International Journal of Electronics Communication and Computer Engineering
Volume 4, Issue (6) NCRTCST-2013, ISSN 2249–071X

National Conference on Recent Trends in Computer Science and Technology (NCRTCST)-2013

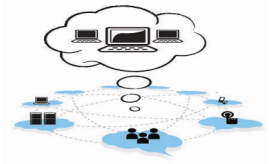
The Theoretical Approach to Cloud Computing

-A Congenerical Approach

Hemanth Kumar TS MCA, [M.Tech.(IT)]
Associate
First American India, Bangalore, Karnataka
Email: hemanthkumarts11@gmail.com

***Abstract* – Being the vast area in research, the cloud stands first in the Storage and Security. Though the demand is more, some ethics have to be followed for the security. The paper unravels the basic service models, deployment of the clouds and the security architecture. The different security aspects is being discussed in the paper.**

***Keywords* – Cloud Computing, Security, Private, Public, Architecture.**



I. INTRODUCTION

The importance of Cloud Computing is increasing and it is receiving a growing attention in the scientific and industrial communities. Cloud Computing enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. A 'cloud' is an elastic execution environment of resources involving multiple stakeholders and providing a metered service at multiple granularities for a specified level of quality (of service). Cloud Computing appears as a computational paradigm as well as a distribution architecture and its main objective is to provide secure, quick, convenient data storage and net computing service, with all computing resources visualized as services and delivered over the Internet.

Cloud Computing combines a number of computing concepts and technologies such as Service Oriented Architecture (SOA), Web 2.0, virtualization and other technologies with reliance on the Internet.

Security concerns relate to risk areas such as external data storage, dependency on the "public" internet, lack of control, multi-tenancy and integration with internal security. Compared to traditional technologies, the cloud has many specific features, such as its large scale and the fact that resources belonging to cloud providers are completely distributed, heterogeneous and totally virtualized. Traditional security mechanisms such as identity, authentication, and authorization are no longer enough for clouds in their current form. Security controls in Cloud Computing are, for the most part, no different than security controls in any IT environment.

II. CLOUD SERVICE MODELS

Infrastructure as a Service (IaaS) involves the vendor providing physical computer hardware including CPU processing, memory, data storage and network connectivity. The vendor may share their hardware among multiple customers referred to as "multiple tenants" using virtualisation software. IaaS enables customers to run operating systems and software applications of their choice.

Platform as a Service (PaaS) involves the vendor providing Infrastructure as a Service plus operating systems and server applications such as web servers. PaaS enables customers to use the vendor's cloud infrastructure to deploy web applications and other software developed by the customer using programming languages supported by the vendor.

Software as a Service (SaaS) involves the vendor using their cloud infrastructure and cloud platforms to provide customers with software applications. Example applications include email and an environment for users to collaboratively develop and share files such as documents and spreadsheets. These end user applications are typically accessed by users via a web browser, eliminating the need for the user to install or maintain additional software. Typically the vendor controls and maintains the physical computer hardware, operating systems and software applications.

III. DEPLOYMENT OF THE CLOUD

Public cloud involves an organisation using a vendor's cloud infrastructure which is shared via the Internet with many other organisations and other members of the public. This model has maximum potential cost efficiencies due to economies of scale. However, this model has a variety of inherent security risks that need to be considered.

Private cloud involves an organisation's exclusive use of cloud infrastructure and services located at the organisation's premises or offsite, and managed by the organisation or a vendor. Compared to the public cloud model, the private cloud model has reduced potential cost efficiencies. If the private cloud is properly implemented

and operated, it has reduced potential security concerns. A well architected private cloud properly managed by a vendor provides many of the benefits of a public cloud, but with increased control over security.A managed private cloud may enable enterprise customers to more easily negotiate suitable contracts with the vendor, instead of being forced to accept the generic contracts designed for the consumer mass market that are offered by some public cloud vendors.

Community cloud involves a private cloud that is shared by several organisations with similar security requirements and a need to store or process data of similar sensitivity. This model attempts to obtain most of the security benefits of a private cloud, and most of the economic benefits of a public cloud. An example community cloud is the sharing of a private cloud by several agencies of the same government.

Hybrid cloud involves a combination of cloud models. An example is using commodity resources from a public cloud such as web servers to display non-sensitive data, which interacts with sensitive data stored or processed in a private cloud.

How does Cloud Computing differ from traditional IT outsourcing? The use of cloud services is similar in many ways to classic outsourcing, but there are certain differences which need to be taken into account:

- For financial reasons, multiple users in a cloud share a common infrastructure.
- Cloud services are dynamic, so they can be scaled upwards and downwards far more quickly. Thus cloud-based offerings can be adjusted to the customer's actual needs more swiftly.
- The managing of services that are used from the cloud is usually done via a web interface by the cloud user themselves. Thus, the user can automatically tailor the services used to suit their needs.
- The technologies used in Cloud Computing enable the IT service to be dynamically shared across multiple locations which may be geographically very dispersed (both nationally and internationally).
- The customer can easily administer the services used and their resources via web or other suitable interfaces, and little interaction with the provider is required.

IV. CLOUD SECURITY ARCHITECTURE

A close look at the underlying reference architecture reveals that a provider needs to address a large number of tasks in order to provide cloud services.

Another key task is to monitor the services provided to be able to comply with the guaranteed service quality.

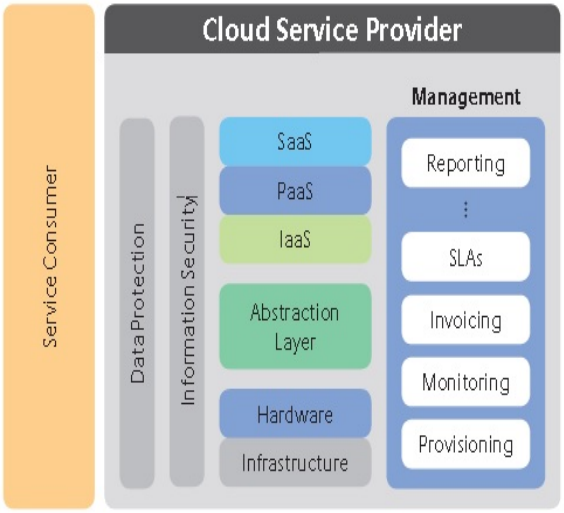


Fig.1. Reference architecture for cloud computing platforms

4.1 Data centre security

Data centres form the technical basis for Cloud Computing. To this extent, it is important that every CSP ensures their systems are secure in compliance with the current state of technology. This includes permanent monitoring of access, for example using video monitoring systems, movement sensors, alarm systems and trained security personnel. Any provision components which are essential for operations, for example the power supply, air-conditioning and Internet connection, should be designed to be redundant.

Modern fire protection precautions also need to be taken, and tested on a regular basis. Overall, a data centre should form a security area that affords adequate protection against both damage by the elements, e.g. caused by storms and flooding, and against unauthorised entry. If a customer requires a particularly high level of availability for their services, the CSP should also reserve capacities in backup or redundant data centres which can compensate for another data centre failing. The data centres should be located far enough away from each other geographically so that a controllable damage event, e.g. fire, explosion, road, rail, water or air accidents and natural disasters with a limited impact such as flooding does not simultaneously affect both the data centre originally being used and the one containing the backup capacities.

4.2 Server security

The servers represent the environment for performing the processes and their computations. For this reason the operating systems deployed on the servers should be hardened to the extent that they offer the smallest possible area to attack. To achieve this, when the basic installation is being undertaken, only the necessary software packages should be added and any superfluous programs and services should be disabled or, better, uninstalled.

Standard measures to protect IT systems, such as host firewalls, host-based intrusion detection systems, etc. should be implemented and regular integrity reviews run on important system files. Host-based intrusion detection systems are characterized by the fact that they are run on the IT system to be monitored. They are typically deployed to detect attacks made at the application or operating system level. Examples of such attacks are policy violations by users, failed login attempts and malware such as Trojan horses. The technical basis for providing and using cloud services reliably and securely are provided by a broadband connection, standardised and widely-used transmission protocols, a service-oriented architecture and, above all, virtualisation. Providers deploy different hypervisors for server virtualisation. The hypervisor is the central component of server virtualisation controlling access to shared resources.

4.3 Network security

In the past, Cloud Computing platforms have often been misused either by placing malware there which is then used to send spam, or their processing power has been exploited to crack passwords using brute force attacks or to hide command and control servers (C&C servers) used to control botnets. To prevent these and similar attacks as well as the misuse of resources, each CSP should take effective security measures to defend against network-based attacks. As well as the usual IT security measures such as anti-virus protection, Trojan detection, spam protection, firewalls, Application Layer Gateway and IDS/IPS systems, particular care should be taken to encrypt all communication between the CSP and the customer and between the provider's sites. If a third party provider is required to deliver the services, the communication with them also needs to be encrypted.

Because of the concentration of resources in centralised data centres, an attack which is a particular threat to public Cloud Computing platforms is the Distributed Denial of Service (DDoS) attack. All CSPs should also ensure that their networks are suitably segmented, preventing any faults from spreading freely.

4.4 Application and platform security

In the case of offerings in the PaaS area, customers no longer have to worry specifically about database accesses, scalability, access controls, etc., as the platform provides these functionalities for them.

When developing software, all CSPs must have established security as a fixed component in the software development life cycle process (SDLC process). Security issues need to be addressed at each phase of the software development process, and programs and modules may only be deployed if they have been properly tested and approved by the CSP's security manager. While software developed by the customer requires a secure basis (to be provided by the CSP), security issues also need to be considered in this respect. It is recommended that the CSP provides appropriate user guidelines for customers to create secure applications so that the programs the customer develops themselves fulfill certain minimum requirements in terms of security, documentation and quality. This is not only helpful for the customers but also emphasises the provider's expertise and reduces the danger of security vulnerabilities in customer software impacting on other customers. Where there is a higher level of protection requirement, the CSP should also automatically check the code the customers have developed themselves for vulnerabilities.

4.5 Data security

The data life cycle comprises its generation, data storage, data usage, data distribution and data destruction. Each CSP should support all these phases in the data life cycle with appropriate security mechanisms. A number of storage technologies, e.g. NAS, SAN, Object Storage, etc., are used to store data. Common to all these storage technologies is the fact that any customers share common data storage. In this type of constellation, a secure separation of customer data is essential and should, therefore, be guaranteed.

With SaaS, for example, customer data is usually stored in a common table. The distinction between customers is then achieved using a so-called tenant ID. If the web application (shared application) is insecurely programmed, a customer could possibly use an SQL injection to gain unauthorised access to another customer's data, and delete or manipulate it. To prevent this, appropriate security measures must be implemented. As with traditional IT, in Cloud Computing data losses are a threat that must be taken seriously. To avoid data losses, each CSP should do regular data backups based on a data security plan. Technical defects, incorrect parametrisation, obsolescent media, inadequate data media administration and non-compliance with regulations stipulated in a data security plan can result in an inability to reinstall backups and reconstruct the data inventory. So there is a need to sporadically check whether the data backups created to restore lost data can be re-used. Depending on the length of time between backing up the data and restoring the data due to data loss or some other incident, the most recent data modifications may be lost. So a CSP should immediately notify its customers if data backups need to be restored, and in particular indicate the status of the backup. The backing up of data (scope, save intervals, save times, storage duration, etc.) should be transparent and auditable for the customers.

4.6 Encryption and key management

To be able to store, process and transport sensitive data securely, suitable cryptographic methods and products should be used. The management of cryptographic keys in Cloud Computing environments is complex, and there are currently no appropriate tools for key management. For this reason, most providers do not encrypt data categorised as 'at rest'. With "IaaS storage" offerings, however, the customer has the option of encrypting their data

themselves prior to storage. In this way, they retain complete control over the cryptographic keys and also obviously need to deal with key management. If the provider encrypts the data, suitable security measures should be implemented at each phase in a cryptographic key's life cycle to ensure that keys are generated, stored, shared, used and destroyed on the basis of confidentiality, integrity and authenticity. As highly complex factors need to be considered when using cryptographic methods, each CSP should draw up a cryptography strategy. If customers are to know which tasks the CSP is taking on with respect to cryptography, and which issues they themselves need to consider, it is a good idea if providers provide customers with an overview of the cryptographic mechanisms and methods used.

V. CONCLUSION

The paper was just an attempt to bring light on the theoretical aspects of the cloud and its research area. The advances in the cloud are unexpectedly more due to its reliability and optimality. The future challenges are extensively more and few areas are: Security, Reliability, Vulnerability to Attacks, Cluster Distribution, Network Optimization, interoperability and Applications.

REFERENCES

[1] Globus Alliance homepage. http://www.globus.org, 2008.
[2] Gray J. Sort Benchmark home page. http://research.microsoft. com /barc/SortBenchmark, 2006.
[3] IBM homepage. IBM and Google announce university initiative to address internet-scale computing challenges [Internet]. http:// www-03.ibm.com/press/us/en/pressrelease/22414.wss, 2007.
[4] Amazon Web Services. Amazon Elastic Compute Cloud homepage. http://aws.amazon.com/ec2, November 2008.
[5] Chappel D. Microsoft Azure homepage. Introducing the Azure Services Platform [Internet]. http://www.microsoft.com/azure/ whatisazure.mspx, October 2008.
[6] Microsoft Azure homepage. http://www.microsoft.com/azure, 2008.
[7] IBM homepage. IBM launches cloud services initiative [Internet].http://www-03.ibm.com/press/us/en/pressrelease/ 25341. wss, 2008.
[8] Open Virtualization Format Specification, February 2009 http://www.dmtf.org/standards/published_documents/DSP0243_ 1.0.0.pdf
[9] Open Cloud Computing Interface - Core & Models, January 2010 http://www.ggf.org/Public_Comment_Docs/Documents/ 2010-01/occicore.pdf