Security Problems in Cloud Infrastructure

Amir DJENNA
Department of Computer Science
University of Constantine2
Constantine, ALGERIA
adjenna@gmail.com

Mohamed BATOUCHE
Department of Computer Science
University of Constantine2
Constantine, ALGERIA
batouche@yahoo.fr

***Abstract*—Cloud computing is the emergence of a logical continuation of the computing history, following in the footsteps of mainframes, PCs, Servers, Internet and Data Centers, all those had changed radically the way of our everyday life which adopt the technology. Cloud Computing is able to provide its customers numerous services through Internet. The Virtualization is the secret to the establishment of a Cloud infrastructure. With any technology, it presents both benefits and challenges; the virtualization is not an exception to this rule. In this context, the Cloud infrastructure can be used as a springboard for the generation of new types of attacks. Therefore, security is one of the major concerns for the evolution and migration to the Cloud. In this paper, an overview of security issues related to Cloud infrastructure will be presented, followed by a critical analysis of the various issues that arise in IaaS Cloud and the current attempts to improve security in the Cloud environment.**

Keywords—Cloud Computing; Cloud Security; Virtualization

I. INTRODUCTION

As each technological advance, Cloud Computing brings its own risks in terms of security that should be taken into account before reap the full benefits of the technology. Management issues of compliance and risk, identities and access control, service continuity and endpoints integrity should be considered in the evaluation, implementation and deployment solutions. Therefore, Cloud security is a multifaceted challenge as we talk about infrastructure as a Service (IaaS), Platform as a Service (PaaS) or Software as a Service (SaaS). This means that the Cloud leads IT divisions into unknown sites. It is easy to understand that for company, entrusted their data to an external service provider is not a trivial matter, since then, many unknown parameters are added to the equation. The feeling of loss can be felt quickly. Indeed, the company is no longer controlling at all, or at least in part the hardware and software that allowed it to develop secure solutions, adapted to their needs. Even if the major actors would make further efforts to provide secure services, they have generally enough resources to do so. The fact of not having a management and more control of this aspect can be a major obstacle to the adoption of Cloud services. Systematically, some legitimate questions keep coming back:

- Are our Data secured in the Cloud?
- Where are stored our Data?
- Who will have access to the Data?
- Do we have access to our Data at any time?
- What will become our Data if there are incidents or service disruptions?

In other words, although the cloud offers many potential benefits, services provided can also create new problems, some of them are not yet fully understood. By adopting a Cloud service, companies must for example adapt to the fact that data management is no longer under their direct control. This is particularly true in the case of a "Public Cloud" model, in which a portion of the process is performed on-site and the other part on the Cloud. This requires the implementation of new security process and extended policies to support multiple service providers, and to ensure thorough protection of information.

Moreover, the distributed nature and the full open Cloud infrastructure constitute a point of vulnerability that affects security. We can follow the roots leading to the advent of Cloud, observing the progress of several technologies that contribute to the emergence of this paradigm, (virtualization, Internet, Service-Oriented Architectures, Web 2.0, Distributed Systems, Clusters, Grid Computing, Self-Management Systems, and Data Centers). Indeed, Cloud Computing has complex network architecture. However, it inherits all the security problems of existing systems, as well as new problems related to its open architecture and aspects.

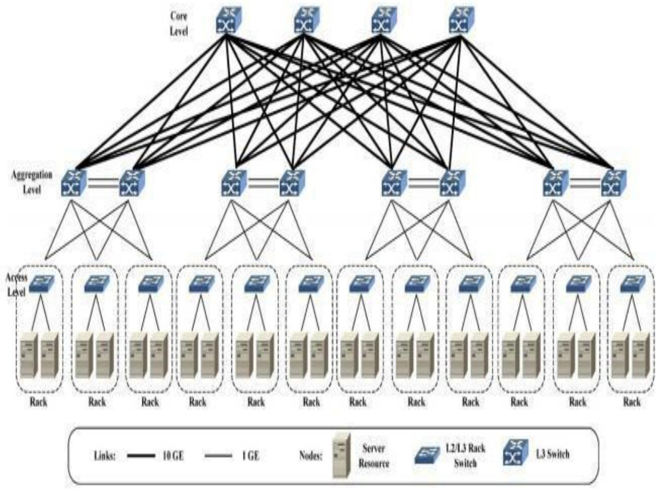
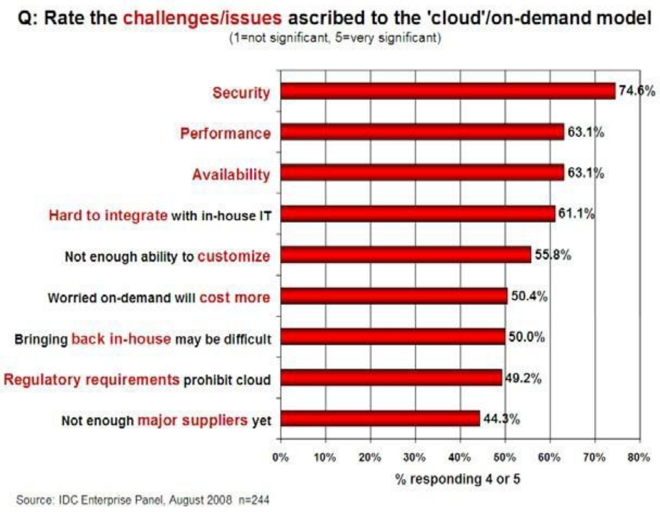


Fig. 1. Generic Architecture for Data Center Networks [15].

978-1-4799-5874-0/14/$31.00 ©2014 IEEE

Cloud Computing is also faced with many security problems, including access to sensitive data, data segregation, confidentiality, authentication and identity management, policies integration of bugs exploits, recovery, accountability, visibility under virtualization, malicious scripts, management console security, auditability and multi-tenancy problem [8] [1]. The public Cloud must be managed with correct caution because it entails the greatest risk of data exposure. This is why the understanding of stakes and security risks in Cloud environment and appropriate solutions is an essential element for the success evolution of this paradigm [10]. A survey was conducted by the International Data Corporation [27] IT Group for the evaluation of Cloud services and issues in 2008. The following figure shows a summary of this survey.


Q: Rate the challenges/issues ascribed to the 'cloud'/on-demand model
(1=not significant, 5=very significant)

Source: IDC Enterprise Panel, August 2008 n=244

Fig. 2. Barriers to Cloud adoption [27].

As can be clearly seen in the figure 2, the security is the most important element and it's regarded as the major concern in Cloud Computing paradigm.

Before exploring and discussing new challenges, it is paramount to define what is Cloud Computing Security?

II. What is Cloud Computing Security ?

In a Cloud environment, the basic idea is that the data and programs can be stored in Data Centers, and accessed at any time from any location via light clients or mobile devices. Certainly, this brings many benefits, including data ubiquity, access flexibility and mobility. However, in fact that the CSP (Cloud Service Provider) necessarily puts data outside the control of the owner, this inevitably creates thorny security problems. Security of Cloud Computing covers all aspects of security specific to such an environment. Many of these aspects are not adequate to the Cloud implementation: Data are vulnerable to several attacks, regardless of location where they are stored. Therefore, computer security in the Cloud encompasses all topics of IT security, including the designing secure architectures, reducing attack surfaces, protection against malwares and application of strong access control, well as physical and logical security of Data Centers. However, there are some Cloud security aspects that seem to be specific only to this field [28] [26] [3].

The National Institute of Standards and Technology [22] asserts that the security, interoperability and portability are the main obstacles for wider adoption of Cloud. A panel of researchers from Berkeley University of California [19] has identified ten barriers to Cloud adoption, which are: services availability, data lock-in, data confidentiality and auditability, data transfer bottlenecks, unpredictable performance, scalable storage and bugs in large distributed systems, rapid expansion, huge sharing and software licenses. Ness [9] combines three main obstacles to Cloud. First, Cloud depends on new security approaches, second, the Cloud can break the traditional networks and third, network automation is essential. However, Leavitt [21] describes six challenges that are: monitoring, performance, bandwidth costs, standards and transparency, latency and reliability, security and privacy.

III. Security threats

The security of computer networks in general and Data Centers in particular has never been an easy task. The nature of an on demand sharing in the Cloud still does a laborious job, selecting an appropriate security policy requires a correct judgment on the threat environment [4].

In this section, our main goal is to fill the gaps related to Cloud security threats.

A. *Abuse and nefarious use of Cloud Computing*

Cloud Security Alliance (CSA) notes that some of Infrastructure-as-a-Service providers (IaaS) do not maintain enough control against hackers, spammers and other people involved in criminal activities that can take advantage of opportunities such as free trials. The CSA suggests strict procedures recording to identity control, increased monitoring for possible credit card fraud, complete introspection of network traffic and monitoring of public blacklists [4].

The results of some researchers [17] [6] [2] corroborate the fact that even if the CSP offer increases monitoring on the overall introspection of network traffic and other actions, the current privacy laws will limit Cloud providers to become the first to know if certain activities are being abused in their infrastructures.

B. *Unsecured Application Programming Interfaces (API's)*

Given that Cloud service providers offer some sort of software interfaces to a customer to manage and interact with their services, relatively a simple user with more convivial interfaces may expose different types of security problems. The proposed solutions to solve the problem rested on the analysis of the API security model, strong authentication of access control with encrypted transmission and understanding of the dependency chain [13]. API functions share numerous vulnerabilities with web application layer. In view of the most Cloud Computing services are likely to be web services, accessible through URL, customers need to use web applications via browsers that share more vulnerability. According to the work done in this context, we can say that there are some advantages of API control in Cloud system, but web applications based on API share above all more vulnerabilities. Despite that the CSA has suggested some measures, there are still some gaps. These are the inability to audit events associated to using APIs and incomplete logs to allow the reconstruction of management activities.

C. *Internal Malicious*

It is common for a provider to hide his own company policies on the recruitment of employees and the level of access that it offers them, however, with a higher level of access, an employee can access to data and confidential services. The CSA suggests the strict management application of the supply chain, indicating the need for human resources in the context of (SLA) Service Level Agreement, transparency in the global information security and compliance management practices, reporting and processes notifications of security violations [13].

If a Cloud provider has no notification policies, it will come time when a customer may not even be aware of a serious security incident. According to the research literature studied until now [13], we may deduce that the most suggestions are mainly about monitoring activities of users and the policy formulation of Cloud provider as zero tolerance policy. Unfortunately, in the foreseeable future, it is likely that there is a tendency of Cloud provider that hides its policy management and put in place insufficient monitoring measures for economic reasons!

D. *Shared technology vulnerabilities*

The nature of on demand sharing in Cloud environment requires the virtualization. However, flaws in virtualization sometimes allow an appropriate access and taking control on the platform, and therefore affect other clients of course [24]. These flaws generate unauthorized access to the installation, configuration and modification of the virtualized environment. Cloud Computing has been designed to share infrastructure profitably, which inherently lack of basic protection and compartmentalization of customers. This class of vulnerability is evident at all levels of the infrastructure stack. The shield of network traffic, data and client applications are very difficult due to hardware limitation. Hackers can hijack privileged user accounts, run other virtual machines and intercept network traffic.

E. *Loss and data leakage*

Cloud customers should ensure that the cost saving methods adopted does not compromise their valuable data. Indeed, there are multiple ways in order to compromise data. One example consist to the removal or alteration of documents without saving, another example might be the absence of measures to restore a large context after a disaster.

The loss of the encryption key may also be crucial. Some of these problems may be specific to Cloud systems in which the data restoration is very complex due to its architecture [13].Other researchers have raised other risks, that relates to data theft and data leakage. The reasons for the data loss can be corrupted storage, insufficiency storage spaces, accidental deletion of partitions, the lack of adequate backup providers, untested backup procedures and strategies, poor policies and inadequate practices for data recovery.

F. *Sessions and services hijacking*

These types of attacks with stolen ID information are generally perpetrated. There are different methods of attack to steal ID information such as phishing, fraud, DoS (Denial of Service), exploring vulnerabilities and account hijacking. In a Cloud environment, if an attacker can access to ID information of a person's session, it can spy on all activities, make transactions and modify data.

In the literature, there are four types of attacks that correspond to this kind of threat. These are: the middle attacks (man-in-the-middle), phishing, spam and DoS attacks. Some researchers have proposed three defensive actions to deal with these types of attacks. The most important points are the following: ensure strong encrypted authentication of system and Cloud users, increased defense against sessions hijacking at the application level and allow one trusted party of system belonging to the company to access and manage the Cloud resources for a given customer.

Currently, the majority of Cloud Computing systems use digital identity of their users to access specific services, this could be a disadvantage particularly for hybrid Cloud.

IV. New security problems related to Cloud Infrastructure

Based on our exploration of the security domain in Cloud Computing, our concerns are the security problems in Cloud infrastructure. In this context, we propose new problems classification related to an IaaS (Infrastructure as a Service) as follows:

A. *Security issues related to virtualization*

Virtualization is considered as the backbone for Cloud Computing infrastructure. In such environment, physical servers are consolidated by multiple instances of VMs (virtual machines) running on physical or virtualized servers. Virtualization is a very important technology which has the ability to hide the physical characteristics and provide the user an abstract environment for access.

Indeed, there are several types of virtualization used: OSs virtualization level (Operating Systems virtualization), APPs virtualization level (Applications virtualization), Storage virtualization level and Network virtualization level.

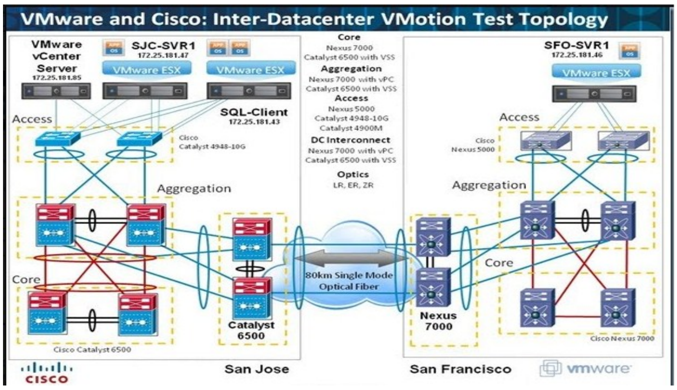


Fig. 3. Network virtualization example [15].

In this type of configuration, an attacker can gain control over all guest OS through compromise of host operating system. Regarding application virtualization level, this latter is enabled on the upper layer of host OS. In this configuration, each virtual machine has a guest OS and related applications. This virtualization also suffers from the same vulnerabilities than those based OS.

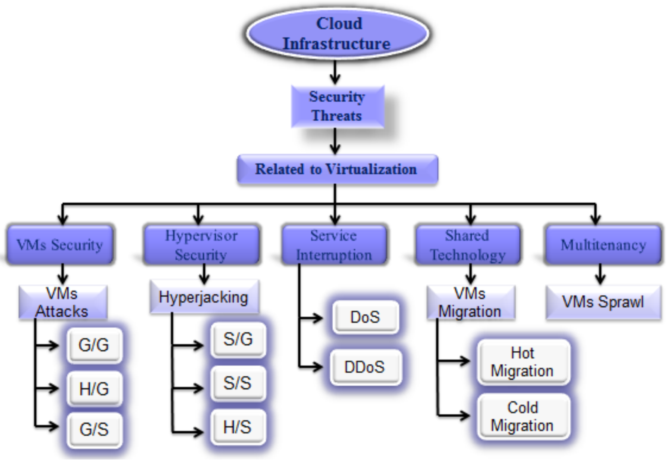
Hypervisor or Virtual Machine Monitor (VMM) is as an integrated code of host operating system. Such code may contain errors and bugs. Furthermore, this code is required during running the host operating system to control multiple guest operating systems. If the hypervisor is compromised then controlled set of guests OSs may also be compromised. Vulnerabilities in hypervisors allow an attacker to lunch VMs attacks.

For example, an incorrect code in Microsoft Hyper-V allowed multiple users authenticated on virtual machines to generate Denial of Service attacks. Networks virtualization, in general involves sharing the same physical infrastructure (bandwidth, routers, switches, servers ... etc.) in favor of several isolated virtual networks. Storage virtualization level is a process that will separate logical and physical representation of storage space.

This type of virtualization uses an application management by logical volume LVM (Logical Volume Manager). Virtualization process can be seen as an extension of classical model of hard drive partitioning.

Cloud providers work seriously on the development of virtualization to maintain a maximum level of isolation between virtual machine instances, including isolation between inter-processes users [20]. So, virtualization is another important technology for Cloud Computing implementation. However, security risks and issues that arise in a virtualized environment produce adverse consequences.

In this context, we propose the classification of security issues related to virtualization in a Cloud infrastructure under different categories as follows: The taxonomy looks like the classification proposed by Nagaraju Kilari [29] on points and differs in other



G: Guest, H: Host, S: Hypervisor. (G/G: Guest to Guest), (H/G: Host to Guest), (S/G: Hypervisor to Guest), (G/S: Guest to Hypervisor), (S/S: Hypervisor to Hypervisor), (H/S: Host to Hypervisor) Attacks

Fig. 4. Attempted attacks related to virtualization.

1) VMs attacks: one of the main benefits of virtualization relies on the technical isolation [18]. This advantage, if not deployed properly, will generate a threat to the environment [14]. Inappropriate access control policy or poor isolation will lead inter-attacks between two virtual machines or between virtual machines and their associated VMM (Virtual Machine Monitor), example : G/G or G/S attacks.

2) Hyper-jacking: system security depends on the quality of the underlying software core that controls the execution of multiple processes [16]. In the case of virtualized architectures, a single hypervisor can host multiple virtual machines and therefore have the respective configuration file for all virtual machines. Security can be a main problem when all these information are stored on a shared storage system. By accessing to this information, virtual machines attacks that are hosted on the same hypervisor becomes an easy task, example: S/G or S/S attacks.

3) Service interruption: this threat may occur when an attacker gains access to the credentials of the organization which can lead to other vulnerable activities such as DoS (Denial of Service) or DDoS (Distributed Denial of Service) attacks, these threats are attempted attacks to make unavailable services and computing resources [25]. An attacker typically uses multiple machines to achieve this goal.

4) Shared technology: This problem arises when IaaS vendors offer their services in sharing infrastructure [12]. These infrastructures were not designed to provide a strong isolation.

5) Multi-tenancy: during the running of multiple virtual machines on the same host, multiple users can share applications and the physical hardware [16]. This can lead to information leakage and other exploitations. For example, in a virtual system, inappropriate policy of VMs management, perform a sprawling virtual machine [18] in the case where the number of virtual machines increase rapidly while most of them are slow or never be standby, which can cause a large waste of resources of the host machine. Virtualization sprawl is a phenomenon that occurs when the number of virtual machines reaches a point where the administrator can no longer manage them effectively. Virtualization sprawl may also be referred to as virtual machine sprawl or virtual server sprawl. Despite the fact that virtual machines are easily created, they have the same licensing, support and security issues that physical machines do.

B. *Security issues related to data geolocation*

In traditional IT outsourcing, customers always know where their data are stored and processed. Generally, customers can visit physically Data Center to inform themselves on the security measures taken by a provider for data protection. Users need to know the exact location of their data and the jurisdiction of their Cloud providers. In the current offer of Cloud Computing, customers do not have the ability to know where the data are stored or processed. Only an approximate decision of Cloud Data Center continental location can be made, for example, AWS (Amazon Web Service) Data Center in Northern Ireland. However, currently, there is no way to prove if the data are not outsourced by a Cloud provider. This affects the fundamental principles of information security: data protection, confidentiality and availability.

C. *Security issues related to storage*

Data stored in the Cloud may be lost for other reasons than attacks caused by hackers. Indeed, all accidental deletion by the Cloud provider services, or extreme case, a disaster such as a fire or an earthquake, can lead to permanent loss of customer data. Unless the provider take an appropriate measures to data restore of its customers [17].

Therefore, Cloud security for storage is paramount, it actually refers to data security on storage mediums specific to a large scale infrastructure, which means the non-volatile backup and fast recovery after disaster. This security must be taken into account by the Cloud provider in the design phase of Cloud storage strategies. It includes not only the dynamic data redundancy, but also the isolation.

D. *Security issues related to confidentiality*

Confidentiality in Cloud systems is a major barrier for users and institutions hosted their data in CSP (Cloud Service Provider). Currently, Cloud Computing system offers services which are essentially public and shareable through networks. Therefore, keeping secret all confidential data of Cloud users, this constitutes a fundamental requirement. Confidentiality in a Cloud system policy is concerned with data protection during transfers, at the time of backup and after processing.

E. *Security issues related to session hijacking*

Sessions and accounts hijacking, generally performed with stolen ID information given rise to a big threat. With stolen ID information, attackers can often access to critical areas of Cloud systems. This access allows them to compromise the confidentiality, integrity and availability of services.

In addition, the instance of hijacked account can become a new base for attacker, where he can take advantage to launch higher attacks. For example, in April 2010, Amazon had a bug type (XSS : Cross-Site Scripting), which allowed attackers to steal the session IDs that are used to grant users access to their accounts after they enter their password. XSS bugs are the most commonly found security vulnerability. A similar flaw was recently exploited to give malicious hackers access to a heavily fortified server operated by the security-conscious Apache Foundation.

F. *Unknown risks*

The fact that the Cloud relies on complex networking architecture, using the internet to provide on demand services to the customers, Cloud Computing inherits certainly all the security issues raised and encountered in previous architectures, besides new problems and unknown risks that will emerge after its widespread adoption and its complete development.

V. Current attempts to improve the security in Cloud Computing

To improve security in the Cloud, institutions, organizations, standards, universities, researchers, specialists and IT security experts gathered dealing rigorously this famous problem by creating several groups and alliances. Common objectives include strengthening and improving security in the Cloud systems through the use of best practices to ensure acceptable protection. The following list describes some alliances and security organizations pioneering in this field.

1) *Cloud Security Alliance (CSA) [4]:* It is a nonprofit organization where the mission is to upgrade using of best practices and providing solid research activities to providing security assurance in Cloud Computing. The CSA has more than 48,000 members around the world.

2) *Open Cloud Consortium (OCC) [23]:* This consortium supports the development of Cloud Computing standards, and the secured framework of interoperability between different Clouds.

3) *Storage Networking Industry Association (SNIA) [24]:* The aim of this organization is to contribute to the storage and management of a large amount of information. This is important for Cloud Computing, including security issues relating to storage.

4) European Network and Information Security Agency (ENISA) [7]: This organization is an excellence center for the European member states and European institutions in network and data security. The center Provides advices, guidance, consulting and acts as a standard for information on best practices. ENISA has recently made recommendations to ensure security in the Cloud and its customers.

5) National Institute of Standards and Technology (NIST) [22]: The aim of the institute is to support the economy by developing technologies and standards with industry. Currently, the main mission is to promote the guidance and technical standards to provide an efficient security of using Cloud technologies. NIST wants to approve Cloud standards security by offering roadmaps for the required standard and catalysts to help industry to develop its own standards.

VI. Researches and Challenges

Although Cloud Computing systems are becoming popular, research in the Cloud is still in its primary stage. Many existing problems were not fully taken into account, while new challenges continue to emerge. Below, some issues and research challenges in the Cloud Computing security field:

- Service provisioning automation;
- Energy management;
- Servers consolidation;
- Virtual machines migration;
- Traffic analysis and management;
- Storage technologies;
- Infrastructure and data Security;
- Big Data.

VII. Conclusion and Perspectives

In this paper, we have presented an overview of the main security threats in Cloud IaaS (Infrastructure as a Service). After, we have talked about security issues related to virtualization, followed by the current attempts to improve Cloud security. Remains to be said that there are new security issues arising from the Cloud. These problems may occur after the maturation and the widespread adoption of Cloud Computing as a technology. As a future work, we plan to propose a Security model to ensure the confidentiality, availability and integrity within a Cloud infrastructure.

References

[1] A. Mladen et al., “Cloud Computing–Issues, Research and Implementation,” International Journal of Computing and Information Technology - CIT 16, 2008.

[2] A. T. Monfared., “Monitoring intrusions and security breaches in highly distributed Cloud environment,” 2010.

[3] Christodorescu et al., “Cloud security is not just virtualization security,” In Proceedings of Workshop on Cloud Computing Security. Chicago USA, ACM 2009.

[4] Cloud Security Alliance (CSA)., “Security Best Practices for Cloud Computing,” 2009. http://www.csa.com

[5] D. Hamilton., “Cloud Computing seen as next wave for technology investors,” Repport 2008.

[6] E. Grosse et al., “Cloud computing roundtable, Security & Privacy,” IEEE 2010.

[7] ENISA, http://www.enisa.europa.eu/

[8] G. M. Jensen et al., “On Technical Security Issues in Cloud Computing,” IEEE International conference on Cloud Computing 2009.

[9] G. Ness., “3 Major barriers to Cloud Computing,” 2009, http://www.infra20.com/post.cfm/3-major-barriers-to-cloudcomputing

[10] H. Takabi et al., “Secure Cloud: Towards a Comprehensive Security Framework for Cloud Computing Environments,” 34th Annual IEEE Computer Software and Applications Conference Workshops, 2010.

[11] IDC., “New IT Cloud services survey 2009: top benefits and challenges,” http://blogs.idc.com/ie/?p=730

[12] J. Amarnath., “Security in Multi-tenancy Cloud,” IEEE 2010.

[13] J. Archer et al., “Top threats to Cloud Computing,”Version 1.0, CSA 2010.

[14] J. Sahoo et al., “Virtualization: A Survey on Concepts, Taxonomy and Associated Security Issues,” IEEE 2010.

[15] J. Venkata et al., “Cloud Computing, Automating the virtualized Data Center,” ISBN : 1-58720-434-7. Cisco Press 2012.

[16] L. Haoyong et al., “Analysis and Research about Cloud Computing Security Protect Policy,” IEEE 2011.

[17] L. Hongjiao et al., “A Deep Understanding of Cloud Computing Security,” NCIS, Springer-Verlag 2012.

[18] L. Shengmei et al., “Virtualization security for Cloud Computing service,” IEEE 2011.

[19] M. Armbrust et al., “A view of Cloud Computing,” ACM Communication 2010.

[20] M. Janbeglou et al., “A Novel Agent-Based Framework in Bridge-Mode Hypervisors of Cloud Security,” 7th International Conference on KMO, AISC 172, Springer-Verlag 2013.

[21] N. Leavitt., “Is Cloud Computing really ready for prime time?” Growth 2009.

[22] NIST,http://www.nist.gov/itl/cloud/

[23] OCC, http://opencloudconsortium.org/

[24] S Nepal et al., “Security, Privacy and Trust in Cloud Systems,” ISBN : 978-3-642-38585-8. Springer-Verlag 2014.

[25] S. Sengupta et al., “Cloud computing Security - Trends and Research Directions,” IEEE 2011.

[26] SNIA, http://www.snia.org/

[27] Source: IDC (International Data Cortporation) Entreprise Panel, Auguest 2008 n=244.

[28] W. M. Halton et al., “The top ten Cloud security practices in next-generation networking,” International Journal of Communication Networks and Distributed Systems, Inderscience 2012.

[29] N. Kilari et al., “A survey on Security threats for Cloud Computing,” International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181. Vol. 1 Issue 7, September – 2012.