Volume 3, Issue 7, July 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Trusted Third Party in Cloud Architecture to Implement Security Issues

Kollati Vijaya Kumar
Dept. Of CSE,
Vignan Institute of Engineering for Womens(VIEW), India

CH.V.T.E.V.Laxmi
Dept. Of CSE,
Raghu Engineering College,India

Abstract— Cloud computing is set of resources and services offered through the Internet. Cloud services are delivered from data centers which are located throughout the world. Cloud computing is a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. In cloud computing, the word cloud (also phrased as "the cloud") is used as a metaphor for "the Internet," so the phrase cloud computing means "a type of Internet-based computing," where different services -- such as servers, storage and applications are delivered to an organization's computers and devices through the Internet. The rapid growth in field of "cloud computing" also increases severe security concerns. Security has remained a constant issue for Open Systems and internet, when we are talking about security cloud really suffers. From a security perspective, a number of risks and challenges have been introduced to the clouds, deteriorating much of the effectiveness of traditional protection mechanisms. As a result the aim of this paper is to evaluate cloud security by identifying unique security requirements and secondly to attempt to present a viable solution that eliminates these potential threats. This article proposes cloud security through the trusted third party mechanisms. And by implementing trusted third party model of network security within the cloud architecture. This article also proposes network access security model in the cloud computing so that cloud services can be protected from information access threats and services threats.

Keywords— Cloud computing ,cloud architecture, network security, trusted third party, open systems, cloud security, cloud services

I. INTRODUCTION

The term "cloud" is analogical to "Internet". The term "Cloud Computing" is based on cloud drawings used in the past to represent telephone networks "and later to depict Internet in".

Cloud computing is Internet based computing where virtual shared servers provide software, infrastructure, platform, devices and other resources and hosting to customers on a pay-as-you-use basis. All information that a digitized system has to offer is provided as a service in the cloud computing model. Users can access these services available on the "Internet cloud" without having any previous know-how on managing the resources involved. Thus, users can concentrate more on their core business processes rather than spending time and gaining knowledge on resources needed to manage their business processes. Cloud computing customers do not own the physical infrastructure; rather they rent the usage from a third-party provider. This helps them to avoid huge. They consume resources as a service and pay only for resources that they use. Most cloud computing infrastructures consist of services delivered through common centres and built on servers. Sharing resources amongst can improve, as servers are not unnecessarily left idle, which can reduce costs significantly while increasing the speed of application development.

II. CLOUD: OVERVIEW

A. The 5 essential characteristics of cloud computing.

Cloud Computing has 5 Important Characteristics, they are Rapid Elasticity, Measured service, on demand self service; everywhere network access and Resource pooling. Figure 1.1 shows the essentials of cloud computing

- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured Service

1) On-demand self-service.

This is where you can provision computing capabilities based on your needs. Our needs may change from time to time. This is why it's called "on-demand". It's based on your needs. The cool thing is that, all these provisioning processes don't need human intervention!

2) *Broad network access.*

By using cloud, you have the option on whether to burden the end users laptop or in another word, thin or thick client. Thin client is where users have to download a small size file and they can access to all the resources and features

available. For thick client, users will have to download a big size of files to their workstations before using the features. In another word, it's about how much you rely on the cloud and workstation.

Figure 1 shows the essentials of cloud computing

3) Resource pooling.

This is another cool thing about cloud computing. Resource pooling is about assigning computing resources to multiple customers dynamically. It is something that can change from time to time based on users demands.

4) Rapid elasticity.

For me, this is the coolest characteristic in cloud computing. Imagine you are hosting a web site and your average hit per day is 100. Suddenly, you are launching a project and for a particular day, a lot of users will be signing in online at the same time. Your hit for that particular time may rise to 10,000 in a day. For this type of scenario, during a normal day, the cloud will assign you let's say, 1 server and during peak time, it will rise to 5 servers and back to 1 server during normal hour. The best thing is that, you only pay for how much you use! If you are hosting it yourself, you'll need to purchase 5 servers to prepare for the peak hours which only will occur once in a blue moon. During the rest of the time, the other 4 servers will just sit there doing nothing. Waste of resources.

5) Measured service.

Since cloud is a pay-as-you-go type, you will be charged based on the amount of resources you use only. Cloud provides usage metering.

B. Cloud Architectures

Cloud computing architecture refers to the components and subcomponents required for cloud computing. These components typically consist of a front end platform (fat client, thin client, mobile device), back end platforms (servers, storage), a cloud based delivery, and a network (Internet, Intranet, Intercloud). Combined, these components make up cloud computing architecture. Cloud computing architectures consist of front-end platforms called clients or cloud clients. These clients comprise servers, fat (or thick) clients, thin clients, zero clients, tablets and mobile devices. These client platforms interact with the cloud data storage via an application (middleware), via a web browser, or through a virtual session. The Cloud Computing Architecture of a cloud solution is the structure of the system, which comprise on premise and cloud resources, services, middleware, and software components, geo-location, the externally visible properties of those, and the relationships between them. The term also refers to documentation of a system's cloud computing architecture. Documenting facilitates communication between stakeholders, documents early decisions about high-level design, and allows reuse of design components and patterns between projects. Figure 2 shows the cloud computing architecture.

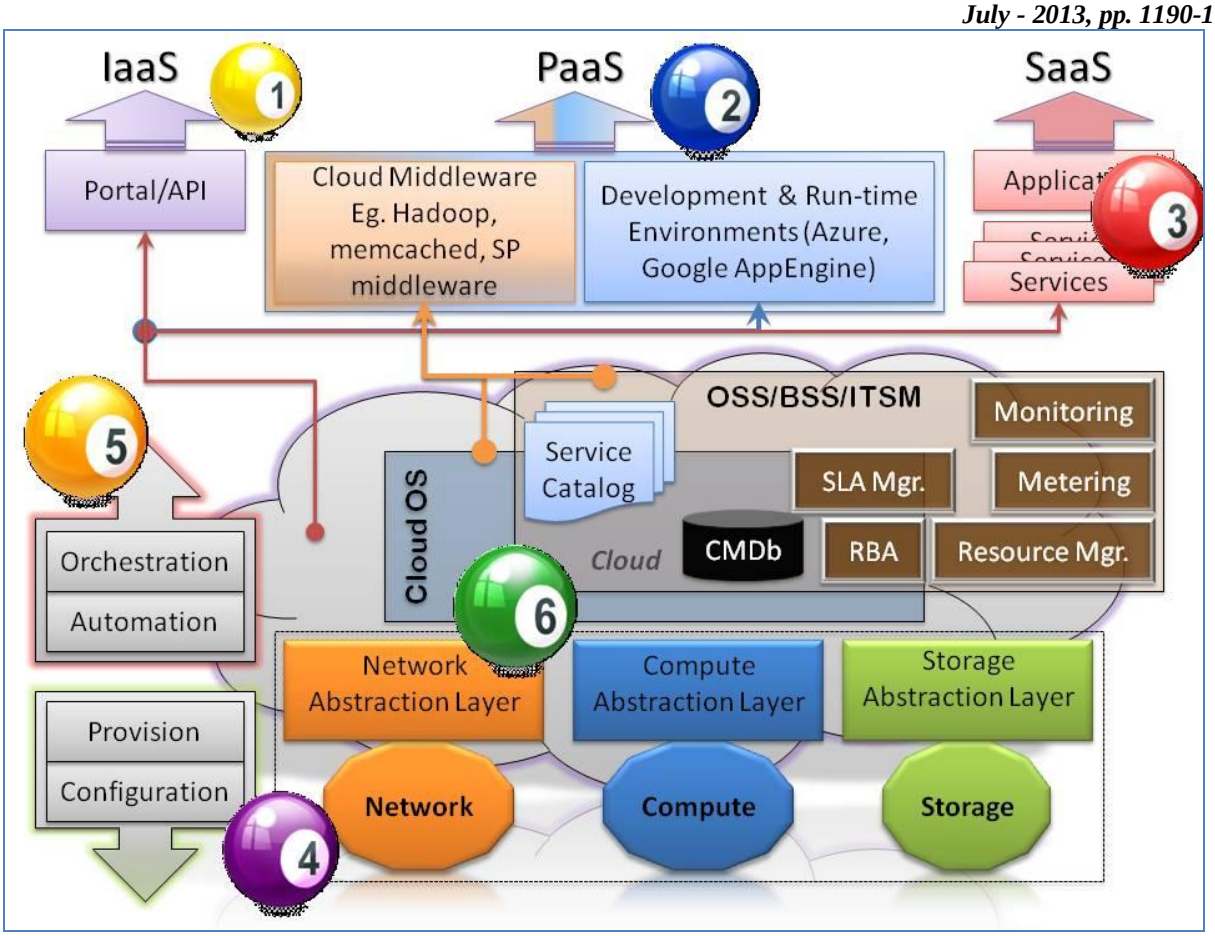

Figure 2 Cloud computing architecture

C. Cloud Deployment Models

There are primarily four cloud deployment models. These models have been recommended by the National Institute of Standards and Technology (NIST). Figure 3 demonstrates the deployment models of cloud computing.

1) The Private Cloud

This model doesn't bring much in terms of cost efficiency: it is comparable to buying, building and managing your own infrastructure. Still, it brings in tremendous value from a security point of view. During their initial adaptation to the cloud, many organizations face challenges and have concerns related to data security. These concerns are taken care of by this model, in which hosting is built and maintained for a specific client. The infrastructure required for hosting can be on-premises or at a third-party location.

Security concerns are addressed through secure-access VPN or by the physical location within the client's firewall system.

In addition to security reasons, this model is adopted by organizations in cases where data or applications are required to conform to various regulatory standards such as SOX, HIPAA, or SAS 70, which may require data to be managed for privacy and audits that govern the corporation. For example, for the healthcare and pharmaceutical industries, moving data to the cloud may violate the norms. Similarly, different countries have different laws and regulations for managing and handling data, which can impede the business if cloud is under different jurisdiction.

Several SaaS applications, such as Sugar CRM, provide options to their clients to maintain their data on their own premises to ensure data privacy is maintained according to the requirements of the particular business. Amazon also provides the option of a virtual private cloud.

2) The Public Cloud

The public cloud deployment model represents true cloud hosting. In this deployment model, services and infrastructure are provided to various clients. Google is an example of a public cloud. This service can be provided by a vendor free of charge or on the basis of a pay-per-user license policy.

This model is best suited for business requirements wherein it is required to manage load spikes, host SaaS applications, utilize interim infrastructure for developing and testing applications, and manage applications which are consumed by many users that would otherwise require large investment in infrastructure from businesses.

This model helps to reduce capital expenditure and bring down operational IT costs.

3) The Hybrid Cloud

This deployment model helps businesses to take advantage of secured applications and data hosting on a private cloud, while still enjoying cost benefits by keeping shared data and applications on the public cloud. This model is also used for handling cloud bursting, which refers to a scenario where the existing private cloud infrastructure is not able to handle load spikes and requires a fallback option to support the load. Hence, the cloud migrates workloads between public and private hosting without any inconvenience to the users.

Many PaaS deployments expose their APIs, which can be further integrated with internal applications or applications hosted on a private cloud, while still maintaining the security aspects. Microsoft Azure and Force.com are two examples of this model.

4) The Community Cloud

In the community deployment model, the cloud infrastructure is shared by several organizations with the same policy and compliance considerations. This helps to further reduce costs as compared to a private cloud, as it is shared by larger group.

Various state-level government departments requiring access to the same data relating to the local population or information related to infrastructure, such as hospitals, roads, electrical stations, etc., can utilize a community cloud to manage applications and data.

Cloud computing is not a "silver–bullet" technology; hence, investment in any deployment model should be made based on business requirements, the criticality of the application and the level of support required.

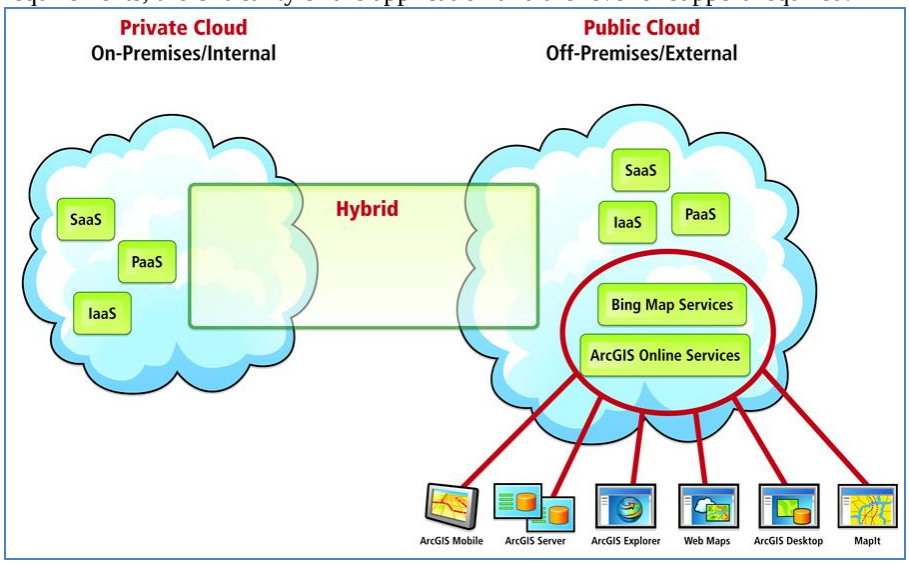

Figure 3 Deployment model of cloud computing

III. DATA SECURITY IN CLOUD COMPUTING

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.

A. Key security challenges

1) 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.

2) 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.

3) 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.

4) 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.

IV. PROPOSED APPROACH

The rapid growth of usage of "cloud computing" also increases severe security concerns. Security has remained a constant issue for Open Systems and internet, when we are talking about security cloud really suffers. Therefore we proposed an approach to provide security in cloud architecture through implementing trusted third party model of network security. The main aim of this paper is to propose a trusted third party e.g. arbiter, distributer of secret information in the cloud architecture.This paper also proposes network access security model in the cloud computing so that cloud services can be protected from information access threats and services threats.

A. Third party model of network security in cloud architecture

Figure 4 demonstrates model of Network security through trusted third party in cloud architecture, where various services of cloud such as on-demand self-service, broad network access, resource pooling and measure services takes place. The two parties who are the principals in this transaction must cooperate for the exchange to take place. A logical information channel is established by defining a route through the internet from source to destination and by the cooperative use of communication protocols by two principals.

Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity and so on. All the techniques for providing security in cloud can have two components.

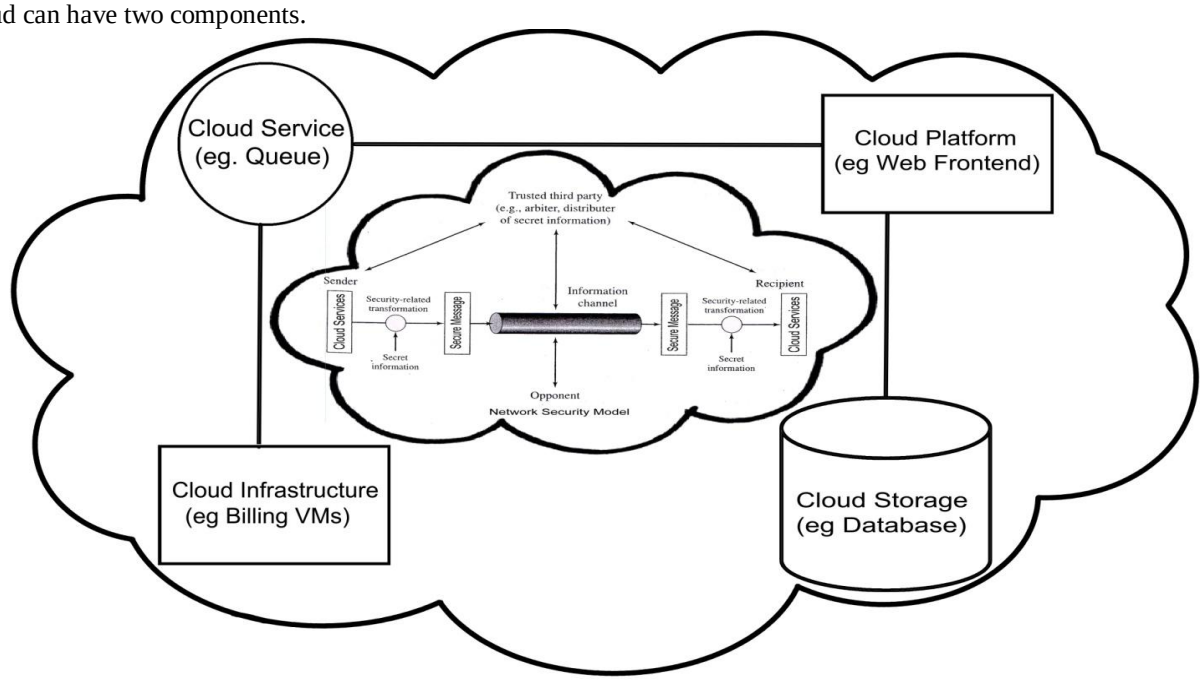

Figure 4 Trusted Third Party model of network security in cloud architecture

B. Two components for Trusted Third party model of network security in cloud architecture

- A security –related transformation on the information to be sent. It include the encryption of the data, which scrambles the data so that it is unreadable by the opponent and the addition of a code based on the contents of the cloud services, which can be used to verify the identity of the sender.
- Some secret information shared by the two principals and, it is hoped unknown to the opponent, it can be implemented by using encryption key in conjunction with the transformation to scramble the cloud services before transmission and unscramble it on reception.

A trusted third party may be needed to achieve secure transmission. For instance a third party may be responsible for distributing the secret information to the two principals while keeping it from any opponent. Or a third may be needed to arbitrate disputes between the two principals concerning the authenticity of a cloud services transmission.

The following are the four basic tasks in designing a security service in cloud architecture:

1) Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.
2) Generate the secret information to be used with the algorithm.
3) Develop methods for the distribution and sharing of the secret information.
4) Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service in cloud.

C. Network Access Security Model in Cloud Computing

In cloud computing there is a need for protecting an information system from unwanted access. Network access security model is necessary in cloud computing in order to protect from the hackers, who attempt to penetrate systems that can be accessed over network. The hacker can be someone who, with no malign intent, simply gets satisfaction from breaking and entering cloud systems. The intruder can be disgruntled employee who wishes to do damage or a criminal who seeks to exploit computer assets for financial gain such as obtaining credit card numbers or performing illegal money transfers etc.

The other type of unwanted access is the placement in a computer system of logic that exploits vulnerabilities in the system and that can affect application programs as well as utility programs, such as editors and compliers. Programs can present two kinds of threats:

- Information access threats: Intercept or modify data on behalf of users who should not have access to that data.
- Service threats: Exploit service flaws in computers to inhibit use by legitimate users.

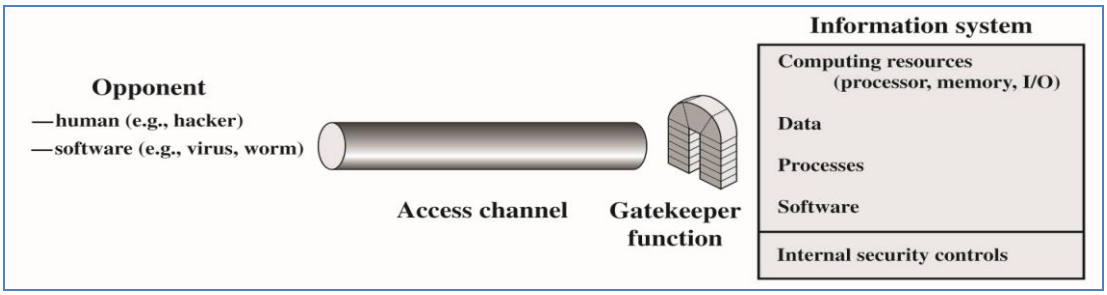

Figure 5 Network Access Security Model

In cloud computing security mechanisms needed to cope with unwanted access fall into two broad categories as per the figure 5. The first category might be termed a gatekeeper function. It includes password-based login procedures that are designed to deny access to all but authorized users and screening login that is designed to detect and reject worms, viruses and other similar attacks. Once either an unwanted user or unwanted software gains access, the second category is of defense consists of a variety of internal controls that monitor activity and analyze stored information in an attempt to detect the presence of unwanted intruders.

V. CONCLUSION

This paper carries out a survey on cloud computing from the study of different researches carried out on this field. Rapid growth and usage of cloud computing also increased essentiality of implementing security in various ways. Security has remained a constant issue for Open Systems and internet, when we are talking about security cloud really suffers. Therefore we proposed an approach to provide security in cloud architecture through implementing trusted third party model of network security. The main aim of this paper is to propose a trusted third party e.g. arbiter, distributer of secret information in the cloud architecture so that cloud information can have security over the cloud. This article also proposes network access security model in the cloud computing so that cloud services can be protected from information access threats and services threats.

References

[1] http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc
[2] Ramgovind S, EloffMM, Smith E, "The Management of Security in Cloud Computing", Information Security for South Africa (ISSA) conference, pp 1-7, Sep 2010
[3] Meiko Jensen, Jorg Sehwenk et al., "On Technical Security Issues in cloud Computing" IEEE International conference on cloud Computing, pp 109-116, October 2009.
[4] Mladen A. Vouk, "Cloud Computing – Issues, Research and Implementations" Journal of Computing and Information Technology - CIT 16, 4, pp 235–246, 2008
[5] Herminder Singh & Babul Bansal "Analysis Of Security Issues And Performance Enhancement In Cloud Computing" International Journal of Information Technology and Knowledge Management, Volume 2, No. 2, pp. 345-349, July-December 2010
[6] Hassan Takabi, James B.D.Joshi, Gail Joon Ahn, "SecureCloud: Towards a Comprehensive Security Framework for Cloud Computing Environments" 34th Annual IEEE Computer Software and Applications Conference Workshops, pp 393-398, 2010
[7] Jonathan Spring Software Engineering, "Monitoring Cloud computing by layer part 1" Security & Privacy, IEEE vol 9, Issue 2, pp 66-68, Mar 2011
[8] Jonathan Spring Software Engineering, "Monitoring Cloud computing by layer part 2" Security & Privacy, IEEE vol 9, Issue 3, pp 52-55, May 2011
[9] Balachandra Reddy, Ramakrishna Paturi, Dr.Atanu, "Cloud security Issues", IEEE International conference on Services Computing, pp 517-520, 2009
[10] Hassan Takabi and JamesB.D., "Security and Privacy Challenges in Cloud Computing Environments", Security & Privacy, IEEE, vol 8, Issue 6, pp 24-31, Dec 2010.
[11] Nelson Gonzalez, Charles Miers, "A quantitative analysis of current security concerns and solutions for cloud computing", Third IEEE International conference on Cloud Computing Technology and Science, pp 231-238, 2011
[12] Subhashis Sengupta, Vikrant Kaulgud and Vibhu Saujanya Sharma, "Cloud Computing Security-Trends and Research Directions", IEEE World Congress on Services, pp 524-531, 2011
[13] Siani Pearson and Azzedine Benameur, "Privacy, Security and Trust Issues Arising from Cloud Computing" 2nd IEEE International Conference on Cloud Computing Technology and Science, pp 693-702, 2010

[14] Cloud Security Alliance Web site, http://www.cloudsecurityalliance.org/
[15] Lijun Mei, W.K. Chan and T.H. Tse, "A Tale of Clouds: Paradigm Comparisons and Some Thoughts on Research Issues", IEEE Asia-Pacific Services Computing Conference, pp 464-469, 2008
[16] Pankesh Patel, Ajith Ranabahu and Amit Sheth1, "Service Level Agreement in Cloud Computing", Cloud Workshops at OOPSLA, 2009
[17] www.idc.com
[18] "Service Level Agreement Definition and contents",http://www.service-level-agreement.net, accessed on March 10, 2009.

