Sub-Saharan Journal of Computer Science,2016,4(1):05-07
ISSN: 2307-9169
Available Online: http://sjcs.rstpublishers.com/

CLOUD COMPUTING: CONCEPTS AND CHALLENGES

Anuj Kumar Gupta
Department of Computer Science and Engineering, Chandigarh Engineering College, Mohali, Punjab, India.
Email: anuj21@hotmail.com

Received:23,Jan,2016 ***Accepted: 02, Mar2016***

Abstract

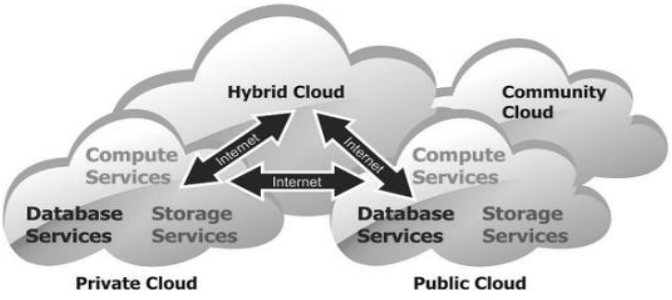
In recent years, computing is being make over by a fresh representation, named as cloud computing, which refers to the hardware, software: both systems and application, that act as services over the Internet. Cloud computing is growing rapidly and gaining popularity because of reduced costs, quicker implementations, and enhanced flexibility. In this paper, a survey has been done on cloud computing with a major focus on its security issues. Concepts and challenges have been discussed which will give the researchers an idea about this latest emerging technology being tossed around in the world. This paper presents an overview of the cloud deployment models, the services they offer and cloud security issues and challenges of cloud computing in both data storage and virtual applications.

Keywords: *Cloud architecture, IaaS, Paas, Saas, cloud security.*

INTRODUCTION

The word cloud is used as a simile for the Internet based on how the Internet is portrayed in computer networks and is a perception to mask the multifaceted infrastructure.

National Institute of Standard and Technology (NIST) defined cloud computing as "a model for enabling convenient, on demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction".



Fig(1) Cloud computing deployment models

Cloud computing is a dominant network architecture which is implemented in large scale and multifaceted computing on the Internet. It focuses on broad three models based on infrastructure, platform and software as services that are referred to as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) respectively. Cloud computing is a combination of many different computing technologies and concepts like grid computing, virtualization, ubiquitous computing etc.

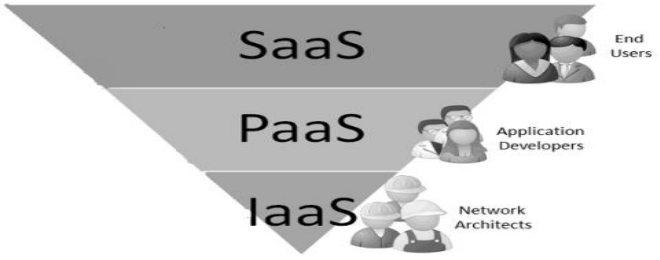
Jamil and Zaki (2011) described three types of cloud models as shown in figure 1. When a cloud is formed and is made available to all users publicly it is called a public cloud, and when it is operated solely for a particular organization it is called a private cloud. And the combination of these two types is called a hybrid cloud.

Rani and Marimuthu (2012) outlined one more type of cloud computing model named as Community cloud which is for a particular community formed by many organizations having common goals.

Cloud Architecture

Cloud computing is generally viewed as a collection of layers or services which form a layered architecture; SaaS, IaaS, PaaS and dSaaS as shown in figure 2. SaaS allows users to execute applications remotely from the cloud. IaaS refers to computing resources with guaranteed power and bandwidth for storage. PaaS includes operation system in addition to IaaS. Last layer dSaaS provides the storage that the users actually use or storing data on cloud, Mathisen (2011).

Rittinghouse and Ransome (2010) outlined two extra models through which cloud computing services are delivered, namely Communication as a Service (CaaS) and Monitoring as a Service (MaaS). CaaS provides communications solution to governments and enterprises. MaaS provides security as a service to; Government, Colleges, Universities, and Businesses against cyber-crimes or network threats.



Fig(2)Cloud computing architecture

Cloud computing types & Characteristics

A cloud provider falls into three categories: public, private and hybrid. In public or external cloud all the computing resources are generally provided by the third parties. Private or internal cloud is built up to be exclusively used by only one user who has full control over the data and security. Usually private cloud is built and managed by the company. A hybrid cloud combines both public and private cloud environments. It basically deals with how to distribute services across both public and private clouds, Cheng and Lai (2012).

Characteristics of Cloud Computing

There are basically five fundamental features of cloud computing;

a) Virtualized resource pool,
b) broad network access,
c) rapid elasticity,
d) on-demand self-service, and
e)Measured service.

Cloud computing challenges

Clouds being multifaceted, large and diverse distributed systems, network management is a big challenge which needs to be programmed and incorporated, Popovic and Hocenski (2010). Cloud infrastructure promises a consistent, secure and cost effective service. But it is a challenging job as it requires optimization at several layers of cloud architecture. Some of the major key challenges include:

Quality of Service (QoS)

The major challenge of cloud computing is to make sure that the resources must be enough to fulfill the QoS requirements of cloud users. A cloud service provider (CSP) must be aware of the breaches that need to be avoided or minimized by conditioning the right amount of resources to its cloud users in time.

Energy efficiency

A proficient amount of energy is consumed in the infrastructure, avoiding consumption of those resources which are essentially required by the cloud applications.

Security

The cloud computing security model considers three sub-models: IaaS, PaaS, and SaaS. The relationship and dependencies between these are important to fully grasp the security risks to cloud computing – IaaS is the base of all cloud services, PaaS is layered on top of IaaS, SaaS is built upon PaaS.

Cloud security reference model

Layered architectures inherit capabilities – operations and functionality, risks including security risks. IaaS includes the infrastructure stack from facilities to hardware, and the interfaces required to manage them. PaaS, residing on top of IaaS, adds an additional layer of integration and application development. This may include middleware, such as MQ series, and databases. Developers are able to build applications using the PaaS stack. SaaS resides upon PaaS and IaaS providing a self-contained operating unit that delivers the entire user experience, including all required software, such as presentation, content management, and user interface, graphical or other. Cloud providers offer more services for customers at the top of the stack. Therefore, SaaS, security from the customer's perspective, is contractual. As customers move down the stack, such as an IaaS customer, they are responsible for building the security in their application and middleware layers.

Cloud security risks

There are good reasons that security, as on the last slide, is of top concern. IT security in cloud computing adds at least one critical layer of complexity. You, the consumer, are trusting security to an external source. This trusted relationship may add the challenge of monitoring and validating the security of the cloud provider, especially if the provider does not wish to expose their internal infrastructure to customers. When an organization is relying on itself to meet service level agreements (SLA), there is a certain amount of control available to the customer. If there are problems within the organization's IT infrastructure, a manager may be able to get an executive to apply internal pressure, getting the attention required to meet the SLA. However, when the IT infrastructure, or layered services, are outside on an organization, the ability to apply pressure to get the required attention needed to fix the problem may rely on the details of the cloud contract and an external resource. With a poorly constructed contract, a consumer loses leverage.

Security dangers to cloud computing

The principal security dangers to cloud computing include dangers that currently exist in pre-cloud computing. Cloud computing heightens the risks in certain dangers, such as data corruption, while introducing some new risks, such as virtualization and multitenancy.

Virtualization and multitenancy

Cloud offers take advantage of economies of scale, offering shared services within their infrastructure. Virtualization and multitenancy architectures make this possible. However, these technologies were not designed with strong isolation in place – Hypervisors have extended these risks, potentially exposing the operating system – Creating an environment where attackers can gain access at the operating system level (hypervisors) and higher level services (functionality and data). To reduce these risks, consider: – Implement operating system security best practices, such as patch management – Implement application systems security best practices, such as AAA (authentication, authorization, and auditing).

Nonstandard and vulnerable APIs

Application programming interfaces (API) are the software interfaces that cloud providers offer to allow their customers access into the services. Cloud API is not standardized, forcing users of multiple cloud providers to maintain multiprogramming interfaces, increasing complexity and security risk. Since an API offers access to the internals of a system, a weak API exposes consumers to a variety of security issues encompassing all of the operational exposure the of the compromised API's functionality. To reduce these risks, consider: – Implement API security best practices, such as requiring AAA (authentication, authorization, and auditing) – Review the cloud provider's security model being used for the API, including any API trusted chain.

Internal security breaches

The IT industry has well documented that over 70% of security violations are internal – This threat is amplified in cloud computing as both IT providers and consumers are under a single management domain. To reduce these risks, consider the following key components of the contractual agreement between the customer and cloud provider: – Transparency in information and internal management practices – Understand the human resources requirements – Have a clear level of escalation and notification of a breach – Ensure that contractually you are in the loop if an internal breach occurs with the cloud provider.

Data corruption or loss

Data corruption or loss is amplified since the cloud provider is the source for a company's data, not the company itself. These operational characteristics of the cloud environment, at the PaaS and SaaS layers, amplify the threat of data loss or leakage increase. To reduce these risks, consider: – Implement application systems security best practices, such as AAA (authentication, authorization, and auditing) – Implement strong encryption, SSL, digital signatures, and certificate practices – Ensure that strong disaster recovery processes exist and are tested on a periodic basis – Require that the persistent medium used to store your data is erased prior to releasing it back into the pool, Pearson and Benameur (2010).

User account and service hijacking

User account and service hijacking occurs when a attacker obtains your cloud services information and uses it to take over your cloud access. If attackers gain access to a cloud user's identification, they can snoop on activities and transactions, manipulate or steal data, return falsified data, and redirect clients to illegal sites. To reduce these risks consider: – Implement security best practices, including human processes, such as strong passwords, two-factor authentication, and prohibiting the sharing of users' credentials – Implement application systems security best practices, such as AAA (authentication, authorization, and auditing) – Implement strong encryption, SSL, digital signatures, and certificate practices – Ensure that auditing and logging is being used to monitor activities.

Steps to reduce cloud security

The following steps offer a guideline to reducing cloud security breaches:

a) Implement security best practices including human processes

b) Implement operating system security best practices, such as patch management

c) Implement application and API systems security best practices

d) Implement strong encryption, SSL, digital signatures and certificate practices

e) Ensure that auditing and logging are being used to monitor activities

f) Ensure that strong disaster recovery process exist

g) Transparency in information and internal management practice

h)Understand the human resources requirements

i)Have a clear level of escalation and notification of a breach, ensuring that you are in the loop if an internal breach occurs with the cloud provider (with your data or another customer's).

Identity management

It deals with identifying users in an organization and controlling access to the resources in that organization by inserting boundaries on the recognized identities of the users. It is principally significant in a cloud environment since the cloud shares physical resources across many internal and external users and to control the access to diverse services is very decisive. Identify management helps avert security infringes and supports organizations in meeting IT security agreement rules.

Benefits of identity management

a) It helps in providing improved user productivity by simplifying the interface.

b) It also advances the customer and associate services by secure processing during data access.

c) It helps in reducing desk costs.

d) And above all it minimizes the overall IT costs by providing and withdrawing user rights.

Detection and forensics

a) Activity logs to provide information

b) Host based Intrusion Protection Systems (HIPS) and Network Based Intrusion Protection Systems (NIPS) monitors which look for traces of hackers in log files

c) Network Intrusion Detection Systems (NIDS) programs which examine data packets as they pass through the network

d) Digital Deception Software that purposely misinform anybody who is attempting to attack the IT network

e) White Listing Software that inventories legitimate executable programs running on a computer and prevents other executable files from running

f) Unified threat management — to analyze combined information for threats

g) Fooling attackers by spoofing — pretending to be something else, such as IP addresses, email accounts, etc

h) Honey pot — a system that pretends to be something else (something of value) that tricks attackers into revealing details about where they are attacking from

i) Data audit — a type of logging that checks the data.

Encrypting data

Encryption is a critical component of cloud computing which is used to ensure that data moving from point X to point Y with being altered or intercepted. The journey from point X to point Y may include: – Within the cloud environment (internal to the cloud) – The Internet between a corporation (cloud user) and the cloud provider – Between multiple clouds (external to the cloud).

Encrypting methods include – Symmetric keys – Asymmetric keys – Digital signatures. Secure Sockets Layer (SSL) addressing cloud client connection issues – SSL overview – SSL handshake.

CONCLUSION

In this paper, a review of the concepts of cloud architecture has been presented. Further some security considerations in cloud computing have been described which include cloud security risks and cloud security breaches, etc. Various security options have been identified and discussed that are available in cloud computing such as identity management techniques, detection and forensics and encryption. Lastly the top security threats to cloud computing have been identified.

Acknowledgment

The author wishes to thank all the reviewers and editors for their valuable suggestions and expert comments that help improve the paper.

References

[1]. Cheng, F.C. and Lai, W.H. (2012). The Impact of Cloud Computing Technology on Legal Infrastructure within Internet: Focusing on the Protection of Information Privacy. Procedia Engineering, 29, 241-251.

[2]. Jamil, D. and Zaki, H. (2011). Cloud Computing Security. International Journal of Engineering Science, 3(4), 3478-3483.

[3]. Kumar, A. (2012). World of Cloud Computing & Security. International Journal of Cloud Computing and Services Science, 1(2), 53-58.

[4]. Mathisen, E. (2011). Security challenges and solutions in cloud computing. Digital Ecosystems and Technologies Conference (DEST), 2011 Proceedings of the 5th IEEE International Conference.

[5]. Pearson, S. and Benameur, A. (2010). Privacy, security and trust issues arising from cloud computing. Cloud Computing Technology and Science, 2010 IEEE Second International Conference, 693-702.

[6]. Rani, A.M.G. and Marimuthu, A. (2012). A Study on Cloud Security Issues and Challenges. International Journal, 3(1), 344-347.

[7]. Rittinghouse, J. W. and Ransome, J. F. (2010). Cloud computing; implementation, management, and security. London: CRC Press.

[8]. http://csrc.nist.gov/groups/SNS/cloud-computing.