Security Related Risks and their Monitoring in Cloud Computing

Sachin Achara
Department of Computer Engineering
Govt. Engineering College, Ajmer

Rakesh Rathi, Ph.D
Department of Computer Engineering
Govt. Engineering College, Ajmer

ABSTRACT
Cloud services is one of the most rapidly growing services over internet, which at the same time also faces serious security challenges. Recently, several cloud-storage service providers started to provide encryption protection to client data in the cloud. However, encryption imposes significant limits on data us .In this paper, we report security related risks and their monitoring in cloud computing. Cloud services data can be accessed only by authorized users. The security of data will be in control of the data owner. This paper shows the security challenges and monitoring and management of these security risks involved in cloud computing services. And a methodology is proposed for performing security risk assessment for cloud computing architectures presenting some of the initial results**.**

General Terms
Security, System malfunction, Evaluation

Keywords
Risk Monitoring, Threats, Risk assessment, Cloud computing.

1. INTRODUCTION
Cloud Computing is evolving as a key technology for sharing resources. Grid Computing, distributed computing, parallel computing and virtualization technologies define the shape of a new era. Traditional distance learning systems lack reusability, portability and interoperability. The most suitable definition of cloud computing was made by National Institute of Standard and Technology (NIST) [1] where cloud is described as a convenient model using efficient computing resources stressing on deployment models. Private cloud is solely operated for an organization by either itself or a third party. General public can use public cloud service and this one is owned by an organization. The term "cloud" originates from the world of telecommunications when providers began using virtual private network (VPN) services for data communications [2]. Cloud computing means a complete combination of computation, software, and data access and storage services.

The main goal of cloud computing is to make a better use of distributed resources, combine them to achieve higher throughput and be able to solve large scale computation problems. Cloud computing deals with virtualization, scalability, interoperability, quality of service and the delivery models of the cloud, namely private, public and hybrid. Community cloud provides an infrastructure that is shared by several organizations, also called federation of clouds. Hybrid cloud is a composition of two, more clouds multi-clouds (community, private, public).While cloud computing is another way of implementing distributed systems; it is unique such that the infrastructure is transparent to users and programmers alike. This allows new ways of selling and sharing resources altogether. Cloud computing offers a new economic model which enables enterprises to shift from the conventional way of developing their own IT departments to outsourcing their needs of software, platform and infrastructure. We envision that this shift would enable hybrid clouds to become a commonplace, realized by private clouds interacting with a rich eco system of various different types of cloud. We are already witnessing research being conducted to enable organizations to automatically externalize services and applications to trustworthy and auditable cloud providers in the hybrid model [4].Each of these deployment scenarios can bring a number of challenges in various aspects of the clouds like risks on the infrastructures, data protection or security. Across these models, security requirements can be associated with interoperability, reliability, portability, maintainability, availability, integrity and confidentiality. These will also differ depending on the point of view of the involved actors; for instance, the end user or cloud consumer may have concerns about their data usage, whereas the service providers would be concerned over malicious intent. Various policies for authentication and software assurances are used to build confidence of customers to use clouds.

This paper presents the security issues faced in cloud computing and analyses it as a risk measure of the providers involved in the cloud – the service provider (SP) and the infrastructure provider (IP). Later section explains the motivation and presents the background for the security issues that need to be addressed in clouds. Next section explains a systematic approach for threat analysis based on standard threats for distributed systems, adopted in cloud computing. The methodology discussed uses the CORAS risk modeling methodology [3] coupled with Information Risk Analysis Methodology (IRAM), using the Threat and Vulnerability Assessment tool (T&VA) performed using data provided by the Information Security Forum (ISF) [5] and public data [6] tailoring for specific cloud computing security risk assessment. This research is exploited into a risk model for security and presented in next section with an evaluation of the suggested methodology.

The results have been based on the implementation work carried out in an EU-projectOPTIMIS [4] presenting analyses across different deployment scenarios. Section 3 &4 presents related security research in cloud computing. Finally Section 5 presents the conclusions of the risk modeling methodology and future research directions to adopt using it.

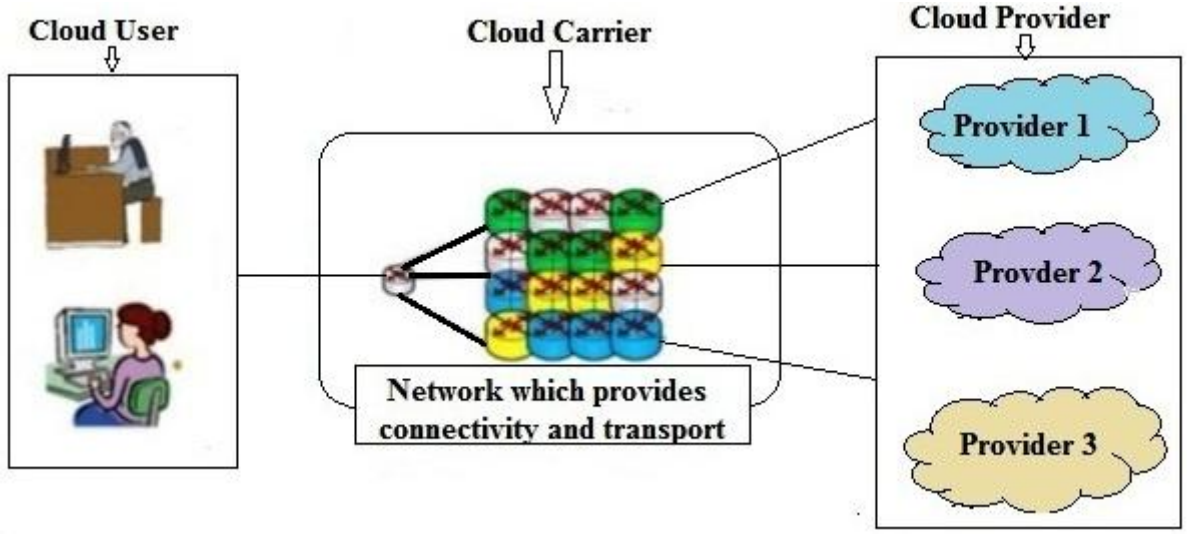

Fig 1: Cloud user and Provider interaction

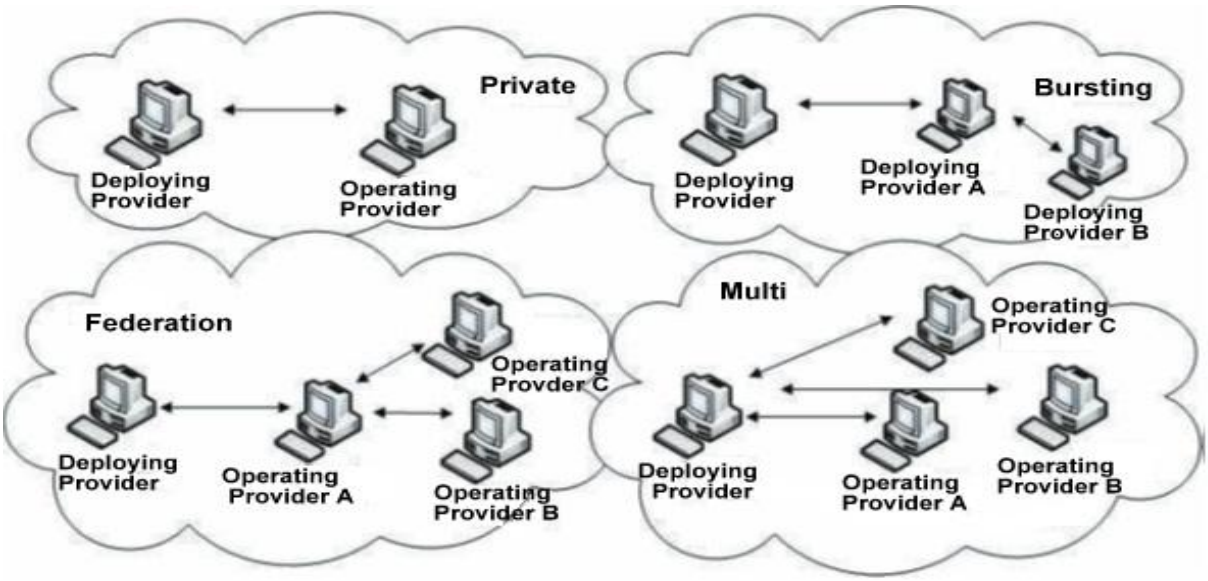

Fig 2: Cloud scenarios

2. SECURITY RISK ANALYSIS

Risk analysis can be considered at various phases of interactions in clouds. Each provider involved in the cloud will have security concerns from their own point of view towards the others in terms of trust, service risks or legal issues. They might consider the risk of working with other providers or may have specific security demands that need to be honored. These assessments also depend on the cloud deployment scenarios - private, public or hybrid. The analysis of security concerns in the context of cloud computing solutions shows that each issue brings different impacts on distinct assets. Aiming to create a security model both for studying security aspects in this context and for supporting decision making, in this section we consider the risks and vulnerabilities previously presented and arrange them in hierarchical categories. In risk analysis step some fair amount of data and their security related constraints is checked and then verified through various tool available in the business environment. So that the risk monitoring gets easy and efficiently mitigate the amount of risk over the cloud services and cloud data storage. There is multiple number of scenario present in the cloud storage ranging from easy to moderate complexity of data storage. Despite the obvious advantages of cloud storage being among others ubiquitous access to data, immediate scalability and the pay-per-usage billing model, there are still concerns which define a widespread adoption. These concerns are mainly devoted to missing or inadequate security and privacy related features, requiring customers to fully trust in the integrity of the cloud provider as well as the provider's security practices. However, besides securing the cloud from within the cloud infrastructure, an alternative possibility is to (transparently) add relevant security and privacy features from the outside

Without affecting the cloud provider's interfaces and inner workings. Within the last few years several approaches to

eliminate security deficiencies within state of the art cloud storage systems have been proposed.

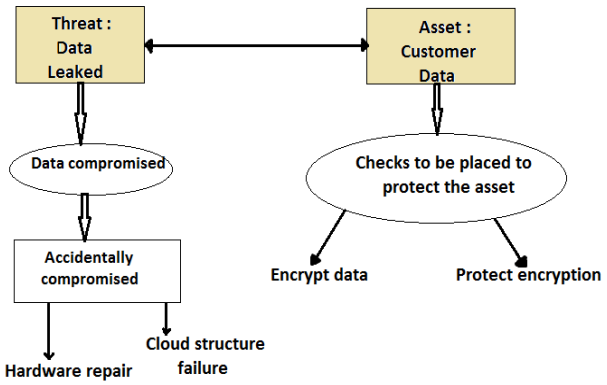

Fig 3: Threat and Asset

3. METHOD FOR RISK MITIGATION

Risk mitigation methodology can be categorized in various phases which includes risk identification, risk assessment, risk management, risk planning, risk resolution, risk monitoring. They might consider the risk of working with other providers or may have specific security demands that need to be honored. These assessments also depend on the cloud deployment scenarios - private, public or hybrid. The following sequences of steps show the risk analysis. Cloud storage is an increasingly popular class of online services for archiving, backup, sharing of data, and synchronization of multiple devices.

It is also envisioned for future primary storage of (enterprise) data. Meanwhile there are lots of services from infrastructure providers, like Amazon S3, Microsoft Windows Azure Blob Storage, Nirvanix SDN, etc. which provide simple (web based) interfaces to their block-oriented storage services. These services are focusing on enterprises and may be used as storage backend for arbitrary applications in order to improve availability due to time and location independent access to enterprise data. This seems absolutely realistic as long as client-side caching and weak consistency models are used to avoid accessing the cloud on every operation. A number of stages have been identified for performing a complete risk assessment on clouds by considering core risk assessment approaches as explained below. The following explained steps are the basic steps for risk monitoring and management of security risks. There is a three layered figure shows the complete assessment and formulation of risk and therefore mitigating the risk involved in a certain services offered by a company. First risk is identified by a certain methodology and then apply assessment phase. This phase takes the output of the identification phase send the calculated output into further phase.

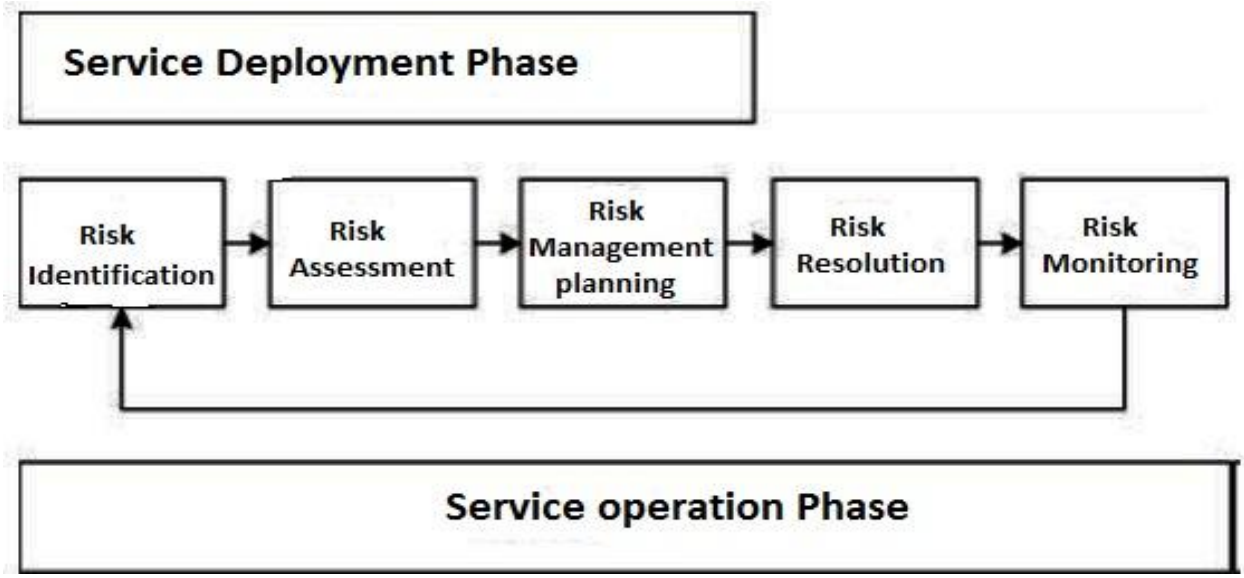

Fig 4: Risk assessment lifecycle during service deployment operation

3.1 Define the level of analysis of a system

An initial high-level analysis of the deployment scenarios helps identifying the actions and assets involved at the different stages in the cloud. This helps identify the vulnerabilities of the cloud environment. Generally security needs to be assessed before deployment of the service to check for security concerns of the other provider or if service level agreements (SLAs) demand certain security aspects to be met. During the operation, security concerns are monitored while the service is executing.

3.2 Identification of threats in each cloud development segment

Threat classification is based on two sources of information, the information security forum [38] for providing data on attacks on IT systems and the frequency of attacks and the public data on attacks on the cloud platforms such as Amazon EC2 and Google Apps Engine. The T&VA[13] provides a standard list of threats relating to IT systems, adopting the threats relevant to the cloud deployment scenarios being investigated. Further threats have been added to introduce the differences between cloud computing and other forms of distributed computing.

Threat modeling is a systemic approach by which threats and vulnerabilities of a system can be identified**.** The information risk analysis methodology is coupled with the threat and vulnerability assessment tool (T&VA) [13] because it contains a threat model for distributed systems and software in general. This model has been adapted to cloud applications using the CORAS risk modeling technique [3]. We have adapted a formal risk methodology, CORAS to further substantiate and filter the threats coming in from the T&VA. The following are the six main attack types.

3.2.1 External attacks

These include all the threats in scenarios involving use of public infrastructures. Examples include problems with Amazon public cloud, using audits such as that of SAS type 2 audit [8] and ISO 27001[9].These threats results in loss of confidentiality and integrity as multiple enterprises.

In attack services are defined in which cloud platforms can be infected with malicious code. An example is Blue pill that can infect hypervisor which can then be used to control the virtual machines (VMs). In Amazon EC2 cloud, it was used to distribute spam which lead to the banning of EC2 related IP addresses by anti-spam groups [11].

3.2.2 Theft

Cloud computing supports multi-tenant architecture in which multiple users can consume the same computing resources allowing possible theft of data. Potential adversaries can use advance data recovery tools to recover data owned by other customers. Google in its security data sheet mentions that only references to the data are deleted rather than data itself. The likelihood of this threat being exploited is low but some companies employ high end physical security measures to secure data [10].

3.2.3 System malfunction

A bug in the cloud software used can have adverse consequences. The likelihood of this threat is high and is classified as one of the most frequent [12].

3.2.4 Service interruption

Natural disasters like earthquakes can lead to the interruption of service. System overload causes excessive system activity leading to the degradation of performance such as the unavailability of services. Although theoretically, cloud computing offers unlimited amount of computing resources, it still depends on how the websites or the cloud services are configured and the availability zone they reside in. Wiki-leaks used EC2 platform to host their website, protecting against DoS attacks by paying a high end package to protect their website. The threat is difficult to recognize as it is challenging to distinguish between a genuine peaks in demand for usage of cloud services with a DoS attack as both create similar patterns of data usage.

3.2.5 Human error

Infrastructure providers like EC2 have designed automated systems with no human intervention for provisioning of cloud services. However, once provisioned human errors cannot be controlled. It is hard to predict human behavior. Therefore we classify this threat as a high threat [5]. Google Apps in its SLAs promise 0.01% for data outages but does not take responsibility for data loss due to human error. The IT policy compliance group suggests that 75% of all data loss is due to user error.

3.2.6 System specific abuse

Data Leakage is defined as an unauthorized transmission of data (or information) from within an organization to an external destination or recipient, in electronic form or by a physical method. This threat becomes more critical in cloud environments as enterprises who are hosting their data on clouds have no control over the provider's infrastructure. In cloud specific environments where data from multiple enterprises may reside in the same data center, it is necessary to build controls for data access. This threat has been classified as medium by Google Docs [12]. Hypervisor level attacks enable an adversary to exploit vulnerability at the virtualization layer that is running underneath the VMs. There are numerous attacks that have been recorded at the hypervisor level ranging from the injection of malware to the hijacking of a VM by a thin undetectable hypervisor, classifying this as a high threat**.**

3.3 High level analysis of each Threat

Each of the threats can be further analyzed in terms of who causes them and the incidents leading up to them, which can then be prioritized depending on this information. This also helps measure the impact of the security risk on the service and the providers. Figure 4 depicts an example of the hacking threat and its related asset and vulnerabilities.

3.4 Evaluation of Risk and Treatment

We can evaluate the risk according to the priorities and their nature. And can be dependent on the assets and the data likelihoods of the threads occurring, the threat items can be plotted into an evaluation matrix to document their occurrences. The likelihood and impact rating is set using the data collected [5, 6]. The impact also denotes the affect the threat will have on the business such as loss of confidentiality can cause loss in trust having the highest impact.

Once evaluated, the risk mitigation strategies can be generated in terms of the actions taken to resolve them. These can be to accept, treat or outsource the risk. For instance, in a situation of multiple log-ins, the system logs can be scanned to detect this. Once observed the system administrator can be made aware to take appropriate action on the user account. Once the risk is identified then we can easily remove from the different parts of the system. The below figure shows that how a hacker can stole customer’s data. The main reason behind the theft and stealing important information is insufficient security policy. If there is insufficient security in the system then a hacker can break the system into different parts for data stolen. This is done by different tricks and technique and software and security application.

Hacking can be done by different way according to network security and extra security assigned by a user. But typically hacking is based on the login detail and breaking the firewall.

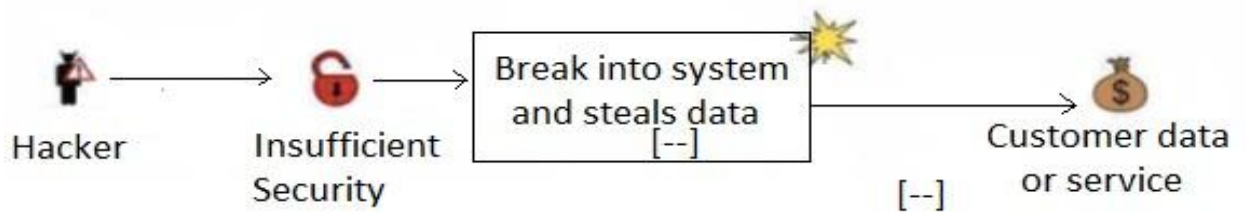

Fig 5: Analysis of threat Hacking

4. IMPLEMENTING THE RISK REMOVAL METHOD

In this section we implement the risk removal strategy. Some specified methods are used to remove the evaluated risks in the cloud system or company provided services. Security risk assessment needs to be done at the service deployment and operation stages of the infrastructure provider's (IP) cloud lifecycle. Risk components involved at deployment and operation stages of the cloud lifecycle. The security of the data that is being transported depends on the availability of a secure cloud carrier connecting the user to the provider. Risk is the potential that something will go wrong [7]. In other words, risks are the possibility of the occurrence of a harmful event. Risk can be formally defined as a function of the likelihood of the adverse event happening and the impact of the adverse event. So we define the risk as

Risk = Probability of the occurrence of adverse event *Impact of the adverse event

Sensitivity analysis is a technique which is used to determine the variation in output when the dependent variable is changed. This technique is commonly used in risk analysis systems to test the robustness of the model. Implement the framework for risk calculation; collect the data from real world routers. This usually raises an ethical debate as scanning remote network device scan sometimes lead to adverse attacks. At the same time, a robust framework for risk assessment is very difficult without collecting data from the real world. Simulation tools cannot replicate the randomness of the real world network traffic. However at the operation stage, along with the calculated security risk for this stage, the risk assessment tool will be interacting with the monitoring database and additional tools like the network and historical database to monitor if certain threats are becoming live. The stages 1-2 are similar to the deployment stage but in addition new stages are added for operation phase. Above depicted figure 4 shows the real modeling of risk at different stages as one is at the deployment stage and another one is operation stage. Infrastructure includes the storage system components having different operational environment. The main purpose of this concept is first define the risk criteria and then follow the strategy according to the nature of the risk and associated factors that affect the cost, security and other issue during the service period.

5. CONCLUSION

Security challenges remain the main barrier to migrate the services and applications into the cloud. In this paper we define a methodology to evaluate the potential risks and then provide a methodology to mitigate the risks. We also have included the different types of risk in the cloud system. From the threat analysis performed; we have shown that the information security principles of integrity, confidentiality and availability are most relevant to the cloud related scenarios. The information risk ratings performed shows the loss of confidentiality is rated as the highest level of risk followed by availability and integrity.

As various cloud providers offer various services, it is important for cloud user to choose the cloud provider which is connected to the most cloud carrier with minimum security risk. In this paper, we proposed a risk assessment frame work to assess the security of the cloud carrier between cloud users and cloud providers. Our framework characterizes the security of the cloud carrier, including confidentiality and integrity.

6. ACKNOWLEDGMENTS

I take this opportunity to express my profound gratitude and deep regard to my friend Mahesh Gochar for his exemplary guidance and constant encouragement throughout the course of this paper. The blessing, help and guidance given by teachers time to time shall carry me a long way in the journey of life on which I am about to embark.

7. REFERENCES

[1] Yashpa lsinh Jadeja & Kirit Modi,(2012) "Cloud Computing-Concepts,ArchitectureandChallenges", International Conference on Computing, Electronics and Electrical Technologies[ICCEET].

[2] Wayne Jansen,Timothy Grance,(2012)IEEE,"Draft NIST SpecialPublicationGuidelinesonSecurity and Privacy in Public Cloud Computing", Computer Security.

[3] Folker den Braber, Gyrd Brændeland, Heidi E. I. Dahl, Iselin Engan, Ida Hogganvik, Mass S. Lund, Bjørnar Solhaug, Ketil Stølen, Fredrik The Coras Model-based method for security risk analysis, SINTEF Oslo September 2006.

[4] A. Juan Ferrer, F. Hernandez, J. Tordsson, E. Elmroth, C. Zsigri, R. Sirvent, J. Guitart, R.M.Badia,K. Djemame, W.Ziegler,T.Dimitrakos, S.K. Nair, G. Kousiouris, K.Konstanteli,T.VarvarigouB.Hudzia, Kipp, S. Wesner, M. Corrales, N. Forgo, T. Sharif, and C.Sheridan, OPTIMIS Holistic Approach to Cloud Service Provisioning, Proceedings of 1st International Conference on Utility Cloud Computing (UCC 2010), Chennai, India, December 2010

[5] Information risk analysis methodology (IRAM), Information Security Forum (ISF), Available at: https://www.securityforum.org/iram

[6] P. Mell and T. Grance, The NIST Definition of Cloud Computing, National Institute of Standards and Technology, October 2009.

[7] P. Saripalli and B. Walters, QUIRC: A Quantitative Impact and Risk assessment framework for Cloud

security, pgs: 280-288, Proceedings of IEEE 3rd International Conference on Cloud Computing, 2010.

[8] SAS 70 Type 2 Audit, SAS 70, Website Available at http://sas70.com/sas70_overview.html

[9] ISO 27002 Standard, The ISO 27000 Directory, Website Available at http://www.27000.org/iso-27002.htm

[10] Sales force Security Data sheet, Availableathttp://www.salesforce.com/assets/pdf/datasheets/security.pdf

[11] B. Krebs, Amazon: Hey Spammers, Get Off My Cloud! The Washington Post, Article Available at http://voices.washingtonpost.com/securityfix/2008/07/amazon_hey_s pammers_get_off_my.html Last Accessed November 2010.

[12] I. Thomson, Google Docs Leaks Private User Data Online, Article, March 2009, Available athttp://www.v3.co.uk/vnunet/news/2238122/google-docs-leaks-privateLast Accessed November 2010.

[13] Information risk analysis methodology IRAM, available at: https://www.securityforum.org/iram#iramtva