Cloud Security: Theory and Practice

Vaishali Balhara
Department of Computer Science and Engineering,
Baba MastNath University, Asthal Bohar, Haryana, India

ABSTRACT

Cloud computing is an upcoming technology that promises for a very scalable and agile computing. The world is experiencing a major breakthrough in resource pooling at a bigger platform than ever before. Although the adoption of this technology is taking place at considerable rate but we still witness some serious hazards here which are inhibiting the IT sector to take full advantage of such a useful technology. This paper discusses about the biggest hazard in the way of cloud computing which is undoubtedly the security. Security in clouds is a major research area these days. So this paper reviews the security concern with their requirement and best practices in cloud architecture.

KEYWORDS

Cloud computing, Cloud security, Risk, Risk Management

1. INTRODUCTION

1.1 Concepts and definitions

Cloud computing has evolved from various technologies that we already know from quite a tie now. These technologies are: virtualization, grid computing, utility computing, web services, internet, www and SOA. Cloud computing is a technology that has changed the way we perform computing. With cloud computing, now everything is in the clouds. By that it is meant that we can develop, deploy and deliver an application in the cloud without having the need of those six digit software licensing, a rapid ROI, and massive decrease in TCO for starting any sized business.

Now let us define cloud computing as NIST [1] has defined it. They say:

"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources(such as networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction This cloud model promotes availability and is composed of five essential characteristics, three service models and four deployment models".

Also, NIST have defined the cloud model's characteristics, service models and deployment models like this :

- **Cloud service models :**
  - **Software as a Service** - "A Saas cloud implementation delivers software or, more generally described, an application to its end user. The end user doesn't usually need to understand or be concerned with the supporting infrastructure and simply utilizes an application. All the back office details are masked and provided as a service behind the scenes of that application."
  - **Platform as a Service** - "PaaS providers usually deliver a bundling of software and infrastructure in the form of a programmable container and provide a cloud for an end user to host their own developed applications or services. PaaS is similar to SaaS, but with PaaS, the service is the entire application environment- typically, PaaS includes the computing platform as well as PaaS providers usually deliver a bundling of software and infrastructure in the form of a programmable container and provide a cloud for an end user to host their own developed applications or services. PaaS is similar to SaaS, but with PaaS, the service is the entire application environment- typically, PaaS includes the computing platform as well as the development and solution stack."
  - **Infrastructure as a Service** - "IaaS clouds deliver virtualized resources, such as guest virtual machines (ready to load an operating system), storage, or database services. The tenant interacts with IaaS clouds in a similar way as giving a system's architecture to an IT department to provide the necessary systems. This is the virtual equivalent to physically deploying servers, storage or database.
- **Cloud Deployment Model**
  - **Public Clouds** -NIST definitions a public cloud as: "The cloud infrastructure is made available to the general public or large industry group and is owned by the organization selling cloud services."
  - **Private Clouds** - NIST defines it as this : "The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise."
  - **Community Clouds** - NIST defines it as : "The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns. It may be managed by the organizations or a third party and may exist on premise or off premise. These deployments are all documented in the SLAs to get a common agreement on the terms of services usage. Such cloud deployment model can be very beneficial for these organizations as they can have cost efficiencies and grow better. "
  - **Hybrid Clouds** - NIST defines a hybrid cloud as: "The cloud infrastructure is a composition of two or more clouds that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability."

Now looking at the characteristics of Cloud Computing we have following main characteristics : resource pooling, on-demand, user defined, metered billing, scalability, elasticity, agile, utility

1.2 Historical background

John Mc Carthy had a view of computing as a utility when in 1960s he proposed the idea of computation being delivered as a public utility similar to other public utilities as electricity or telephone services.[10]

This very view started to get a platform when many organizations believed in this view and continued working in order to achieve this objective or in other words we can say that this era of cloud computing was arriving.

But it took Amazon to establish their data centers in cloud. In 1990s and 2000 they actually introduced cloud to the world. Amazon played the key role by moving a number of their data centers in cloud. And by doing this they saved more than 10% on expenditure on day t o day tasks. Then in 2006 Amazon introduced the world with Amazon Web Services(AWS). [4]

In 2008, concept of private cloud was introduced by Eucalyptus which is an open source API compatible for deploying our applications in the private cloud.

In 2008, Open Nebula mutually used clouds for federation of clouds and for introducing hybrid clouds. [4]

2. WORKING OF CLOUDS

The cloud does not work on a single front, but this technology is divided in two major parts :

- Front end
- Back end

Front end constitutes the : desktop, laptop, tablet or mobile)

- GUI application for a user to interact with the technology

Back end constitutes the:

- Servers
- Data storage
- Processors
- Clusters

Eg. A simple example can be : GMail which has a GUI interface for the user to read, write or send mails; and at the back end it has a number of mail servers who actually send or receive mails.

Cloud's working style is similar to that of a multi-tier technology where the logics are separated from each other for better.

Cloud accomplishes many *advantages* as :

less expensive, flexibility, ROI, lesser TCO and many more which helps a new business of any size(small, medium, big) to grow more with less investment.

Although every technology is not complete in itself and so is the case with cloud computing, so obviously we have some *disadvantages* in it such as : **security, extra charges for data transfer, migration is a difficult task in clouds.**

3. BIG PLAYERS

Taking advantage of the fact that by implementing the technology of cloud a large number of organizations of different sizes have been benefited and it is still accounting for their better growth by cutting cost while still increasing their productivity. To name a few we can highlight some known organizations which use cloud technology for working, and they are :

Skype : an application used all over the world and it is running over clouds

Basecamp : a major project management tool and it is running its business over cloud infrastructure

force.com : a platform to build social and mobile applications in cloud

Now, talking about the providers who are serving our IT world with this technology, they are known as Cloud Service Provider(CSP). There are some big names for CSP and they are :

AmazonWebServices(AWS)
GoogleAppEngine
Microsoft Azure
Hadoop

4. RISK IN CLOUDS

Security approaches should be pragmatic in terms of security controls and system functionality. What we mean is that the same architecture and the same controls are generally not appropriate both a low risk and high risk environment. [2]

Talking of risk, we have several types of risks in our information world (as privacy, integrity, security, vulnerability and like). Among these is a vital risk with due respect to our paper and that is the security risk which needs to be managed scientifically in order to get ris of it to a great extent.

So what is a risk? Well risk is a function of threats as they seek to exploit vulnerabilities, and in light of the countermeasures, we apply to protect our assets. [2]

We can view security as the most desirable attribute that one system should have for being called as "secure".

5. MANAGING SECURITY

Well known IT organizations that are in the IT world since quite a long time now, are managing their information assets through well planned security architectures. The choice of level of establishment in a organization's architecture for security depends upon the following factors:

- requirement of the cloud consumer who analyze the type of data one handles in cloud (i.e., whether it is data on a social site or data of a secrecy department of a government body)
- type of service model to be used
- type of deployment model to be used

Security architectures and models have been influenced by various processes, engineering and model efforts. Initially

CMM was adapted for security which was basically derived from ISO/IEC 17799:2005 which came to a head in the late 1990s and early 2000s and is called the SSE-CMM (System Security Engineering Capability Maturity Model). [2]

Although there are a huge number of models as well as standards for security architecture but a few are listed below here :

- ITIL - Information Technology Infrastructure library
- COBIT - Control object for Information and related Technology [2]
- ISO 27001 - ISO 27006 [5]
- ENISA - European Network and Information Security Agency [6]

6. RISK MANAGEMENT IN CLOUDS

Cloud Computing has tremendous potential for organizations to improve their overall information security posture. [2]

Risk management is a series of phases that are carried out and which support any architecture or model of security to mitigate risks in its architecture and achieve confidence in that model or architecture.

When talking of software development through SDLC, in its very basic terms risk management comprises of these fundamental steps :

- Risk Analysis
- Risk Identification
- Risk Abatement

And when talking of cloud computing risk management we can divide this activity into further sub-activities.

According to Mather, Kumaraswamy & Latif [3] there are two main activities in managing risk in a cloud architecture, and they are :

- Risk Management
- Risk Monitoring

They have done it some other way hence forth.

These two activities can in turn be divided into following sub-activities :

Risk Management comprises of three main tasks which are as follows :

- **Identify** - A customer should first of all identify and come to know about how much risk is affordable according to him. And this directly depends upon the requirements of a customer in cloud with respect to the type of information one deals.
- **Planning** - Here looking at the type of architecture and after knowing that how much valuable our data is to us, we plan and propose for the desired techniques and tools to be implemented to mitigate security risk.
- **Design and Implement** - Here we design and develop the techniques and tools that were proposed in the planning phase. And once developed these tools are implemented in the security architecture.

Risk Monitoring comprises of two main tasks which are as follows :

- **Testing And Auditing** - We look for the success and reliability of the tool implemented in the previous phase by testing those tools on the real platform. Then auditing is done to verify the tool's reliability.
- **Maintenance** - Here certain responsibilities are defined on the part of consumer and the CSP. These responsibilities are listed in form of roles each party (consumer and CSP) have to practice to improve the security of a cloud.

7. KEY ELEMENTS AND BEST PRACTICES IN CLOUD SECURITY

Here we discuss some security patterns and elements that contribute to cloud security.

According to Winkler[2] these elements are :

- Defence in-depth, honeypots, sandboxes, network patterns, isolation of virtual machines, isolation of subnets and like.
- Now let us talk about the best practices that are to be adopted for experiencing better security in cloud architectures.
- The Cloud Computing Use Case Discussion Group "Cloud Computing Use Cases White Paper", in version 4.0, have identified following practices for security in cloud computing :
- Asset management, cryptography (key and certificate management), Data/Storage Security, Endpoint Security, Event Auditing and Reporting, Identify, Roles, Access Control and Attributes ; Network Security ; Other Controls listed by the Cloud Computing Use Case Discussion Group.

8. RESEARCH IN CLOUD SECURITY

A lot of researches are going on the security issues in the cloud computing. And a number of new algorithms are designed for providing better security in cloud.

Ajay Jungra, Renu Bala [9] proposed Privacy Aware Security Algorithm - PASA which gives a user to have control and freedom to manage the privacy mechanisms to maintain the security of sensitive data.

Sunil Sanka et al [11] proposed a technique for handling security and access control problems and also proposed a modified Diffie-Hellman key for higher security between customer and a CSP.

Wassim Itani et al [8] prposed PaaS - Privacy as a service protocol that ensures the privacy and legal compliance of customer data i cloud computing architectures.

Also there are many other researches that are going on. But still there is a lot of scope for new features providing security in a cloud computing architecture.

9. CONCLUSION AND FUTURE WORK

Cloud Computing is facing some challenges in field of security. It is inhibiting cloud's way to proper as a true public utility which can indeed help new and upcoming organizations to develop with less investments. This paper discusses the security concerns in a cloud computing architecture. Here we have started by discussed the theory of cloud computing. And then, we highlighted the working of a cloud. Then we explained the security risk in detail along with its management in a cloud. Finally we discussed about the security elements and best practices of cloud security. This paper serves to be useful for providing platform to anyone who wish to do work in cloud security by reviewing various security risk issues. The future work defines a novel and innovative cloud security algorithm for achieving better standards in the security aspects in a cloud computing architecture.

10. REFERENCES

[1] http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, accessed May 2013

[2] W. Vic (J.R.), Securing the Cloud- Cloud Computer Security Techniques and Tactics, United States of America: Syngress : an imprint of Elsevier, 2011.

[3] M. Tim, K. Subra and L.Shahed, Cloud Security and privacy- An Enterprise Perspective on Risks and Compliance, United States of America: O'Reilly Media, Inc., 2009.

[4] Innobuzz knowledge solutions, "Certified Cloud Computing Expert", Reference Guide.

[5] http://www.iso27001security.com/html/iso27000.html, accessed May 2013

[6] ENISA, "Cloud Computing : benefits, risks and recommendations for information security", 2009, http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment, accessed May 2013

[7] Ahronovitz M, et al. The Cloud Computing Use Case Discussion Group "Cloud Computing Use Cases White Papers" version 4.0, http://cloudusecases.org, accessed May 2013 Itani, W., Kayssi, A., Chehab, A.: Privacy as a service: privacy- aware data storage and processing in cloud computing architecture. In: 2009 Eighth IEEE International Conference on Dependable Autonomic and Secure Computing, 978-0-7695-3929-4/09 ©, pp. 711–717. IEEE (2009)

[8] Jangra A., Bala R. : PASA : Privacy-aware Security Algorithm for Cloud Computing, http://link.springer.com/chapter/10.1007%2F978-3-642-32063-7_52

[9] Mohamed A., "A history of Cloud Computing", http://www.computerweekly.com/feature/A-history-of-cloud-computing, accessed May 2013

[10] Sanka, S., Hota, C., Rajarajan, M.: Secure data access in cloud computing. In: 2010 IEEE 4th International Conference on Internet Multimedia Services Architecture and Application, 978-1-4244-7932-0/10 ©, pp. 1–6. IEEE (2010)