Cloud Specific Issues and Vulnerabilities solutions

Author 1: C.Kishor Kumar Reddy (M.Tech),
Dept. of C.S.E, VCE,
Samshabad, R.R (Dist), A.P, India.
Kishoar23@gmail.com,
Ph: +91 9493024236.

Author 2: SK. Lokesh Naik (Assistant Professor),
Dept. of C.S.E, VCE,
Samshabad, R.R (Dist), A.P, India.
lokessh@yahoo.com,
Ph: +91 9885601370

Author 3:S.K.Prasanth (Associate Professor),
Dept. of C.S.E, VCE,
Samshabad, R.R (Dist), A.P, India.
Sk_p21@yahoo.co.in,
Ph: +91 9908965812.

Author 4: B.Suresh Kumar (M.Tech),
Dept. of C.S.E, VCE,
Samshabad, R.R (Dist), A.P, India.
sureshkumargoud2006@gmail.com,
Ph: +91 9533444094.

Abstract:
The current discourse about cloud computing security issues makes a well-founded assessment of cloud computing's security impact difficult for two primary reasons. First, as is true for many discussions about risk, basic vocabulary such as "risk," "threat," and "vulnerability" are often used as if they were interchangeable, without regard to their respective definitions. Second, not every issue that's raised is really specific to cloud computing. We can achieve an accurate understanding of the security issue "delta" that cloud computing really adds by analyzing how cloud computing influences each risk factor. One important factor concerns vulnerabilities: cloud computing makes certain well-understood vulnerabilities more significant and adds new vulnerabilities. Here, we define four indicators of cloud-specific vulnerabilities, introduce security-specific cloud reference architecture, and provide examples of cloud-specific vulnerabilities for each architectural component. This paper highlights and categorizes many of security issues introduced by the "cloud"; surveys the risks, threats and vulnerabilities, and makes the necessary recommendations that can help promote the benefits and mitigate the risks associated with Cloud Computing.

Index-Terms: *cloud-specific vulnerabilities, risk, threat, delta.*

Vulnerability: An Overview

Vulnerability is a prominent factor of risk ISO 27005 defines risk as "the potential that a given threat will exploit Vulnerability of an asset or group of assets and thereby cause harm to the organization," measuring it in terms of both the likelihood of an event and its con- sequence. The Open Group's risk taxonomy offers a useful overview of risk factors (see Figure 1).

• The frequency with which threat agents try to exploit vulnerability. This frequency is determined by both the agents' motivation (What can they gain with an attack? How much effort does it take? What is the risk for the attackers?) and how much access ("contact") the agents have to the attack targets.
• The difference between the threat agents' attack capabilities and the system's strength to resist the attack

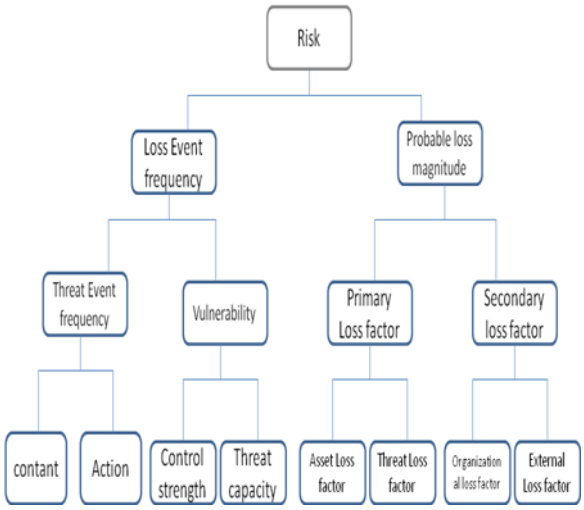

Figure 1: Factors contributing to risk according to the open Group's risk taxonomy.

This second factor brings us toward a useful definition of vulnerability.

Defining Vulnerability:

According to the Open Group's risk taxonomy, Vulnerability is the probability that an asset will be unable to resist the actions of a threat agent. Vulnerability exists when there is a difference between the force being applied by the threat agent, and an object's ability to resist that force. So, vulnerability must always be described in terms of resistance to a certain type of attack.

Vulnerabilities and Cloud Risk

We'll now examine how cloud computing influences the risk factors in Figure 1, starting with the right-hand side of the risk factor tree. From a cloud customer perspective, the right-hand side dealing with probable magnitude of future loss isn't changed at all by cloud computing: the consequences and ultimate cost of, say, a confidentiality breach, is exactly the same regardless of whether the data breach occurred within a cloud or a conventional IT infrastructure. For a cloud service provider, things look somewhat different: because cloud com- puting systems were previously separated on the same infrastructure, a loss event could entail a considerably larger impact. But this fact is easily grasped and incorporated into a risk assessment: no conceptual work for adapting impact analysis to cloud computing seems necessary. So, we must search for changes on Figure 1's left-hand side—the loss event frequency. Cloud computing could change the probability of a harmful event's occurrence. As we show later, cloud computing causes significant changes in the vulnerability factor. Of course, moving to a cloud infrastructure might

change the attackers' access level and motivation, as well as the effort and risk—a fact that must be considered as future work. But, for supporting a cloud-specific risk assessment, it seems most profitable to start by examining the exact nature of cloud-specific vulnerabilities.

Architectural Components of could computing

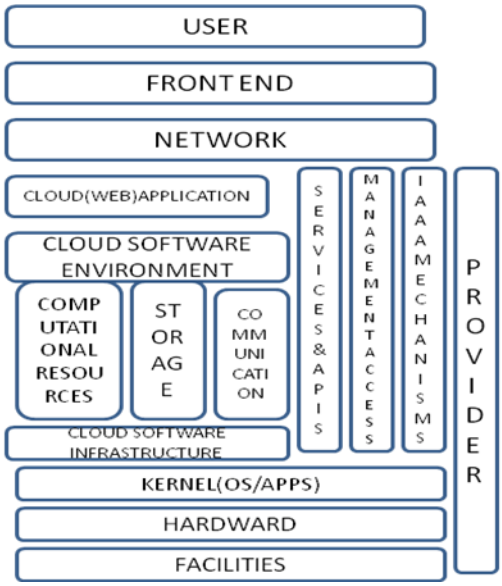

Figure 2: The cloud reference architecture.

Architectural Components and Vulnerabilities:

Cloud service models are commonly divided into SaaS, PaaS, and IaaS, and each model influences the vulnerabilities exhibited by a given cloud infrastructure. It's helpful to add more structure to the service model stacks: Figure 2 shows a cloud reference architecture that makes the most important security-relevant cloud components explicit and provides an abstract overview of cloud computing for security issue analysis.

In addition to the original model, we've identified supporting functions relevant to services in several layers and added them to the model as vertical spans over several horizontal layers.

Our cloud reference architecture has three main parts:

Supporting (IT) infrastructure. These are facilities and services common to any IT service, cloud or otherwise. We include them in the architecture because we want to provide the complete picture; a full treatment of IT security must account for a cloud service's non-cloud-specific components.

Cloud-specific infrastructure. These components constitute the heart of a cloud service; cloud-specific vulnerabilities and corresponding controls are typically mapped to these components.

Cloud service consumer. Again, we include the cloud service customer in the reference architecture because it's relevant to an all-encompassing security treatment.

Using the cloud reference architecture's structure, we can now run through the architecture's components and give examples of each component's cloud-specific vulnerabilities.

CloudSoftwareInfrastructure and Environment:

The *cloud software infrastructure* layer provides an abstraction level for basic IT resources that are offered as services to higher layers: computational resources (usually VMEs), storage, and (network) communication. These services can be used individually, as is typically the case with storage services, but they're often bundled such that servers are delivered with certain network connectivity and (often) access to storage. This bundle, with or without storage, is usually referred to as IaaS.

Computational Resources:

A highly relevant set of computational resource vulnerabilities concerns how virtual machine images are handled: the only feasible way of providing nearly identical server images—thus providing on-demand service for virtual servers—is by cloning template images.

Because cryptography is frequently used to overcome storage-related vulnerabilities, this core technology's vulnerabilities—insecure or obsolete cryptography and poor key management—play a special role for cloud storage.

Communication:

The most prominent example of a cloud communications service is the networking provided for VMEs in an IaaS environment. Because of resource pooling, several customers are likely to share certain network infrastructure components: vulnerabilities of shared network infrastructure components, such as vulnerabilities in a DNS server, Dynamic Host Configuration Protocol, and IP protocol vulnerabilities, might enable network-based cross-tenant attacks in an IaaS infrastructure.

Cloud Web Applications:

A Web application uses browser technology as the front end for user interaction. With the increased uptake of browser-based computing technologies such as JavaScript, Java, Flash, and Silverlight, a Web cloud application falls into two parts:

• An application component operated somewhere in the cloud, and

• A browser component running within the user's browser.

Identity, Authentication, Authorization, and Auditing Mechanisms:

Most vulnerability associated with the IAAA component must be regarded as cloud-specific because they're prevalent in state-of-the-art cloud offerings. Earlier, we gave the example of weak user authentication mechanisms; other examples include

• ***Denial of service by account lockout***. One often-used security control—especially for authentication with username and password—is to lock out accounts that have received several unsuccessful authentication attempts in quick succession. Attackers can use such attempts to launch DoS attacks against a user.

• ***Weak credential-reset mechanisms.*** When cloud computing providers manage user credentials themselves rather than

using federated authentication, they must provide a mechanism for resetting credentials in the case of forgotten or lost credentials. In the past, password-recovery mechanisms have proven particularly weak.

• ***Insufficient or faulty authorization checks.*** State-of-the-art Web application and service cloud offerings are often vulnerable to insufficient or faulty authorization checks that can make unauthorized information or actions available to users. Missing authorization checks, for example, are the root cause of URL-guessing attacks. In such attacks, users modify URLs to display information of other user accounts.

• ***Coarse authorization control.*** Cloud services' management interfaces are particularly prone to offering authorization control models that are too coarse. Thus, standard security measures, such as duty separation, can't be implemented because it's impossible to provide users with only those privileges they strictly require to carry out their work.

• ***Insufficient logging and monitoring possibilities.*** Currently, no standards or mechanisms exist to give cloud customers logging and monitoring facilities within cloud resources. This gives rise to an acute problem: log files record all tenant events and can't easily be pruned for a single tenant. Also, the provider's security monitoring is often hampered by insufficient monitoring capabilities. Until we develop and implement usable logging and monitoring standards and facilities, it's difficult—if not impossible—to implement security controls that require logging and monitoring.

Of all these IAAA vulnerabilities, in the experience of cloud service providers, currently, authentication issues are the primary vulnerability that puts user data in cloud services at risk.

Provider:

Vulnerabilities that are relevant for all cloud computing components typically concern the provider—or rather users inability to control cloud infrastructure as they do their own infrastructure. Among the control challenges are insufficient security audit possibilities, and the fact that certification schemes and security metrics aren't adopted to cloud computing. Further, standard security controls regarding audit, certification, and continuous security monitoring can't be implemented effectively.

Cloud Computing Technologies:

Cloud computing builds heavily on capabilities available through several core technologies:

• ***Web applications and services***. Software as a service (SaaS) and platform as a service (PaaS) are unthinkable without Web application and Web services technologies: SaaS offerings are typically implemented as Web applications, while PaaS offerings provide development and runtime environments for Web applications and services. For infrastructure as a service (IaaS) offerings, administrators typically implement associated services and APIs, such as the management access for customers, using Web application/service technologies.

• ***Virtualization IaaS offerings***. These technologies have virtualization techniques at their very heart; because PaaS and SaaS services are usually built on top of a supporting IaaS infrastructure, the importance of virtualization also extends to these service models. In the future, we expect virtualization to develop from virtualized servers toward computational resources that can be used more readily for executing SaaS services.

• *Cryptography*. Many cloud computing security requirements are solvable only by using cryptographic techniques.

As cloud computing develops, the list of core technologies is likely to expand

. **Essential Characteristics :**

In its description of essential cloud characteristics,2 the US National Institute of Standards and Technology (NIST) captures well what it means to provide IT services from the conveyor belt using economies of scale:

• ***On-demand self-service.*** Users can order and manage services without human interaction with the service provider, using, for example, a Web portal and management interface. Provisioning and de-provisioning of services and associated resources occur automatically at the provider.

• ***Ubiquitous network access***. Cloud services are accessed via the network (usually the Internet), using standard mechanisms and protocols.

• ***Resource pooling***. Computing resources used to provide the cloud service are realized using a homogeneous infrastructure that's shared between all service users.

• *Rapid elasticity*. Resources can be scaled up and down rapidly and elastically.

• *Measured service*. Resource/service usage is constantly metered, supporting optimization of resource usage, usage reporting to the customer, and pay-as-you-go business models.

Core-Technology Vulnerabilities:

Cloud computing's core technologies—Web applications and services, virtualization, and cryptography— have vulnerabilities that are either intrinsic to the technology or prevalent in the technology's state-of-the-art implementations. Three examples of such vulnerabilities are virtual machine escape, session riding and hijacking, and insecure or obsolete cryptography.

First, the possibility that an attacker might successfully escape from a virtualized environment lies in virtualization's very nature. Hence, we must consider this vulnerability as intrinsic to virtualization and highly relevant to cloud computing.

Second, Web application technologies must overcome the problem that, by design, the HTTP protocol is a stateless protocol, whereas Web applications require some notion of session state. Many techniques implement session handling and—as any security professional knowledgeable in Web application security will testify—many session handling implementations are vulnerable to session riding and session hijacking. Whether session riding/hijacking vulnerabilities are intrinsic to Web application technologies or are "only" prevalent in many current implementations is arguable; in any case, such vulnerabilities are certainly relevant for cloud computing.

Finally, crypto analysis advances can render any cryptographic mechanism or algorithm insecure as novel methods of breaking them are discovered. It's even more

common to find crucial flaws in cryptographic algorithm implementations, which can turn strong encryption into weak encryption (or sometimes no encryption at all). Because broad uptake of cloud computing is unthinkable without the use of cryptography to protect data confidentiality and integrity in the cloud, insecure or obsolete cryptography vulnerabilities are highly relevant for cloud computing.

Essential Cloud Characteristic Vulnerabilities:

As we noted earlier, NIST describes five essential cloud characteristics: on-demand self-service, ubiquitous network access, resource pooling, rapid elasticity, and measured service.

Following are examples of vulnerabilities with root causes in one or more of these characteristics:

• ***Unauthorized access to management interface***. The cloud characteristic on-demand self-service requires a management interface that's accessible to cloud service users. Unauthorized access to the management interface is therefore an especially relevant vulnerability for cloud systems: the probability that unauthorized access could occur is much higher than for traditional systems where the management functionality is accessible only to a few administrators.

• ***Internet protocol vulnerabilities***. The cloud characteristic ubiquitous network access means that cloud services are accessed via network using standard protocols. In most cases, this network is the Internet, which must be considered untrusted. Internet protocol vulnerabilities—such as vulnerabilities that allow man-in-the-middle attacks—are therefore relevant for cloud computing.

• ***Data recovery vulnerability.*** The cloud characteristics of pooling and elasticity entail that resources allocated to one user will be reallocated to a different user at a later time. For memory or storage resources, it might therefore be possible to recover data written by a previous user.

• ***Metering and billing evasion.*** The cloud characteristic of measured service means that any cloud service has a metering capability at an abstraction level appropriate to the service type (such as storage, processing, and active user accounts). Metering data is used to optimize service delivery as well as billing. Relevant vulnerabilities include metering and billing data manipulation and billing evasion.

Thus, we can leverage NIST's well-founded definition of cloud computing in reasoning about cloud computing issues.

Defects in Known Security Controls

Vulnerabilities in standard security controls must be considered cloud specific if cloud innovations directly cause the difficulties in implementing the controls. Such vulnerabilities are also known as *control challenges*.

Here, we treat three examples of such control challenges. First, virtualized networks offer insufficient network-based controls. Given the nature of cloud services, the administrative access to IaaS network infrastructure and the ability to tailor network infrastructure are typically limited; hence, standard controls such as IP-based network zoning can't be applied. Also, standard techniques such as network-based vulnerability scanning are usually forbidden by IaaS providers because, for example, friendly scans can't be distinguished from attacker activity. Finally, technologies such as virtualization mean that network traffic occurs on both real and virtual networks, such as when two virtual machine environments (VMEs) hosted on the same server communicate. Such issues constitute a control challenge because tried and tested network-level security controls might not work in a given cloud environment.

The second challenge is in poor key management procedures. As noted in a recent European Network and Information Security Agency study,3 cloud computing infrastructures require management and storage of many different kinds of keys. Because virtual machines don't have a fixed hardware infrastructure and cloud-based content is often geographically distributed, it's more difficult to apply standard controls—such as hardware security module (HSM) storage—to keys on cloud infrastructures.

Finally, security metrics aren't adapted to cloud infrastructures. Currently, there are no standardized cloud-specific security metrics that cloud customers can use to monitor the security status of their cloud resources. Until such standard security metrics are developed and implemented, controls for security assessment, audit, and accountability are more difficult and costly, and might even be impossible to employ.

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

Injection vulnerabilities are exploited by manipulating service or application inputs to interpret and execute parts of them against the programmer's intentions. Examples of injection vulnerabilities include

• SQL injection, in which the input contains SQL code that's erroneously executed in the database back end;

• Command injection, in which the input contains commands that are erroneously executed via the OS; and

• Cross-site scripting, in which the input contains JavaScript code that's erroneously executed by a victim's browser.

In addition, many widely used authentication mechanisms are weak. For example, usernames and passwords for authentication are weak due to

•Insecure user behavior (choosing weak passwords, reusing passwords, and so on), and

• Inherent limitations of one-factor authentication mechanisms.

Also, the authentication mechanisms' implementation might have weaknesses and allow, for example, credential interception and replay. The majority of Web applications in current state-of-the-art cloud services employ usernames and passwords as authentication mechanism.

Security Issues and Solutions in Cloud Computing:

This paper concerns security issues and solutions in cloud computing. Cloud computing is a catch-all phrase that covers virtualized operating systems running on virtual hardware on untold numbers of physical servers. The cloud term has consumed High-Performance Computing (HPC), Grid computing and Utility Computing. The Cloud Security Alliance has adopted the definition developed by NIST; a computing in the cloud is a model exhibiting the following

characteristics, on-demand self-service, Broad Network Access, Resource pooling, and Rapid elasticity and Measured service (*Cloud Security Alliance Guidance Version 2.1*, 2009, p. 15). This is an area that appears to be growing larger and more pervasive as the benefits of cloud architectures become better understood. More organizations start their own cloud projects and more application developers sign on for cloud development as the hyperbole is shaken out and the real parameters of the key technologies are discovered and perfected. The basic areas of cloud vulnerability are similar to the standard issues that surround networking and networked applications. The issues specific to cloud architectures include network control being in in the hands of third parties and a potential for sensitive data to be available to a much larger selection of third-parties, both on the staff of the cloud providers, and among the other clients of the cloud.

The quick adoption of the cloud model is plain in the success of the Amazon Elastic Cloud Computing (EC^2) product, the buy-in from IBM with their backing of the highly concurrent, massively parallel language X-10 (Saraswat, Vijay, 2010) and Microsoft's investment in its Azure cloud (Qiuet al., 2009). Janine Milne reported that eight of ten businesses surveyed in the UK were opting for private cloud initiatives rather than public cloud projects and they stated the issues of concern to be data security in transit, in storage or during processes (Milne, 2010). It is plain that the field is full and the harvest for the IT security profession and IT in general are excellent.

The literature available on cloud security is plentiful, and there is enough higher-quality work to develop a conceptual framework for security issues and solutions

Security Solutions:

There are several groups interested in developing standards and security for clouds and cloud security. The Cloud Security Alliance (CSA) is gathering solution providers, non-profits and individuals to enter into discussion about the current and future best practices for information assurance in the cloud (Cloud Security Alliance (CSA) – security best practices for cloud computing, 2009) The Cloud Standards web site is collecting and coordinating information about cloud-related standards under development by other groups (Clouds Standards, 2010). The Open Web Application Security Project (OWASP) maintains a œ top 10 list of vulnerabilities to cloud-based or Software as a Service deployment models which is updated as the threat landscape changes (OWASP, 2010). The Open Grid Forum publishes documents to containing security and infrastructural specifications and information for grid computing developers and researchers (Open Grid Forum, 2010).

Web Application Solutions

The best security solution for web applications is to develop a development framework that shows and teaches a respect for security. Tsai, W., Jin, Z., & Bai, X. (2009) put forth a four-tier framework for web-based development that though interesting, only implies a security facet in the process (Tsai, Jin, & Bai, 2009, p. 1). Towards best practices in designing for the cloud by Berre, Roman, Landre, Heuvel, SkÃ, Udn, Lennon, & Zeid (2009) is a road map toward cloud-centric development (Berre et al., 2009), and the X10 language is one way to achieve better use of the cloud capabilities of massive parallel processing and concurrency .(Saraswat, Vijay, 2010)

Accessibility Solutions

KrÃngel, C., Toth, T., & Kirda, E. (2002) point out the value of filtering a packet-sniffer output to specific services as an effective way to address security issues shown by anomalous packets directed to specific ports or services (KrÃngel et al., 2002)

(KrÃngel et al., 2002) An often-ignored solution to accessibility vulnerabilities is to shut down unused services, keep patches updated, and reduce permissions and access rights of applications and users.

Authentication Solutions

Halton and Basta (2007) suggest one way to avoid IP spoofing by using encrypted protocols wherever possible. They also suggest avoiding ARP poisoning by requiring root access to change ARP tables; using static, rather than dynamic ARP tables; or at least make sure changes to the ARP tables are logged. (Basta & Halton, 2007, p. 166).

Data Verification, Tampering, Loss and Theft Solutions

Raj, Nathuji, Singh and England (2009) suggest resource isolation to ensure security of data during processing, by isolating the processor caches in virtual machines, and isolating those virtual caches from the Hypervisor cache (Raj, Nathuji, Singh, & England, 2009, p. 80). Hayes points out that there is no way to know if the cloud providers properly deleted a client's purged data, or whether they saved it for some unknown reason (Hayes, 2008, p.(Hayes, 2008, p. 11). Would cloud-providers and clients have custody battles over client data?

Privacy and Control Solutions

Hayes (2008) points out an interesting wrinkle here, allowing a third-party service to take custody of personal documents raises awkward questions about control and ownership: If you move to a competing service provider, can you take a data with you? Could you lose access to a document if you fail to pay a bill? (Hayes, 2008, p. 11). The issues of privacy and control cannot be solved, but merely assured with tight service-level agreements (SLAs) or by keeping the cloud itself private.

Physical access solutions

One simple solution, which Milne (2010) states to be a widely used solution for UK businesses is to simply use in-house private clouds (Milne, 2010). Nurmi, Wolski, Grzegorczyk, Obertelli, Soman, Youseff, & Zagorodnov show a preview of one of the available home-grown clouds in their (2009) presentation. The Eucalyptus Open-Source Cloud-Computing System (Nurmi et al., 2009).

Conclusion:

Cloud computing is in constant development; as the field matures, additional cloud-specific vulnerabilities certainly will emerge, while others will become less of an issue. Using a precise definition of what constitutes a vulnerability from the Open Group's risk taxonomy and the four indicators of cloud-specific vulnerabilities we identify

here offers a precision and clarity level often lacking in current discourse about cloud computing security. Control challenges typically highlight situations in which otherwise successful security controls are ineffective in a cloud setting. Thus, these challenges are of special interest for further cloud computing security research. Indeed, many current efforts—such as the development of security metrics and certification schemes, and the move toward full-featured virtualized network components—directly address control challenges by enabling the use of such tried-and-tested controls for cloud computing.

Acknowledgements:

The authors would like to acknowledge S.K.Prasanth, SK.Lokesh for the useful discussions on this topic and their inputs and feedback while writing this paper.

References:

1. *ISO/IEC 27005:2007 Information Technology—Security Techniques—Information Security Risk Management*, Int'l Org. Standardization, 2007.
2. P. Mell and T. Grance, "Effectively and Securely Using the Cloud Computing Paradigm (v0.25)," presentation, US Nat'l Inst. Standards and Technology, 2009; http://csrc.nist.gov/groups/SNS/cloud-computing.
3. European Network and Information Security Agency (ENISA), *Cloud Computing: Benefits, Risks and Recommendations for Information Security*, Nov. 2009; www.enisa.europa.eu/act/rm/files/deliverables/cloud -computing-risk-assessment/at_download/fullReport.
4. L. Youseff, M. Butrico, and D. Da Silva, "Towards a Unified Ontology of Cloud Computing," *Proc. Grid Computing Environments Workshop* (GCE), IEEE Press, 2008; doi: 10.1109/GCE.2008.4738443.
5. E. Grosse, "Security at Scale," invited talk, ACM Cloud Security Workshop (CCSW), 2010; http://wn.com/2010_Google_Faculty_Summit_Security_at_Scale.
6. Basta, A., & Halton, W. (2007). *Computer Security and Penetration Testing* (1st ed.). Delmar Cengage Learning.
7.http://www.guardian.co.uk/technology/2008/sep/29/cloud.computing.richard.stallman.
8. http://cloud-standards.org/wiki.