CLOUD COMPUTING: SECURITY AND APPLICATIONS

BY

AWANTIKA * NEHA RAWAT ** POONAM RAWAT *** SHIKHA SINGH ****

*-**** Govind Battabh Pant University of Agriculture and Technology, Patnagar, Uttarakhand.

ABSTRACT

Cloud computing is becoming a fundamental part of Information Technology. Resource sharing is a pure plug and play model that effectively simplifies infrastructure planning. This is the aim of cloud computing. The two key advantages of this model are ease- of-use and cost-effectiveness. This paper explores some of the basics of cloud computing along with its security and application concerns. The paper also aims to provide the means for understanding the model and exploring options available for complementing your technology and infrastructure needs.

Keywords: Applications, Attack, Cloud Computing, Denial-of-Service, Man in Middle Attack, Risk, Security.

INTRODUCTION

Cloud computing is an emerging area in the field of information technology. Forrester defines cloud computing as: "A pool of abstracted, highly scalable, and managed compute infrastructure, capable of hosting end- customer applications and billed by consumption." [1,2]. Cloud computing is a model for enabling 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. This cloud model is composed of five essential characteristics, three service models, and four deployment models[3]. A large pool of system is connected in private or public networks in cloud computing paradigm, to provide dynamically scalable infrastructure for file storage, data and application. With the advancement of this technology, the cost of computation, application hosting, content storage and delivery is reduced significantly. It is a practical approach to experience direct cost benefits. The idea of cloud computing is based on a very fundamental principle of reusability of IT capabilities.

1. Cloud computing models

There are many levels of cloud computing offerings and every player have their own diverse services. Some of the big cloud players are namely: IBM, Amazon, Google, Microsoft, SalesForce.com and Sun etc. Although listing all of them is beyond the scope of this document, there are three major types of services in the cloud environment: SaaS, PaaS, and IaaS [4] as shown in Figure 1.

1.1 Software as a Service (SaaS)

SaaS is offered by companies such as Google, Salesforce, Microsoft, Zoho, etc. This model is based on the concept of service on demand. An application is offered to the customer on demand. A single instance of the service runs on the cloud and multiple end users are served. Users need not make investment in software licenses or for servers, while for the provider, the costs are becoming less, since only a single application needs to be hosted & maintained.

1.2 Platform as a Service (PaaS)

This model provides a platform to the end users. A layer of software, or development environment is encapsulated &

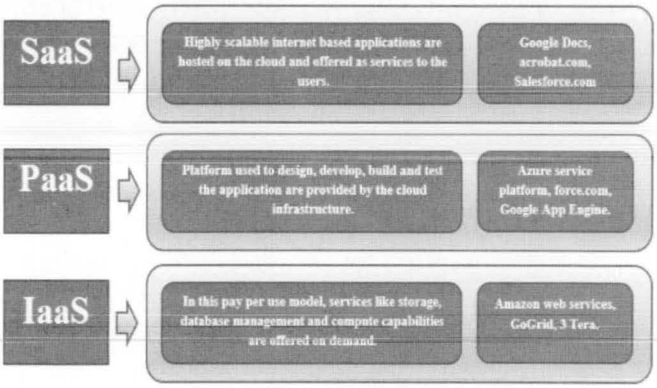

SaaS
Highly scalable internet based applications are hosted on the cloud and offered as services to the users.
Google Docs, acrobat.com, Salesforce.com
PaaS
Platform used to design, develop, build and test the application are provided by the cloud infrastructure.
Azure service platform, force.com, Google App Engine.
IaaS
In this pay per use model, services like storage, database management and compute capabilities are offered on demand.
Amazon web services, GoGrid, 3 Tera.

Figure 1. Cloud computing model

offered as a service to the users, upon which other higher levels of service can be implemented. This model provides the freedom to customers to build their own applications, while infrastructure to run that application is provided by the provider. To manage the scalability requirements of the applications, here providers offer an already defined combination of operating system and application servers such as Linux, Apache, MySql and PHP (LAMP platform), Ruby etc. Some common examples of PaaS are Googles App Engine, Force.com, etc.

1.3 Infrastructure as a Service (IaaS)

IaaS provides basic storage and computing capabilities as standardized services over the network. Servers, networking equipment storage, systems, data centre space etc. are made available to handle workloads. What customer need to do is simply deploy required software on the infrastructure. 3Tera, GoGrid, Amazon etc. are some common examples of IaaS.

2. Cloud Computing Attacks

As more companies are moving to cloud computing, probability of attacks also increases. Some of the potential attack vectors criminals attempt include:

2.1 Denial of Service (DoS) attacks

Some security professionals have argued that the cloud is more vulnerable to DoS attacks. Cloud is shared by many users, which makes DoS attacks much more damaging. In 2009, one of the famous social site-Twitter suffered from DoS attack.

2.2 Side Channel attacks

An attacker could attempt to compromise the cloud by placing a malicious virtual machine in close proximity to a target cloud server and then launching a side channel attack.

2.3 Authentication attacks

Authentication is a weak point in hosted and virtual services and is commonly targeted. Many different ways are for authentication; for example, based on what a person knows, has, or is. The mechanisms used to secure the authentication process and the methods used are a frequent target of attackers.

2.4 Man-in-the-middle cryptographic attacks

This attack is carried out when an attacker places himself between two users. Anytime attackers can place themselves in the communications' path, and there is the possibility that they can intercept and modify communications.[5]

3. Cloud security

Security is a state of being free from any type of danger. It can be defined as the degree of protection against danger or loss. The information housed in the cloud is often seen as valuable to individuals with malicious intent. Potentially secure and personal data that people store on their computers, is being shifted to the cloud. As we don't know security measures provided by the cloud providers, it is important to take precautions to secure our data. The first thing we should know is the security measures provided by cloud provider. Which encryption mechanism/methods they are using to encrypt data in order to protect it ?. These measures may vary from provider to provider and among the various types of clouds. It's also important to know whether they will have backups of data? Do they have firewalls set up? In case of community cloud, we must know about those barriers those are being placed to keep information secure from other companies.

Generally, cloud providers have their standard terms and conditions that may answer these questions, but the home user will probably have little negotiation room in their cloud contract. No matter how careful we are with our personal data, by subscribing to the cloud, we will be giving up some control to an external source.[6] To take advantage of the benefits of the cloud, you will have to knowingly give up direct control of your data. On the converse, keep in mind that most cloud providers will have a great deal of knowledge on how to keep your data safe. A provider likely has more resources and expertise than the average user to secure their computers and networks. The biggest cloud computing concern is security (Figure 2). Now-a-days cloud is emerging and interesting area in the field of information technology. Nearly every enterprise is evaluating or deploying cloud

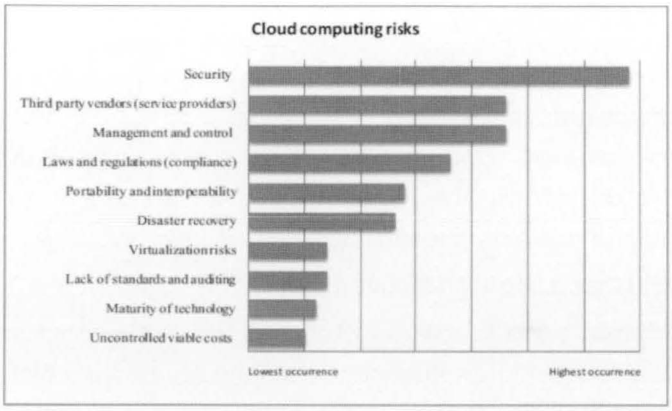


Figure 2. Cloud computing Risks

solutions. We used to share confidential data on the cloud. Now the question is who is responsible for security in the new world of cloud computing? We store our confidential data at cloud so there should be some mechanism to ensure the security and reliability of that data. Increasingly, we see third-party application providers, who are not necessarily security vendors being asked to verify the thoroughness and effectiveness of their security strategies [7].

3.1 Security Concerns of Cloud Computing

In cloud, similar to every proposed technology, there are some issues involved in it and one of them is RAS (Reliability, Availability and Serviceability) factor. For having good and high performance, cloud providers must meet several management features to ensure improved RAS parameters of its service such as Availability management, Access control management, Vulnerability and problem management, Patch and configuration management, countermeasure, Cloud system usage and access monitoring.[8]

While cost and ease of use are two great benefits of cloud computing, there are significant security concerns that need to be addressed when considering moving critical applications and sensitive data to public and shared cloud environments. To address these concerns, the cloud provider must develop sufficient controls to provide the same or a greater level of security than the organization would have if the cloud were not used. Listed here are five items to review when considering cloud computing.

3.1.1 Secure data transfer

Traffic traveled between network and service being accessed must traverse the internet. Make sure your data are always travelling on a secure channel; only connect your browser to the provider via a URL that begins with "https."[9] There are protocols such as IPsec, those are developed specially for protecting internet traffic. Make sure that data is authenticated and encrypted using these protocols.

3.1.2 Secure software interfaces

The Cloud Security Alliance (CSA) recommends that you should be aware of the software interfaces, or APIs (Application Programming Interface), that are used to interact with cloud services. "Reliance on a weak set of interfaces and APIs exposes organizations to a variety of security issues related to confidentiality, integrity, availability, and accountability," says the group in its Top Threats to Cloud Computing document. The CSA recommends learning how any cloud provider you're considering integrates security throughout its service, from authentication and access control techniques, to activity monitoring policies [9].

3.1.3 Secure stored data

Secure encryption mechanism should be used to encrypt data when it's on the provider's servers and while it's in use by the cloud service. In Q&A: Demystifying Cloud Security [10], Forrester warns that few cloud providers assure protection for data being used within the application or for disposing of your data [9]. We must ask questions of the potential cloud providers who have authority to access the data, what mechanism they are using to provide security, authenticity and confidentiality?. We must also know about the security disposal of the data by cloud providers.

3.1.4 User access control Data is stored on cloud service provider's server

It can be easily accessed by an employee of that company as we have limited control of data stored there. To avoid this, firstly we must consider carefully the sensitivity of the data before transferring it to the cloud. Second, follow research firm Gartner's suggestions [11] to ask providers for specifics about the people who manage your data and the level of access they have to it.

3.1.5 Data separation

Every cloud-based service shares resources, namely space on the provider's servers and other parts of the provider's infrastructure. Hypervisor software is used to create virtual containers on the provider's hardware for each of its customers. But CSA notes that "attacks have surfaced in recent years that target the shared technology inside Cloud Computing environments." So, investigate the compartmentalization techniques, such as data encryption, the provider uses to prevent access into your virtual container by other customers.[9].

3.2 Cloud security control

Cloud security architecture is effective only if the correct defensive implementations are in place. An efficient cloud security architecture should recognize the issues that will arise with security management [12]. The security management addresses these issues with security controls. These controls are kept to provide safety in the system and reduce the effect of an Attack.There are many types of controls for cloud security architecture and are described below.

3.2.1 Hold back controls

These controls are deterrent controls placed to prevent any purposeful attack on a cloud system. These controls do not reduce the actual vulnerability of a system, but leave a warning message.

3.2.2 Hinder controls

These are also known as preventive controls. These controls manage the vulnerabilities, and thus upgrade the strength of the system. The Hinder control will provide safety against vulnerabilities of the system. The preventative controls are to cover the attack and reduce the damage and violation to the system's security in case of occurrence of an attack.

3.2.3 Remedy controls

Remedy controls are also known as corrective controls and are used to reduce the effect of an attack. Unlike the hinder controls, the remedy controls take action as an attack is occurring.

3.2.4 Investigative controls

Investigator or Detective controls are used to detect any attacks that may be occurring in the system. In the event of an attack, the detective control will signal the preventative or corrective controls to address the issue.

3.3 Cloud Security Requirements

Various cloud security requirements are- Authentication, Single Sign On, Delegation, Confidentiality, Integrity, Non-repudiation, Privacy, Trust, Policy, Authorization, Accounting and Audit .

4. Cloud Application

An application program that functions in the cloud, with some characteristics of a desktop application and some characteristics of a web application is Cloud application. A desktop application exists on a single device at the user's location that necessarily have not to be a desktop computer, while a web application is stored entirely on a remote server and is transferred over the Internet through a browser interface. Cloud applications take the benefits of both i.e desktop applications and web applications. Similar to desktop applications, cloud applications can provide fast responsiveness and can work offline. Like web applications, cloud applications need not permanently reside on the local device, but they can be easily updated online. With these reasons cloud applications are therefore under the user's control, yet they need not always consume storage space on the user's computer or communication device. A well-written cloud application offers all the interactivity of a desktop application along with the portability of a web application with the assumption that the user has a reasonably fast Internet connection. Cloud application can be used by anyone with a Web browser and a communication device that can connect to the Internet. Tools which exist in the cloud can be modified, the actual user interface exists on the local device. Data can be cached locally by the user, enabling full offline mode when desired. Unlike a web application, a cloud application will function even when the Internet connection is disabled. So cloud application can be used on board, an aircraft or in any other sensitive situation where wireless devices are not allowed. In addition, Cloud apps have become popular among people who share content on the Internet. "CloudApp," is a cloud application provided by Linebreak S.L., based in Spain, which allows users to share files, images, links, music, and videos. Google offers a solution called "AppEngine" that allows users to develop and run their own applications on Google's infrastructure. Google also offers a popular calendar (scheduling) cloud app. Amazon Web Services offer an "AppStore" that facilitates quick and easy deployment of programs and applications stored in the cloud. One of the well suited example of cloud application is Around Me iphones.

4.1 AroundMe iPhones

Suppose you were going for an outing with family and friends to a place that is not familiar to any one of you. As a result, you forever have to ask people where the nearest market is, where to find a taxi, for decent bars or restaurant. In this situation, AroundMe iPhones may be very helpful to you. The program is able to facilitate you with this information in a blink of an eye. All you need to do is a click on the iPhone and iPhone software automatically detects your current location and provides just one-click access to lists of the closest restaurants, supermarkets, banks, cafes, gas stations, hotels, hospitals, pharmacies, movie theaters, parking, bars, pubs, taxis and theaters, etc. Just click on any of these categories and AroundMe iPhone will bring up a list of those types of business quickly. You can then click on one of the suggestions to get the full address and phone number of the business, which you can add to your iPhone's contacts with a single click. Now if facing problem to find the location, Hit 'Show Route' and AroundMe will display the directions from your current location, via Google Maps. You will be surprised by the amount of results returned by AroundMe. AroundMe is very quick and simple to use but it's usefulness could still be improved. For example, it's not possible to view the results in order of vicinity, meaning you often have to strike through a few pages before you find the closest. Also, it would've been great to see more information about each place, such as guides, reviews or even just a link to the company's web site. AroundMe is a very handy thing to have in your pocket when you're out and about.

4.1.1 Advantages

AroundMe is really easy to use, displays decent amount of results and provides routes and directions.

4.1.2 Disadvantages

You can't order results by proximity

Conclusion

In this paper, we discussed service models of cloud that include SaaS, PaaS & IaaS. Then we have gone through various attacks on cloud and security concern of cloud computing. Finally we discussed about the applications of cloud. Like every technology, there are some issues that are needed to be focused upon in order to provide security in cloud computing, but we believe that due to the complexity of the cloud, it will be less hard to achieve end-to-end security.

References

[1]. **J.Staten, et al., (2008).** *"Is Cloud Computing Ready for Enterprise?"* Published in Forrester Research, March 7,2008.

[2]. **Parks R., Harvey J. (2008).** "Cloud Computing: What to Ask When the Clouds Roll In", *Presentation to the ACC Information Technology & Ecommerce Committee* June 5, 2008.

[3]. **P. Mell and T. Grance (2011),** "The NIST definition of cloud computing", *NIST special publication*, Vol. 800, No. 145.

[4]. **S. Roschke, et al., (2007).** "Intrusion Detection in the Cloud", *8th IEEE International Conference on Dependable, Autonomlc and Secure Computing*, Chengdu, China.

[5]. **A. Singh and M. Shrivastava, (2012).**"Overview of attacks on cloud computing," *International Journal of Engineering and Innovative Technology (IJEIT)*, Vol. 1, No. 4, pp.321-323.

[6]. http://www.mbaskool.com/business-articles/operations/5005-cloud-computing-a-better-way-to-do-it-.html CLOUD CCOMPUTING- A BETTER WAY TO DO IT. April 24th, 2014.

[7]. http://www.dman.com/cloud-computing-multi-

tenancy-and-application-security.html. Cloud Computing Security. April 20th ,2014.

[8]. **Farzad Sabahi, (2011).** "Cloud computing security threats and responses", *IEEE*, pp.245-249.

[9]. **Jeff Beckham, (2011).** *"The Top 5 Security Risks of Cloud Computing"*, CISCO BLOG, May 3.

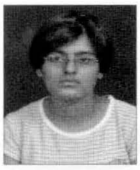
[10]. http://resources.idgenterprise.com/original/AST-0036145_G2A_demystifying_cloud_security.pdf . For Security & Risk Professionals. April 20th, 2014.

[11]. http://www.networkworld.com/news/2008/070208-cloud.html. Gartner: Seven cloud computing security risks. April 24th, 2014.

[12]. **Krutz, Ronald L., and Russell Dean Vines (2010).** "Cloud Computing Security Architecture." *Cloud Security: A Comprehensive Guide to Secure Cloud Computing*. Indianapolis, IN: *Wiley*, pp. 179-80. Print.

ABOUT THE AUTHORS

Awantika is working as Teaching Personnel in I.T. Department in G.B. Pant University of Agriculture and Technology. She has completed her M.Tech degree in Information Technology from G.B. Pant University of Agriculture and Technology. Her area of interest are Networking, Theory of Computation and Operating system.



Neha Rawat is pursuing M-Tech in Information Technology from Govind Ballabh Pant University of Agriculture & Tehnology, Pantnagar.She received her B-Tech degree in Computer Science Engineering from Dev Bhoomi Institute of Technology (DBIT), Dehradun (U.K.), INDIA in 2012.Her Research areas are Cloud Computing and Computer Networks.

Poonam Rawat is pursuing M-Tech in Information Technology from Govind Ballabh Pant University of Agriculture & Tehnology, Pantnagar.She received her B-Tech degree in Computer Science Engineering from Dev Bhoomi Institute of Technology (DBIT), Dehradun (U.K.), INDIA in 2012.Her research areas are Web Search algorithms, web mining and cloud computing.

Shikha Singh is pursuing M-Tech in Information Technology from Govind Ballabh Pant University of Agriculture & Tehnology, Pantnagar. She received her B-Tech degree in Information Technology from Uttaranchal Institute of Technology (UIT),Dehradun (U.K.), INDIA in 2012.Her research areas are digital image processing and crptogrpahy.