

Migration of Services to the Cloud Environment: Challenges and Best Practices

Vikas Kumar
Asia-Pacific Institute of Management
3&4 Institutional Area, Jasola
New Delhi – 10025, India

Kavindra Kumar Garg
Institute of Management Studies
C-238, Lal Quan
Ghaziabad – 201009, U.P., India

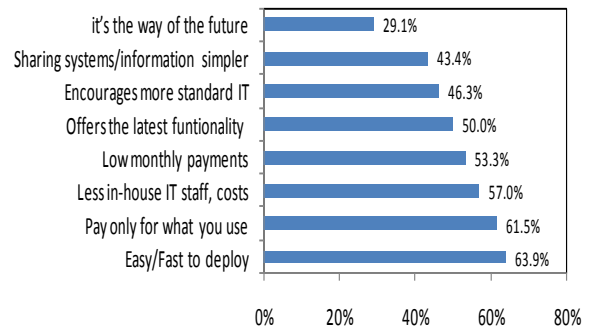
ABSTRACT

Cloud computing is coming-up as a new generation business paradigm with significant potential to increase the agility and lower the costs. Business people are looking for better ways to migrate their existing applications to a cloud-based infrastructure to enjoy the immense cloud potential. However, the security risks, lack of mature technology and standards, and other concerns prevent widespread enterprise adoption of external clouds. Companies are developing a cloud computing strategy based on growing the cloud from inside-out. Still, many applications are not suitable for hosting at external clouds. Hence, migration of services to the external cloud becomes a major issue whenever there is a paradigm shift. There are many key Challenges of Enterprise Cloud Computing like Data Governance, Manageability, Monitoring, Reliability, Availability and Virtualization. Present work discusses the major challenges towards the migration of services in cloud environment, considering both the public as well hybrid clouds. In order to signify the challenges, both technical and business issues have been considered. The best practices by IT giants have also been highlighted, considering the present day business environment.

Keywords: Cloud Computing, Migration of Services, Enterprise Computing.

1. INTRODUCTION

Cloud Computing [1-4] is widely recognized as a revolutionary IT concept that can fit the needs of diverse customers: from large enterprises to start-ups and end-users. It delivers a hosting environment that doesn't limit an application to a specific set of resources, but a set of pooled services is made available via internet. All the software applications and data is hosted on a server without the need for very high capacity memory or processors. This allows the usage of light weight client computers at the end user. In some cases, the client is simply a device equipped with a minimal Operating System and running a web browser. There are plenty of benefits for working with a cloud computing, and many out weigh the reasons why not to use cloud computing. The IDC Enterprise Panel (2008) has outlined the eight most important benefits of the Cloud Computing as shown in Fig. 1.



Source: IDC Enterprise Panel (August 2008)

Fig. 1 Benefits of the Cloud on-demand Model

Switching from the traditional, own and operate model to a service model involves replacing existing licenses with new license that include service level agreements (SLAs). However, existing SLAs can not successfully guarantee performance levels. Depending on the platform, an application can scale dynamically and increase its share of resources. It seems that everyone in this industry, from experts to cloud providers, have their own definition about what the cloud computing is? Still, there is no consensus on, what exactly this term means? Examining some of the existing definitions helps to clarify the term and what it involves?

“A Cloud is a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements established through negotiation between the service provider and consumers” - Buyya, Yeo, and Venugopal [5]. A number of most prominent definition have been given by, NIST [6], Forrester Research[7] and Gartner [8]. Cloud Computing promises to deliver the Information Technology as ‘services’ in most cost effective manner. Although cloud enabled services are certainly not the simplest solution for every technology challenge, yet they are maturing rapidly and offer a lot of game changing business opportunities. The services offered by cloud may range from infrastructure to communication and software, depending upon the particular service model and deployment model of the cloud.

1.1 Cloud Computing Service Models

Cloud computing can be classified by the model of service, it offers in different groups. The general description is given by the XaaS taxonomy, first used by Scott Maxwell in 2006, where “X” stands for Software, Platform, or Infrastructure, and the final “S” stands for Service. The three basic service models can be categorized as:

(a) Infrastructure as a Service (IaaS)

The capability provided by IaaS is in the form of raw storage space and computing, or network resources with which the customer can run and execute an operating system, applications, or any software that they choose. The cloud customer is not able to control the distribution of the software to a specific hardware platform or change parameters of the underlying infrastructure, but the customer can manage the software deployed (generally from the boot level upward). Various companies are providing IaaS like Amazon, Cisco, Proofpoint, RightScale, 3Leaf Systems, 3PAR, 10Gen, Adaptivity and many more.

(b) Platform as a Service (PaaS)

In case of PaaS, a development platform is provided in the cloud environment. This may include a development toolkit and a number of supported programming languages to build higher level services. The users of PaaS are typically the software developers, who host their applications on the platform and provide these applications to the end-users. Google App Engine is a good example of PaaS, which provides a web development platform and is very popular among the developers. A number of companies are providing Platform as a Service such as Salesforce.com, Microsoft Azure Service Platform etc.

(c) Software as a Service (SaaS)

SaaS is the most commonly used application of Cloud computing. The SaaS customer is an end-user of complete applications running on a cloud infrastructure and a wide variety of SaaS services are available from different vendors. The applications are typically accessible through a thin client interface, such as a web browser. The customer does not control either the underlying infrastructure or platform, other than application parameters for specific user settings. A number of companies are providing such software application. Salesforce.com, Google, Workday, Proofpoint, Rackspace Email & Apps, SAP Business ByDesign, Rackspace, American Data Technology, Gogrid, WebECS and Vembu Technologies are good examples. Cloud based software services have a great market potential and their share is increasing day by day. As per the Deloitte Consulting Report [9], the share of SaaS will significantly grow in the application like Content Communication and Collaboration (CCC), Customer Relationship Management (CRM), Integration as a Service (IntaaS), Enterprise Resource Planning (ERP), Supply Chain Management (SCM) and Digital Content Creation (DCC). The report has predicted the numbers for next five years as shown in Fig. 2.

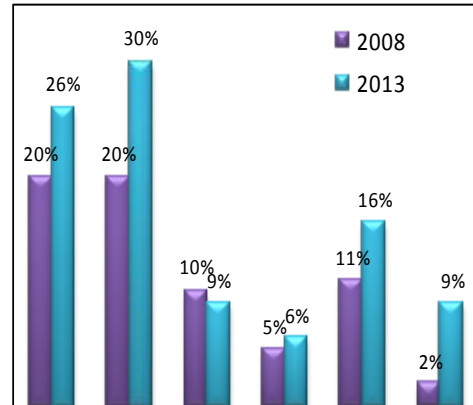


Fig.2 SaaS Share in the Enterprise Application

Cloud Platforms can also be classified based upon the underlying infrastructure deployment model as Public, Private, Community, or Hybrid Clouds [10]. Different infrastructure deployment models are distinguished by their architecture, location of the datacenter where the cloud is realized, and also in accordance with the customer needs.

Private Cloud

The cloud infrastructure is operated solely for an organization in case of the Private Clouds. However, it may be managed by the organization itself or a third party and may exist on premise or off premise.

Public Cloud

The Public Cloud infrastructure is made available to the general public or a large industry group and is generally owned by an organization selling cloud services. Resources are dynamically provisioned on a fine-grained, self-service basis over the Internet, via web applications/web services. The third-party provider is responsible for provisioning of the resources as well as usage billing.

Hybrid Cloud

The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

2. MIGRATION TO CLOUD COMPUTING

Some Cloud based applications, such as Gmail, had a great success; but as the diversity of the offerings grows, it increases the reluctance to trust the sensitive data and services on off-site computers. At the enterprise level, in a number of cases, the decision makers keep rejecting a move to the cloud [11]. At present most organizations are only willing to outsource applications that involve less sensitive information. According to a survey [12] of more than 500 chief executives and IT managers of 17 countries, “trust is more with the existing internal systems over cloud-based systems due to the fear about security threats and loss of control of data and systems”. Those who agree to move to the cloud still demand third party risk assessments or at least ask the cloud providers:

- Who will have access to the data and applications and how will that be monitored?
- What security measures are used for data transmission and storage?
- How the applications and data from different customers are kept separate?
- Where, in terms of geographical location, will be the data stored? Could the choice of the location affect me?
- Can these measures and details be stipulated in a service level agreement?

All these customer worries can be translated into what can be identified as the main obstacle to the adoption and growth of cloud computing. The unpredictable nature of cloud computing workloads requires that clouds be architected for extremely high levels of efficiency, service-level availability, scalability, manageability, security, and other systemic qualities. The most important challenges to the Cloud Computing Model, as outlined by IDC Enterprise Panel (Aug, 2008) are shown in the Fig. 4

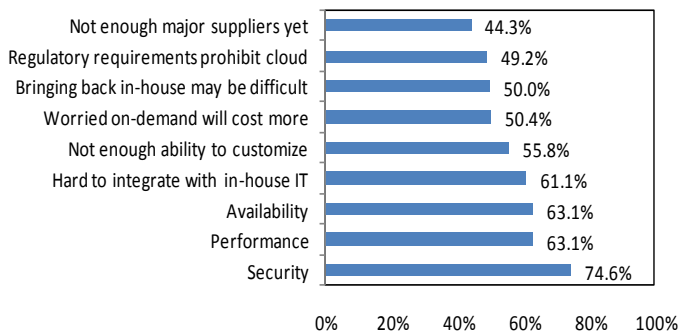


Fig. 3: Challenges the Cloud On-Demand Model

Source: IDC Enterprise Panel, August 2008

Initially, the cloud computing platforms appear to be attractive for their low-cost development and deployment capabilities. But as the cloud platforms are used for actual production environments, they require enterprise-level SLAs. Maximizing systemic qualities require integrating the development of these qualities into the design process of large-scale architectures. For cloud computing, the focus of systemic qualities is different from the host-based, client-server models and Web-based models of the past. In some ways the challenge to achieve systemic qualities is more complex. On the other hand, if these architectures are properly designed from the beginning, this can lead to the perfect systemic qualities. Each of these obstacles can be classified as the technical or business issues, both of these aspects must be taken care of, for smooth migration to the Cloud environment.

2.1 Technical Issues

Availability of Service

Outages of a service become a major worry when customers have stored all of their information in the cloud and might need it at anytime. Given that the customer management interfaces of public clouds are accessible via Internet, there is

an increased risk of failure when compared to traditional services. In fact, there are more weak points in the chain of elements needed to access the information or application. For instance, web browser vulnerabilities can lead to service delivery failures. A feasible means to obtain a high degree of availability would be using multiple cloud computing providers. Cloud providers are well aware of these risks and today provide more information about the current state of the system, as this is something that customers are demanding. Salesforce.com [13] for instance shows the real-time average response time for a server transaction at Trust.salesforce.com. Amazon has implemented a service dashboard that displays basic availability and status history.

Data Lock-In

As some people, such as GNU creator Richard Stallman have advised [14], the use of proprietary cloud-based applications could end up in situations where migration off the cloud to another cloud or to an in-house IT environment would be nearly impossible. The reason for the current poor portability and limited interoperability between clouds is the lack of standardized Application Programming Interfaces (APIs). As a consequence migration of applications between clouds is a hard task. There are plenty of examples for the same, Amazon reaches into customers' Kindles and remotely deletes already-purchased books. Facebook launches Beacon, an advertising mechanism that collects and publishes information about what is being done on external web sites on your Facebook profile (only to apologize and offer opt-out later). Apple denies approval for the Google Voice application in the App Store. MySpace and Facebook don't immediately remove photos from their servers when you delete them. Thus, living in the cloud, allows a third party to make decisions about your own data and platform. Google is truly advancing to achieve a more standard environment and they even have an initiative, called Data Liberation Front [15], to support users moving data and applications in and out of their platform.

Privilege Abuse

The threat of a malicious insider with a privileged role (e.g. a system administrator) is inherent to any outsourced computation model. Abuse by insiders could impact and damage the customer's brand, reputation, or directly damage the customer. Although this kind of attack can in a traditional (i.e., non-cloud) computing infrastructure, still customers have a lot of concerns for the cloud provider. Cloud customers should conduct a comprehensive assessment of access privileges (i.e. stating who will have access to their data and what level of access they will have) as well as transparency measures. Availability of an additional trust system will be of great use as this will significantly reduce the risk of user's blind trust [16].

Resource Scaling

Ability of scaling up or down the resources to meet the workload is one of the most desired cloud computing advantages. However, this great advantage can lead to service failures, if it is not well implemented or if a maximum response time is not agreed upon in advance. A web application developer hosting services on a cloud may see how the response time steadily increases with the usage of application - because the scaling-up of resources is not so quick by the cloud. On the other hand, scaling must be limited by some threshold. This threshold would stop the continuous increase in the allocation of resources to prevent the cloud provider from a denial of service attack. In either case, the

customer could be billed for service that they did not want. Existing service level agreements determine quality of service requirements, but not in terms of response time with workload variations. Hence, the scaling remains a big challenge to the cloud providers.

Data Governance

The distributed nature of the Cloud Model, necessarily involves more transits of data over networks. Thus, Data Handling offers new challenging security risks. The confidentiality of the data must be assured whether it is at rest (i.e. data stored in the cloud) or in transit (i.e. to and from the cloud). It would be desirable to provide a closed box execution environment, where the integrity and confidentiality of the data could be verified by its owner. While encryption is an answer to securely storing data in the cloud, it does not fit well with cloud-based processing. In most cases, the data has to be decrypted at some time when it is inside the cloud. Some operations would be impossible with encrypted data and, also the computations with the encrypted data would consume more computing resources, hence increasing the expenses.

There are recent steps towards dealing with this issue and a number of corporate initiatives have come. One is the Trusted Cloud Computing Platform [17], which aims to apply the Trusted Computing model (developed in 2003 by Intel, AMD, HP, and IBM) to the cloud. However the scope of this initiative is to protect against malicious insiders, in the cloud provider organization. Another project of the Microsoft Cryptography Group is a “searchable encryption mechanism” introduced by Kamara and Lauter in [18]. The underlying process in this system is based on a local application, installed on the user’s machine and these user machines are generally composed of three modules (data processor, data verifier, and a token generator). The user encrypts the data before uploading it to the cloud. The enterprise version of the solution consists of adding a credential generator to simplify the collaboration process. Other relevant projects are also being conducted. One example is a recently published PhD dissertation from Stanford University done by Craig Gentry in collaboration with IBM [19]. This research proposes “A fully homomorphic encryption scheme”, through which the data can be searched, sorted, and processed without decrypting it. This is certainly an innovative refreshing mechanism necessary to maintain low levels of noise.

Although the present initiatives are too slow to have high efficiency, which limits their commercial utilization in the present scenario. In addition to the topology of the cloud network, the geographic location of the data also matters in some cases. Knowing the data location is fundamental to secure it, as there might be important differences between regulatory policies in different countries. Cloud computing customers must tackle this issue by understanding the regulatory requirements for every country, they will be operating in. Not only the data location, but the path followed by data also matters. According to Forrester’s “Cloud Privacy Heat map” [20], this is really hard for an application operator to deploy applications at a minimum “distance” from the user. In the latest report of European Network and Information Security Agency (ENISA) [21], it has been suggested that the level of this risk would be considerably lower if the encryption is applied to data at rest. This can be highly significant for the cloud computing environment.

The “Offline Services”

Being completely dependent upon an Internet connection might turn out to be impossible or highly risky for some users who need an application (or data) to be available at all times. This creates a bigger problem if the user is moving and the quality of the connection can change. Hence in some situations, relying on Internet service provider is simply not an option. The so-called “Pure Cloud Computing Model” causes this impediment. This model is based on the fact that the most commonly used software application is the web browser and complete applications can be delivered as a service through the Internet. Thus all of the end-user’s interaction can occur through a web browser. Some independent software vendors are developing web desktop offerings, such as the eyeOS [22]. In this pure Cloud model, losing connectivity to the cloud is a major problem because it means that the local computer becomes almost useless. HTML5 [23] is new version of the HTML, that addresses the offline issue with a couple of elements: AppCache and Database. These elements provide methods to store application data locally on a user’s computer in amounts beyond what can be stored in an HTTP cookie. Hence, adding to the offline work.

Unpredictable Performance

One of the main features of any Cloud Computing Service is the level of abstraction from the underlying physical infrastructure. The end user is unaware about the location of the hardware. The only source of information the user has about these servers is the hardware specifications provided by the cloud provider for each type of service. Moreover, the hardware metrics could not have the same meaning in a cloud server as they did in a traditional server, because the users may be sharing computing and I/O resources at a given instance of physical processor. Users expect always the same performance for the same money, but this could simply not be true as the performance depends on various factors and most of them are not under the control of the end user. In fact, this is currently a main concern that enterprise customers have about cloud computing, according to a survey by IDC [24]. Cloud Computing’s economic benefits are based on the ability to increase the usage level of the infrastructure through multi-tenancy, but it is not clear that one user’s activity will not compromise another user’s application performance. On top of that, the latency to the datacenter, where the server is hosted, along with other network performance parameters, could vary as a function of the time of day, the particular location of the current servers, and the competing traffic in the communication links. Therefore, the performance might not be as per expectations and could fluctuate. This variance in performance may cause a problem if the customer is unable to predict these variations, their magnitude, and duration - as the price remains deterministic.

2.2 Business Issues

Manageability

There are some great IaaS/PaaS implementations, including Amazon’s web services (S3, EC2, EBS, etc), Google’s App Engine, Salesforce’s Force.com, Joyent, etc. However, most of these are being offered as raw infrastructure and platforms having little management capabilities. Throughout the computing history, raw capabilities generally appear on the market first, then only the management of these capabilities become a differentiator with competition. Just look at the blade server and virtualization spaces as these are great

examples of that trend. The hypervisor is a key technology that enabled enterprise virtualization; however, that piece is now being given away (e.g. VMware's ESXi) and management capabilities become the main differentiator. Cloud computing is no different. An example of missing management capabilities for cloud infrastructures is auto-scaling. Amazon EC2 claims to be elastic; however, it really means that it has the potential to be elastic. Amazon EC2 will not automatically scale your application as your server becomes heavily loaded. It is still up to the developer to manage that scalability problem. Many startups have recognized the need for management early on and have built management capabilities on top of the existing cloud infrastructure/platforms. RightScale is one of the early pioneers in this space. Their solution solves many of the management issues such as auto-scaling and load balancing.

Monitoring

Monitoring, whether is for performance or availability, is critical to Information Technology. This not only talks about the CPU or memory but also about the performance of transactions, disk I/O and others. CPU and memory usage are misleading most of the time in virtual environments. The only real measurement is how long time the transactions are taking and how much is the latency [25]. Amazon found every 100ms of latency cost them 1% in sales. [26] Google found an extra .5 seconds in search page generation time dropped traffic by 20%. A broker could lose \$4 million in revenues per millisecond if their electronic trading platform is 5 milliseconds behind the competition [27]. Hypernic's CloudStatus is one of the first to recognize monitoring issue and developed a solution for it. They started with monitoring of Amazon's web services, and then recently added monitoring for Google App Engine. In addition, RightScale's solution can also provide monitoring for the virtual machines under their management.

Virtualization Security

Security is a huge area that encompasses many different things, including the standard enterprise security policies on access control, activity monitoring, patch management, etc. Typically, security improves with the centralization of data and increased security-focused resources, so cloud computing raises concerns about loss of control over certain sensitive data. Accesses are typically logged, but accessing the audit logs themselves can be difficult or impossible. Many companies address the challenges with a range of innovations. On top of that, virtualization security is something that the innermost enterprises to. Many IT people still believe that the hypervisor and virtual machines are safe. However, it becomes a big consideration for moving to the cloud. For security, there are quite a few startups like Reflex, Blue Lane and Catbird that are creating privileged VAs that claim to protect the VAs running on VMware's ESX servers. There are other startups, which are creating interesting solutions in protecting the actual virtual infrastructure themselves, e.g. how do you protect and monitor access to the ESX servers? how do you control and monitor the movement of virtual machines using live migration or VMotion?

Economy Vs Efficiency

Efficiency and Economy are the success paths to any technology and same applies to the Cloud Computing as well. The "green"-computing movement with energy-efficient CoolThreads™ technology [28] and the use of printed circuit boards using far less hazardous materials have saved millions

of dollars in the energy costs alone. There are a number of low-cost initiatives, which are offering a lot of innovation in (a) Datacenter Design (b) Hardware (c) Operating System and (d) Software Components to provide economy benefits. Also, the use of open-source software and virtualization technologies in all aspects of product design and development enables large numbers of servers to function more efficiently and saves costs on energy, cabling, HVAC etc. to reduce the capital expenditures (in the infrastructure owned by the provider). The major factors that add to the cost for an enterprise are:

- Resources, including the use of VM instances and processing
- Data storage, including the cost of virtual images and input data.
- Data transfer, including charges for transferring input data into the cloud, and
- Transferring output data and log files between the submit host and a Cloud.

Reliability

Due to redundancy in the SaaS and PaaS configurations, we can increase reliability. With cloud computing systems like AppLogic offering highly reliable storage as part of the package, many customers are tempted to skip backup. But, data loss and the resulting unplanned downtime can result not just from failures in the cloud platform, but also from software bugs, human error, or malfeasance such as hacking. If you don't have a backup, you'll be down a long time - and this applies equally to cloud and non-cloud solutions. The advantage of cloud solutions is that there is usually an inexpensive and large storage facility coupled with the cloud computing offering, which gives convenient backups. In Cloud Computing facilities are identical and transactions are mirrored almost instantly, making interruption of service related to hardware problems or data issues virtually impossible. If one of these facilities goes down (e.g. because of a natural disaster), the applications will run on the other site with minimal interruption.

3. CONCLUSIONS

Cloud Computing has tremendous business potential, still has many implicit limitations that could restrict its usefulness. A number of technical and business issues put boundaries on the adoption and growth of cloud computing. Service Level Agreements become most complex, when offering applications as a service. The current state of SLAs in cloud computing is inadequate and there is a need for fine-grained specifications with enhanced performance parameters than simply the resource availability. Cloud Computing is ready to successfully host the most typical web applications with great cost savings, but the applications with (a) strict latency requirements (b) large datasets, (c) strict needs for availability, are critical to the success of Cloud Migration. Even with the evolution of SLAs, all-purpose clouds might not be willing to offer guarantees for the most demanding applications Hence, the compensation models for violation of the SLA is also very crucial. In order to offer best migrated services, consideration of specific performance requirements is highly important for each deployment and service model. This however, offers an excellent opportunity for clouds targeted and designed for particular workloads. The issues discussed in the paper are certainly of great concern for

migration of services and hence the work will be a guiding path to the present day migration scenario.

4. REFERENCES

- [1] Borko Furht, “ Cloud Computing Fundamentals”, In Furht and Zhu (Ed.), Handbook of Cloud Computing, New York : Springer, 2010 pp. 3-20
- [2] Jinzy Zhu,“ Cloud Computing Technologies and Applications”, in Handbook of Cloud Computing : Furht and Escalante, New York : Springer,2010 pp. 21-46
- [3] John w. Rittinghouse and James F. Ransome, Cloud Computing: Implementation, Management and Security, Florida: CRC Press, 2010
- [4] <http://computinginthecloud.wordpress.com/2008/09/25/utility-cloud-computingflash-backto-1961-prof-john-mccarthy/>, [Accessed Jan 5, 2009].
- [5] R. Buyya, C.S. Yeo, and S. Venugopal, “Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities,” Proceedings of 10th IEEE International Conference on High Performance Computing and Communications, 2008. (HPCC’08), pp 5–13.
- [6] Mell and T. Grance. “The NIST definition of cloud computing.” National Institute of Standards and Technology, 2009.
- [7] J. Staten, “Is cloud computing ready for the enterprise?” Forrester Research, March, 7, 2008.
- [8] DC Plummer, TJ Bittman, T. Austin, D. Clearley, and DM Smith. “Cloud computing: Defining and describing and emerging phenomenon,” Gartner, Inc., 2008.
- [9] Market overview and perspective consulting Cloud Computing Forecasting change by Patrick Callewaert, Paul A. Robinson and Peter Blatman-Deloitte Consulting October 2009
- [10] DC Plummer, TJ Bittman, T. Austin, D. Clearley, and DM Smith. “Cloud computing: Defining and describing and emerging phenomenon,” Gartner, Inc.,2008.
- [11] Kelton Research. Survey: Cloud Computing "No Hype", but fear of security and control slowing adoption. <http://tv.sys-con.com/node/852659>
- [12] <http://www.gartner.com/technology/research/cloud-computing/>, [Accessed Sep 22, 2010]
- [13] Salesforce. <http://www.salesforce.com/> [Accessed September 19, 2010]
- [14] GNU founder Richard Stallman. <http://www.guardian.co.uk/technology/2008/sep/29/cloud.computing.richard.stallman>.
- [15] <http://www.dataliberation.org/> [Accessed Oct 22, 2010]
- [16] John W. Rittinghouse and James F. Ransome “Cloud Computing Implementation, Management, and Security” CRC Press.
- [17] N. Santos, K.P. Gummadi, and R. Rodrigues. “Towards trusted cloud computing:” Proceedings of Conference on Hot Topics in Cloud Computing, 2009, p.3
- [18] S. Kamara and K. Lauter, “Cryptographic cloud storage. Financial Cryptography and Data Security”, pp 136–149, 2010.
- [19] C. Gentry. A fully homomorphic encryption scheme. PhD thesis, Stanford University, 2009.
- [20] Cloud privacy heat map. Forrester Inc. [<http://www.forrester.com/cloudprivacyheatmap,2010>]
- [21] D. Catteddu and G. Hogben. Cloud computing: benefits, risks and recommendations for information security. Technical report, European Network and Information Security Agency, 2009.
- [22] EyeOS. Cloud computing operating system. <http://eyeos.org/>.
- [23] <http://latimesblogs.latimes.com/technology/2009/11/google-gears.html>, 2009. [Accessed Nov 15, 2010]
- [24] IDC IT Cloud Services. <http://blogs.idc.com/ie/?p=730>, 2009. [Accessed Nov15, 2010]
- [25] William Stallings. Data computer Communication 7th ed. LPE Prentice Hall imprint of Pearson 2006 New Delhi.
- [26] <http://aws.amazon.com/ec2-sla/> .[Accessed Nov 22, 2010]
- [27] G. Wang and TSE Ng, “The impact of virtualization on network performance of amazon EC2 data center” Proceedings of IEEE INFOCOM, 2010, pages 1–9
- [28] <http://cloudcomputing.sys-con.com/node/160275> .[Accessed Nov 30, 2010]