Volume 3, Issue 4, April 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Insight of Cloud-Specific Culpabilities, Risks, Threats

K. Thejaswi[a], I. Sheeba[b], C. Bhuvana[c], P. Lavanya[d]
[a, d] M.Tech Student, Dept. of Computer Science and Engineering,
Sree Vidyanikethan Engineering College, Tirupati, India.
[b, c] Assistant Professor, Dept. of Computer Science and Engineering,
Sree Vidyanikethan Engineering College, Tirupati, India.

Abstract: ***Even though cloud computing provides compelling benefits and cost effective services to IT, new risks, threats, culpabilities are introduced in every way. Risks, threats, culpabilities sounds same meaning but they differ technically in terms of security. Every day, a news item, a blog or an email warns us about security risks of cloud computing. May not all the risks specified come into accordance with cloud computing. Thus we define a new strategy in defining a cloud specific risks, cloud specific threats, cloud specific culpabilities. We also specify the top most in them which bothers security of cloud in high. This paper describes what to worry and what not to worry in specific to cloud security.***

Key Words: cloud computing, cloud security, cloud specific risks, cloud specific threats, cloud specific culpabilities, remedies.

I. Introduction

Today we know the one of the hot topic in field of IT is "how our data is secure in cloud?". Everyday business organizers think how can we trust cloud?. Even we know about the risks in cloud users need cloud for its beneficial services. Users are confused with what really related to cloud computing? And what not?

"Insight of Cloud-Specific Vulnerabilities, Risks, Threats" this will be helpful to users to know about the cloud specific risks, cloud specific threats, cloud specific culpabilities i.e., vulnerabilities. This paper is easily understandable to the readers for what to worry and what not to. Anyway risks are always to worry. Making risk management prior and after can help to worry little. In this paper the threats, risks, vulnerabilities are tabulated. We know threat, risk, vulnerabilities sound similar but to the context in technology they differ. Thus we define definitions for the risk, threat, culpabilities.

Some of the risks, threats and vulnerabilities are mentioned briefly. Cloud specific risks, cloud specific threats, cloud specific vulnerabilities are defined and the top most in them are highlighted. If the pros and cons are well known then it's easy to know whether to approach it or not. This helps the starters of business organizers to step towards cloud architecture.

II. An Overview

As we all know the definitions, deployment models, cloud service models of cloud computing even let us define what they are in brief.

A. Cloud Computing:

The services either software or hardware or both that are delivered to the users of the cloud using a network.

Figure 1: General view of Cloud Computing

B. Cloud Deployment Models:

1) Public Cloud: This type of clouds are available to public this may be owned by an organization who sells cloud services.

2) Private Cloud: This type of clouds infrastructure are available to specific organization may be owned itself or any third party.
3) Community Cloud: Belongs to a specific community like military, finance etc.,
4) Hybrid Cloud: It's a combination of any of the above.

C. Cloud Service Models:
The most common cloud service providers are SaaS, PaaS, IaaS. In addition to them there are several other services they are XaaS, STaaS, Naas, DaaS, DBaaS, TEaaS etc,.

Terminology:
The title "Insight of cloud specific culpabilities, risks, threats" has three terms in specific i.e., Culpabilities, Risks, Threats. Let me define them in general. The culpability is nothing but the vulnerability which is the prominent factor of risk. Risk is the probability of suffering from a loss in future. Threat is an indication of a danger which is close at hand. According to the terminology of cloud computing threat is a harm to an asset or an organization. culpability is a probability that the capability of a threat in resisting a threat exceeds. Risk is the probable frequency and probable magnitude of future loss.

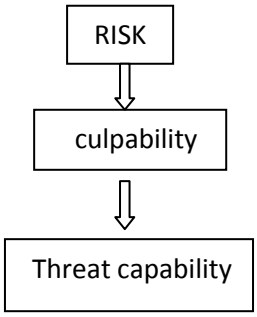

Figure 2: Defining relation between risk, culpability and threat capability.
To understand the brief taxonomy of risk can refer technical standard [1] which provides a clear picture.

III. Cloud Specific Threats

A. *Data Loss or Leakage:* Cloud is all about data. Storing our data in third party cloud leads to data loss or leakage. Data which is sensitive is leaked or lost without backing up may lead to severe losses sometimes the reputed organizations has to freeze. Hackers may hack even the encrypted data by gaining keys. According to CSA [2] survey 2012 data loss has threat upto 91 percent. To gain trust in cloud we need to implement strong encryption keys or license keys, strong back ups, preventions at the time of design and even at working etc.,
B. *Insecure API's:* Users of cloud may require different API's for accessing. As users are heavy difficult to manage authentication. Securing API is the basic control of cloud. This threat troubles the cloud by 90 percent. The security models has to be securely designed and the authentication methods are to be strong.
C. *Malicious Insiders:* This is most commonly known threat where most of the IT organizations has faced. This threat has 88 percent impact on cloud. This depends on hiring process. Employees level of access is not known thus generally this is opportunity for the hackers. The legal proceedings must be severe for such fellows and the level of accessing must be well organized.
D. *Account or Service Hijacking:* This is a common known abuse we often see. Gaining of passwords by a hackers may cause altering data, misusing sensitive data etc ., Once hackers gain access to our credentials then our activities are evesdropped. Monitoring unauthorized accessing, protecting passwords etc., by often changing may better the situation. There are other threats which are not addressed are abuse of cloud computing, unknown risk profile, DDoS, CSP maturity levels, improper auditing, MIM Attackers etc..

IV. Cloud Specific Vulnerabilities

A. *Cloud Related Technology Vulnerabilities:* The cores related to cloud computing are mainly cryptography, web apps, web services, virtualization. Cryptography is for protecting data or providing secure authentication purposes but cryptography also has vulnerabilities like breaking the algorithms. Web apps and services vulnerabilities include account hijacking etc., virtualization vulnerabilities may include as the environment is virtualized easy for attackers to in.
B. *Vulnerabilities of Cloud Characteristics:* There are several characteristics of cloud like pay per use, on demand services etc., these characteristics also has vulnerabilities.
1) ***Unauthorized access:*** When compared to traditional systems and cloud systems the users are more thus need to manage more. So probability of vulnerabilities are high.

2) ***Billing per use****:* As we pay per what we use managing the bills are difficult. Vulnerabilities may cause for billing the authorized actors but the use of it by an unauthorized ones.

C. *Back up vulnerabilities:* Cloud require several data bases to store such a big data. The vulnerabilities like SQL injections, insecure user behavior like storing passwords, reusing passwords etc.,

D. *Architectural vulnerabilities:* There exists several architectures for cloud but still suffering from vulnerabilities in making best architecture. This may include network vulnerabilities, services like SaaS, IaaS, PaaS may cause vulnerabilities.

There are other cloud specific vulnerabilities are mentioned in paper [3].

V. Cloud Specific Risks

ENISA report [4] has well architecture the risks, vulnerabilities of cloud computing. In one of its publications risks are classified as policy risks, technical risks, legal risks. some of them are

A. *Loss of Governance:* Users may cedes cloud many times thus security control is lost.

B. *Lock In:* The standards, tools followed by one cloud service provider may differ from other. Thus users cannot easily move.

C. *Isolation failure:* Multi tenancy leads to gap between tenants as the resources are shared.

D. *Compliance Risk:* Certification achievement is risk at investment.

E. *Lack of Transparency:* Cloud providers cannot specify the algorithms, processors, operations, controls to the users. This leads transparency to users about cloud. This risk is clearly given in [5] which specifies the transparency between user and provider.

F. *Reliability and performance issues:* System failures are common in computing environment. Even there may be agreements between tenants and providers sometimes providers cannot meet the requirements.

G. *Insecure or Incomplete Data Deletion:* Replicating the data is serious concern to this because when user need to delete the data completely its highly impossible to an OS to know the copying files of the data where in the huge cloud.

H. *Cloud service provider viabilities:* Still the cloud providers are young may lead to viabilities for achieving the profits.

I. *Malicious insiders:* This is well known threat which leads to high risk probability. May include CP system administrators, managed security service providers.

J. *Management Interface Compromise:* Providers of customer management in providing large resources may pose increase in risk.

There are several risks which are cloud specific but the above mentioned are top. Some of the non cloud specific risks are network breaks, natural disasters, loss or compromise of security or operational logs, theft of computer equipments, unauthorized access to premises, backups lost or stolen etc…

Conclusion

There are several surveys have been done and doing for securing the cloud computing. The organizations like CSA, NIST, ENISA etc., are being involved in surveying the cloud risks and finding out the remedies of some. As cloud increases every minute risks increases in proportion. Thus need a perfect strategy for building up the cloud architecture in providing the security. As we are at learner stage we just made a report on the cloud specific risks, cloud specific threats and cloud specific culpabilities. In accordance to the survey references we mentioned the top among them.

References

1. Technical Standard, **Risk Taxonomy,** *The Open Group*, ISDN 1-931624-77-1 , Document Number C081, published by The Open Group January 2009.
2. Cloud Security Alliance CSA , *WITH RANKINGS AND RISK ANALYSIS AT CSA SUMMIT @ RSA 2013*, Top Threats To Cloud Computing, Survey Results Update 2012.
3. Bernd Grobauer, Tobias Walloschek, and Elmar Stöcker *Siemens,* UNDERSTANDING CLOUD COMPUTING VULNERABILITIES, ieee journal on computer and reliability socities, vol. 9, issue :2,page no: [50-57], march/april 2011.
4. Daniele Catteddu and Giles Hogben *cloud computing benefits, risks and recommendations for Information Security*, http://www.enisa.europa.eu/, November 2009.
5. Crowe Horwath LLP ,Warren Chan , Eugene Leung , Heidi Pili *COSO Enterprise Risk Management In Cloud Computing,www.COSO.org.*

