Security and Risk Assessment in Cloud Computing

Dr. Alok Singh Chauhan
Department of Information Technology
IMS, Ghaziabad (University Courses Campus), Uttar Pradesh, India
alok.chauhan@imsuc.ac.in

Abstract- As of late, Cloud Computing has been a developing registering model in the IT business. Machines engaged with cloud computing convey benefits in a versatile way. This paper fundamentally means to feature the significant security issues existing in current cloud computing conditions. This paper introduces an investigation about the risk issues associated with cloud computing. I likewise propose a risk examination approach that can be utilized by an imminent cloud administration for breaking down the data security chances before putting his secret information into a cloud computing condition. Finally, the risk assessment will be examined to mitigate the danger of data security. The trust among clients and cloud specialist organizations will fortify through along these lines.

Keywords - Cloud Computing; Data Security; Trust Matrix; Risk Analysis; Risk Assessment.

I. INTRODUCTION

The cloud computing has turned into another vehicle for conveying assets, for example, figuring and capacity to clients on interest.

Cloud computing is a processing model in which virtualized assets are given as an administration over the Internet. Cloud computing is a web based model of registering, where the mutual data, programming and assets are given to PCs and different gadgets upon interest. This empowers the end client to get to the cloud computing assets whenever from any stage, for example, a wireless, versatile processing stage or the work area. The information and the product applications required by the clients are not put away individually PCs; rather they are put away on remote servers which are under the control of different hosts. The clients are not really mindful about which server running on which have is giving the administration. The present real cloud specialist organizations are Microsoft, Hewlett Packard, IBM, Salesforce, Amazon and Google.

Data security has reliably been a noteworthy issue in data innovation. In the cloud computing condition, it turns out to be especially genuine in light of the fact that the information is situated in better places even in the whole globe. Data security and protection assurance are the two fundamental components of client's worries about the cloud innovation. In spite of the fact that numerous procedures on the subjects in cloud computing have been examined in the two scholastics and enterprises, data security and protection assurance are ending up progressively significant for the future improvement of cloud computing innovation in government, industry and business. This examination is to audit data security issues for ensuring information in the cloud and goes for upgrading the data security and dissect dangers for the dependable cloud condition.

II. CLOUD COMPUTING

Cloud is associated in nursing setting of the hardware and software package resources with in the information centers that give various services over the network or the net to satisfy user’s necessaties. The explanation of “cloud computing” from the National Institute of Standards and Technology (NIST) is that cloud computing enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. According to the explanation, cloud computing provides a convenient on-demand network access to a shared pool of configurable computing resources. Resources visit to computing applications, network resources, platforms, software services, virtual servers, and computing infrastructure. A cloud service has 3 distinct characteristics that differentiate it from ancient hosting. It is sold on demand, typically by the minute or the hours; it is elastic-a user can have as much or little of services as they want at any given time; and the services are fully managed by the provider.

Clouds can be divided into:

Public: Available publicly any organization.

Private: Services designed in keeping with cloud computing principles, but accessible only within a private network

Partner: Cloud services offered by a supplier to a restricted and well-defined variety of parties.

Cloud computing could be a model for empowering advantageous, on-request arrange access to a common pool of configurable figuring assets (e.g., systems, servers, stockpiling, applications, and administrations) that can be quickly provisioned and discharged with insignificant administration toil or specialist co-op association. The concept of cloud computing incorporate infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS) and other recent technology trends that have the common on the Internet for satisfying the computing needs of the users. Cloud computing services sometimes give common business applications on-line that are accessed from an Internet browser. They are summarized in visual form in figure 1.

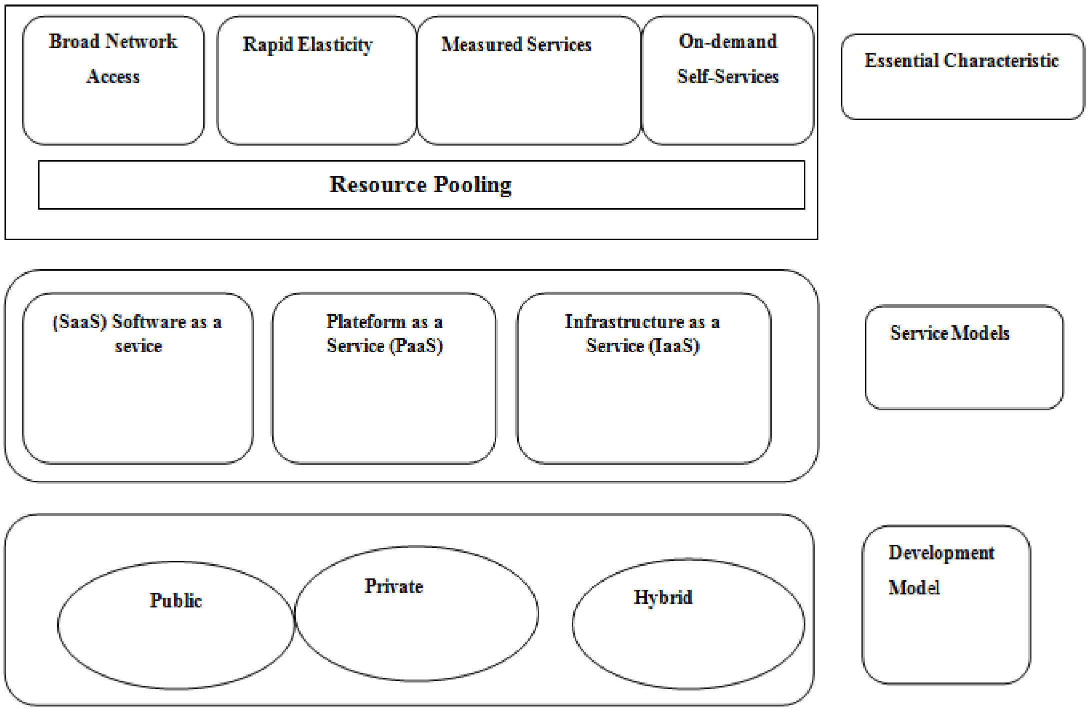

Figure 1: Visual Model of Cloud Computing

III. CLOUD COMPUTING ARCHITECTURE

The frameworks engineering of the product frameworks associated with the conveyance of cloud computing, normally includes numerous cloud parts speaking with one another. The two hugest segments of cloud computing design are known as the front end and the back end. The front end is the part observed by the customer, i.e., the PC client. The back end of the cloud computing design is simply the cloud, involving different PCs, servers and information stockpiling gadgets.

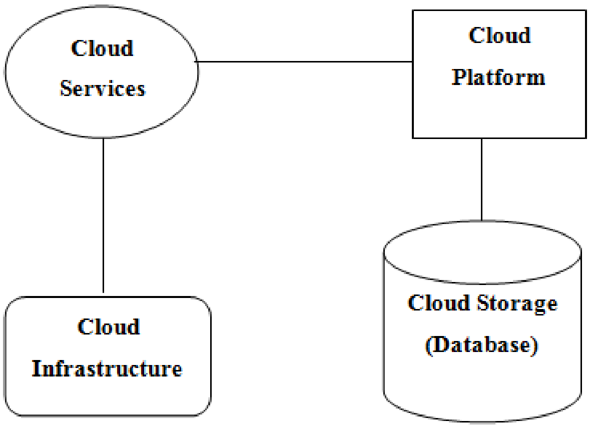

Figure 2: Cloud computing architecture

IV. DATA STORAGE IN CLOUD COMPUTING

Cloud storage is a model of organized PC information stockpiling where information is put away on numerous virtual servers, when all is said in done facilitated by third gatherings, instead of being facilitated on devoted servers. The server farm administrators, out of sight, virtualized the assets as per the prerequisites. In the physical sense, the asset may range over various servers.

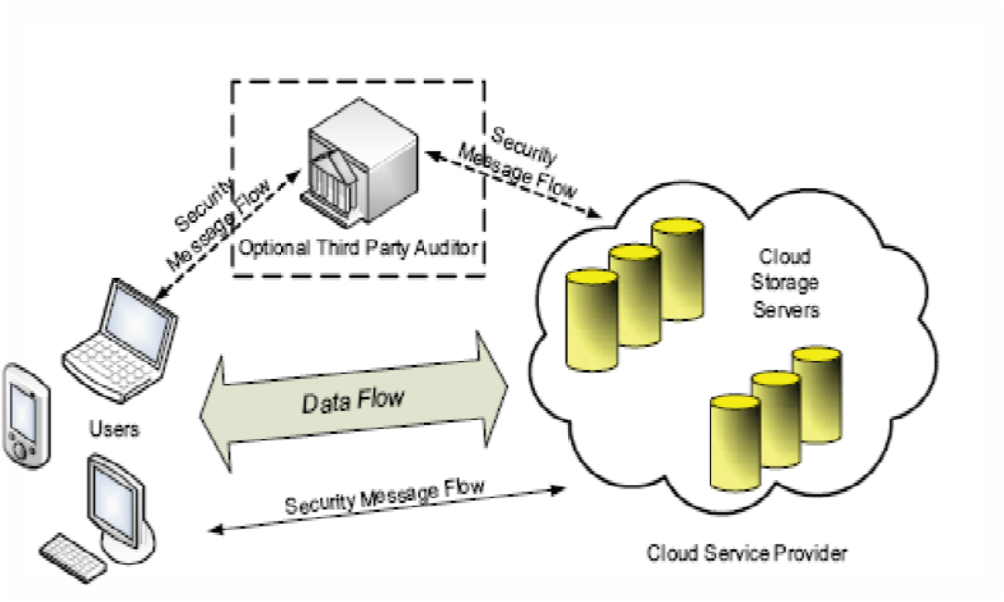

Figure 3: Cloud data storage architecture

V. DATA SECURITY IN CLOUD COMPUTING

Data security has reliably been a noteworthy issue in IT. Data security turns out to be especially genuine in the cloud computing condition, since information are dispersed in various machines and capacity gadgets including servers, PCs, and different cell phones, for example, remote sensor systems and advanced mobile phones. Data security in the cloud computing is more confused than data security in the customary data frameworks. To make the cloud computing be embraced by clients and endeavor, the security worries of clients ought to be corrected first to make cloud condition dependable. The dependable condition is the fundamental essential to win certainty of clients to receive such an innovation. In this way, a standout amongst the most basic worries of cloud computing is data security. By moving information into the cloud an association is giving up care of that information to the cloud supplier. In this way, the association needs to see how its cloud supplier will ensure the information and what security norms and techniques are being connected to help avoid information burglary or a security rupture.

An association can help diminish security dangers related with cloud computing by guaranteeing that the accompanying things are tended to in the agreement with the cloud supplier:

1. Data Segregation and Ownership: The utilization of shared framework can make information mixing together and isolation issues. Therefore, an association may decide not to move touchy or classified data into the cloud. Further, contingent upon the idea of the data that is being put away or handled, the association may need to guarantee that its information can be isolated from all other outsider information as a major aspect of the cloud-administration. The responsibility for information by the association ought to be affirmed in the agreement and the cloud supplier ought to be required to return or crush the information in its ownership toward the finish of the relationship.

2. Location of Data: A cloud supplier's foundation might be situated in various purviews which can result in various lawful issues for the association. In addition to other things, if information is exchanged to another nation it might wind up subject to the security laws of that nation. Hence, the physical area of the servers where the association's information will be put away ought to be indicated in the concurrence with the cloud supplier. The agreement ought to likewise limit the areas where the information might be held (for instance, if the cloud-administration is given from an area in India, the agreement ought to preclude transmission of information outside of India without the association's particular assent).

3. Security Procedures/Standards: The dimension of security and the encryption techniques that will apply to the association's information ought to be recognized. On the off chance that conceivable, a real, explicit and autonomous security standard ought to be distinguished in the agreement.

4. Access Protocols: The particular access security conventions that are being actualized by the cloud supplier ought to be recognized so as to help decrease the danger of unapproved access or information robbery.

5. Audit Rights: The agreement ought to incorporate a privilege for the association to review the cloud supplier's security methods just as the cloud supplier's consistence with the agreement for the most part. The agreement ought to likewise incorporate a privilege for the association (and the association's outside reviewer) to get to the cloud supplier's server farm or premises where the association's information is found.

6. Notification of Security Breaches: The cloud supplier ought to be required to give the association prompt notice of any security/information ruptures with the goal that the association can deal with these occasions as adequately as could be expected under the circumstances.

VI. RISKS ANALYSIS IN CLOUD COMPUTING

The cloud computing specialist co-ops utilize different security systems to guarantee that all the security dangers are completely dealt with. Be that as it may, there are two wide inquiries:

– How to gauge the risk to data security before putting an occupation into the cloud?

– How to guarantee clients that their information and projects are sheltered in supplier's premises?

On the off chance that a cloud administration client can appraise the danger of his data security then he can have a dimension of trust with the specialist co-op. In the event that there is a high risk about the data security, at that point it prompts a diminishing in trust and the other way around.

VII. RISK ASSESSMENT

Risk assessment is the process of identifying the security risks to a system and determining their probability of occurrence, their impact, and the safeguards that would mitigate that impact. The primary goal of risk evaluation is to characterize fitting controls for diminishing or disposing of those dangers. Generally there are 4 steps of risk assessment which are as follow [6]:

1. Risk Identification

This initial step distinguishes every single potential risk to the framework. It permits distinguishing the potential risk sources and builds up a rundown of a danger articulation that is potential danger sources that are relevant to the framework.

2. Vulnerability Identification

In the second step, the objective of defenselessness recognizable proof is to build up a rundown of framework vulnerabilities (blemishes or shortcomings) that could be abused by the potential risk sources.

3. Risk Determination

In the third step, the motivation behind risk assurance is to survey the dimension of risk to the framework.

4. Control Recommendation

In the fourth step, the objective is to reason a few controls that could moderate or take out the distinguished dangers, as suitable to the framework association's activities, are given.

VIII. TRUST MATRIX FOR RISK ASSESSMENT

Albeit no single unit of measure is satisfactory to the meaning of trust, a few ward factors, (for example, data cost), can be utilized to portray it. To fabricate the trust framework, various heuristics can be utilized for choosing the security parameters. In a cloud computing a trust matrix can be calculated with the variables represented along the axes. X axis represents the cost of data. Y axis represents the service provider’s history. Z axis represents the location of data. The trust matrix consists of areas representing the Low Risk/ High Trust Zone and High Risk/ Low Trust Zone. A common cloud computing circumstances is considered with some past statistics from the service providers. Thus the trust has been measured and used for all the future transactions.

High trust zone means the district of high trust. It can indicate the security chance for the present exchanges and furthermore for future exchanges with that specialist organization. So also, Low trust zone connotes the locale of low trust. As a hazard preventive methodology, we likewise characterize here a trust move, which can be taken as a component of a preventive or responsive measure.

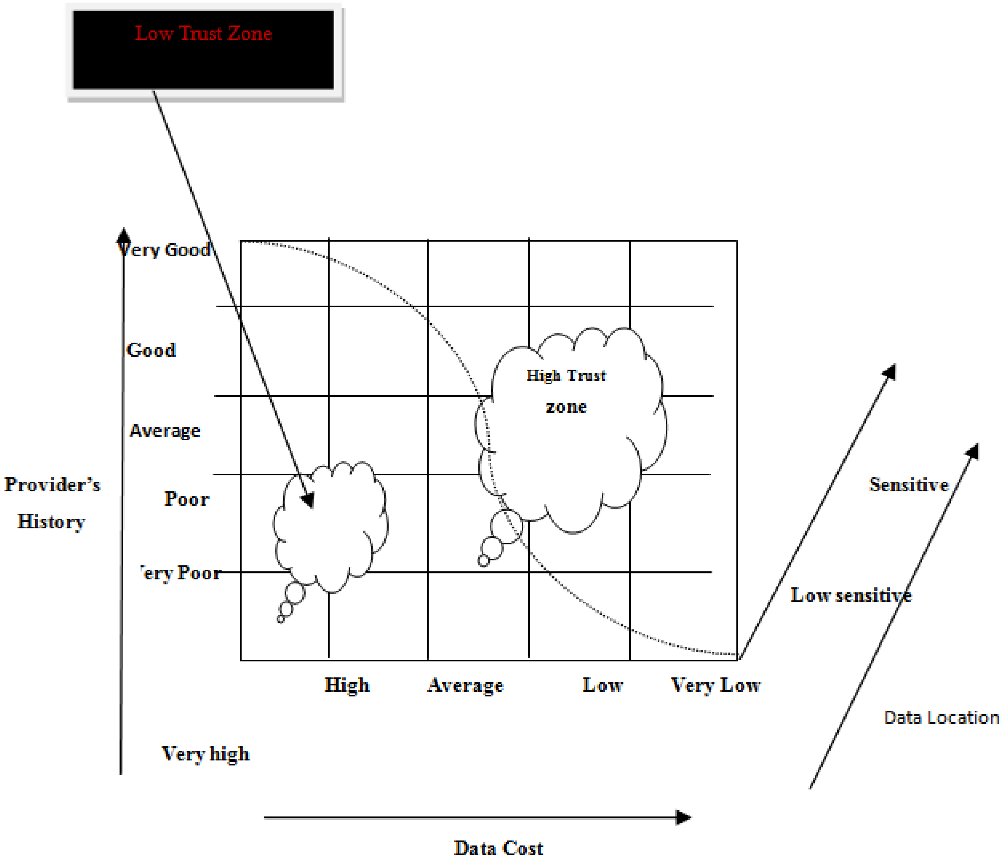

Figure 4: Trust Matrix for Risk Assessment

For example, an added level of authentication and/or verification can be used for the activities which are related to the low trust zone. We have utilized these factors in a typical cloud computing situation, where we have some past measurements about the specialist co-op. The strategy has been utilized to gauge the trust and will be utilized for every future exchange.

IX. RISK ASSESSMENT FRAMEWORK

Risk assessment is one of the essential segments in the association wide risk the executive's procedure (RMP), which is characterized in NIST Special Publication 800-39, Managing Data security Risk: Organization, Mission, and Information System View. RMP incorporates four parts: (a) system chance; (b) assessing risk; (c) Responding to risk; and (d) Monitoring risk. Risk structure is the main advance to assess chance, emphasizing how associations mount dangers or fabricate chance settings. Also, the "settings" depicts the earth of cloud or some other data framework. It is really difficult to set up a viable and high-productivity structure, since the associations cause suitable assessments as well as to recognize as far as possible.

Table 1: Components in RMF

Components	*Introduction/Purpose*
Framework	(1)To establish a risk context (2)To engender a risk management scheme
Evaluating	(1) To identify the threats and vulnerabilities (2) To identify the harm
Responding	To develop alternative countermeasures
Monitoring	To certify that risk response measures are put in to practice effectively

Risk assessment is the optional advance after risk confining, which tends to the risk assessment issues. It comprises of two viewpoints: one is distinguishing the imperilments and vulnerabilities; the other is recognizing the harm. The imperilments incorporate both inward and outer elements. Furthermore, the harm implies the unfriendly occasion when the foes control some helplessness effectively. Risk is a capacity representing the likelihood of an imperilment occasion's occurrence and potential side impact should the occasion happen. As a rule, chance assessment process comprises of four stages: (a) planning for the assessment; (b) leading the assessment; (c) conveying assessment results; and (d) keeping up the assessment.

Based upon the aftereffect of risk assessment, chance reacting parts will react to the risk to take care of the issues and intercede the symptom at the earliest opportunity. Associations will do risk reactions as indicated by techniques and controls appropriately. The two different ways that associations screen risk after some time and assess the risk on progressing establishments are the two key parts of risk checking. Predictable observation can group design related varieties to cloud and the situations of activity. After that whether the risk reaction measures are adequate of not can be determinate. Through this strategy, the risk could be maintained at a nearly low dimension all through.

X. CONCLUSION

In a developing control, similar to cloud computing, security should be examined more frequently.With progression in cloud advances and expanding number of cloud clients, data security measurements will consistently increment. In this paper, I have broken down the data security dangers and vulnerabilities which are available in current cloud computing situations. The clearest finding to rise up out of this examination is that, there is a need of better trust the executives. I have assembled a risk investigation approach dependent on the noticeable security issues. The security examination and risk investigation approach will help specialist organizations to guarantee their clients about the data security. Thus, the methodology can likewise be utilized by cloud administration clients to perform risk examination before putting their basic information in a security delicate cloud.

REFERENCES

[1] R K Balachandra, P V Ramakrishna, Dr. A Rakshit (2009), Cloud Security Issues', IEEE International Conference on Services Computing. (pp. 517-520).

[2] B. Hayes, (2008): Cloud Computing Communications ACM 51. (pp 9–11).

[3] Scott Paquette, Paul T., Jaegar, C. Wilson Susan (2010). Identifying the security risks associated with governmental use of cloud computing, Journal of Government Information Quarterly 27. (pp. 245-253).

[4] Dan Svantesson, Roger Clarke (2010), Privacy and consumer risks in cloud computing. Privacy consumer risks journal, (pp 391-397).

[5] Z. Xiao and Y. Xiao (2013), Security and privacy in cloud computing, IEEE Communications Surveys & Tutorials, vol. 15, no. 2. (pp. 843–859).

[6] N. Kshetri (2013), Privacy and security issues in cloud computing: the role of institutions and institutional evolution, Telecommunications Policy, vol. 37, no. 4-5. (pp. 372–386).

[7] A. Avižienis, J. Laprie, B. Randell, and C. Landwehr (2004), Basic concepts and taxonomy of dependable and secure computing, IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 1. (pp. 11–33).

[8] Z. Mahmood (2011), "Data location and security issues in cloud computing," in Proceedings of the 2nd International Conference on Emerging Intelligent Data and Web Technologies (EIDWT '11), IEEE. (pp. 49–54).

[9] D. Sun, G. Chang, L. Sun, and X. Wang (2011), Surveying and analyzing security, privacy and trust issues in cloud computing environments in Proceedings of the International Conference on Advanced in Control Engineering and Information Science. (pp. 2852–2856).

[10] A. Pandey A., R. M. Tugnayat, and A. K. Tiwari (2013), Data Security Framework for Cloud Computing Networks, International Journal of Computer Engineering & Technology, vol. 4, no. 1. (pp. 178–181).

[11] A. Behl (2011), Emerging security challenges in cloud computing: an insight to cloud security challenges and their mitigation in Proceedings of the World Congress on Information and Communication Technologies. (pp. 217–222).

[12] D. Chen and H. Zhao (2012), Data security and privacy protection issues in cloud computing in Proceeding of the International Conference on Computer Science and Electronics Engineering (ICCSEE '12), vol. 1. (pp. 647–651).

[13] D. H. Rakesh, R. R. Bhavsar, and A. S. Thorve (2012), Data security over cloud, International Journal of Computer Applications, no. 5 (pp. 11–14).

[14] N. Leavitt (2009), Is cloud computing really ready for prime time? Computer, vol. 42, no. 1, (pp. 15–25).

[15] P. Mell and T. Grance (2009), The NIST definition of cloud computing. National Institute of Standards and Technology, vol. 53, no. 6, article 50.

[16] A. Kaur and M. Bhardwaj (2012), Hybrid encryption for cloud database security, Journal of Engineering Science Technology, vol. 2. (pp. 737–741).

[17] C. Delettre, K. Boudaoud, and M. Riveill (2011), Cloud computing, security and data concealment in Proceedings of the 16th IEEE Symposium on Computers and Communications (ISCC '11). (pp. 424–431).

[18] S. Subashini and V. Kavitha (2011), A survey on security issues in service delivery models of cloud, Journal of Network and Computer Applications, vol. 34, no. 1. (pp. 1–11).

[19] C. Cachin and M. Schunter (2011), A cloud you can trust," IEEE Spectrum, vol. 48, no. 12. (pp. 28–51).

[20] Z. Shen, L. Li , F. Yan, and X. Wu (2010), Cloud computing system based on trusted computing platform in Proceedings of the International Conference on Intelligent Computation Technology and Automation (ICICTA '10), vol. 1, IEEE. (pp. 942–945).

[21] R. Neisse, D. Holling, and A. Pretschner (2011), Implementing trust in cloud infrastructures," in Proceedings of the 11th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid '11). (pp. 524–533).

[22] R. Yeluri, E. Castro-Leon, R. R. Harmon, and J. Greene (2012), Building trust and compliance in the cloud for services in Proceedings of the Annual SRII Global Conference (SRII '12), San Jose, Calif, USA. (pp. 379–390).

[23] K. Hwang and D. Li (2010), Trusted cloud computing with secure resources and data coloring, IEEE Internet Computing, vol. 14, no. 5. (pp. 14–22).
[24] www.wikipedia.org: Introduction to cloud computing and Architecture.
[25] ISO 31000:2009, Risk management—Principles and guidelines.
[26] Cloud computing use cases whitepaper (2009).http://www.scribd.com/doc/17929394/Cloud-Computing-Use-Cases-Whitepaper.
[27] SP 800-39, (2010), Managing data security risk organization, mission, and information system view, NIST Special Publications.
[28] SP 800-30 revision 1 (2012), Guide for conducting risk assessments," NIST Special Publications.