

Cloud infrastructure and security threats in the world of cloud computing

Subramanian Anbazhagan* and **K. Somasundaram**

*Department of Computer Science and Engineering, Karpagam University, Coimbatore, Tamilnadu, India,
Department of Computer Science and Engineering, Vel Tech High Tech Dr RR and Dr SR Engineering College, Avadi, Chennai,
Tamilnadu, India.

Abstract

Cloud computing is the set of resources and services provides through the Internet. These services are facilitates from the data centers which are situated throughout the world. Common example of cloud services is Google apps, it is presented by Microsoft share point and Google. The massive growth in the area of cloud computing affects by security concerns. Security is still a constant issue for Internet and Open systems, when the people are talking about the cloud security really suffers. Cloud computing comes with the security challenges such as data securing and observing the cloud utilization by cloud vendors. The explosion of cloud computing has given lots of security issues for consumers and service providers. Current research developments on cloud computing have been motivated on the technology, costs, applications, benefits, and majorly with the security of cloud computing at the organizational level within small sized and medium sized enterprises. This paper provides an introduction about cloud computing environment with its infrastructure. The four different types of clouds and the three types of cloud services are explained. The security issues in this cloud computing environment are also presented in this paper. It is recommended that any cloud model or services should be incorporated with the security algorithms in order to facilitate a private and secure environment to the cloud users.

Keywords : cloud computing, cloud users, microsoft share point, Google, security, internet and open systems.

INTRODUCTION

Nowadays, the term “Cloud” is becoming progressively popular in IT. It is very usual to hear about Cloud Database, Cloud Drive, Cloud Server, Cloud Ecosystem and Cloud Security. Actually, the “Cloud” here does not mention to a natural occurrence. The denotation is short for “Cloud Computing” which is a new combined computing technology that is dispersed rapidly from small domain researching to huge-scale developing and utilizing. Clearly, the promotion of “Cloud” is not a coincidence but it is a demand from Internet market. Moreover, it is going to be the groundwork of Internet in the next generation and establishes the new design of Internet services.

Usually, Cloud Computing is the combination of traditional networking technologies and computing methods such as Parallel Computing, Distributed Computing, Network Storage Technologies, Utility Computing, Virtualization, High Available, Load Balance, etc. For example, Distributed Computing is dividing a huge computation into small segments and allocating multiple computer systems to compute, then gathering all of the results and accumulating them together. Whereas, parallel computing gathers a huge number of computational possessions to process a particular job, which is a highly efficient solution for parallel issues. Fig.1 illustrates the comparison between distributed computing and parallel computing.

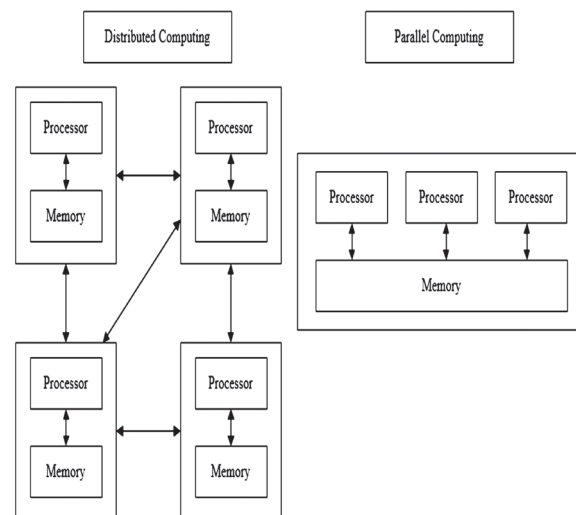


Fig.1. Distributed and Parallel Computing

Network Attached Storage (NAS) technologies attach storage devices with a group of computer system through standard network topology. It accomplishes the need for rapidly growing storage volumes, and facilitating adequate storage space for the connected hosts. Whereas, another Network

These two technologies are only part of Cloud Computing, which indirectly representing the huge scale of Cloud Computing. Hence, Cloud Computing is another massive transformation since the 80s in IT, from mainframe computer system to client-server system. Till now, several famous IT companies have deployed and

*Corresponding Author :
email: anba.subra@gmail.com

utilized the research and development of Cloud Computing due to its latent of commercial value and new technology.

Structure of Cloud Computing

This section discusses about the four types of cloud (private, public, community and hybrid) and the three cloud services (Infrastructure as a service (IaaS), Platform as a service (PaaS) and Software as a service (SaaS)).

Storage Technology called Storage Area Network (SAN), which uses the Fiber Channel (FC) to connects to a group of computer systems without standard topology. It is usually used in large volume storage environment. Fig.2 illustrates the different topology of NAS and SAN.

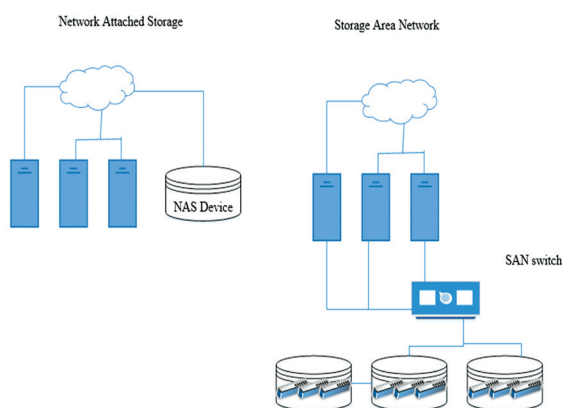


Fig.2. NAS and SAN

TYPES OF CLOUD

Private cloud

A private cloud is constructed for a single organization or client, which can efficiently control data, data security and quality of service (QOS). The company has organization and operates the deployment of applications through it. The principal value of private cloud is private resources. It can be recognized by a company or a Cloud Service Provider (CSP). Based on this hosted organization, CSPs such as IBM and Sun are supposed to configure, install, and manage the infrastructure to support the private cloud holding the commercial datacenter possessed by a certain company. In this manner, the usage of cloud resources are strongly controlled by the organization, at the same time, the expert knowledge of building and running this environment can be developed.

The benefits of private cloud are noticeable. First, the data is comparatively more secure than other placement methods. Even though, many public cloud providers

declared that their service is enormously secure in all features, and the data cannot be damaged by any threat.

Public cloud

Usually, public cloud denotes to the cloud offered by third-party CSPs attained by accessing internet. The cost is comparatively free or low. In this way, an organization offers its service external users access to their own infrastructure directly, and external users access the service through Internet without possessing cloud computing resources. There are also some advantages to the public cloud. It offers a consistent and secure data storage center compare to other storage approaches. Most of the peoples in the past thought the data can only be safe in their own computers; actually it is not true. The user computers may be physically impaired.

It may be attacked by hackers or virus, even malicious act from someone who can access the computer. Otherwise, if the files are stored in public cloud storage, then the data will be preserved in the servers permanently and legal access will be mandatory. In the meantime, a public cloud can support diverse hardware systematically. Also, due to the enormous number of users in public cloud, it is moderately convenient to share files or file storage with someone as well as access huge number of public resources. It incorporates upstream like ads and VAS with downstream end users. It formulates a new value chain and ecosystem. Table 1 provides the major differences between public cloud and private cloud.

Community cloud

A community cloud permits multiple independent entities to obtain cost benefits in a mutual non-public cloud. It is an element in public cloud, which is deployed on definite range of area and designed as a community. This approach has huge potential for organizations or companies that are subject to identical compliance, regulatory or legal restriction. Usually, these clouds are built in the place where users have similar offering unified services and requirements. For instance, in university towns, the users are students, teachers, and staff from all types of universities, research facilities, and service agencies. The services comprises cloud servers, cloud hosts, cloud datacenter and a cloud storage.

Hybrid cloud

A hybrid cloud is a structure of multiple clouds that remain various entities but also bound together. The benefits come from multiple deployment. As discussed in previous sections, a private cloud is more safe and secure than a public cloud, but a public cloud owns a tremendous number of public resources. Therefore, a combination of a public and a private cloud called hybrid cloud provides a perfect solution to this

Table 1. Public vs Private Cloud

Public Cloud	Private Cloud
Publically shared virtualized resources	Privately shares virtualized resources
Supports multiple customers	Cluster of dedicated customers
Supports connectivity over internet	Connectivity over internet, private and fiber network
Suited for less confidential information	Suited for secured confidential information and core systems

conflicting situation. It has the security properties of private cloud which conserves internal important data in the local datacenter. It also utilize the computing resources from the public cloud to complete the work effectively and efficiently. Moreover, it overcomes the hardware limitation of a private cloud by taking the advantage of extensibility of the public cloud. It helps to gain higher computation capacity. In addition, the cost also be lower because it can change between public cloud and private cloud based on the users' constraint. Hybrid cloud allocates data and application on the most suitable platform.

SERVICE MODELS

The cloud computing offers services affording to the following levels:

- Infrastructure as a service (IaaS),
- Platform as a service (PaaS) and
- Software as a service (SaaS)

These services are defined by NIST and it is broadly accepted around the world.

Infrastructure as a service (IaaS)

IaaS offers the service focusing on the utilization of all computing infrastructure, comprising memory, network, CPU, storage, and other basic computing resources which can be deployed and run by users such as applications and operating system. Consumers are not asked to control or manage any cloud computing infrastructures, but they can manage the selection of operating system, storage space and installed application as well as obtain the right of control of controlled network components.

Usually, there are three methods to apply IaaS:

- public cloud,
- private cloud and
- hybrid cloud

They are already mentioned before. Amazon EC2 uses public server pools as infrastructure. Different private

services will use a set of private or public server pools in a company's datacenter. If the company's datacenter environment is utilized to make software development, in this manner, the public, private and hybrid cloud are all accessible.

Platform as a service (PaaS)

In this method, CSPs provides a computing platform, which chiefly comprising of a database, an operating system, a programming language execution environment, and a web server. The idea is to utilize server platform as a business model which provides services. The service which offers programs through the Internet is called SaaS (Software as a Service), hence the server platform or the emerging environment are the carrier of it. Hypothetically, PaaS is one of the SaaS applications. PaaS is also the application of infrastructure service in the cloud computing environment, which is called middleware as a service. PaaS is positioned in the middle of the service models, which is under SaaS and above IaaS shown in fig.3.

Based on customary deployment, there are plenty of diverse middleware, such as database, portal, application server, ESBs, BPM, and AM. Usually, PaaS is divided into two types;

1. One aims on application deployment and running Application Platform as a Service (APaaS).
2. The other one is termed as Integration as a Service (IPaaS). Fundamentally, PaaS denotes to APaaS, like Google App Engine and Force.

The maximum difference between the PaaS service with other services is that it delivers the entire infrastructure platform as a substitute of a certain application. In traditional idea, the platform is the essential service station for exteriors. Moreover, it must be guarded and formulated by the Application Service Providers (ASPs) but PaaS has inverted this idea. The Platform Service Providers (PSPs) are responsible for launching and maintaining this platform and transport it to the application system providers through services.

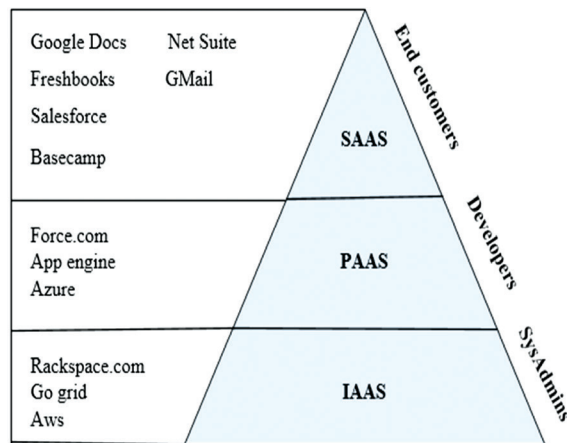


Fig.3. Cloud service types and example

Software as a service (SaaS)

With the development of IT and the development of applied software, there is a new software application model growing in the 21st century. It has a similar idea to ASP, On-demand software, and hosted software. This model offers software through the Internet, where productions place software on their own clients and servers can contribute to applied software services through the Internet on their demand. This service fees is based on the number of services and the time of practice. Instead, users do not requisite to purchase software anymore, they obtain web-based software through providers in order to manage company operations without the help of local software maintenance. It will be completely managed and organized by providers. Software companies not only deal the Internet application but also protect local data storage and offline operations, which is helpful to users because they can use the services anytime in anywhere. For many small scale companies, SaaS is the finest way to apply high technologies because it removes the obstacle of purchase, formation and infrastructure maintenance for companies. Fig.3 demonstrates cloud service types and it offers an examples in a pyramidal model, which helps with better understanding of it.

SECURITY ISSUES IN CLOUD COMPUTING

Nowadays, security is becoming more challenging in cloud computing due to its popularization. Hence, it is essential to examine the main risks systematically to guarantee the safeguard to our information. In the recent years, huge security issues occurred frequently with cloud computing providers. Amazon experienced network server interruption on Feb 15th 2008 which affected thousands of websites that applied S3 cloud storage, and Amazon EC2 cloud computing, comprising SmugMug, Adaptive Blue, Twitter, and 37Signals. Google Gmail had a worldwide breakdown and services were suspended longer than four hours in 2009, because one of the datacenter in Europe was under

preservation while the others was loaded and this affected chain effect to other datacenters. In the same year, a huge number of user files disclosed in Google. Microsoft Azure was suspended about 22 hours on 15 March 2009, though the detail of cause has not been specified by Microsoft. On 11 June 2009, Amazon EC2 service was disturbed for several hours due to the damaged electrical equipment which supplied datacenter spoiled by lightning stroke.

Privacy Management

One of the feature of cloud computing is the involvement of enormous number of users, and it is unavoidable to have privacy and security problems. Many users are worried that their private data will be collected via cloud technology. Hence, a plenty of service providers assured to avoid collecting user's privacy information and keep them private if they attained that information. However, users still cannot be fulfilled with the guarantee is trustworthy, while their concerns make sense.

In cloud environment, one of the most vital is that user data is not kept in local device, as a substitute, it is kept in the cloud, in which some delicate data will result in privacy leakage. Even though, many cloud guidelines about not uploading sensitive data to cloud, it is not a faultless solution and probably deactivate certain benefits brought by cloud. Moreover, it delays the growth of cloud computing. Also, the on demand service provided by cloud computes service fees by retrieving user data on the cloud, and some commercial operation or local laws have particular requests regarding the storage and utilization of data. In this condition, an effective mechanism is required to screen and audit data without leaking sensitive content.

Data Confidentiality and Security

In cloud computing, users cannot have full accessibility of their data when they upload them to cloud, hence it is critical that a CSP delivers effective safety guarantee, preserving the integrity and data availability. When compared with the traditional computing, cloud computing brings new challenges. In terms of cloud computing services, IaaS generally provided by the interface of web service which means retrieved by web browser. PaaS is accomplished by applying the grouping of above mentioned technologies, while XML is the transporter of protocols belongs to network application layer in data parameters and transmission and there is evidence representing that certain security issues associated to the web service and browser have a association with it such as attack to XML signature. Moreover, the security challenges of browser not only need to be solved by transmission layer security technology, but also imposes XML encryption in the core code of the browser. Due to the security problem

with browser, the identification based on the browser is also susceptible. Further, the feature on integrity and virtual machine functional to cloud, there are existing metadata fraud, malwares, and DoS attacks to server. Hence, in the view of application, it is hypothetical to focus on web service and we browser framework to enhance security

Data Audit

The user data in the cloud is not controlled by users, hence it is important to make sure their data having been saved and processed properly, called conducting integrity verification. Furthermore, in the point of data security, network supervision and legal issues, a system is required to progress audit publicly and remotely. Specific methods have performed to verify the data remotely. For instance, executing provable data possession by applying a RSA-based homomorphic tag. With the development of it, by applying the traditional Merkle hash tree, the model of proof of retrievability was enhanced. Lastly, it accomplished the goal of data integrity verification with privacy protected via third party audit that user's participation is redundant and avoids privacy leakage.

Authentication and Access Control Policy

When a client is using cloud storage and a cloud computing service, the authentication should be applied by the CSPs. It utilize certain access control policy to achieve the access of data and service. Moreover, diverse service providers must be able to authenticate each other. SSLAP is used in cloud computing

authentication, but this protocol is quite refined and overloaded in communication. In the point of cloud computing, each user has own digital ID, hence one of the possible solution is to apply ID as the primary information of authentication. In IBE and IBS protocol, it has encryption and signature used in cloud computing and cloud service, and it is also based on the identity authentication has been proposed. When compared with SSLAP, it does not enquire for authentication certificate, and it perfectly fulfils the requirements of cloud computing. By testing on a simulation platform Grid-Sim, it shows more benefits than SSLAP with the lower load.

Virtual Machine Security and Automated Management

Virtualization and virtual machine technology are one of the basics of establishing the cloud computing concept. In SaaS, the application is generated on the visualized platform, and users can share physical computing resources with others in a translucent way. In IaaS and PaaS schemes, the application is aided as a virtualized platform or virtual machine. Except for the traditional network, software and system, diverse

virtual machines should be remote when sharing with the physical computing resources and storage resources. Moreover, the virtual machine surveillance program is invented to be trustable and not mention to user privacy information.

CONCLUSION

This paper presents a cloud infrastructure and its services. It comprises of four types of clouds such as private, public, community and hybrid. The cloud services are also presented in this paper. The security threats are discussed to understand the users about the issues in this environment. The rising of cloud computing consequences the beginning of the new age of information technology which steps in the aggregated computing model. This leads to the change of application from local to cloud environment that intensely welfares our life and work. The word "Cloud" seems to be abstract and deceptive, and it is difficult to visualize the connection between "Cloud" and IT. Instead, it will be more understandable and acceptable for the public to define the technology in a visual manner. Further, this dynamic developing industry will have an effects on other fields in the future.

Cloud computing has grown-up from being an encouraging business idea to one of the fast rising segments of the IT business. However, as more and more information on companies and individuals are placed in the cloud, worries are beginning to raise about just how safe an environment it is. The construction of cloud stances such a hazard to the security of the cloud technologies when organized in a cloud environment. Cloud service users requisite to be attentive in understanding the risks of security breaches in this new environment.

REFERENCES

- Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A. 2010. A view of cloud computing, *Communications of the ACM*, vol. 53, P. 50-58.
- Bertino, E., Paci, F., Ferrini, R., and Shang, N. 2009. Privacy-preserving Digital Identity Management for Cloud Computing, *IEEE Data Eng. Bull.*, P.32:21-27
- Braun, T.D., Siegel, H.J., Beck, N., L. Bölöni, L.L., Maheswaran, M., Reuther, A.I., 2001. A comparison of eleven static heuristics for mapping a class of independent tasks onto heterogeneous distributed computing systems. *Journal of Parallel and Distributed computing*, P. 61: 810-837.
- Brand, A., 2009. Storage device and method thereof for integrating network attached storage with cloud storage services, ed: Google Patents.
- Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R. 2009. Controlling data in the cloud: outsourcing computation without outsourcing

- control, In : *Proceedings of the 2009 ACM workshop on Cloud computing security*, P. 85-90.
- Cusumano, M. 2010 . Cloud computing and SaaS as new computing platforms, *Communications of the ACM*, 53 : 27-29.
- Dinesha, H. , and Agrawal, V.K. 2012 . Multi-level authentication technique for accessing cloud services, In: *2012 International Conference on Computing, Communication and Applications (ICCCA)*, P. 1-4.
- Doelitzscher, F., Sulistio, A., Reich, C., Kuijs, H. and Wolf, D., 2011. Private cloud for collaboration and e-Learning services: from IaaS to SaaS, *Computing*, P. 91:23-42.
- Khajeh-Hosseini, A., Greenwood, D., and Sommerville, I. 2010. Cloud migration: a case study of migrating an enterprise IT system to IaaS, In : *2010 IEEE 3rd International Conference on Cloud Computing (CLOUD)*, P. 450-457.
- Krutz, R.L. and Vines, R. D., 2010. *Cloud security: A comprehensive guide to secure cloud computing*: Wiley Publishing.
- Kumar, V., Grama, A., Gupta, A., and Karypis, G., 1994. *Introduction to parallel computing: design and analysis of algorithms* vol. 400: Benjamin/Cummings Redwood City, CA.
- Li, A. , Yang, X., Kandula, S., and Zhang, M. , 2010, CloudCmp: comparing public cloud providers, in *Proceedings of the 10th ACM SIGCOMM conference on Internet measurement*, P. 1-14.
- Marinos, A., and Briscoe, G., 2009. "Community cloud computing," in *Cloud Computing*, ed: Springer, 472-484.
- Prahlad, A., Kottomtharayil, R., Vijayan, M.K., Gokhale, P., Attarde, D.R., and Lad, K. K. , 2010. Data transfer techniques within data storage devices, such as network attached storage performing data migration, ed: Google Patents.
- Sotomayor, B., Montero, R.S. , Llorente, I.M ., and Foster, I. 2009. Virtual infrastructure management in private and hybrid clouds, *IEEE Internet computing*, 13 : 14-22.
- Vikas, S., Gurudatt, K., Vishnu, M., and Prashant, K., 2013, Private Vs Public Cloud, *International Journal of Computer Science & Communication Networks*, 3: 79.
- Vaquero, L.M. , Rodero-Merino, L., Caceres, J. , and Lindner, M. , 2008 . A break in the clouds: towards a cloud definition, *ACM SIGCOMM Computer Communication Review*, 39 : 50-55.
- Wang, C. , Wang, Q. , Ren, K. , and Lou, W. 2010. Privacy-preserving public auditing for data storage security in cloud computing, in *2010 Proceedings IEEE INFOCOM*, P. 1-9.
- Wei, J. , Zhang, X. , Ammons, G. , Bala, V. , and Ning, P. , 2009. Managing security of virtual machine images in a cloud environment. In : *Proceedings of the 2009 ACM workshop on Cloud computing security*, P. 91-96.
- Yu, S. , Wang, C. , Ren, K. , and Lou, W. , 2010. Achieving secure, scalable, and fine-grained data access control in cloud computing, in *Infocom, 2010 proceedings IEEE*, P. 1-9.
- Zomaya, A.Y., 1996, *Parallel and distributed computing handbook* vol. 204: McGraw-Hill New York.