Volume 8, No. 2, March 2017 (Special Issue)
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
REVIEW ARTICLE
Available Online at www.ijarcs.info

Analysis and Assessment of the Vulnerabilities in Cloud Computing

Nailah Afshan
Department of CSE, SEST
Jamia Hamdard, New Delhi, India
anumwani04@gmail.com

Abstract: The field of cloud computing has become a highly popular means for the smooth provision of various Information Technology (IT)-enabled business services. In today's dynamic and rapidly changing computing era, most of the organizations have chosen it as basic technology resource. Consequently, due to the expansion in usability and functionality unique security vulnerabilities and threats are emerging which act as the most substantial roadblock for cloud computing thereby, requiring timely attention. It is the need of hour to understand and mitigate such threats and vulnerabilities so as to gain a better insight into the required techniques and infrastructure. This would help in making the cloud architecture less vulnerable which in turn will make our future easier and technologically more sound. This paper focuses on exploring the various threats and vulnerabilities associated with the cloud computing technologies.

Keywords: virtual escape; cloud architecture; cloud-specific vulnerabilities; risk taxonomy

INTRODUCTION

Cloud computing can be defined as distributed web-based computing which involves the delivery of different information technology (IT) services through the internet [1]. It is setting a new business trend over the Internet allowing all the shared resources; and information and application programs being distributed around systems on demand. The cloud computing model comprises four deployment models, three service models and five essential characteristics. The four deployment models are public cloud, private cloud, hybrid cloud and community cloud. Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) are the three service models. Cloud computing has become possible and successful through several core technologies [2].

Core Cloud Computing Technologies

- Web applications and services:-Web application and Web services technologies are the foundations of SaaS and PaaS. This is so because the Web applications are actually the SaaS offerings, for which the development and runtime environments are provided by the PaaS offerings. For the IaaS offerings, the web applications and the web service technologies are used to implement the APIs and the rest of the similar services.
- Virtualization IaaS offerings:-Virtualization of the infrastructure has played a key role in making cloud computing a possible technology. The importance of virtualization also extends to PaaS and SaaS service models, as they are usually built on the top of a supporting IaaS infrastructure.
- Cryptography:-Cryptographic techniques have proved highly beneficial in solving many cloud computing security requirements [2].

The list of core technologies is likely to expand as cloud computing develops and gets more mature.

Essential Characteristics

Five essential characteristics of the cloud computing that have been specified by the US National Institute of Standards and Technology (NIST) have become the de facto standard for defining it. They are:

- On-demand self-service:- It meansthat the different customers of the cloud services (usually organizations) can easily request, order or manage their own computing resources without any interference or interaction with the cloud service providers.
- Ubiquitous or broad network access:-The differentservices offered by the cloud are accessed through the network (the Internet or other private networks). It uses some standard mechanisms and protocols.
- Resource pooling:-Pooled resources means that the various computing resources that are needed for the cloud service delivery are organised in a homogeneous shared form called resource pool from which the resources are drawn by all service users or customers.
- Rapid elasticity: - Cloud computing uses horizontal and vertical scaling to scale up and down the various resources rapidly and elastically.
- Measured service:-All the cloudresource/service usage is constantly measured and the customers are billed accordingly [2, 3].

Vulnerability

All the attributes, service models and the characteristics of cloud computing have led to its tremendous development as well as have made it vulnerable to different types of the security attacks. Each day we come across some fresh news or other publications warning us about the security of cloud computing which has become the most substantial roadblock for its uptake. So we must analyse how the established security issues are influenced by the cloud computing. A highly important and worth understanding factor here is the security

vulnerabilities. Many well-established and already existing vulnerabilities in the conventional networks are made more significant by the introduction of cloud computing and it also adds some more new ones to the mix Now before taking a closer look at the cloud specific vulnerabilities, let us first establish what vulnerability really is [1, 2].

Vulnerability is an important factor of risk. The term risk is defined by the ISO 27005 as "the possible potential that a given threat will exploit vulnerabilities of an asset or a group of assets and thereby cause harm to the organization," assessing it in terms of both the possibility of occurrence of an event and its possible outcomes. A useful summary of risk factors is provided by the Open Group's risk taxonomy (see Fig. 1).

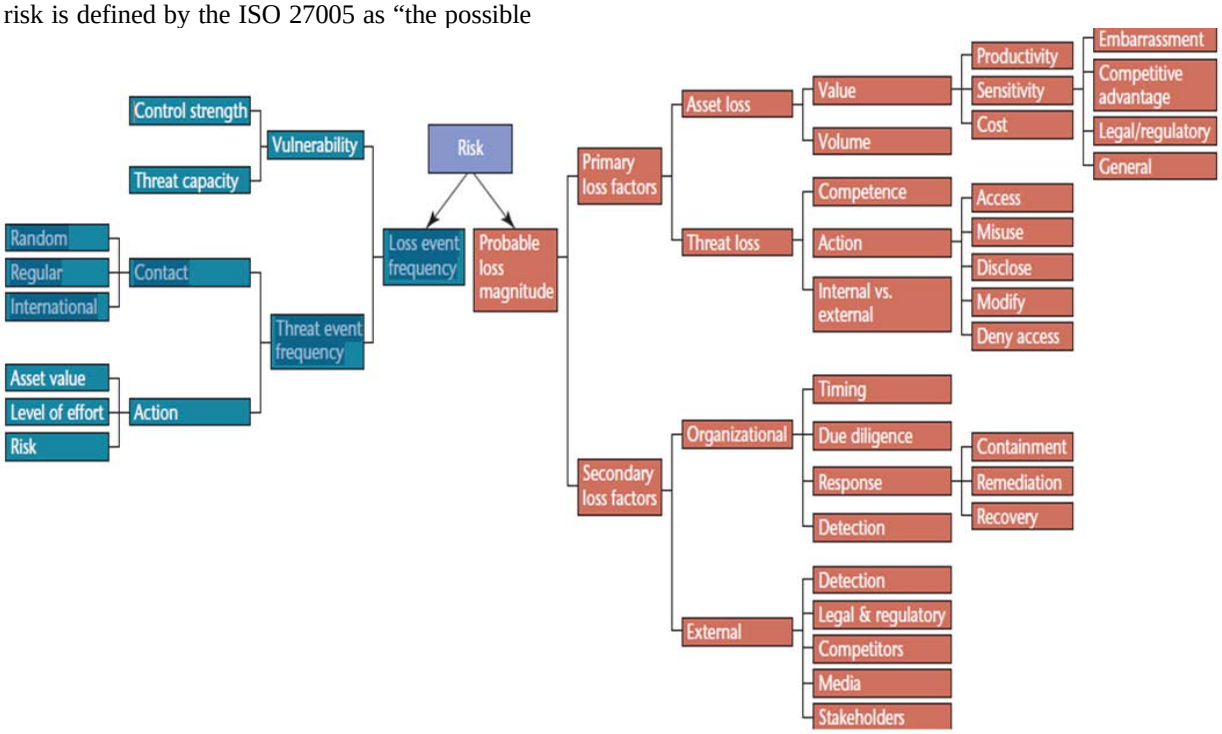

Fig. 1: Different risk factors as per Open Group.

It uses the same two high magnitude risk factors as provided by the risk definition by ISO 27005: the possible occurrence of a harmful event (here defined as the loss event frequency) and its results or outcome (here defined as the probable loss magnitude).

The final cost of a loss event is highly impacted by the subfactors of the probable loss magnitude while as the subfactors of harmful event's frequency are a bit more complex. Successful exploitation of a vulnerability by a hacker or a threat agent leads to the occurrence of a loss event and the frequency of its happening depends on two important factors as: - The frequency with which the hacker or attacker tries and succeeds to leverage the vulnerability which is further determined by the agents' momentum or impetus and his access level to the targets of the security attack. The second factor is the difference between the attack potential of the attackers; and the potential and strength of the system to withstand and oppose the attack. This second factor leads us towards a powerful definition of vulnerability. The Open Group's risk taxonomy defines vulnerability as the probability that an asset will be unable to oppose the actions of an attacker. Whenever there is a difference between the force being imposed by the attacker, and the system's potential to resist that force, a vulnerability crops up. Thus vulnerability is always described in terms of the opposition or strength shown against any type of attack [2].

There is a close relation between the vulnerabilities and the cloud risk that can be examined by having a look on the risk factor tree beginning from the right side. As far as the cloud customer's perspective is concerned, cloud computing has no impact at all on the right-hand side dealing with probable magnitude of future loss. However, the left hand side dealing with the loss event frequency is significantly changed by cloud computing. Moving from the conventional IT infrastructure to the cloud computing infrastructure might change the access level of the attacker, its motivation as well as the effort and risk [4].

CLOUD SPECIFIC VULNERABILITIES

As an abstract view of the cloud computing model and the concept of vulnerability have been discussed above, we can now easily go for a proper definition of a cloud-specific vulnerability. A vulnerability that arises due to the introduction of different cloud services and characteristics can be termed as a cloud-specific vulnerability [5]. On a broader scale, it is defined by four indicators. A vulnerability qualifies to be cloud-specific if it

a) is natural to or indigenous in a core cloud computing technology,
b) has its main cause in one of the five essential cloud characteristics ,
c) is caused when cloud innovations and other core computing technologies make the implementation of different security controls cumbersome or impossible or

d) is customary to the different state-of-the-art cloud offerings [2].

Now each of these four pointers of a cloud-specific vulnerability is discussed below.

Core Cloud Technology Vulnerabilities

The core technologies used by the cloud may have vulnerabilities in two different forms. This means they may be either inherent to the technology or may crop up from its various state-of-art implementations. As already discussed, the main core technologies used in cloud include the Web applications and Services, Virtualisation IaaS offerings and cryptography each of which leads to different vulnerabilities . An example of each includes session riding and hijacking (associated with the Web applications), virtual machine escape (that results from the implementation of virtualization), and insecure or obsolete cryptography. First, due to the very nature of virtualization, it becomes possible that an attacker might successfully escape from a virtualized environment. Hence, the vulnerability of virtual escape can be considered as inherent or prevalent in virtualization and thus, highly pertinent to cloud computing [6]. Second, some notion of session state is required by the Web application technologies but use the HTTP protocol, which is stateless. Though many techniques implement session handling, but most of the implementations are vulnerable to session riding and session hijacking [3, 7] Thus, the vulnerabilities of session riding/hijacking are certainly relevant for cloud computing. Finally, due to cryptanalysis advances, new methods of breaking the cryptographic algorithms are being discovered rendering them insecure.[3] Thus insecure cryptography vulnerabilities are also highly popular in cloud computing as implementation of cloud computing is almost unthinkable without the use of cryptography to protect the confidentiality and integrity of data in the cloud.

Essential Cloud Characteristic Vulnerabilities

We have already discussed in the previous section the five essential characteristics of cloud computing as prescribed by the NIST. Following are some illustrations of the vulnerabilities having their root cause in any of these essential characteristics:

- Distributed nature vulnerabilities: - The distributed nature of cloud computing leads to higher probability of intrusion prospects as well as infringements in the security [1].
- Missing standards at each of the cloud tiers: - It is a big challenge to maintain a proper level of flexibility in cloud computing. Consequently, the customers become more dependent on one cloud service provider due to which chances of becoming “cloud locked” are increased making it more vulnerable [8].
- Data recovery vulnerability: - Resource pooling and elasticity features make it possible to allocate a set of resources to different users at different times. If the resource is used for storage purposes or as memory, it is quite possible to access and recover the data written by some previous user [2].
- Multi-User Administrative Infrastructure / Unauthorized access to management interface: - The “on-demand self-service” characteristic of cloud requires a management interface that is accessible to cloud service users. The probability that unauthorized access could occur is much more for cloud as compared to the traditional systems where only a few administrators can access the management functionality. Thus, the multi-user administrative infrastructure qualifies to be a vulnerability for cloud systems [2, 3, 8].

Thus the well founded definition of cloud by NIST can be leveraged in reasoning about the cloud computing issues.

Defects in Known Security Controls

If cloud innovations directly create difficulties in implementing standard security controls, then the vulnerabilities associated with these controls must be considered cloud specific. *“Control challenges”* is another name for such vulnerabilities. Let us take some examples of such control challenges. First, insufficient network-based controls are offered by the virtualized network. Moreover, IP-based network zoning which is one of the standard controls can’t be applied. Proper management and the storage of different security keys is needed by the infrastructure and the implementation of cloud computing So, poor key management procedures also offer an important challenge. Due to virtualization, the cloud doesn’t have a fixed hardware infrastructure and also the cloud-based content is often geographically distributed, which makes it more difficult to apply standard controls to keys on cloud infrastructures. Moreover, different security metrics are not adapted to cloud infrastructures [8]. Currently, we don’t have any standard cloud-specific security metrics that could be followed by the cloud service users to have a check on the security status of their resources on cloud. So unless and until such standard metrics for cloud security are created and implemented, all the controls for assessing the security and the controls for audit, and accountability are highly complicated and expensive, and even impossible to implement [2].

Prevalent Vulnerabilities in State-of-the-Art Cloud Offerings

In spite of being relatively young, there are already varied cloud offerings in the market. Vulnerability can undoubtedly be referred as cloud-specific when it is prevailing in state-of-the-art cloud offerings. Injection vulnerabilities and weak authentication schemes are some common examples that are popular in state-of-the-art cloud offerings [9].

Manipulation of service or application inputs so as to interpret and execute parts of them against the planning and aim of the programmer leads to the exploitation of injection vulnerabilities. SQL injection, Command injection and Cross-site Scripting are some main examples of the injection vulnerabilities where the inputs are erroneously executed in the database back end, OS and victim browser, respectively.

Most of the widely used authentication mechanisms are weak. Take the case of username and password used for authentication. The two important factors that are responsible for their vulnerable behavior include the negligent behavior of the user itself (choosing weak passwords, reusing passwords, and so on), and the implementation of one-factor

authentication mechanisms which fail to provide a better authentication and security. So it becomes highly important to switch to multi-factor authentication. These have been discussed in [10,11].

CONCLUSION

Cloud computing is developing continuously and rapidly. It is being welcome warmly by different public as well as private organizations. But due to tremendous expansion in its functionality and usability, it has become more vulnerable to different types of security attacks. As this field gets more mature, it is quite certain that some new cloud-specific vulnerabilities will continue to emerge and some of the earlier vulnerabilities will become less of an issue. These vulnerabilities are acting as the greatest hindrance for both the cloud service providers as well as for the cloud service consumers in the delivery and use of the cloud services. So it is highly important that the respective authorities understand these vulnerabilities as the risk in cloud will be minimized helping them in making right investment. Thus it is concluded that the concept of Cloud computing is a novel one that has brought many laurels but several security threats and vulnerabilities have emerged with this new concept, so the cloud providers must identify and address these security issues on a continuous basis so that our future becomes more technology oriented.

REFERENCES

[1] R. Goel, M. Garuba and A. Girma, "Cloud Computing Vulnerability: DDoS as Its Main Security Threat, and Analysis of IDS as a Solution Model," 2014 11th International Conference on Information Technology: New Generations, Las Vegas, NV, 2014, pp. 307-312.

[2] B. Grobauer, T. Walloschek and E. Stocker, "Understanding Cloud Computing Vulnerabilities," in IEEE Security & Privacy, vol. 9, no. 2, pp. 50-57, March-April 2011.

[3] A. M. Al Zadjali, A. H. Al-Badi and S. Ali, "An Analysis of the Security Threats and Vulnerabilities of Cloud Computing in Oman," 2015 International Conference on Intelligent Networking and Collaborative Systems, Taipei, 2015, pp. 423-428.

[4] A. Gkortzis, S. Rizou and D. Spinellis, "An Empirical Analysis of Vulnerabilities in Virtualization Technologies," 2016 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), Luxembourg City, 2016, pp. 533-538.

[5] Madria, Sanjay K. "Security And Risk Assessment In The Cloud". Computer 49.9 (2016): 110-113. Web.

[6] F. Zhou, M. Goel, P. Desnoyers and R. Sundaram, "Scheduler Vulnerabilities and Coordinated Attacks in Cloud Computing," 2011 IEEE 10th International Symposium on Network Computing and Applications, Cambridge, MA, 2011, pp. 123-130.

[7] M. Derfouf, A. Mimouni and M. Eleuldj, "Vulnerabilities and storage security in cloud computing," 2015 International Conference on Cloud Technologies and Applications (CloudTech), Marrakech, 2015, pp. 1-5.

[8] A. Girma, M. Garuba and J. Li, "Analysis of Security Vulnerabilities of Cloud Computing Environment Service Models and Its Main Characteristics," 2015 12th International Conference on Information Technology - New Generations, Las Vegas, NV, 2015, pp. 206-211.

[9] L. Krishnakumar and N. M. Varughese, "High speed classification of vulnerabilities in cloud computing using collaborative network security management," 2013 International Conference on Advanced Computing and Communication Systems, Coimbatore, 2013, pp. 1-6.

[10] Sameena Naaz, Firdoos Ahmad Badroo, “Investigating DHCP and DNS Protocols using Wireshark”, IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 3, Ver. II (May-Jun. 2016), PP 01-08

[11] Sameena Naaz, Faizan Ahmad Siddiqui, “Comparative Study of Cloud Forensics Tools”, Communications on Applied Electronics (CAE) ISSN: 2394-4714, Foundation of Computer Science FCS, New York, USA Volume 5 – No.3, June 2016, page 24-30.