Security Issues and challenges in Cloud Computing

T.Ambika, Department of Computer Science, Periyar University/ShriSakthikailassh Women's College, Salem,India.

Abstract

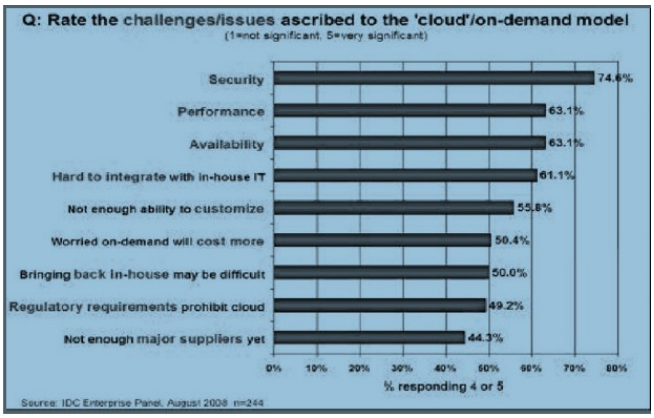
Cloud computing is an Internet-based computing, where shared resources, software and information, are provided to computers and devices on-demand. Since cloud computing uses distributed resources in open environment, thus it is important to provide the security and trust to share the data for developing cloud computing applications. This paper show how we secure the cloud security, privacy and reliability when a third party is processing sensitive data.The introduction of numerous cloud based services and geographically dispersed cloud serviceproviders, sensitive information of different entities are normally stored in remote servers and location with the possibilities of being exposed to unwanted parties in situations where the cloud servers storingthose information are compromised. If security is not robust and consistent, the flexibility and advantagesthat cloud computing has to offer will have little credibility.We have also explained cloud computing strengths/benefits, weaknesses, and applicable areas in information risk management. This paper also cover the advantages and disadvantages in the way of cloud computing. This paper also tackles the important aspect of security concerned challenges which the researchers and authors are facing in the security of cloud computing.

Keywords

Cloud Computing , Infrastructure,IaaS, PaaS, Risk, SaaS, Security, Quality Assurance.

1.INTRODUCTION

The Internet has been represented on network diagrams by a cloud symbol until 2008when a variety of new services started to emerge that permitted computing resources to beaccessed over the Internet termed cloud computing. Cloud computing encompasses activities
such as the use of social networking sites and other forms of interpersonal computing; however,most of the time cloud computing is concerned with accessing online software applications, datastorage and processing power. Cloud computing is a way to increase the capacity or add
capabilities dynamically without investing in new infrastructure, training new personnel, orlicensing new software. It extends Information Technology's (IT) existing capabilities. In the lastfew years, cloud computing has grown from being a promising business concept to one of the fastgrowing segments of the IT industry. But as more and more information on individuals andcompanies are placed in the cloud, concerns are beginning to grow about just how safe anenvironment 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 inslowing down its acceptance, in fact security ranked first as the greatest challenge issue of cloudcomputing as depicted in figure1.



The following section highlights a brief review of literature on securityissues in cloud computing and the remaining sections are organized as follows. wediscusses security issues in cloud computing laying emphasis on SaaS, PaaS and IaaS; andcloud computing deployment methods. deliberates on associated cloud computing
challenges; and presents the conclusion.

2. CLOUD COMPUTING INFRASTRUCTURE

The term cloud computing is rather a concept which is a generalized meaning evolved fromdistributed and grid computing. Cloud computing is described as the offspring of distributed andgrid computing by some authors (Che, Duan, Zhang & Fan, 2011).The straightforward meaning of cloud computing refers to the features and scenarios where total computing could be done byusing someone else's network where ownership of hardware and soft resources are of externalparties. In general practice, the dispersive nature of the resources that are considered to be the'cloud' to the users are essentially in the form of distributed computing; though this is notapparent or by its definition of cloud computing, do not essentially have to be apparent to the
users.In recent years, the cloud has evolved in two broad perspectives – to rent the infrastructure incloud, or to rent any specific service in the cloud. Where the former one

ISSN: 2278 – 1323

deals with the hardwareand software usage on the cloud, the later one is confined only with the 'soft' products or services from the cloud service and infrastructure providers. The computing world has been introducedwith a number of terminologies like SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service) with the evolution of cloud computing. As discussed earlier, the term 'cloud computing' is rather a concept, so are the terminologies to define different blendsof cloud computing. At its core essence, cloud computing is nothing but a specialized form of gridInternational Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014.And distributed computing which varies in terms of infrastructure, services, deployment andgeographic dispersion (Hashizume et al. 2013; Westphall et al., 2011; Hamlen, Kantarcioglu,Khan, & Thuraisingham, 2010). In a pervasive meaning within the context of computer networks, infrastructure could be thought of as the hardware as well as their alignment where platform is theoperating system which acts as the platform for the software (Singh &jangwal, 2012; Lee, 2012).Thus the concept of cloud based services is hierarchically built from bottom to top in the order ofIaaS, PaaS and SaaS. This is merely the level of abstraction that defines the extent to which anend-user could 'borrow' the resources ranging from infrastructure to software – the core concernof security and the fashion of computing are not affected by this level of abstraction. As a result, security is to be considered within any form of cloud computing (Bisong&Rahman, 2011)regardless of flavour, hierarchy and level of abstraction. It is the virtualization technology that complements cloud services specially in the form of PaaS and SaaS where one physical infrastructure contains services or platforms todeliver a number of cloud users simultaneously. This leads to the addition of total security aspectsof virtualization technology on top of the existing security concerns and issues of cloud computing.

Figure 2 illustrates a typical cloud based scenario that includes the cloud service provider and thecloud users in a cloud computing architecture.

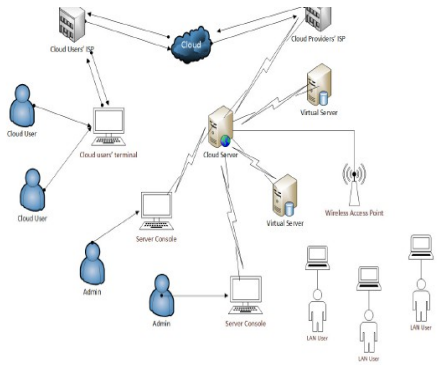


Figure 1: A Typical Cloud Architecture

The illustration of cloud architecture in figure 1 is a simplest one where few complexcharacteristics of cloud computing (e.g. redundancy, server replication, and geographic dispersionof the cloud providers' network) are not shown – the purpose of the illustration is to establish thearrangement that makes the concept of cloud computing a tangible one. The network architectureInternational Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014 ,28is self explanatory with the identification of cloud users when considered in-line with thediscussion of the cloud computing concept presented earlier. One notable part from thearchitecture is that, while the cloud users are clearly identified and named accordingly due to theirremote location and means of remote access to the cloud servers, the admin users who are administering the cloud servers are not cloud users in any form with respect to the cloud serviceprovider's network in the scenario. It is arguable whether the LAN users in figure 1 are cloud users or not. Such room for argument could exist due to the phrase 'cloud computing' being aconcept rather than a technical terminology. If the definition of cloud computing is taken to haveessential arrangements of being the servers located remotely that are accessed through publicinfrastructure (or through cloud), then the LAN users in figure 1 may not be considered as thecloud users in the context. With respect to distributed and grid computing as the mothertechnology that define the infrastructural approach to achieve cloud computing, the LAN users in the scenario are essentially the cloud users when they use the cloud services offered by theservers.

2.1 Software as a Service (SaaS)

If provide software services on demand. The use of single instance of the application runs on the cloud services and multiple end users or client organizations. The most widely known example of SaaS is salesforce.com, though many other examples have come to market, including the Google Apps offering of basic business services including email and word processing. Although salesforce.com preceded the definition of cloud computing by a few years, it now operates by leveraging its companion force.com, which can be defined as a platform as a service.

Figure 3 Cloud Services and Applications

2.2 Platform as a service (PaaS)

Platform as a service encapsulates a layer of software and provides it as a service that can be used to build higher-level services. There are at least two perspectives on PaaS depending on the perspective of the producer or consumer of the services:

• Someone producing PaaS might produce a platform by integrating an OS, middleware, application software, and even a development environment that is then provided to a customer as a service. For example, someone developing a PaaS offering might base it on a set of Sun™ xVM hypervisor virtual machines that include a NetBeans™ integrated development environment, a Sun GlassFish™ Web stack and support for additional programming languages such as Perl or Ruby.

ISSN: 2278 – 1323

• Someone using PaaS would see an encapsulated service that is presented to them through an API. The customer interacts with the platform through the API, and the platform does what is necessary to manage and scale itself to provide a given level of service. Virtual appliances can be classified as instances of PaaS. A content switch appliance, for example, would have all of its component software hidden from the customer, and only an API or GUI for configuring and deploying the service provided to them. PaaS offerings can provide for every phase of software development and testing, or they can be specialized around a particular area such as content management. Commercial examples of PaaS include the Google Apps Engine, which serves applications on Google's infrastructure. PaaS services such as these can provide a powerful basis on which to deploy applications, however they may be constrained by the capabilities that the cloud provider chooses to deliver.

2.3 Infrastructure as a service (IaaS)

Infrastructure as a service delivers basic storage and compute capabilities as standardized services over the network. Servers, storage systems, switches, routers, and other systems are pooled and made available to handle workloads that range from application components to high-performance computing applications.Commercial examples of IaaS include Joyent, whose main product is a line of virtualized servers that provide a highly available on-demand infrastructure.

3.CLOUD COMPUTATION IMPLEMENTATION GUIDELINES

3.1 Steps to Cloud Security Edwards (2009) stated that, with the security risk and vulnerability in the enterprise cloud computing that are being discovered enterprises that want to proceed with cloud computing should, use the following steps to verify and understand cloud security provided by a cloud provider:

 Understand the cloud by realizing how the cloud's uniquely loose structure affects the security of data sent into it. This can be done by having an in-depth understanding of how cloud computing transmit and handles data.

 Demand Transparency by making sure that the cloud provider can supply detailed information on its security architecture and is willing to accept regular security audit. The regular security audit should be from an independent body or federal agency.

 Reinforce Internal Security by making sure that the cloud provider's internal security technologies and practices including firewalls and user access controls are very strong and can mesh very well with the cloud security measures.

 Consider the Legal Implications by knowing how the laws and regulations will affect what you send into the cloud.

 Pay attention by constantly monitoring any development or changes in the cloud technologies and practices that may impact your data's security.

3.2 Information Security Principles

C I A (Confidentiality, Integrity, Availability)

• *Confidentiality*

Prevent unauthorized disclosure

• *Integrity*

Preserve information integrity

• *Availability* Ensure information is available when needed confidentiality, integrity, and availability.

3.3 IssuestoClarify Before Adopting Cloud Computing

The world's leading information technology research and advisory company, has identified seven security concerns that an enterprise cloud computing user should address with cloud computing providers (Edwards, 2009) before adopting:

 *User Access.*Ask providers for specific information on the hiring and oversight of privileged administrators and the controls over their access to information. Major Companies should demand and enforce their own hiring criteria for personnel that will Operatetheir cloud computing environments.

 Regulatory Compliance. Make sure your provider is willing to submit to external Audits and security certifications.

 Data location. Enterprises should require that the cloud computing provider store and process data in specific jurisdictions and should obey the privacy rules of those Jurisdictions.

 Data Segregation. Find out what is done to segregate your data, and ask for proof that encryption schemes are deployed and are effective.

 Disaster Recovery Verification. Know what will happen if disaster strikes by asking whether your provider will be able to completely restore your data and service, and find out how long it will take.

 Disaster Recovery. Ask the provider for a contractual commitment to support specific types of investigations, such as the research involved in the discovery phase of a lawsuit, and verify that the provider has successfully supported such activities in the past. Without evidence, don't assume that it can do so.

 Long-term Viability. Ask prospective providers how you would get your data back if they were to fail or be acquired, and find out if the data would be in a format that you could easily import into a replacement application.

4.SECURITY ISSUES IN CLOUD COMPUTING

4.1 Cloud Deployments Models

In the cloud deployment model, networking, platform, storage, and software infrastructure areprovided as services. TheCloud Computing model has three main deployment models which are:

4.1.1 Private cloud

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

4.1.2 Public cloud

ISSN: 2278 – 1323

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

4.1.3 Hybrid cloud

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 ITsolutions through a mix of both public and private clouds. Hybrid Cloud provides more secure.

4.2 Solution of Security Issues

4.2.1 Find Key Cloud Provider First solution is of finding the right cloud provider. Different vendors have different cloud IT security and data management. A cloud vendor should be well established, have experience, standards and regulation. So there is not any chance of cloud vendor closing.

4.2.2 Clear Contract Contract with cloud vendor should be clear. So if cloud vendor closes before contract, enterprise can claim.

4.2.3 Recovery Facilities Cloud vendors should provide very good recovery facilities. So, if data are fragmented or lost due to certain issues, they can be recovered and continuity of data can be managed.

4.2.*4 Better Enterprise Infrastructure* Enterprise must have infrastructure which facilitates installation and configuration of hardware components such as firewalls, routers, servers, proxy servers and software such as operating system, thin clients, etc. Also should have infrastructure which prevents from cyber attacks.

4.2.*5 Use of Data Encryption for security purpose* Developers should develop the application which provides encrypted data for the security. So additional security from enterprise is not required and all security burdens are placed on cloud vendor. IT leaders must define strategy and key security elements to know where the data encryption is needed.

4.2.*6 Prepare chart regarding data flow*

There should be a chart regarding the flow of data. So the IT managers can have idea where the data is for all the times, where it is being stored and where it is being shared. There should be total analysis of data.

4.2.7 Cloud Computing Security

Cloud Computing Security as “Cloud computing security (sometimes referred to simply as "cloudsecurity") is an evolving sub-domain of computer security,network security, and, more broadly, information security. Itrefers to a broad set of policies, technologies, and controlsdeployed to protect data, applications, and the associated infrastructure of cloud computing.” Note that cloud computingsecurity referred to here is not cloud-based security software products such as cloud-based anti-virus, anti-spam, anti-DDoS,and so on.

4.2.8 Security Issues Associated with the Cloud

There are many security issues associated with cloud computing and they can be grouped into any number of dimensions .According to Gartner [4], before making a choice of , users should ask the vendors for seven specific safetyissues: Privileged user access, regulatory compliance, datalocation, data segregation, recovery, investigative support andlong-term viability. In 2009, Forrester Research Inc. [5]evaluated security and privacy practices of some of the leadingcloud providers (such as Salesforce.com, Amazon, Google, andMicrosoft) in three major aspects: Security and privacy compliance, and legal and contractual issues. Cloud SecurityAlliance (CSA) [6] is gathering solution providers, non-profitsand individuals to enter into discussion about the current andfuture best practices for information assurance in the cloud.The CSA has identified thirteen domains of concerns on cloud computing security.

5.CLOUD COMPUTING CHALLENGES

The current adoption of cloud computing is associated with numerous challenges because usersare still skeptical about its authenticity. Based on a survey conducted by IDC in 2008, the majorchallenges 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 hinderingCloud computing acceptance. Without doubt, putting your data, running your software onsomeone else's hard disk using someone else's CPU appears daunting to many. Well-knownsecurity issues such as data loss, phishing, botnet (running remotely on a collection of machines)pose serious threats to organization's data and software. Moreover, the multi-tenancy model and the pooled computing resources in cloud computing has introduced new security challenges thatrequire novel techniques to tackle with. For example, hackers can use Cloud to organize botnetas Cloud often provides more reliable infrastructure services at a relatively cheaper price for themto start an attack.

B. Costing Model: Cloud consumers must consider the tradeoffs amongst computation,communication, and integration. While migrating to the Cloud can significantly reduce theinfrastructure cost, it does raise the cost of data communication, i.e. the cost of transferring anorganization's data to and from the public and community Cloud and the cost per unit ofcomputing resource used is likely to be higher. This problem is particularly prominent if the consumer uses the hybrid cloud deployment model where the organization's data is distributedamongst a number of public/private (in-house IT infrastructure)/community clouds. Intuitively, ondemandcomputing makes sense only for CPU intensive jobs.

C. Charging Model: The elastic resource pool has made the cost analysis a lot more complicatedthan regular data centers, which often calculates their cost based on consumptions of staticcomputing. Moreover, an instantiated virtual machine has become the unit of cost analysis rather than the underlying physical server. For SaaS cloud providers, the cost of developingmultitenancy within their offering can be very substantial. These include: re-design and redevelopmentof the software that was originally used for single-tenancy, cost of providing newfeatures that allow for intensive customization, performance and security enhancement forconcurrent user access, and dealing with

ISSN: 2278 – 1323

complexities induced by the above changes.Consequently, SaaS providers need to weigh up the trade-off between the provision of multitenancyand the cost-savings yielded by multi-tenancy such as reduced overhead throughamortization, reduced number of on-site software licenses, etc. Therefore, a strategic and viablecharging model for SaaS provider is crucial for the profitability and sustainability of SaaS cloudproviders.[9]

D. Service Level Agreement (SLA): Although cloud consumers do not have control over theunderlying computing resources, they do need to ensure the quality, availability, reliability, andperformance 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 fromproviders on service delivery. Typically, these are provided through Service Level Agreements(SLAs) negotiated between the providers and consumers. The very first issue is the definition of SLA specifications in such a way that has an appropriate level of granularity, namely the tradeoffsbetween expressiveness and complicatedness, so that they can cover most of the consumerexpectations and is relatively simple to be weighted, verified, evaluated, and enforced by the Kuyoro S. O., Ibikunle F. &Awodele O.resource allocation mechanism on the cloud. In addition, different cloud offerings (IaaS, PaaS,and SaaS) will need to define different SLA metaspecifications. This also raises a number ofimplementation problems for the cloud providers. Furthermore, advanced SLA mechanisms needto constantly incorporate user feedback and customization features into the SLA evaluationframework.

E. What to migrate: Based on a survey (Sample size = 244) conducted by IDC in 2008, the sevenIT 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 StorageCapacity (15.5%). This result reveals that organizations still have security/privacy concerns inmoving their data on to the Cloud. Currently, peripheral functions such as IT management andpersonal applications are the easiest IT systems to move. Organizations are conservative inemploying IaaS compared to SaaS. This is partly because marginal functions are oftenoutsourced to the Cloud, and core activities are kept in-house. The survey also shows that inthree years time, 31.5% of the organization will move their Storage Capacity to the cloud.However this number is still relatively low compared to Collaborative Applications (46.3%) at that time.

F. Cloud Interoperability Issue: Currently, each cloud offering has its own way on how cloudclients/applications/users interact with the cloud, leading to the "Hazy Cloud" phenomenon. Thisseverely hinders the development of cloud ecosystems by forcing vendor locking, which prohibitsthe ability of users to choose from alternative vendors/offering simultaneously in order to optimizeresources at different levels within an organization. More importantly, proprietary cloud APIsmakes it very difficult to integrate cloud services with an organization's own existing legacysystems (e.g. an on-premise data centre for highly interactive modeling applications in apharmaceutical company).The primary goal ofinteroperability is to realize the seamless fluid data across clouds and between cloud and local applications. There are a number of levels thatinteroperability is essential for cloud computing. First, to optimize the IT asset and computingresources, an organization often needs to keep in-house IT assets and capabilities associatedwith their core competencies while outsourcing marginal functions and activities (e.g. the humanresource system) on to the cloud. Second, more often than not, for the purpose ofoptimization,an organization may need to outsource a number of marginal functions to cloud services offered by different vendors. Standardization appears to be a good solution to address the interoperabilityissue. However, as cloud computing just starts to take off, the interoperability problem has notappeared on the pressing agenda of major industry cloud vendors.

intrackling the cloud security management problem. Models will help in the problem abstraction and the capturing of security requirements of different stakeholders

6.CONCLUSIONS

Cloud computing has enormous prospects, but the security threats embedded in cloud computingapproach are directly proportional to its offered advantages. Cloud computing is a greatopportunity and lucrative option both to the businesses and the attackers – either parties can havetheir ownadvantages from cloud computing. Cloud computing has a potential for cost savings to the enterprises but the security risk are also enormous. Enterprise looking into cloud computing technology as a way to cut down on cost and increase profitability should seriously analyze the security risk of cloud computing. The strength of cloud computing in information risk management is the ability to manage risk more effectively from a centralize point. Although Cloud computing can be seen as a new phenomenon which is set to revolutionize the way we use the Internet, there is much to be cautious about. There are many new technologies emerging at a rapid rate, each with technological advancements and with the potential of making human's lives easier. However, one must be very careful to understand the security risks and challenges posed in utilizing these technologies. Cloud computing is no exception. In this paper key security considerations and challenges which are currently faced in the Cloud computing are highlighted.We tried to solve many issues. In our future work, we will include the developing of testing of data flow and security in cloud computing.

7.FUTURE WORK

We are investigating in the cloud security management problem. Our objective is to block the hole arise in the security management processes of the cloud consumers and the cloud providers from adopting the cloud model. To be able to resolve such problem we need to Capture different stakeholders security requirements from different perspectives and different levels of details map security requirements to the cloud architecture, security patterns and security enforcement mechanisms and Deliver feedback about the current security status to the cloud providers and consumers.

We propose to adopt an adaptive model-based approach at different levels of details. Addictiveness will help in delivering an integrated, dynamic and enforceable cloud security model. The feedback loop will measure the security

ISSN: 2278 – 1323

status to help improving the current cloud security model and keeping cloud consumers aware with their assets' security status.

ACKNOWLEDGMENT

We thank all sponsors in the footnote on the first page for funding this ongoing research project and all volunteers for their involving this research project. We would also like to thank the anonymous referees for their constructive and valuable comments.

REFERENCES

[1] F. Gens, "New IDC IT Cloud Services Survey: Top Benefits and Challenges",Feb. 18, 2010.
[2] J. Brodkin, "Gartner: Seven cloud-computing security risk ,Mar. 13, 2009.
[3] Cloud Computing Use Case Discussion Group. "Cloud Computing UseCases Version 3.0,"2010.
[4] ENISA, "Cloud computing: benefits, risks and recommendations for information security.", Jul. 10, 2010.
[5] 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.
[6] P. Kresimir and H. Zeljko,"Cloud computing security issues and challenges." In PROCThird International Conference on Advances in Human-oriented and PersonalizedMechanisms, Technologies, and Services, 2010, pp. 344-349.
[7] B. Grobauer, T. Walloschekand E. Stöcker, "Understanding Cloud ComputingVulnerabilities," *IEEE Security and Privacy*, vol, 99, 2010.
[8] S. Subashini and V. Kavitha, "A survey on security issues in service deliverymodels of cloud computing." *J Network Comput Appl*doi:10.1016/j.jnca.2010.07.006, Jul. 2010.
[9] S. Ramgovind, M. M. Eloff, E. Smith, "The Management of Security in Cloud Computing" In PROC 2010 IEEE International Conference on Cloud Computing 2010.
[10] M. A. Morsy, J. Grundy and Müller I, "An Analysis of the Cloud Computing Security Problem" In PROC APSEC,Mar.19,2010.
[12] S. Arnold, "Cloud computing and the issue of privacy." *KM World*, pp14-22, Aug 19, 2009.
[13] A Platform Computing Whitepaper, "Enterprise Cloud Computing: Transforming IT". *Platform Computing*, pp6, 2010.
[14] GlobalNetoptex Incorporated. "Demystifying the cloud. Important opportunities, crucial choices" , Dec. 13, 2009.
[15] M. Klems, A. Lenk, J. Nimis, T. Sandholmand S. Tai. "What's Inside the Cloud? AnArchitectural Map of the Cloud Landscape".*IEEE Xplore*, pp 23-31, Jun. 2009.
[16] C. Weinhardt, A. Anandasivam, B. Blau, and J. Stosser. "Business Models in the ServiceWorld."*IT Professional*, vol. 11, pp. 28-33, 2009.
[17] N. Gruschka, L. L. Iancono, M. Jensen and J. Schwenk. "On Technical Security Issues inCloud Computing" In PROC 09 IEEE International Conference on Cloud Computing, 2009.
[18] N. Leavitt, "Is Cloud Computing Really Ready for Prime Time?" *Computer*, vol. 42, pp. 15-20, 2009.
[19] M. Jensen, J. Schwenk, N. Gruschka and L. L. Iacono, "On Technical Security Issues inCloud Computing." in PROC IEEE ICCC, Bangalore 2009.
[20] C. Soghoian, "Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era" The Berkman Center for Internet & Society Research Publication Series, Aug.22, 2009.

AUTHOR PROFILE:

T.Ambika received her M.Sc Degree in Information Technology from AnnaUniversity,Chennai, India. Her interest of area for Research Work is in Cloud Computing and Networking.

ISSN: 2278 – 1323