A CHALLENGE FOR SECURITY AND SERVICE LEVEL AGREEMENT IN CLOUD COMPUTINGE

R. Chawngsangpuii[1], Rohit Kumar Das[2], Vanlalhruaia[3]

[1]*Senior Asst. Professor, Department of Information Technology, Mizoram University, Mizoram, India*
[2]*Lecturer, Department of Information Technology, Mizoram University, Mizoram, India*
[3]*Assistant Professor, Department of Information Technology, Mizoram University, Mizoram, India*

Abstract

One of the most promising field in computing is regarded as cloud computing, which allows users to store their data virtually over the cloud without the need of any fixed infrastructure. It offer user to manipulate their data regardless of the geographical position, hence providing a scalable, feasible and flexible way to connect user to their data. The cloud can be considered as of the Internet where data are usually stored and computing refers to the applications and services that it can provide. Users are connected to cloud by Cloud Service Providers through the Internet connection. Both users and cloud service provider agree on a protocol known as service level agreements for exchange of information. Cloud computing provides increase in capacity and grants the capability to perform computation on cloud infrastructure to its users. Cloud Computing is capable of providing more convenient communication and instant multi-point collaboration feature. Cloud computing provides better utilization of distributed resource over large amount of data and they can be access remotely through the internet. Quality of service should be kept in mind will designing the service level agreement. There are many problem related to cloud computing such as traffic managements, security and privacy. This paper provides a survey on the basic working principle of clouding computing. This paper provides an overview of the cloud architecture including the different types and level of clouds services. In this paper focus has been made upon the service level agreement, issue and security prospectus over the cloud computing.

Keywords: *Architecture, Cloud Computing, Cloud Security, Cloud Services Service Level Agreements*

----------***----------

1. INTRODUCTION

Storing user data in clouds where clouds acts as a virtual storage system is term as cloud computing and is an emerging field in relation to computing. The basic idea is that if a user wants to store data over the cloud, user simply send data files over the internet that are stored in data server through a web interface and when wants the data back from the server, user need to send request to the server. The server then sends back the data in which the user can manipulate and update the data. Data centre acts as a house for cloud storage system capable of storing different kind and amount of data.

Infrastructure, platform, software and other resources are providing scalable, feasible and flexible access to clouds for the users to virtually store their data. In cloud computing, network resources like servers, storage applications and services are performing as opportune assets to the user for meeting the demand of storage for cloud data. The merchants that are providing access to cloud are known as Cloud Service Providers (CSPs) [1]. Service Level Agreements (SLA) is an agreement between the service provider and their customer who agrees on the terms and condition specified in the SLA and is been described in detail later in the paper.

The primary types of cloud that CSPs want to provide to their customer can be of three types:

- **Public Cloud:** Large industrial group or the general public use this type of cloud and hence the name public cloud. This type of cloud are generally own and handle by the CSPs itself but the security intensity is quit stumpy where as the advantage is that the resources are provided by the CSPs so the set-up is inexpensive and easy to use. Examples of public clouds include Amazon Elastic Compute Cloud (EC2), IBM's Blue Cloud, Sun Cloud, Google AppEngine and Windows Azure Services Platform.
- **Private Cloud:** A private cloud is own and managed by the organization it serves. This type of cloud provides more control over the data that are stored within the cloud, and it ensures high security level on compare to public cloud, even though with greater potential risk for data loss due to natural disaster. Amazon's Elastic Compute Cloud (EC2) or Simple Storage Service (S3) is the third-party host that can provide this service.
- **Hybrid Cloud:** As the name suggest, hybrid cloud are those which forms from the combination of public and private cloud and takes the advantages like stability, reliability, cost saving aspects from public cloud system and maintainers and security aspects from private cloud systems.

Cloud computing is regarded as one of the immerging topic in the field of computing. The cost effectiveness, scalability and reliability make it more attractive to use. Lots of issues and challenges have been resolved. But how far it is secure is still the prime question.

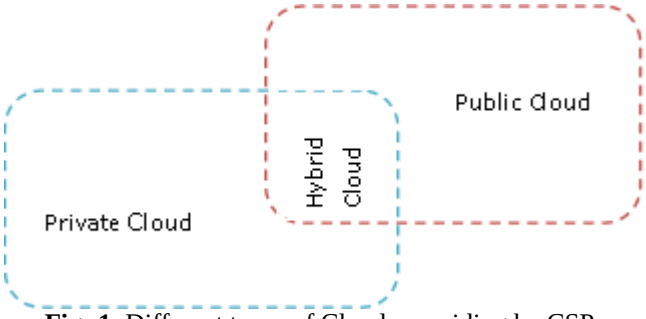

Fig -1: Different types of Clouds providing by CSPs

2. RELATED WORK

The authors of [4] relate the issue regarding the security and privacy to the user data. Data resiliency and reliability of server have also been considered as cloud server can also go downfall. The vulnerabilities of virtualization in cloud computing infrastructure are described by the authors of [5]. The authors of [6] have provided some of security, cost effectiveness and virtualization survey and the current methods addressing them. The aspects of security, comparison of trust/reputation models and privacy-preservation schemes are described by the authors of [7].

3. ARCHITECTURE OF CLOUD COMPUTING

Cloud computing architecture consists of two parts: Front-end (Users) and Back-end (Clouds). Users are connected to cloud through Internet. The Internet acts as a middleware and the connection of Internet can be of point-to-point or peer-to-peer connection depending upon the type of cloud they want to access. Front-end consists of users and the application like web browser whereas the back-end consists of cloud services like providing virtual servers, data storage system, etc [2].

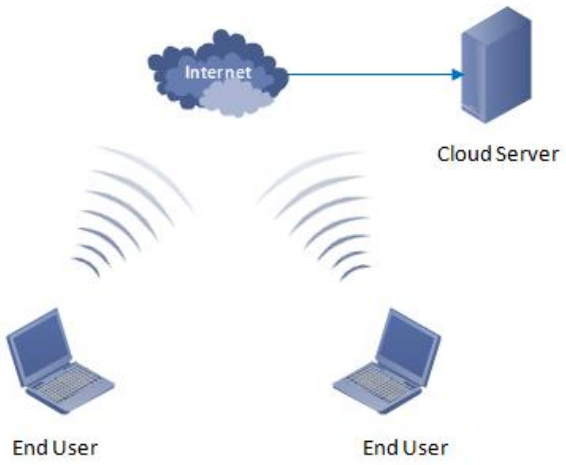

Fig -2: Conceptual diagram of cloud computing

There are certain layers which connects the user to server. These are Application layer, Platform layer and Infrastructure layer as shown in the figure below:

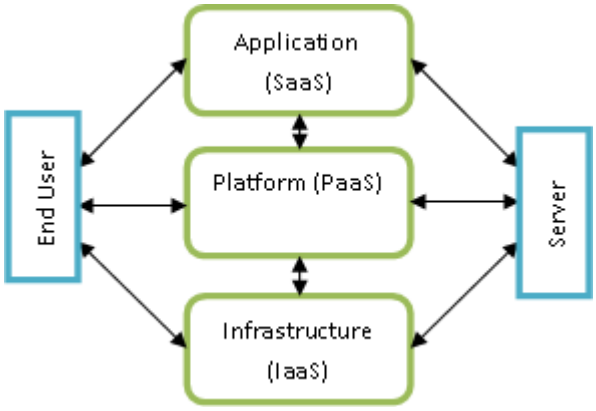

Fig -3: Cloud computing Architectural diagram

Each of the layers can be illustrate as:

- **Software as a Service (SaaS):** It forms the topmost layer where with SaaS, everything is provided as an application or service to the clients who eliminate the need for installation of software or application services in the client side; the only thing is that the client needs to purchase the ability to access them as define in SLA. Standard examples for this are Salesforce.com and Hotmail which are web browser based services.
- **Platform as a Service (PaaS):** It acts as middle layer where with PaaS, using the cloud infrastructure like operating system or software framework computing platform is provided to the clients. Standard example for PaaS can include Windows Azure and Google Apps.
- **Infrastructure as a Service (IaaS):** It is the bottommost layer and the function is to grant the infrastructure based services virtually to the clients that include hardware for storing client data and the network resources, etc for which charges are applied only when the clients are access to those virtual resources, hence making the task cost economical and prompt. Standard example includes GoGrid and Google cloud storage.

4. SERVICE LEVEL AGREEMENT

Service Level Agreement (SLA) is a documenting process which includes some protocol and is sited between the client and cloud service provider (CSPs). Services to the clients are provided based upon the agreements which are agreed by both client and CSPs. SLA can be of both informal contract of legal contract between two parties [8].

The objectives of SLA Agreement are to:

- Provide clear reference to service ownership, accountability, roles and responsibilities.
- Provide a mechanism for review and change to the service levels over the course of the contract.
- Present a clear, concise and measurable description of service provision to the customer.
- Match perceptions of expected service provision with actual service support & delivery.

- Provide an ongoing reporting mechanism for measuring the expected performance standards

Service Level Agreement can be divided based on different levels:

- **Service-based SLA:** Based on the agreement, the service provider provides services to all the customers
- **Customer-based SLA:** Based on the agreement, services are provided with an individual customer groups.
- **Multi-level SLA:** The SLA is split into the different levels, each addressing different set of customers for the same services, in the same SLA.

5. SECURITY ISSUE RELATED TO CLOUD COMPUTING

As with advancement of technology, it comes with disadvantage also. Till date there are lots of issue which has been taken care. Despite the consequences, Security is regarded as one of major issue which need more attention from both the cloud providers and their customer's point of view. Cloud Service Providers (CSPs) furnish different security level to all the services it provides [3] [5].

The following are some of the important aspects related to security measures:

- **Restriction to user access:** As the data are moving out from the clients to the cloud, the level of risk increase in terms of management, multiple placements etc. The enterprise client may want to store huge amount of data in cloud. After storing those data, the enterprise client possibly will want to manipulate that data. Now, multiple accesses to those may create problem in handling those data for the CSP as well. Therefore, access to those valuable data must be restricted to some of the user only.
- **Malicious attack to client's data:** The third party attack to the client data from a former employee or a business partner can cause harm. The passive attacker can have increasing levels of access to more critical systems and eventually to data.
- **Isolation of client's data:** CSP store their client data in alongside manner. Data integrity is one of the major concerns. CSP ensures that the client data are well maintained. But as multiple data are stored in a shared cloud, there is a possibility of getting data conflict though CSP provided proper encryption.
- **Long-term viability of client's data:** Ideally, the CSPs will never go broke or get acquired and swallowed up by a larger company. But the client must be sure that data will remain available even after such an event.

Shared technology vulnerabilities to client's data: To provide a scalable way to access data, CSPs share infrastructure, platforms, and applications. The shared infrastructure may include CPU caches or GPUs which are not specifically designed for multi inhabitant architecture (IaaS), re-deployable platforms (PaaS), or multi-customer applications (SaaS), the threat of shared vulnerabilities exists in all delivery models.

6. CONCLUSION

Cloud computing is an emerging paradigm which provide a feasible way to store data virtually over the internet without the need of any physical infrastructure. The service level agreement plays an important role in cloud computing for which it has been included in this paper. One of the major issue or challenge is refer to be the security meadow as in cloud computing system is shared between many users for which crucial measures are needed to protect the client data.

REFERENCES

[1]. Abdulelah Almishal and Ahmed E. Youssef, "Cloud Service Providers: A Comparative Study", International Journal of Computer Applications & Information Technology Vol. 5, Issue II, ISSN: 2278-7720, 2014

[2]. W. Tsai, X. Sun, J. Balasooriya, "Service-Oriented Cloud Computing Architecture", 7th IEEE International Conference on Information Technology, 2010

[3]. Dinadayalan, P., S. Jegadeeswari, and D. Gnanambigai, "Data Security Issues in Cloud Environment and Solutions", Computing and Communication Technologies (WCCCT), 2014 World Congress on. IEEE, 2014

[4]. Yashpalsinh Jadeja and Kirit Modi, "Cloud Computing - Concepts, Architecture and Challenges", International Conference on Computing, Electronics and Electrical Technologies [ICCEET], 2012

[5]. P.Purniemaa, R. Jagadeesh Kannan and N.Jaisankar, "Security Threat and Attack in Cloud Infrastructure: A Survey", The International Journal of Computer Science & Applications (TIJCSA) ISSN – 2278-1080, Vol. 2 No. 06, 2013

[6]. Nandini Mishra , Kanchan khushwha, Ritu chasta and Er. Abhishek Choudhary, "Technologies of Cloud Computing – Architecture Concepts based on Security and its Challenges", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 3, ISSN: 2278 – 1323, 2013

[7]. Fei Hu, Meikang Qiu, Jiayin Li, Travis Grant, Draw Tylor, Seth McCaleb, Lee Butler and Richard Hamner, "A Review on Cloud Computing: Design Challenges in Architecture and Security", Journal of Computing and Information Technology - CIT 19, 2011

[8]. Patel, Pankesh, Ajith H. Ranabahu, and Amit P. Sheth, "Service level agreement in cloud computing", 2009

BIOGRAPHIES

R. Chawngsangpuii received her M.Sc degree in Computer Science from Bharathiar University, Coimbatore, India. Her interest for area of research work is in Cloud Computing and Grid Computing.

Rohit Kumar Das received his M.Tech degree in Information Technology from Assam University, Silchar, India. His interest for area of research work is in Network Security and Wireless Networking.

Vanlalhruaia received his M.Tech degree in Information Technology from Tezpur University, Tezpur, India. His interest for area of research work is in Cloud Computing and Network Security