A Study of Security Issues and Cloud Models in Cloud Computing

Deepthi.S, Tulasi.V

***Abstract*— the use of cloud computing is rapidly growing in all over the world. Cloud computing is a general term for anything that involves providing hosted services for internet. It has got many advantages like highly scalable, on-demand, web accessed IT resources with major cost and flexibility. Due to all these reasons cloud computing stands next to internet. Today most companies around the world are using cloud computing as a means to increase the efficiency and to reduce the cost of their IT services. There are many challenges in using cloud computing. The main challenge is security because all essential services are out sourced by a third party. The outsourcing makes it harder to maintain data integrity, privacy and security of data etc. Cloud Computing implies that your customer information is exchanged via the internet to qualify for various web services, and involves a serious danger in terms of security. Data on the Internet are highly susceptible, while safer when stored in Home/Office on storage media. It is possible to corrupt irreparably, sensitive information, caused by the death of servers so security is the one of the major challenge on front of us. This paper introduces a detailed analysis of the cloud computing security issues and challenges focusing on the cloud computing types and the service delivery types.**

***Index Terms*— Cloud computing, Hosted Services, On-demand self-service, Hybrid computing, Software as a Service, Platform as a Service, Infrastructure as a Service.**

I. Introduction

Cloud computing is a distributed architecture designed to centralize a server's resources on a scalable platform in order to offer "on demand" computing power. A true cloud platform will allocate new storage spaces, extra bandwidth and extra processing power, when needed. The purpose of cloud computing systems is to reduce administrative tasks and to offer a dynamic environment for the traditional servers. The use of "cloud" is often extended to refer to any client server application such as an e-mail client or the Apple iTunes.

Once a cloud is established, how its cloud computing services are deployed the primary service models being deployed are commonly known as *Software as a Service***:** In this model an application is hosted as a service to customer who accesses it via the Internet as shown in Fig.1.

Platform as a Service: PaaS services include application design, development, testing, deployment and hosting. In this not only services but server, memory and other platforms can be used and subscriber needs to pay as per terms and conditions.

Infrastructure as a Service **:**The Cloud Infrastructure services delivers the platform virtualization which shows only the desired features and hides the other ones using the environment in which servers, software or network equipment are fully outsourced as the utility computing which will based on the proper utilization of the resources by using the Principle of reusability that includes the virtual private server offerings for the tier data center and many tie attributes which is finally assembled up to form the hundreds of the virtual machines.

Data as a Service (DaaS):

Data as a service offers data in various formats and from various sources could be accessed via services by users on the network, in a transparent, logical or semantic way. Users could, for example, manipulate remote data just like operate on a local disk or access data in a semantic way in the Internet.

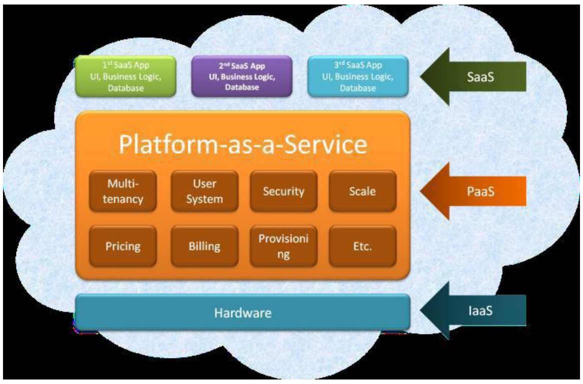


Fig 1.Cloud computing services

cloud computing has grown from being a promising business concept to one of the fast growing segments of the IT industry. But as more and more information on individuals and companies are placed in the cloud, concerns are beginning to grow about just how safe an environment it is.

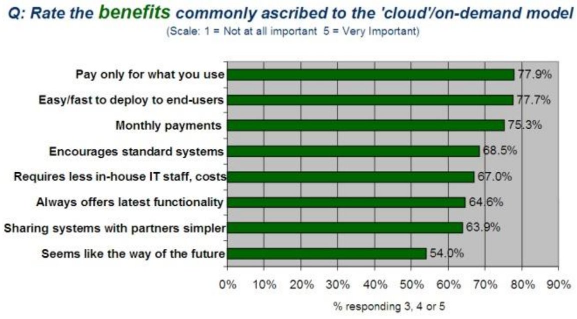
Despite of all the hype surrounding the cloud, customers are still reluctant to deploy their business in the cloud. Security issues in cloud computing has played a major role in slowing down its acceptance, in fact security ranked first as the

Manuscript received Dec, 2013.

Deephi.S, Computer Science and Engineering, Vignan's Lara Institute of Technology and Science. Guntur,A.P,India

Tulasi.V, Computer Science and Engineering, GVP College of Engineering. *Guntur,A.P,India.*

greatest challenge issue of cloud computing as depicted in figure 2.[1]



Source: IDC Enterprise Panel, 3Q09, n = 263

Fig.2 greatest challenge issue of cloud computing

From one point of view, security could improve due to centralization of data and increased security-focused resources. On the other hand concerns persist about loss of control over certain sensitive data, and the lack of security for stored kernels entrusted to cloud providers. If those providers have not done good jobs securing their own environments, the consumers could be in trouble. Measuring the quality of cloud providers' approach to security is difficult because many cloud providers will not expose their infrastructure to customers. This work is a survey more specific to the different security issues and the associated challenges that has emanated in the cloud computing system.

II. CLOUD COMPUTNG SECURITY ISSUES

In the last few years, cloud computing has grown from being a promising business concept to one of the fastest growing segments of the IT industry. Now, recession-hit companies are increasingly realizing that simply by tapping into the cloud they can gain fast access to best-of-breed business applications or drastically boost their infrastructure resources, all at negligible cost. But as more and more information on individuals and companies is placed in the cloud, concerns are beginning to grow about just how safe an environment it is[2].

A. Security

Where is your data more secure, on your local hard driver or on high security servers in the cloud? Some argue that customer data is more secure when managed internally, while others argue that cloud providers have a strong incentive to maintain trust and as such employ a higher level of security. However, in the cloud, your data will be distributed over these individual computers regardless of where your base repository

of data is ultimately stored. Industrious hackers can invade virtually any server, and there are the statistics that show that one-third of breaches result from stolen or lost laptops and other devices and from employees' accidentally exposing data on the Internet, with nearly 16 percent due to insider theft

B. Privacy

Different from the traditional computing model, cloud computing utilizes the virtual computing technology, users' personal data may be scattered in various virtual data center rather than stay in the same physical location, even across the national borders, at this time, data privacy protection will face the controversy of different legal systems. On the other hand, users may leak hidden information when they accessing cloud computing services. Attackers can analyze the critical task depend on the computing task submitted by the users .

C. Reliability

Servers in the cloud have the same problems as your own resident servers. The cloud servers also experience downtimes and slowdowns, what the difference is that users have a higher dependent on cloud service provider (CSP) in the model of cloud computing. There is a big difference in the CSP's service model, once you select a particular CSP, you may be locked-in, thus bring a potential business secure risk.

D. Legal Issues

Regardless of efforts to bring into line the lawful situation, as of 2009, supplier such as Amazon Web Services provide to major markets by developing restricted road and rail network and letting users to choose "availability zones" . On the other hand, worries stick with safety measures and confidentiality from individual all the way through legislative levels.

E. Open Standard

Open standards are critical to the growth of cloud computing. Most cloud providers expose APIs which are typically well-documented but also unique to their implementation and thus not interoperable. Some vendors have adopted others' APIs and there are a number of open standards under development, including the OGF's Open Cloud Computing Interface. The Open Cloud Consortium (OCC) is working to develop consensus on early cloud computing standards and practices.

F. Compliance

Numerous regulations pertain to the storage and use of data require regular reporting and audit trails, cloud providers must enable their customers to comply appropriately with these regulations. Managing Compliance and Security for Cloud Computing, provides insight on how a top-down view of all IT resources within a cloud-based location can deliver a stronger management and enforcement of compliance policies. In addition to the requirements to which customers are subject, the data centres maintained by cloud providers may also be subject to compliance requirements.

G. Freedom

Cloud computing does not allow users to physically possess the storage of the data, leaving the data storage and control in the hands of cloud providers. Customers will contend that this is pretty fundamental and affords them the ability to retain their own copies of data in a form that retains their freedom of choice and protects them against certain issues out of their control whilst realizing the tremendous benefits cloud computing can bring .

H. Long-term Viability

You should be sure that the data you put into the cloud will never become invalid even your cloud computing provider go broke or get acquired and swallowed up by a larger company. "Ask potential providers how you would get your data back and if it would be in a format that you could import into a replacement application

If we consider a business once again need to concentrate on following

A. Reliability: It is essential for all cloud systems – in order to support today's data centre-type applications in a cloud, reliability is considered one of the main features to exploit cloud capabilities. Reliability denotes the capability to ensure constant operation of the system without disruption, i.e. no loss of data, no code reset during execution etc. Reliability is typically achieved through redundant resource utilization. Interestingly, many of the reliability aspects move from hardware to a software-based solution. (Redundancy in the file systems vs. RAID controllers, stateless front end servers vs. UPS, etc.). Notably, there is a strong relationship between availability (see below) and reliability – however, reliability focuses in particular on prevention of loss (of data or execution progress).

B. Quality of Service: It support is a relevant capability that is essential in many use cases where specific requirements have to be met by the outsourced services and / or resources. In business cases, basic QoS metrics like response time, throughput etc. must be guaranteed at least, so as to ensure that the quality guarantees of the cloud user are met. *Reliability* is a particular QoS aspect which forms a specific quality requirement.

C. *Agility and adaptability:* They are essential features of cloud systems that strongly relate to the elastic capabilities. It includes on-time reaction to changes in the amount of requests and size of resources, but also adaptation to changes in the environmental conditions that e.g. require different *types* of resources, different *quality* or different *routes*, etc. Implicitly, agility and adaptability require resources (or at least their management) to be autonomic and have to enable them to provide self-* capabilities.

D.Availability: Availability of services and data is an essential capability of cloud systems and was actually one of the core aspects to give rise to clouds in the first instance. It lies in the ability to introduce redundancy for services and data so failures can be masked transparently. Fault tolerance also requires the ability to introduce new redundancy (e.g. previously failed or fresh nodes) in an online manner non-intrusively (without a significant performance penalty). With increasing concurrent access, availability is particularly achieved through replication of data / services and distributing them across different resources to achieve load-balancing. This can be regarded as the original essence of scalability in cloud systems.

E. Cost reduction: It is one of the first concerns to build up a cloud system that can adapt to changing consumer behavior and reduce cost for infrastructure maintenance and acquisition. *Scalability* and *Pay per Use* are essential aspects of this issue. Notably, setting up a cloud system typically entails additional costs – be it by adapting the business logic to the cloud host specific interfaces or by enhancing the local infrastructure to be “cloud-ready”. See also *return of investment* below.

F. Pay per use: The capability to build up cost according to the actual consumption of resources is a relevant feature of cloud systems. Pay per use strongly relates to quality of service support, where specific requirements to be met by the system and hence to be paid for can be specified. One of the key economic drivers for the current level of interest in cloud computing is the structural change in this domain. By moving from the usual capital upfront investment model to an operational expense, cloud computing promises to enable especially SME’s and entrepreneurs to accelerate the development and adoption of innovative solutions.

G.Improved time to market: It is essential in particular for small to medium enterprises that want to sell their services quickly and easily with little delays caused by acquiring and setting up the infra- structure, in particular in a scope compatible and competitive with larger industries. Larger enterprises need to be able to publish new capabilities with little overhead to remain competitive. Clouds can support this by providing infrastructures, potentially dedicated to specific use cases that take over essential capabilities to support easy provisioning and thus reduce time to market.

H. Return of investment (ROI): ROI is essential for all investors and cannot always be guaranteed – in fact some cloud systems currently fail this aspect. Employing a cloud system must ensure that the cost and effort vested into it is outweighed by its benefits to be commercially viable – this may entail direct (e.g. More customers) and indirect (e.g. Benefits from advertisements) ROI. Outsourcing resources versus increasing the local infrastructure and employing (private) cloud technologies need therefore to be outweighed and critical cut-off points identified.

III. SECURITY ISSUES IN SERVICE MODELS

Following on the cloud deployment models, the next security consideration relates to the various cloud computing service delivery models. The three main cloud service delivery models are:

Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service[4]

(Saas Security Issues in SaaS Following key security element should be carefully considered as an Integral part of the SaaS deployment process:

1. Data Security
2. Network Security
3. Data locality
4. Data integrity
5. Data access
6. Data Segregation
7. Authorization and Authentication
8. Data Confidentiality
9. web Application security
10. Data Breaches
11. Virtualization vulnerability
12. Availability
13. Backup
14. Identity Management on sign-on process

A. Security Issues in PaaS

1. In PaaS, the provider might give some control to the people to build applications on top of the platform. But any security below the application level such as host and network intrusion prevention will still be in the scope of the provider.

2. Applications sufficiently complex to leverage an Enterprise Service Bus (ESB) need to secure the ESB directly, leveraging a protocol such as Web Service (WS) Security (Oracle, 2009).The ability to segment ESBs is not available in PaaS environments. Metrics should be in place to assess the effectiveness of the

Application security programs.

3. Hackers are likely to attack visible code, including but not limited to code running in user context. They are likely to

attack the infrastructure and perform extensive black box testing. The vulnerabilities of cloud are not only associated with the web applications but also vulnerabilities associated with the machine-to-machine Service Oriented Architecture (SOA) applications.

C. Security Issues in IaaS

Taking virtual machines, which contain critical applications and sensitive data, off premise to public and shared cloud environments creates security challenges for organizations that have relied on network perimeter defense as the main method to protect their datacenter.

It may also revoke compliance and breach security policies.OS Security issues also alive in IaaS

D. Security Attacks in Cloud

1. Denial of Service (DoS) attacks: Some security professionals have argued that the cloud is more vulnerable to DoS attacks, because it is shared by many users,which makes DoS attacks much more damaging. Twitter suffered a devastating DoS attack during 2009[5].
2. Side Channel attacks: An attacker could attempt to compromise the cloud by placing a malicious virtual machine in close proximity to a target cloud server and then launching a side channel attack.
3. Authentication attacks: Authentication is a weak point in hosted and virtual services and is frequently targeted. There are many different ways to authenticate users; for example, based on what a person knows, has, or is. The mechanisms used to secure the authentication process and the methods used are a frequent target of attackers.
4. Man-in-the-middle cryptographic attacks: This attack is carried out when an attacker places himself between two users. Anytime attackers can place themselves in the communication's path, there is the possibility that they can intercept and modify communications.

While cloud computing provides compelling benefits, it's highly distributed. A service-based model will also render many of today's existing security architectures obsoletes. Security architects will need to re examine assumptions and derive a security model that can be implemented in a distributed, cloud infrastructure. The traditional "defense-in-depth" approach to security must be expanded beyond on-premise control's to distributed and federated ones that are portable enough to work in a variety of loud architectures.

E Authorization:

In client organizations sometimes unauthorized clients also access the data. So it is important for the organization to provide the authorization for the clients so that any information leakage does not occurs. In addition, clouds introduce a new tier of privileged users: administrators working for the cloud provider. Privileged-user monitoring, including logging activities, becomes an important requirement.

Identity federation and rapid on boarding capabilities mustbe available to coordinate their authentication and authorization with the enterprise back- end or third-party systems. A standards- based, single sign-on capability is required to simplify user logons for both internally hosted applications and the cloud, allowing users to easily and quickly leverage cloud services.

F. Security of data and information:

Data is one of the most important part of the organization. Today all business organizations are concerned about their data security. . Typical concerns include the way in which data is stored and accessed, compliance and audit requirements, and business issues involving the cost of data breaches, notification requirements, and damage to brand value.

It is important that the confidential information is properly secured. One such way used to protect the data is encrypting and decrypting the data.The encryption of mobile media and the ability to securely share those encryption keys between the cloud service provider and consumer is an important and often overlooked need. Because moving large volumes of data quickly and cheaply over the internet is still not practical in many situations, many organizations must send the mobile media such as the archive tape, to the cloud provider. It is important that the data is encrypted and only the cloud service provider and the consumer has the access to encryption keys.

G.Application security:

Cloud providers ensure that applications available as a service via the cloud are secure by implementing testing and acceptance procedures for outsourced or packaged application code. It also requires application security measures be in place in the production environment.

H. Application security

Encompasses measures taken throughout the application's life-cycle to prevent exceptions in the security policy of an application or the underlying system (vulnerabilities) through flaws in the design, development, deployment, upgrade,or maintena nce of the application. Applications only control the use of resources granted to them, and not *which* resources are granted to them. They, in turn, determine the use of these resources by users of the application through application security. In addition, cloud users demand support for image provenance and for licensing and usage control. Suspension and destruction of images must be performed carefully, ensuring that sensitive data contained in those images is not exposed

I. Server and network security:

While SSL helps secure communications between your computer and the cloud, one also need to know the servers you are communicating with are properly secured against hackers and other threats[7].

While it is hard for the average Web user to assess a cloud-based provider's server security, there are services from companies such as McAfee that perform regular security audits on SaaS providers to ensure server security. Ask for evidence of a third party security audit, be it from McAfee or another provider, before entrusting your data to a cloud based provider. In a shared environment, all parties must agree on their responsibilities to review data and perform these reviews on a regular basis.

IV. Cloud computing models:

A. Public clouds:

They are also known as "shared cloud", such services are provided "as a service" over the internet with little or no control over the underlying technology infrastructure. This cloud is appealing to many decision makers as it reduces complexity and long lead times in testing and deploying new products. It is generally cheaper, too. A public cloud does not mean that a user's data is publicly visible; public cloud vendors typically provide an access control mechanism for their users. Public clouds provide an elastic, scalable, cost effective means to deploy solutions.

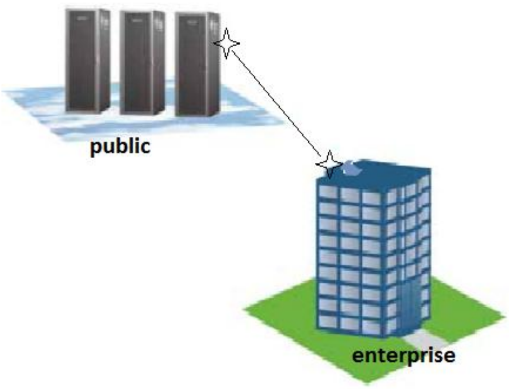


Figure3. Apublic cloud provides services to multiple customers, and is typically deployed at a collocation facility.

Public cloud describes cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned on a fine-grained, self-service basis over the Internet, via web applications/web services, from an off-site third-party provider who shares resources and bills on a fine-grained utility computing basis. It is typically based on a pay-per-use model, similar to a prepaid electricity metering system which is flexible enough to cater for spikes in demand for cloud optimization.[13] Public clouds are less secure than the other cloud models because it places an additional burden of ensuring all applications and data accessed on the public cloud are not subjected to malicious attacks.

B. Private clouds:

It is also called as an internal cloud or enterprise cloud, this also offers activities and functions "as a service" but is deployed over a company intranet or hosted data center. This is private product for a company or an organization offering advanced security and highly available or fault tolerant solutions not possible in a public cloud. Functionalities of private cloud are not directly exposed to the customer, though in some cases services with cloud enhanced features may be offered-this is similar to(cloud) Software as a Service from the customer point of view[8].
Ex: eBay

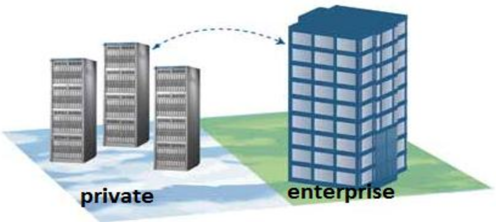


Figure4: Private clouds may be hosted at a collocation facility or in an enterprise datacenter. They may be supported by the company, by a cloud provider, or by a third party such as an outsourcing firm

Private cloud is a new term that some vendors have recently used to describe offerings that emulate cloud computing on private networks. It is set up within an organization's internal enterprise datacenter. In the private cloud, scalable resources and virtual applications provided by the cloud vendor are pooled together and available for cloud users to share and use. It differs from the public cloud in that all the cloud resources and applications are managed by the organization itself, similar to Intranet functionality. Utilization on the private cloud can be much more secure than that of the public cloud because of its specified internal exposure. Only the organization and designated stakeholders may have access to operate on a specific Private cloud.[12]

C. Hybrid clouds:

Though public clouds allow enterprises to outsource parts of their infrastructure to cloud providers, they at the same time would lose control over the resources and the distribution / management of code and data. In some cases, this is not desired by the respective enterprise. *Hybrid clouds* consist of a mixed employment of *private* and *public cloud* infrastructures so as to achieve a maximum of cost reduction through outsourcing whilst maintaining the desired degree of control over e.g. sensitive data by employing local private clouds [17]. There are not many hybrid clouds actually in use today, though initial initiatives such as the one by IBM and Juniper already introduce base technologies for their realization

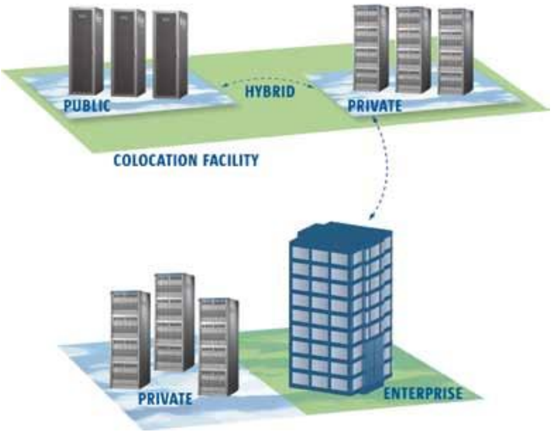


Figure: Hybrid clouds combine both public and private cloud models, and they can be particularly effective when both types of cloud are located in the same facility.

Hybrid cloud is a private cloud linked to one or more external cloud services, centrally managed, provisioned as a single unit, and circumscribed by a secure network [14]. It provides virtual IT solutions through a mix of both public and private clouds. Hybrid Cloud provides more security

V. CLOUD COMPUTING CHALLENGES

The current adoption of cloud computing is associated with numerous challenges because users are still skeptical about its authenticity. Based on a survey conducted by IDC in 2008, the major challenges that prevent Cloud Computing from being adopted are recognized by organizations are as follows:

A. Security: It is clear that the security issue has played the most important role in hindering Cloud computing acceptance. Without doubt, putting your data, running your software on someone else's hard disk using someone else's CPU appears daunting to many. Well-known security issues such as data loss, phishing, botnet (running remotely on a collection of machines)

B. Costing Model: Cloud consumers must consider the tradeoffs amongst computation, communication, and integration. While migrating to the Cloud can significantly reduce the infrastructure cost, it does raise the cost of data communication,

C. Charging Model: The elastic resource pool has made the cost analysis a lot more complicated than regular data centers, which often calculates their cost based on consumptions of static computing.

D. Service Level Agreement (SLA): Although cloud consumers do not have control over the underlying computing resources, they do need to ensure the quality, availability, reliability, and

performance of these resources when consumers have migrated their core business functions onto their entrusted cloud. In other words, it is vital for consumers to obtain guarantees from providers on service delivery. amongst a number of public/private (in-house IT infrastructure)/community clouds. Intuitively, on demand

E. What to migrate: Based on a survey (Sample size = 244) conducted by IDC in 2008, the seven IT systems/applications being migrated to the cloud are: IT Management Applications (26.2%), Collaborative Applications (25.4%), Personal Applications (25%), Business Applications (23.4%),Applications Development and Deployment (16.8%), Server Capacity (15.6%), and Storage Capacity (15.5%). This result reveals that organizations still have security/privacy concerns in moving their data on to the Cloud.

F. Cloud Interoperability Issue: Currently, each cloud offering has its own way on how cloud clients/applications/users interact with the cloud, leading to the "Hazy Cloud" phenomenon. This severely hinders the development of cloud ecosystems by forcing vendor locking, which prohibits the ability of users to choose from alternative vendors/offering simultaneously in order to optimize resources at different levels within an organization.

VI. Conclusion

After discussing the security issues this paper conclude that we should be careful about the security concerns while putting our business on Cloud. There are open research challenges in cloud computing security which demand intensive research. The security model should be probably secure.. In this paper key security considerations and challenges which are currently faced in the Cloud computing are Highlighted. Cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution in the future

Acknowledgment

We take this opportunity to acknowledge those who have been great support and inspiration through the research work.

REFERENCES

[1] F. Gens. (2009, Feb.). “New IDC IT Cloud Services Survey: Top Benefits and Challenges”,*IDC eXchange*, Available: <http://blogs.idc.com/ie/?p=730> [Feb. 18, 2010].

[2] J. Brodkin. (2008, Jun.). “Gartner: Seven cloud-computing security risks.” *InfoWorld*,

[3]. *Cloud Computing Challenges and Related SecurityIssues,*Traian Andrei, http://www.cs.wustl.edu/~jain/cse571-9/ftp/cloud/#introduction

[4]. Software as a Service, Platform as a Service, Infrastructure as a Service − A Review
http://www.ijcsns.com//November.2013-Volume.1-No.3//Article07.pdf

[5] 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 [Jul. 10, 2010].

[6] 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.

[7] 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.

[8] B. Grobauer, T. Walloschek and E. Stöcker, "Understanding Cloud Computing Vulnerabilities," *IEEE Security and Privacy*, vol. 99, 2010.

[9] Cloud Computing Security Issues and Challenges

[10]Cloud Computing Use Case Discussion Group. "Cloud Computing UseCases Version 3.0,"
2010.

[11].M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, *On Technical Security Issues in Cloud Computing*. IEEE, 2009.

[12]. Greg Boss, Padma Malladi, Denis Quan, Linda Legregni, Harold Hall, “Cloud Computing”, tp://www.ibm.com/developerswork/websphere/zones/hipods/library.html, October 2007, pp. 4-4

[13]G. Frankova, *Service Level Agreements: Web Services and Security*, ser. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, vol. 4607.

[14]. “Service Level Agreement and Master Service Agreement”, http://www.softlayer.com/sla.html, accessed on April 05, 2009. [15]. S. Berger, R. Caceres, D. Pendarakis, R. Sailer, E. Valdez, R. Perez, W. Schildhauer, and D. Srinivasan, “Security for the cloud infrastrcture: trusted virtual data center (TVDc).” [Online].
Available: www.kiskeya.net/ramon/work/pubs/ibmjrd09.pdf

[16]. http://www.cloudsecurity.org, accessed on April 10, 2009.

[17] *Hybrid cloud and cluster computing paradigmsfor life science applications*