A Review on Security Concerns in Cloud Computing and their Solutions

Shakir Khan[1], Mohamed F. AlAjmi[2]

[1]College of Computer and Information Sciences
Al Imam Mohammad Ibn Saud Islamic University, Riyadh, Saudi Arabia
[2]College of Pharmacy, King Saud University, Riyadh, Saudi Arabia,

Summary
Cloud computing is a rising internet-based technology to be likely existing in our surroundings particularly computer science and information technology pastures which call for network computing on big level. Cloud computing is a shared pool of services which is fasting reputation because of its cost efficiency, accessibility and great creation. Along with its various benefits, cloud computing conveys much more demanding situation concerning data solitude, data safeguard, authentic access etc. As a result of these questions, implementation of cloud computing is flattering complicated in today's era. In this research, different security issues concerning data privacy and consistency, key factors which are disturbing the cloud computing, have been concentrated and also proposals on exacting areas have been thrashed out.

Key words:
Cloud computing data protection; encryption; digital signature; security issues

1. Introduction

Cloud computing or cloud-based atmosphere is an overhaul that is internet based service offers the capability of distribution workstation resources in conjunction with other devices on demand. It is a method to facilitate on demand mutual resources. For instance, server, networks storage applications and data center which can accumulate data. That can be created with least attempt. Cloud computing gives the capability to the business and users to maintain their data on private or third-party storage site and these site/data centers may be situated distant from user may be in some other city or country in the world.
National institute of Science and Technology (NIST), provides the cloud computing's explanation as "cloud computing is a mock-up for facilitating ubiquitous, expedient, on-demand network admittance to a collective pool of configurable computing resources (e.g., networks, storage, applications, servers, applications and services) that can be speedily provisioned and unconfined with least management sweat or service provider contact" [1].

Figure 1 demonstrates the distinctiveness of cloud services which helps out others to know and figure out the cloud computing in an enhanced way. These individualities are described below [2]:

1.1 On Demand Self-Service:

It refers to the service which facilitates provisioning of cloud assets to merchants on demand or whenever they are necessary such as network storage, service time without the communication of human.

1.2 Wide Network Access:

Services are easy to get over the networks which are recovered through some homogeneous mechanism which encourages the handling of heterogeneous display place (workstations tablets, laptops, mobile phones).

1.3 Resource groups:

Resources of cloud Provider are collective over server. Customers are allocated dissimilar resources which are either physical or virtual one. Usually, customer have no plan of accurate location the resources given to them apart from the concept level like; state, country or data center.

1.4 Quick flexibility:

Services can be elastically unconstrained and observed, for customers services accessible to them can often materialize as unrestricted which can be balanced in capacity anytime.

1.5 Measured Services:

Cloud systems are so planned that they can observe the resources handling; for example, dispensation, bandwidth and active customer accounts, storage to distribute intelligibility provider as well as end user. At some level of idea, they can optimize the resource practice by observance to verify throughout metering potential.

Manuscript received February 5, 2019
Manuscript revised February 20, 2019

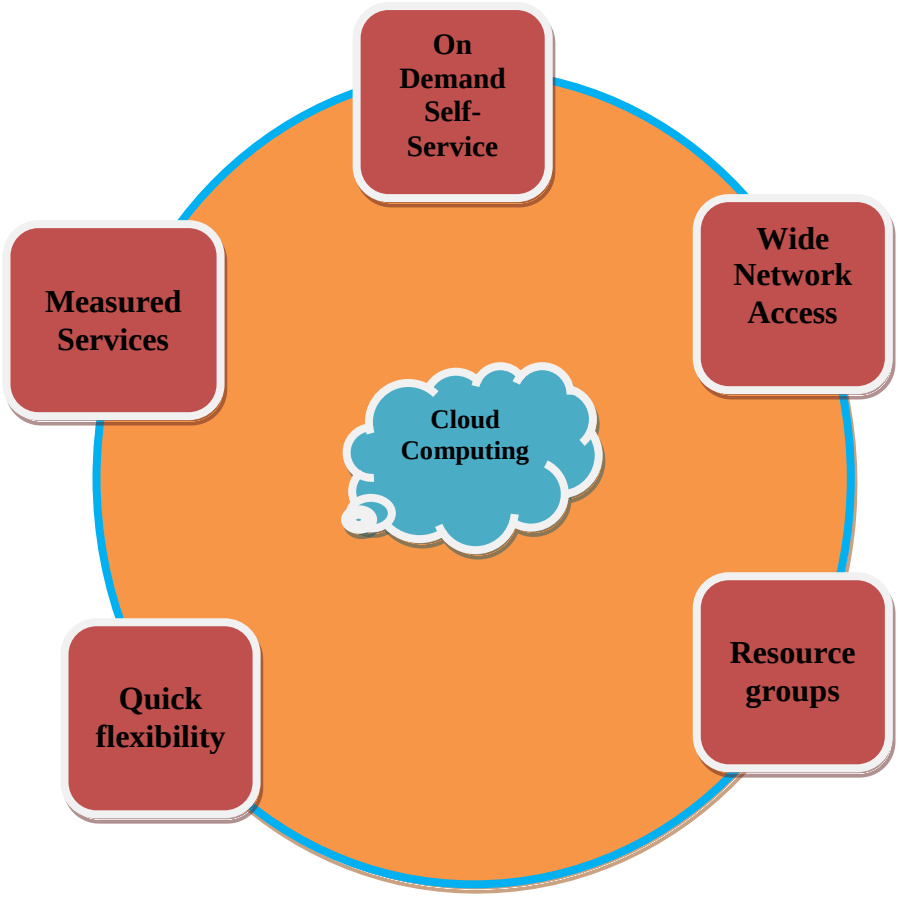

Fig. 1 Cloud Computing distinctiveness

Paper is divided into following sections; section 1 put in the picture about preface of cloud computing, section 2 speaks about the cloud computing representation, section 3 is interrelated work, section 4 is factors touching cloud computing, section 5 feasible fear regarding cloud computing, section 6 is about the solutions to the safety issues and section 7 concludes the research.

2. Cloud Service Models - Architecture

Service models are defined by NIST which includes three categories [3]:

- Infrastructure as a Service (IaaS)
- Software as a Service (SaaS)
- Platform as a Service (PaaS)

Figure 2 depicts the overall three models of cloud computing which are served to the clients according to their requirements. These models are described as under:

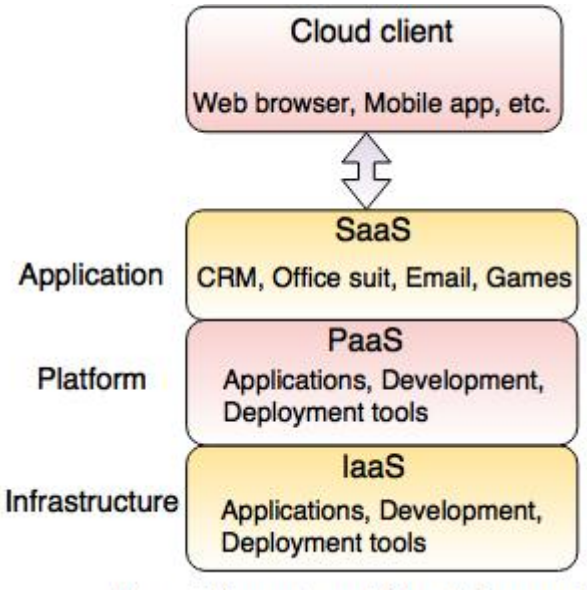

Fig. 2 Different Cloud Service Models

2.1 Infrastructure as a Service (IaaS):

Iaas is all regarding giving the virtual machine, operating system or networks to the end users. Some other computing resources are also sustained in IaaS, where the consumer or customer can run random operating system on virtual machines or any new software. Clients can organize only the operating system or the software which he is operating but he drops his power on the transportation which is given him all these services.

2.2 Software as a Service (SaaS):

In this category of circumstances, consumer is only using the applications which are being given by the vendor and those applications run on the cloud services. Identical application is available by many other customers as well during some ordinary method, for instance via web browser, or email. Again, the consumers or clients have no power over the application or fundamental infrastructures, network server or operating system leading these applications run.

2.3 Platform as a Service (PaaS):

In PaaS, the customer is able to generate their own preferred application via some programming language, associated libraries. These languages or libraries are sustained by the vendor. After generating the consumer preferred application, it is positioned on the server supplied by the vendor. Consumer has also the ability to configure its application or can modify the configuration locations afterward.

The paybacks of cloud computing might be extremely interesting but it has acquired enormous number of risks and safety issues approximating data leakage, data loss, intruders attacks, malicious insiders etc.

3. Related Work

Gartner 2008 recognized seven safety issues that require to be addressed before enterprises think changing to the cloud computing model. They are as follows: (1) privileged consumer access - information sent out from the customer throughout the Internet pretenses a confident degree of risk, because of issues of data ownership; enterprises should use time receiving to be acquainted with their providers and their policy as much as promising before transmission some unimportant applications first to examine the stream, (2) regulatory compliance - customers are responsible for the safety of their solution, as they can decide between supplier that permit to be audited by 3rd party organizations that check levels of security and providers that don't (3) data location – depending on agreements, some customers might never be familiar with what country or what authority their data is located (4) data segregation - encrypted information from multiple companies may be stored on the same hard disk, so a method to break up data should be installed by the supplier. (5) recovery - all supplier should have a tragedy recovery protocol to defend consumer data (6) investigative support - if a customer expects faulty movement from the supplier, it may not have various legal ways follow an inquiry (7) long-term viability - refers to the capability to take back a agreement and all data if the existing provider is bought out by another compact.[16] The Cloud Computing Use Case Discussion Group talks about the dissimilar Use Case circumstances and connected necessities that may continue living in the cloud model. They think use cases from different viewpoints together with consumers, developers and security engineers.[17] ENISA looked into the different safety risks associated to accepting cloud computing along with the pretentious assets, the risks probability, impacts, and vulnerabilities in the cloud computing may guide to such risks.[18] Balachandra et al, 2009 talks about the security SLA's requirements and objectives associated to data positions, isolation and data recovery.[19] Kresimir et al, 2010 talks about high level safety concerns in the cloud computing model such as data integrity, payment and isolation of responsive information.[20] Bernd et al, 2010 talk about the safety vulnerabilities accessible in the cloud platform. The authors grouped the probable vulnerabilities into technology-related, cloud individuality- related, safety controls related.

Ayush Agarwal et al. (2016) emphasize the appearance of cloud computing along with its safety worries like data loss, data breaches, unconfident API's, account hijacking, rejection of service [4]. Prachi Garg et al. (2017) have worked on dissimilar cloud safety features like basic defense which consist of Cross site scripting attacks, Sql booster attacks, Man in the hub attacks [5]. Pradeep Kumar Sharma et al. (2017) safety concerns for cloud like cost model charge model [6], service level concurrences and issue of relocation should be dealt. Naseer Amara et al. (2017) decorated the safety threats, architectural principles and cloud safety attacks with their techniques that can reduce the effects of malicious attacks (mitigation techniques) [7]. Sh. Ajoudanian et al, (2012) said that subsequent four constraints were the mainly critical. (a) Data Confidentiality, used to keep away from leakage of information to any unofficial individual or system [8].

4. Factors Affecting Cloud Security

There are various key features which may influence cloud computing concert because it is bordered by several technologies e.g load balancing, network, concurrency control, virtualization, operating system, database,

memory management etc [9]. Figure 3 shows these anxieties which are talked about as above.

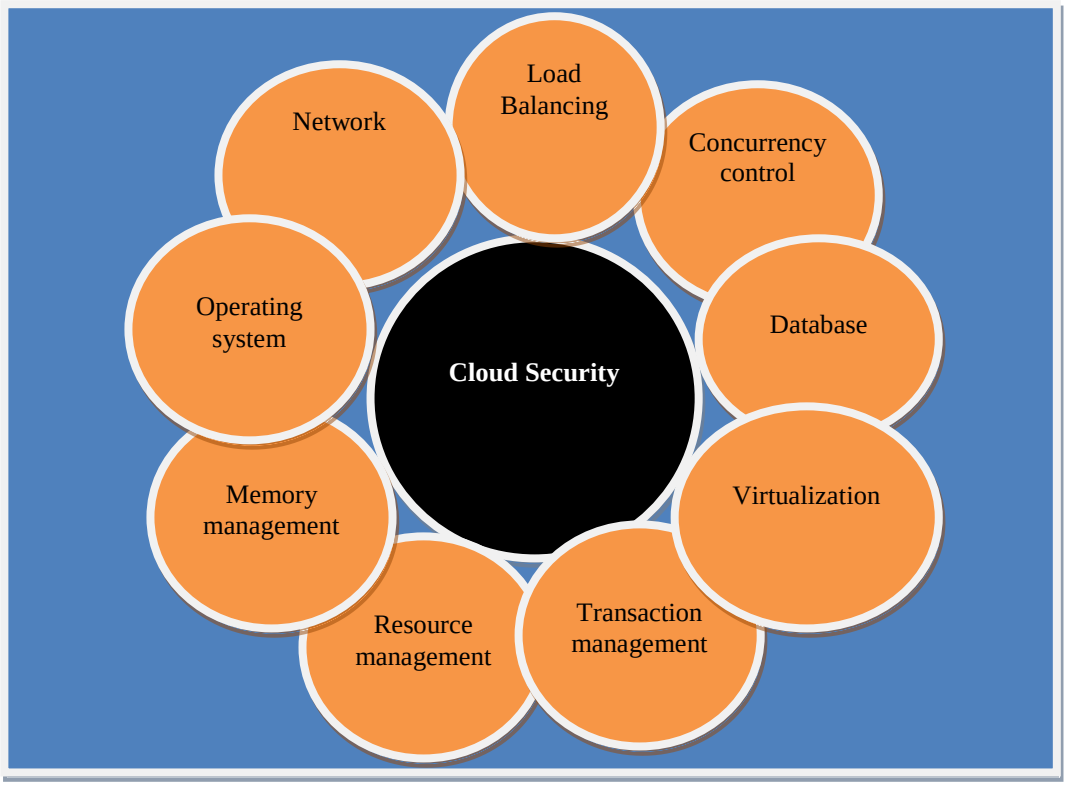

Fig. 3 Factors Affecting Cloud Security

The security factors of these technologies affecting the cloud computing are appropriate e.g. network which connects the cloud computing to the outer world has to be secured. Virtualization concept has to be carried out securely when mapping with the physical systems. Load balancing involves the handling the incoming requests traffic which sometimes overloads the server. Data mining algorithms can be applied to cope with malicious attacks.

5. Possible Threats Concerning Cloud Computing

These days cloud computing is receiving so much reputation that it is in the public eye of today's era. Together with its massive benefits cloud computing is facing a lot security issues which require substantial concentration to decide them for the betterment of this service. Following are the most important concerns as explained below [10];

- **Outsourcing:** in outsourcing the data, customer might acquire lose the control. Some kind of suitable mechanism is required to avoid the cloud service provider (CSPs) to utilize the data in opposition to the approval of their customers.
- **Multi tenancy:** cloud is a shared pool of resources. Protection of data must be in use into account while given that the multi-tenant surroundings.
- **Service Level Agreements:** an obvious agreement between the customer and supplier is required. The main goal of concurrence is to build the belief.
- **Heterogeneity:** special cloud providers have different methods of data protection which leads to incorporation challenges.
- **Server Downtime:** Downtime is the time in which the system begins acting in response to the customer after some service stoppage. Downtime should be kept decreased and power backups must be set up to maintain downtime smallest.
- **Backup:** Data uploaded by the customers, should be backed up in case of any service breakdown. Cloud Seller should point out in SLAs that in case of any tragedy, what should be the tonic or solutions to such troubles. There are very exceptional chances of entire system breakdown like flood etc.

- **Data Redundancy:** Data redundancy is a state in which similar data is being reserved on two different locations. In case of cloud computing, it can be unwritten as to offer copies of equivalent data, systems or equipment to the customers. Cloud vendor should attempt to stay data redundancy least.

6. Solutions to Safety Challenges in Cloud Computing

Safety challenges in cloud computing require to be tackled appropriately. If suitable solutions are not being given acceptance of cloud environment becomes further complex. Apart of acceptance, data transmission and operation have a tendency to become more boring. Figure no.4 sophisticated that data protection and privacy is the most critical factor among all [11].

Figure 4 elaborates the in general crash of safety concerns. The most important security challenge is about data leakage and data isolation because cloud is a shared pool of resources. The subsequently larger challenge is to avoid the data leakage.

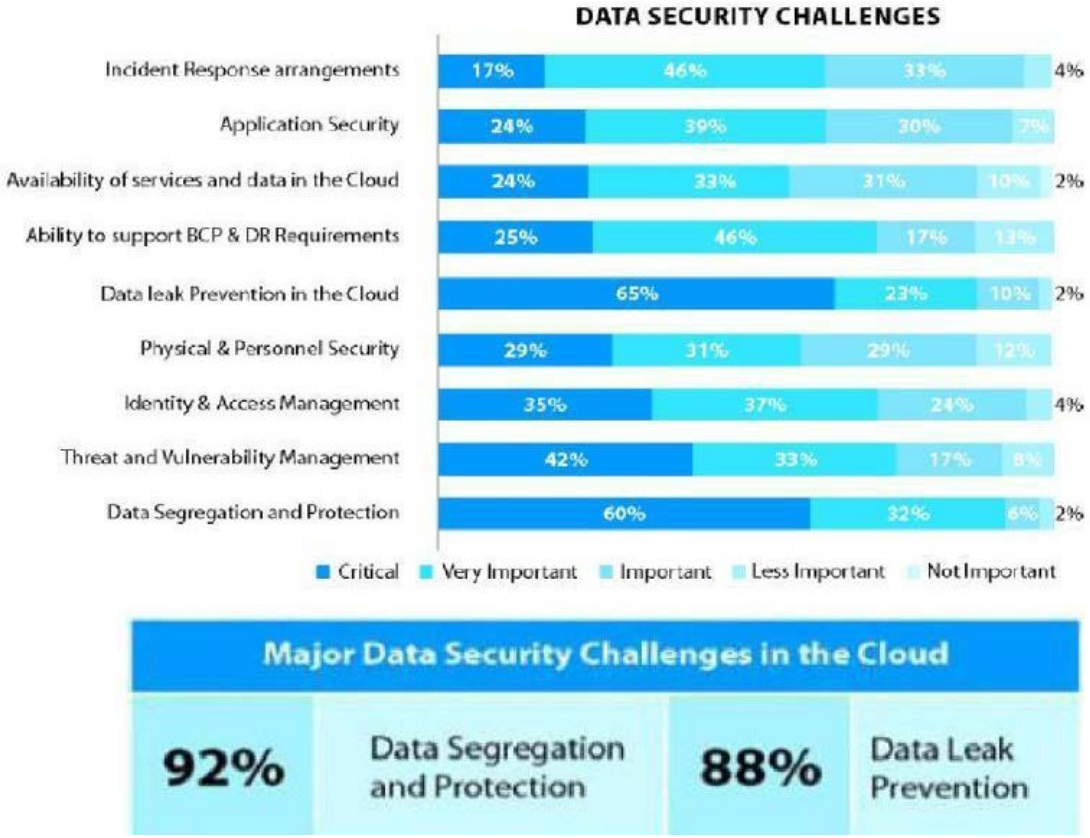

Fig. 4 Data Security Challenges.

To handle with the above challenges, following are several solutions which require to be measured while bearing in mind about cloud computing safety challenges;

7. Data Encryption

Encryption is said to be an enhanced approach concerning data security. Data should be encrypted before transfer it to cloud. Data proprietor can authorize some exacting members to have admittance to that data [11]. The file or data being sent to cloud should be encoded first then before storing it on cloud it should be once more encrypted by the cloud supplier; the procedure is identified as multistage encryption. It has been experiential that grouping of different encryption algorithms supplies better encryption on data. Investigational outcomes show that RSA+IDEA provide the privileged concert of encryption in securing the data [12].

8. Legal Jurisdiction

When it approaches to know and investigate the legal jurisdiction of cloud computing, the very fundamental characteristics of cloud environment confuse the data protection. e.g occurrence of internet, virtualization, vigorously distributed data, multinational elements. Customers usually do not recognize that where their data exist in cloud. For instance, a customer from Saudi Arabia may be utilizing a server set up in US, using an function which has been developed in Japan and storing his critical data at a data center which is actually located in Switzerland [13]. So, the resource billed to the customers should be marked to make sure that data is separated.

9. Distributed Disagreement of Service (DDOS)

Distributed disagreement of service is a category of assault in which assailant generates various automaton machine by tainting the machine above the internet. Then these contaminated machines are utilized to assault on victim. When assaults/traffic from various contaminated machines are aimed at towards one fatality, its resources like CPU, bandwidth and memory begins receiving wormed out and that exacting resource becomes occupied for clients. To handle with this [14] has initiated a level named as vapor level which assembles in between cloud server and consumer. All the requirements completed to server are cleaned throughout this vapor coating and DDOS attacks get reduced.

10. Digital Autograph

Digital autograph is influential tool for locking data in cloud computing. [15] has projected a result using digital signature to protect data in conjunction with Diffie Hellman key switch over with AES encryption algorithm. Diffie Hellman key swap capability marks it ineffective if the key is slashed in broadcast because it is ineffective lacking private key of consumer, which is restricted to legal client only. This three technique mechanism which is projected in this paper formulates it harder to hack security system, therefore, defensive the data that exists in cloud.

11. Conclusion

This paper gave the overview of cloud computing, along with a variety of security characteristics and keys causes which are distressing the cloud security. Cloud customer and supplier might be confident that their cloud is completely protected. Cloud computing is rising in all industry but it suffers from definite issues concerning security and protection which are a difficulty in its acceptance broadly. Solutions to these troubles have been suggested which can be used for healthier concert of cloud service.

References

[1] Cloud Computing Definition. 2011; Available from: https://www.nist.gov/newsevents/news/2011/10/final-version-nist-cloud-computing-definition-published.

[2] Mell, P., Grance, T, The NIST definition of Cloud Computing, version 15 National Institute of Standards and Technology (NIST), Information Technology Laboratory. October, 2009.

[3] What is cloud computing? How it works https://www.ibm.com/cloud/learn/iaas-paas-saas

[4] Agarwal, A., S. Siddharth, and P. Bansal. Evolution of cloud computing and related security concerns in 2016 Symposium on Colossal Data Analysis and Networking (CDAN). 2016.

[5] Garg, P., S. Goel, and A. Sharma. Security techniques for cloud computing environment. in 2017. International Conference on Computing, Communication and Automation (ICCCA) 2017.

[6] Sharma, P.K., et al. Issues and challenges of data security in a cloud computing environment. in 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON). 2017.

[7] Amara, N., H. Zhiqui, and A. Ali. Cloud Computing Security Threats and Attacks with Their Mitigation Techniques. in 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC). 2017.

[8] Ahmadi, S.A.a.M.R., A Novel Data Security Model for Cloud Computing. International Journal of Engineering and Technology, 2012. 4(3)

[9] hangeer Qadiree, M.I.M., Solutions of Cloud Computing Security Issues. International Journal of Computer Science Trends and Technology (IJCST), April 2016. 4(2)

[10] Shahzad, F., State-of-the-art Survey on Cloud Computing Security Challenges, Approaches and Solutions. Procedia Computer Science, 2014. 37: p. 357-362.

[11] Rao, R.V. and K. Selvamani, Data Security Challenges and Its Solutions in Cloud Computing. Procedia Computer Science, 2015. 48: p. 204-209.

[12] Chennam, K.K., L. Muddana, and R.K. Aluvalu. Performance analysis of various encryption algorithms for usage in multistage encryption for securing data in cloud. in 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT). 2017.

[13] Sony, R., K. Sri, and D. Bhukya, Data Protection and Cloud Computing: a Jurisdictional Aspect. 2013. 81-91.

[14] Deepali and K. Bhushan. DDoS attack defense framework for cloud using fog computing. in 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT). 2017.

[15] Rewagad, P. and Y. Pawar. Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing.

in 2013 International Conference on Communication Systems and Network Technologies. 2013.
[16] J. Brodkin. (2008, Jun.). “Gartner: Seven cloud-computing security risks.” Infoworld, Available: <http://www.infoworld.com/d/security-central/gartner-seven-cloudcomputingsecurity-risks-853?page=0,1> [Mar. 13, 2009].
[17] Cloud Computing Use Case Discussion Group. "Cloud Computing UseCases Version 3.0," 2010.
[18] ENISA. (2009, Feb) "Cloud computing: benefits, risks and recommendations for information security." Available: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computingrisk-assessment [Dec. 10, 2012].
[19] R. K. Balachandra, P. V. Ramakrishna and A. Rakshit. “Cloud Security Issues.” In PROC ‘09 IEEE International Conference on Services Computing, 2009, pp 517-520.
[20] P. Kresimir and H. Zeljko "Cloud computing security issues and challenges." In PROC Third International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, 2010, pp. 344-349.