service consumer (CSC) can only trust on the cloud service provider (CSP) for privacy and security of his digital assets. Some security breach incidents that occurred in Amazon EC2 cloud [9], which not only infected and hack the Amazon database but also some data of Sony play station was hacked by unauthorised access of IaaS [5]. In December 2010, first major cloud data breach happened at Microsoft announced that data contained within its Business Productivity Online Suite (BPOS) has been downloaded by non-authorized users [9-10].

There are much similar stories which are on the board in 2010 and 2011.

The solution to this problem is much important which is framed in the current work, which relies on authentication and encryption process. The idea behind securing cloud in all aspect is through a special security agent (SSA), which will provide data security and user authentication through some identity and access management techniques.

The problem related securing identity and access of the data and services are most important. As we seen earlier with data breach incident lots of data has been stolen, so at that end if some lock has been provided for security of information could have prevented breach. The security towards the unauthorised access can be prevented by authenticating user to access the data and encrypting data. Yes it is truth that most of the users are afraid of loss of data during encryption, but having secure and reliable encryption technique put downs the threat. Now, what happens if the encryption agent is on the cloud premises or in the hand of some third party agents, the threat to insider access is still there. But no one has to worry about the insider access as the data will be stored at cloud provider end and the security key is stored at SSA. The interesting fact is that the CSP has the encrypted data and the SSA will have only the key. The problem of lack of security to public cloud user digital asset and services is concerned with the current issue. And the paper deals in details with the working of the conceptual architectural framework for securing public cloud.

## II. Related work

A lot of work has been done in the auditing and preserving the data at the cloud. The consideration of insider access threat is never considered and faith (trust) on the CSP comes in to account. The third party auditor (TPA) is also one of the approaches to have the data integrity [3]. The third party auditor is the agent which checks about the data locality and ensures user that their data are correctly stored and maintained. The main role of TPA is auditing the cloud and check the data integrity and storage on demand of user [4]. All these operations which are carried out by TPA are only to assure the storage of the data, initiated when any consumer or customer request.

Consideration of the other services provided by the cloud should also be focused in the current issue. The cloud provides metered services, platform and infrastructure services through virtualization techniques [18]. These services should also be kept under the security parameters such that they should be monitored and complete security provided towards user's digital assets and services.

### A. Proposed model

A conceptual architectural framework is illustrated in Figure1. There are three entities in the network which are identified as:

1. **User(CSC):** is an entity that will use the cloud service according to need. He may store his data, use platform and infrastructure as a service.
2. **Cloud Service Provider (CSP):** is an entity which is providing the cloud services. Here it is assumed that the CSP is providing the three services or providing the multi-tenant services.

The CSP should be pre-requisite to have communication mechanism i.e. it should be registered with SSA.

3. Special Security Agent (SSA): Special Security Agent identify and authorize the user on one hand, on other hand provides the asymmetric keys for encryption and decryption of the data which has to be stored on cloud.
    a. **Authenticator & key manager**: this server is responsible for authenticating, the user to preserve the identity, and also responsible for the key generation mapped with the user identity and to save the key on storage and provide the key at dynamic time when CSC requests.
    b. **Storage:** The storage is used to store the key and algorithm used to encrypt or decrypt the data, mapped with the cloud provider and user. Here two storage and two connections are provided for back up mechanism.
4. **Encryption n Decryption Agent**

**(EnDa)**: this will authorize the user to access the data by maintain the data identity to user and vice versa and also encrypt and decrypt the data when demanded.

a. Key logics: The model of key logic is such that is ask for public key from the SSA for the encryption of data, but at the time of decryption it sends the file and the public key generated by the CSP is send to the SSA, so that the file will be decrypted by the SSA and re-encrypt it.

In a cloud environment, a user stores the data, uses the services such as PaaS, S aaS through CSP which begins and ends at CSP. Now those data and services which are on the CSP distributed data storage, and virtualized server have no visibility for a user. The data or service at cloud may be having a threat towards the insider access, hacking, and malicious attacks.

### B. Design Goals

To ensure security, identity and access of the cloud resources, we have envisioned a conceptual architectural for dynamic securing the identity and data on the cloud. In the current work, we are proposing a conceptual architectural which should be helpful in managing the user, cloud provider and also the data and resources identity and access. We hereby proposing this model for ensuring the security and identity of the services used by the user provided by cloud provider to achieve the following goals:

1. Data Security: Ensure the user that data stored in cloud is now safe, there is no threat from insider access, malicious attacks.
2. Identity management: A single user on the cloud will have a single identity and the data stored on the cloud will be encrypted such that it will have a unique key for decryption stored at SSA.
3. Access management: The user which has created the data or permitted user can only access the data as the data saved is encrypted by only public key at cloud, the private key is at SSA, and the file is send to SSA for decryption.
4. Key Management: As both the user and cloud provider does not know about the inside mechanism of SSA and End, so to attempt for cracking the key strategy will be difficult.
5. The SSA proposed here should requested to be maintained by government bodies of expert or authority, so that the customer who has its unique identity number or if someone have unique identification as UID, SSN can only be allowed to access the cloud.
6. Audit ability on the user request will be easier.

### C .Working

The working of the proposed architectural work is proposed in the Figure 1, as the task is numbered from 1 to 7. For the sake of simplicity, and understanding the work we just here understand the whole mechanism or process with the assumption that there is user who is accessing the public cloud for say storing his file or some documents. Now as shown above we are having a SSA, CSP with EnDa, user. So let us analyse the whole scenario as in the following steps:

1. At step 1 the user has to login at SSA, with the user name and provided at the time of registration at SSA. The user also has to verify his/her unique identity.

$$\text{User} \xrightarrow{\textit{request authentication}} \text{SSA}$$

$$(IP_U+U_{name}+P_{asswd}+OS_{details})$$

The SSA create the log for the username and password with the details send by the user

2. In step 2, The SSA create the log for the username and password with the details send by the user

$$\text{SSA} \xrightarrow{\textit{request authentication}} \text{User}$$

$$(T_{suc+}E(T_{seesion}(IP_{user}))),$$

3. At step 3 the user logins at CSP by the username and password provided to the CSP at the time of registration, for accessing service.

$$\text{User} \xrightarrow{\textit{request login}} \text{CSP}$$

$$(U_{nameC}+IP_u+P_{wdC}),$$

4. At step 4, the CSP verify the user session on SSA, by providing the details as $IP_{user}$ and the

username at CSP.

$$\text{CSP} \xrightarrow{\textit{request authentication}} \text{SSA}$$

$(IPu+U_{nameC}+S_{tupe})$,

5. At step 5, the SSA checks for the username and IP, if finds a session then replies with a success message. And make the log entry for the user access.

$$\text{CSP} \xrightarrow{\textit{replies}} \text{User}$$

$(P_{CSP}+T_{sCSP})$,

6. At step 6 the user creates the data and wants to save that data, The CSP cannot save the data directly if only user wishes; it has to pass through EnDa that is it has to make entry about the data at SSA and ask for the public key form SSA.

$$\text{User} \xrightarrow{\textit{Creats ,upload file}} \text{CSP}$$

$$\text{EnDa} \xrightarrow{\textit{request for the public key}} \text{SSA}$$

$(IP_u+U_{nameC}+L_{time})$,

7. At step 7, the EnDa gets the key and type of encryption so that to encrypt the user file and save it to CSP.

$$\text{SSA} \xrightarrow{\textit{replies}} \text{EnDa}$$

$(IP_u+U_{nameC}+PK_{unameC})$,

This mechanism and working is supposed to be performed with the proposed architecture. The reverse to decrypt the file can be carried out in the similar manner. The working of the conceptual model clearly shows that how the conceptual architecture is going to preserve the identity and access of the data in the public cloud.

### D. Features

Here through this model we have tried to propose a dynamic model for authentication and key generation and storage. This model may fit to ensure the data is accessed by any of the authorized user. The feature of this model is that this model not only focuses to ensure the data but also focus to ensure the security to each level of cloud whether it is SaaS or PaaS. Since the resource is not located at local site so supporting dynamic operation might be challenging.

For this we purpose to authority or the experts to make some rules and regulation for CSP, which should be followed. The important feature to design such Architecture is that the cloud service provider should have a transparency with SLA and the metered servicer. Also it will helpful in studying the frauds easily.

## IV. CONCLUSION AND FUTURE WORK

The framework in this paper may be the first framework of this kind to provide a secured and transparent view to user and increase the level of security and also as the level of security increases the level of trust and attraction to use the cloud technology will increase rapidly.

Basically, the approach is the conceptual architecture for securing public cloud has been developed to move the security over the trust factor in cloud. The architecture proposed here presents the security to each and every level of the cloud computing present architecture. Here the approach is to identify the trusted data privacy, key management and identification problem is a major issue cloud computing, and that conceptual architecture is solution to this problem. The SSA proposed in the work has following properties:

- SSA should be governed by Government organisation.
- SSA accepts SSA number or any valid photo-proof for identity of user.
- SSA cadre should be installed in every country.
- So that legal action can be done against the defaulter.
- SSA secures the data by providing keys.
- SSA helps in solving the disputes.
- SSA keeps the static of the CSP.

So the SSA is multi-featured solution also the future expansion is also needed.

Cloud computing is the vast and the latest trend in the information technology. As we here are not able to look at each part of the cloud so there are some future works so that this can be extended also here only the SaaS and PaaS model is considered, and was less focus on the IaaS, so in future work there can be some concept regarding to the security focused on IaaS. Also algorithm has to be developed for less time consumption in encryption decryption and user identification.

## REFRENCES

1. Wayne Jansen, Timothy Grace, “Guidelines for security and privacy in pubic cloud”, Draft Special Publication 800-144.
2. Bring hay, Kara Nance, Matt Bishop “Storm cloud rising: security challenges for IaaS cloud computing”, proceedings of the 44th hawii international conference on system science.
3. Quain Wang, Cong Wang, kui ren, wenjing lou, Jin li,” Enabling public Audibility and data dynamics for storage in cloud computing”, IEEE , Parallel and distributed system conference, May -2011.
4. Cong Wang, Quain Wang, Kui Ren, Ning Cao and Wenjing Lou.” Towards secure and Dependable Storage Services in Cloud Computing.” IEEE JAN-2011
5. Neal Leavitt. Is Cloud Computing Really Ready for Prime Time?, IEEE Computer, January 2009.
6. Luis M. Vaquero1, Luis Rodero-Merino1, Juan Caceres, Maik Lindner, A Break in the Clouds: Towards a Cloud Definition, Computer Communication Review (CCR) Online, Short technical Notes, January2009, <URL:http://ccr.sigcomm.org/online/files/p50 -v39n1l- vaqueroA.pdf>.
7. Wayne A Jansen,”Cloud hooks: security and privacy issue in cloud computing.”, Proceeding of 44th Hawaii internation conference on system science-2011,1530-1605-2011.
8. CSI communication special issue on cloud computing volume-35, issue 2, May-2011. Abhay kumar jt.ddg(IT),”Information security policy and regulation issue”<url:http://*www. alttc.bsnl.co.in/altzine/Vol_31122005/ns/l2.pps* >
9. Sony Network Breach Shows Amazon Cloud Appeal for Hackershttp://www .businessweek .com/news/2011-05-16/sony-network-breach-shows-amazon-cloud-s-appeal-for -hackers.html.
10. Pcworld, Microsoft cloud data breach herald’s things to come. <url:http://www. pcworld.com/businesscenter/article/214775/microsoft_cloud_data_breach_heralds_things_to_come.html>
11. S. Subashini n, V.Kavitha “A survey on security issues in service delivery models of cloud-computing”.<url:http://www.elsevier .com/locate/jnca>.
12. Warwick Ashford, Google Confirms Dismissal of Engineer for Breaching Privacy Rules, Computer Weekly, September 16, 2010, URL:http://www.computerweekly .com/Articles/2010/09/16/242877/Google-confir msdismissal-of-engineer-for-breaching-privacy.htm
13. Frederick M. Avolio, Best Practices in Network Security, Network Computing, March 20, 2000, <URL:http://www.network computing.com/1105/1105f2.html>.
14. David Binning, Top Five Cloud Computing Security Issues, Computer Weekly, April24, 2009,<URL:http://www.computerweekly.com/ Articles/2010/01/12/235782/Topfive-cloud-computing-security-issues.htm>.
15. Simon Bradshaw, Christopher Millard, Ian Walden, Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services, Queen Mary School of Law Legal Studies, ResearchPaperno.63/2010,September2,2010,< URL:http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1662374>.
16. Domain 12: Guidance for Identity & Access Management V2.1 Prepared by the Cloud Security Alliance April 2010 URL:http:// www.cloudsecurityalliance.org/guidance/csaguide-dom12- v2.10.pdf
17. Jon Brodkin, Loss of Customer Data Spurs Closure of Online Storage Service, The Linkup, Network World, August 11, 2008, <URL:http:// www.networkworld.com/news/2008/081108-linkup-failure.html?page=1>.
18. Secass, Security as a working group”Defined categories of services 2011”. url:https:// cloudsecurityalliance.org/research/working-groups/security-as-a-service/
19. Mandeep Khera,CTO-Cenzic

<url:http://s1.Sec urityweek.com/addressing-cloud-security-concerns- key-issues-and-recommendations>

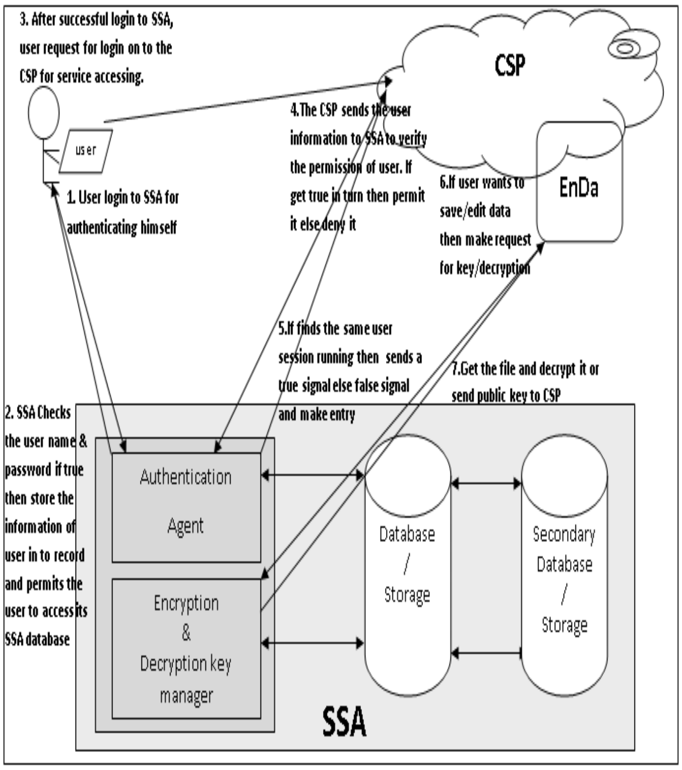
3. After successful login to SSA, user request for login on to the CSP for service accessing.
CSP
user
1. User login to SSA for authenticating himself
4.The CSP sends the user information to SSA to verify the permission of user. If get true in turn then permit it else deny it
6.If user wants to save/edit data then make request for key/decryption
EnDa
5.If finds the same user session running then sends a true signal else false signal and make entry
7.Get the file and decrypt it or send public key to CSP
2. SSA Checks the user name & password if true then store the information of user in to record and permits the user to access its SSA database
Authentication Agent
Encryption & Decryption key manager
Database / Storage
Secondary Database / Storage
SSA

**Figure 1: Proposed Architectural Model for Securing Cloud**

## Author Biography

**Yashpal kadam (Ujjain, 10-March-1988)** received the B.E. degree from RGPV University, India in 2009 in Computer Science & Engineering. He has also received RHCSA certification from Red Hat. He is currently working towards M.Tech degree from RGPV University, India in Computer Science & Engineering. His research interest includes Public cloud computing security and network security and privacy.