ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 4, April 2013

Trust in Cloud Computing

Prasad I. Bhosle andSwapnil A. Kasurkar
PADM. DR. V B KOLTE COE Malkapur

***Abstract*—Cloud computing is the most recent technology in the Information technology industry which a lot of companies and government are putting much concern to make sure that they have benefited from this new innovation. However, the comfort of this innovation is still shaking and a lot of companies are now suffering from still storing their sensitive data in their data centres instead of storing them in the cloud as well. This research will be looking at the trust and privacy concern as the major player in the participation of the cloud and these factors have played a vital role in reducing full patronage of companies in the cloud business. Ideas and different architectures will be discussed to see how the industry has gone to overcome such doubt and as well as proffering solutions to the customers for their comfort and the providers as well. Some providers and incidences could be brought on board to discuss and how these disasters will be handle by both the customers and their providers.**

***Index Terms*—Trust, Saas, Paas,Iaas,TSS,KMTS**

I. INTRODUCTION

Cloud computing provides many opportunities for enterprises by offering arrange of computing services. In today'scompetitive environment, the servicedynamism, elasticity, and choices offered by thishighly scalable technology are too attractive forenterprises to ignore. These opportunities, however,don't come without challenges.

Cloud computing has opened up a new frontier of challenges by introducing a different type of trust scenario. Today, the problem of trustingcloud computing is a paramount concernfor most enterprises. It's not that the enterprisesdon't trust the cloud providers' intentions; rather,they question cloud computing's capabilities.

Yet the challenges of trusting cloud computingdon't lie entirely in the technology itself. The dearth of customer confidence also stems from a lack of transparency, a loss of control over dataassets, and unclear security assurances. Unfortunately, the adoption of cloud computing came before the appropriate technologies appeared to tackle the accompanying challengesof trust. This gap between adoption and innovation is so wide that cloud computing consumersdon't fully trust this new way of computing.

To close this gap, we need to understand thetrust issues associated with cloud computingfrom both a technology and business perspective.Then we'll be able to determine whichemerging technologies could best address these issues.

II. CLOUD COMPUTING ARCHITECTURE

Cloud providers host their resources on the internet on virtual computers and make them available to multiple clients. Multiple virtual computers can run on one physical computer sharing the resources such as storage, memory, the CPU and interfaces giving the feeling to the client that each client has his own dedicated hardware to work on. Virtualization thus gives the ability to the providers to sell the same hardware resources among multiple clients. This sharing of the hardware resources by multiple clients help reduce the cost of hardware for clients while increasing profits of providers. Accessing or selling hardware in the form of virtual computers is known as Infrastructure as Service (IaaS) in the cloud computing terminology [2]. Once a client has procured infrastructure from a service provider, he is free to install and run any Operating System platform and application on it. Other kinds of services that are made available via the cloud computing model are Platform as a Service (PaaS) and Software as a Service. Figure 1, shows the architecture of a typical cloud computing system.

Under PaaS, the development platform in the form of an Operating System has been made available where customers can configure the environment to suit their requirements and install their development tools [3]. PaaS helps developers develop and deploy applications without the cost of purchasing and managing the underlying hardware andsoftware. PaaS provides all the required facilities for the complete life cycle of building and delivering web applications. Thus PaaS usually offers facilities for application design, application development, testing, deployment and hosting as well as application services such as team collaboration, web service integration and marshalling, database integration, security, scalability, storage, persistence, state management, application versioning, application instrumentation and developer community facilitation.

SaaS is the cloud model where an application hosted by a service provider on the internet is made available to users in a ready to use state. SasS eliminates the requirement of installation and maintenance of the application in the user's local computer or server in his premises [3]. SaaS has the

advantage of being accessible from any place at any time, no installation or maintenance, no upfront cost, no licensing cost, scalability, reliability and flexible payment schemes to suit the customer‘s requirements.

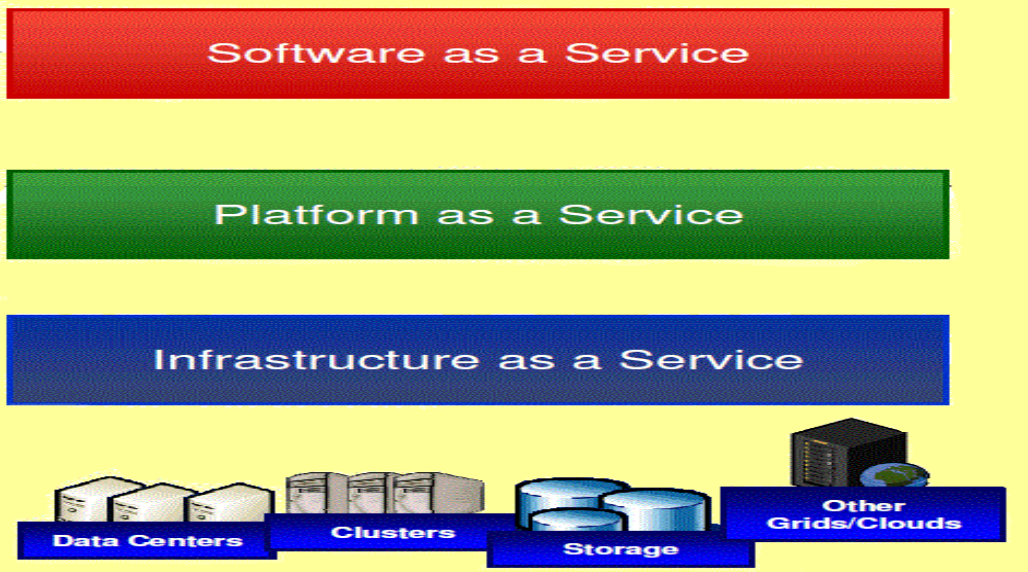

Figure 1 Architecture of cloud computing

III. PROBLEM DEFINITION

A. *Trust*

Broadly speaking, trust means an act of faith;confidence and reliance in something that’s expected to behave or deliver as promised.1,2It’s a belief in the competence and expertise of others, such that you feel you can reasonably rely on them to care for your valuable assets.We trust a system less if it gives us insufficientinformation about its expertise. Mere claimssuch as “secure cloud” or “trust me” don’t helpmuch to boost the trust level of consumerscomputer.org/ITPro2 1unless sufficient information is presented withthe services.[4].

Cloud providers could form security enclaves for their consumers, as is widely practiced in the defense industry. An enclave is a set of computing environment connected by one or more networks that a single authority controls using a common security policy. Enclave could provide a set of standards capabilities, such as incident detection and response, boundary, defense and monitoring. They could be specific to an enterprise or to a set of similar services consume. At the same time, providers could also compartmentalize users‘ data so that it is not mixed up with other users‘ data. This would solve the problem of cross –VM-channel attacks. Cloud providers could as well prevent attackers from creating cloud cartography of the enclave by refusing to disclose the mapping of the physical topology of the cloud computing for a service or users. In an enclave, it is easier to enforce the enterprise‘s security policy because you are only dealing with the part of the cloud related to the client data or processes, rather than the entire cloud[4].

B. *Control*

Control is another important issue in trust. We trust a system less when we don’t have much control over our assets. For example, when we withdraw money from an ATM, we trust that the machine will give us the exact amount because it’s under our control—we receive (“control”) the money. When we make a deposit using the same ATM, we usually don’t have the same level of trust because we’re losing control over our money—we don’t know what happensafter the ATM consumes it. Similarly, the more control consumers have over the data consigned toa cloud, the more they’ll trust the system.

C. *Ownership*

We can also see a variation of trust, depending on the ownership of data assets. Alice might trust an online payment system when she pays with her credit card, but she might have less trust in the same system when using her client’s card, because preserving her client’s interest is one of her business objectives. Similarly, when enterprises consign their data to cloud computing (data representing both their own interests and those of their clients), it creates two folds of a complex trust relationship. First, the enterprise

must trust the cloud provider. Second, the enterprise must ascertain that its clients have enough reason to trust the same provider[5]

D. Prevention

Contractual relationships are often used to establish trust. In a typical business environment, an organization is compensated if the service isn't delivered as expected. Cloud providers similarly use service-level agreements (SLAs) to boost consumers' trust. Unfortunately, these might not help in cloud computing. Trust in cloud computing is related more to preventing a trust violation than to guaranteeing compensation should a violation occur. For most enterprises, a security breach of data is irreparable—no amount of money can guarantee to restore the lost data or the enterprise's reputation. The cloud computing trust model thus should focus more on preventing failure than on post-failure compensation.

E. Security

Security plays a central role in preventing service failures and cultivating trust in cloud computing. In particular, cloud service providers need to secure the virtual environment, which enables them to run services for multiple clients and offer separate services for different clients. In the context of virtualization, the key security issues include identity management, data leakage (caused by multiple tenants sharing physical resources), access control, virtual machine (VM) protection, persistent client-data security, and the prevention of cross-VM side-channel attacks. Vendors and research communities are working to address these cloud-specific security concerns. For example, Intel's SOA Expressway claims to enforce persistent security on client data by extending the perimeter of enterprises into the cloud provider (so the enterprises retain a certain amount of control over the computing tasks and data consigned to cloud)[7]. The VMsafe API provides VM security protection at the host level6]. Its VMotion capabilities can dynamicallyove VMs between physical devices as required. To ensure integrity and authenticity, and to address access control in a cloud-enabled system, some have proposed using claim-based access control, a security assertion markup language, a security token service, and federated identity approaches. 8 Undoubtedly, these low-level security concerns are important, but to understand the issues related to consumer-level trust, we need to take a closer look at cloud computing.

IV. SOLUTION OF THE PROBLEM DEFINED

A. *Challenges to trust in cloud*

There is a necessity of security threats in cloud computing platform, because clients store their critical and confidential data in the cloud. In some cases, the clients require physically or virtually separated data and applications. Cloud providers can invest in better security controls through scale economies, but they can also develop standardized processes for regulatory compliance. Cloud providers improve their offerings to meet clients‘ enterprise-grade security needs, but this might not be sufficient in some key sectors. For example, in the defence, aerospace, and brokerage industries, security and compliance requirements—which include the data‘s physical location—have made SaaS and hardware public clouds currently unacceptable.[7] In a recent survey, 64 percent of respondents in the US federal government said security was their topmost concern in cloud computing.(Chabrow, 2009)[8].

The trust levels toward cloud computing in these sectors have, however, been improving. The launch of the federal cloud services portal for government agencies called Apps.gov is indicative of this shift. Vendors such as Google and Microsoft are close to obtaining accreditation for compliance with the Federal Information Security Management Act, making their cloud computing services acceptable for the public sectorRecently, Microsoft asked the US Congress to pass the Cloud Computing Advancement Act, which also calls for an update to the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act (Chakraborty, et al, 2010)[8].

Cloud computing service providers and their attributes and ranking

Cloud computing providers	Online traffic	Size of the company	Type of the Service
Salesforce.com	Very High	Large	SaaS
Enki Consulting	Low	Small	IaaS
EnterpriseDB	Low	Medium	IaaS
Cloud9 Analytics	Low	Small	IaaS
Yahoo Zimbra	Medium	Large	IaaS
IB M Lotus Live	Low	Large	SaaS
Rackspace Cloud	Medium	Small	IaaS
Layered Technologies	Low	Medium	IaaS
Sun Microsystems	High	Large	PaaS
GoGrid	Low	Medium	PaaS
Amazon	Very High	Large	SaaS
Microsoft SQL Azure	Very High	Large	IaaS
CloudWorks	Low	Small	IaaS
Rackspace Cloud	Medium	Small	IaaS
Google Docs	Very High	Large	SaaS
3Tera	Low	Small	SaaS
Vertica	Low	Medium	IaaS
Absolute Performance	Low	Small	SaaS
Oracle	High	Large	SaaS
Google Apps Engine	Very High	Large	PaaS

Table1 cloud service providers

V. EFFECTIVENESS OF THE SOLUTION

A. Amazon web service simple storage service Disasters S3

Amazon has suffered disasters that made customers to raise doubt on its storage services which has created 2 hours outage. This has made customers to lose grip and confidence in depending on the Amazon storage in the cloud in February 2008. It equally suffered 8 hours service outage in July 2008 causing outages at online companies that solely depend on S3 for file storage (Economist, 2008). Amazon was very proud of this facility and it has made the customers to be pleased with their operational performance for the past two years before 2008‘s incidence. Since S3 was launched in march 2006 a lot of companies have used this medium to outsourced most of their storage infrastructures to AWS including 37 signals, youOS, Smugmug, Elephant drive and jungle disc. Don Markskill the CEO of Smugmug who has fallen amongst the major customers of Amazon and has used S3 medium to stores its company‘s photo on it, was so defending AWS, the Amazon S3 service that their services is very reliable and dependable after such incidence. The CEO further reiterated that his faith on AWS has never encountered problems. In October, 2008 Amazon has moved its elastic compute cloud to (EC2) out of beta and finally published numbers on what its customers can expect in terms of reliability 99.95% uptime (E.Krangel, 2008) This has proven beyond reasonable doubt that it can strive. Now Amazon is striving well in the industry and it has fallen in the category of major companies that provide cloud computing in the world [9].

B. Solution to s3 cloud services

Amazon has been known as one of the leaders in S3 services in the cloud despites its problems in 2008. This is not only happened with them alone a lot of giant cloud providers have also faced these challenges and customers trust have always been the case. Google as it renowned for its search engine, has taken its market share dominance into other areas of enterprise 2.0 (Whittaker, 2008)[11]. The most prominent application in the web such as Gmail and Google Apps which has been known to be cloud services has also faced the challenge of service outage which made a lot of its customers to be in a mess such as Twitters (Needleman, 2008). These outages instituted distrust in the minds of their customers because they are not sure if their valuable data is been protected and if yes, how will they be sure it‘s safe. Having said that, this research has look at different measures to make sure that, trust is embedded in the minds of the providers‘users or customers. Therefore, different architecture were search and this research has supported the architecture of Yao (2010) which has model a trustworthy storage service that will build more trust to the minds of the customers. This need has necessitated the emergence of SSP (storage service providers) to create comfort to the customers. This application has created convenient interface for customers to have direct control of their data storage management in an unlimited capacity. However there are some disadvantages of using

SSP in the cloud which is vulnerable to some two major areas of attacks. These are:

 External Attack- This is where hackers break through the system and steal data, this kind of attack can be protected through the use of the traditional approaches which general techniques of generic umbrella of Intrusion tolerance (Wang, et al 2003)[10].

 Internal Attacks-This is where the malicious employee breaks into the system and steal information for profit benefit. Literature carries most of the malicious confidential data leakage internal (Dhillon, et al, 2010)[12]. However, this attack can be easily protected by the use of firewalls and antivirus etc.

This architecture has looked at these path critically and device a means of solving them, by instituting Trustworthy Storage Service (TSS). Simple data model has been built to analysis on confidentiality and integrity of the data outsourced to the data storage as well as prototype named Trust shops to illustrate the concept. There 3 parties actively participate in the design, these are the Key management service providers (KMSP), the trustworthy storage service (TSS) and the client computer.

 Key Management Service Provider- manages, stores, issues and registers the key for the clients. The KSMP has the knowledge of the stored keys.

 Storage Service Provider- the outsourcing data content are been encrypted and kept in the SSP. In this case, only the cipher text content is left with the SSP.

 Client Computer- The client has the application installed in the machine called the Trust store which is holding the responsibility of conducting data outsourcing process by composing SSP and KMSP.

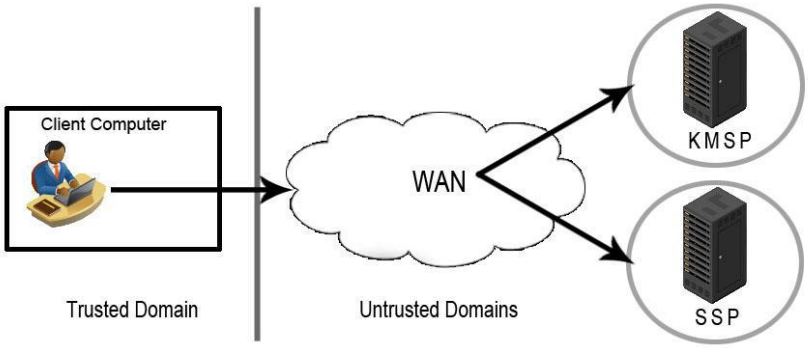

Figure 3: Architecture of TSS

The architecture above is aimed at instituting trust to both the SSP and the KMSP by the client. The client has fully secured and trusted for sensitive data operations and computation. In the case of SSP and the KMSP they are both semi trusted, they aimed to only the services they claimed to provide certain access control are been instituted to both parties. In this case, both are little or no ideas about each other. They should not have access to knowing each other in whatever form. The client computer process sensitive data with encryption mechanism which the data is been transformed into two forms the cipher form and the key form. Then the cipher test form is then uploaded into SSP without the key form in this case the SSP would not be able to access the sensitive data uploaded by the client computer because of unavailability of the key form. The key form is been kept with the KMSP but it does not have the cipher text to do that. This idea of separating the cipher text form from the key form is not a new idea in the industry but it will institute trust into the minds of the customers[10].

VI. RESULTS AND DISCUSSION

A. Virtualization

Virtualization is the key features of cloud computing which refers to as abstraction of computer resources. Number of these virtualization technologies have been proposed and implemented, such as Xen, VMware. VMware is commercial software that implements full virtualization that has been developed in the University of Cambridge which is an open source project[13]. This research has Xen which is to be compared with different technologies in the past and it has been accepted as the trusted computing technology in this generation. Xen hypervisor has been used in many

commercial virtualization products; it acts as the engine of the Amazon Elastic Compute Cloud.

A Xen-based system is made up of several items that work together: hypervisor, dom0 , user-space tools,domU (guest VM). The Xen hypervisor abstracts the hardware for the virtual machines, controls the execution of virtual machines as they share the common processing environment. Dom0 is a privileged VM, it runs a full-fledgedoperating system, it is always booted by the hypervisor. Dom0 is used for platform management. Xen supports two kinds of virtualizations: paravirtualization and fully virtualization. Fully virtualization needs Intel VT or AMD-V hardware supports, it can provide better isolation between VMs without the need to modify guest operating system.In our work, we use fully virtualized Xen VMs. Every fully virtualized VM requires its own Qemu daemon, which exist in dom0. In the existing Xen architecture, dom0 takes full control of all virtual machines running on the same host. When evaluate the trustworthiness of the guest VM, dom0 have to be included in the Trusted Computing Base (TCB), this implies that the system administrator must be trusted, which impairs the usefulness of Xen in clouding computing [12].One of the key solutions to gaining the trust and make the cloud computing more secure is virtualization to accomplish data confidentiality for guest virtual machines. By applying this solution, even the infrastructure as service providers cannot access the private information of their customers. It is very important factor for the customers. The solution only emphasis on data confidentiality, Service provider can still easily control the availability and integrity of the customer‘s services and information. It can be apply by combining the machine virtualization technology with trusted computing technology to reach the privacy of the virtual machines; by running a customized operating system inside the Virtual machines, improve the costumer‘s data confidentiality against the service providers.[13]

VII. PRACTICAL APPLICATION

A. A Cloud Computing Example

Imagine a company called SoftCom that handles thousands of healthcare-related digital images of its clients. The images are sensitive and should remain private and confidential. SoftCom decides to use CloudX, a public cloud provider located in Boston, for

- image processing—using SoftCom’sImagePro software on a remote application server,
- additional image-processing tasks (filtering and searching) that ImagePro doesn’t support but that CloudX’siFilter and iSearch systems can perform, and
- Image archiving.

Note that in a public cloud, an enterprise can offload its computing tasks to the external cloud provider. In a private cloud, the computing services and resources remain within the perimeters of the enterprise’s private network, so the enterprise retains control of the computing tasks.6 A hybrid cloud is a combination of private and public computing.

In this example, SoftCom uses the hybrid model. It retains a private cloud for sensitive research activities to develop new image-processing and data-mining algorithms. Yet it also uses CloudX for other services.

At the CloudX site in Boston, ImagePro— hosted on an application server running in a Unix environment—processes images and stores them temporarily on a disk (Disk 1). CloudX then transmits the images to another cloud site located in Rome for additional processing by iFilter and iSearch. Next, it stores the images on another temporary disk (Disk 2). CloudX archives the processed images on Disks 3, 4, and 5, physically located in Caohang, Shanghai Its cloud infrastructure division manages these archives.SoftCom retains a private cloud for sensitive research activities but employs a public cloud for other services[7].

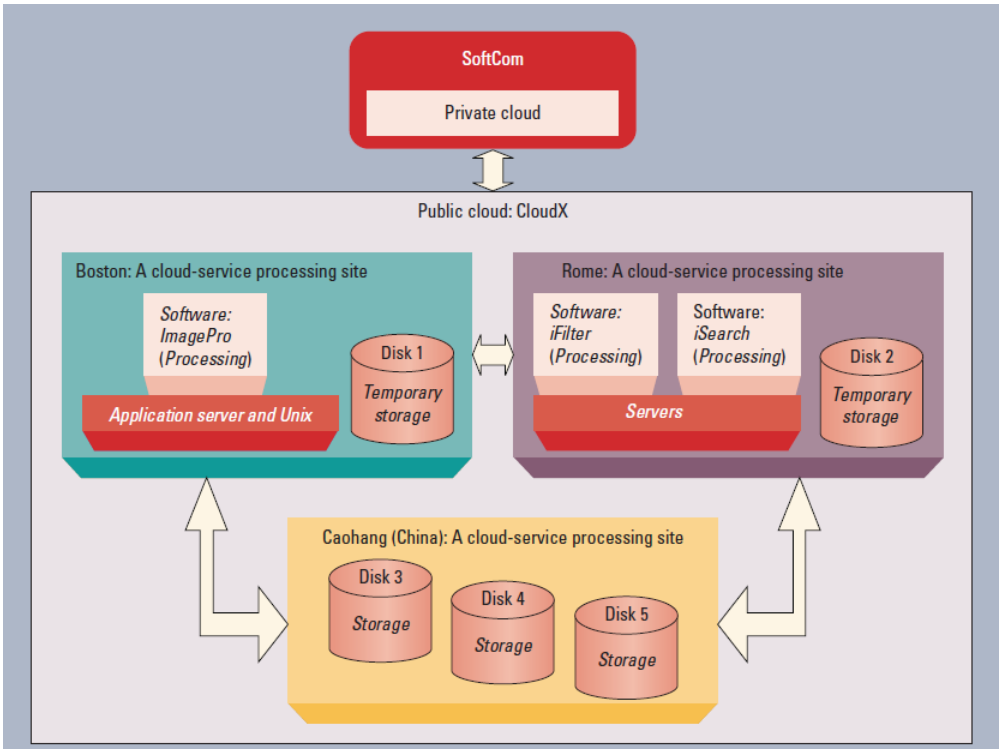

Figure 4.A hybrid cloud computing architecture.

This scenario suggests that SoftCom consumes three types of services (see Figure 1): platform as a service (PaaS), software as a service (SaaS), and infrastructure as a service (IaaS). In PaaS, consumers can build and deploy their applications on the cloud provider's platform as needed. In this case, SoftCom uses CloudX's application server and Unix platforms (in Boston) to deploy its ImagePro software. In SaaS, consumers use software services provided by cloud providers, such as email, payroll processing, and invoice generation. In this case, SoftCom uses CloudX'siFilter and iSearch systems. IaaS provides SoftCom with computing power and disk storage via CloudX's virtual environments. SoftCom can access the virtual servers and storageprovisioned on CloudX's physical infrastructure [6].

VIII. CONCLUSION

It is very important to note here that customers should be 100% confident about the services and interactions they have with their providers in term of security, integrity and trust. If customers would be assured that their special and important data are known to them alone and no one else knows not even the providers, they will do as much to make sure that all their data is been stored in the cloud instead of reserving some vital information to store in their data centres. Having said that, the architectural designs by Yao (2010) which has demonstrated that the three parties are not connected in any way because information are securely safe guarded. The client computer process sensitive data with encryption mechanism which the data is been transformed into two forms the cipher form and the key form. Then the cipher test form is then uploaded into SSP without the key form in this case the SSP would not be able to access the sensitive data uploaded by the client computer because of unavailability of the key form. The key form is been kept with the KMSP but it does not have the cipher text to do that. This has made this architecture to be secured and can develop trust in the minds of its customers [12].

Virtualization technology where even the providers are not eligible to have access to their customers'data this will bring comfort to the customers and the providers as well. Looking at the provider's side of view they usually feel that customers are looking at them as if they look into their data for spy and malicious attempt. Therefore, with the virtualization technology and trustworthy storage service (TSS) in place, trust will definitely be built in the minds of their customers and cloud business will grow appreciable level [9].

REFERENCES

[1] T. Mather, S. kumaraswamy, S.Latif, 2009. ―*Cloud Security and privacy: an Enterprise perspective on Risk and Compliance". Theory in Practice*,1ed, M. Loukides. Ed, USA: O'REILLY.

[2] RaduProdan and Simon Ostermann, "A Survey and Taxonomy of Infrastructure as a Service and Web Hosting Cloud Providers," in *10th IEEE/ACM International Conference on Grid Computing*, Banff, AB, Canada, 2009, pp. 17-25.

[3] Michael Boniface et al., "Platform-as-a-Service Architecture for Real-Time Quality of Service Management in Clouds," in *Fifth International Conference on Internet and Web Applications and Services (ICIW)*, Barcelona, Spain, 2010, pp. 155-160.

[4] A.Squicciarini, S.Sundareswaren, D.Lin, 2010.*" Preventing Information Leakage from Indexing in the Cloud"*, *IEEE 3rd International Conference on Cloud Computing*, pp. 188-195, USA: IEEE Computer Society.

[5] B. Michael, "In Cloud Shall We Trust?" *IEEE Security and Privacy*, Sept./Oct. 2009, p. 3.

[6] N. Riter, "VMware Unveils Security API," *Search Security*, Apr. 2009; http://searchsecurity.techtarget.com.au/articles/31679-VMware-unveils-security-API.

[7] B. Dournaee, "Taking Control of the Cloud for Your Enterprise," white paper, Intel SOA Expressway, June 2010.

[8] E. Chabrow, 2009,‖ *Rules Make doption of Cloud Computing Challenge for Agencies", [Online]* Available at: http://www.govinfosecurity.com/articls.php?art_id=1348 [Accessed 10th November 2010]

[9] Amazon, 2010. *"Amazon Elastic Compute Cloud (Amazon EC2",* [Online] Available at: http://aws.amazon.com/ec2/[Accessed 29 October 2010]

[10]H. Wei, F. Wang, 2010. *"Application of Cloud computing in the network learning environment"*, *International Symposium on Computational Intelligence and Design*, pp. 205-208, Hong Kong: IEEE Computer Society.

[11] Z. Whittaker, 2008. ―*Egnyte: using and sustaining Enterprise 2.0"*, [Online] Available at: http://blogs.zdnet.com/enterprisealley/?p=289 [Accessed 6th November 2010]

[12] G. Dhillon, S. Moores, 2001.*"Computer crimes: theorizing about the enemy within"*, In Computers & Security, volume 20, number 8, pp. 715-723.

[13] J. Kong, 2010. ―*A practical approach to improve the data privacy of virtual machines‖ 10th IEEE International Conference on Computer and Information Technology (CIT 2010)*, pp. 936-941, Bradford: IEEE Computer Society.

[14] Kelton, 2009. ―*Avanade: 2009 Global Survey of Cloud Computin",* [Online] Available at: http://blogs.msdn.com/b/architectsrule/archive/2009/03/03/avanade-2009-global-survey-of-cloud-computing.aspx/ [Accessed 21th November 2010]