# CLOUD COMPUTING CHALLENGES WITH EMPHASIS ON AMAZON EC2 AND WINDOWS AZURE

Azzam Sleit*, Nada Misk[1], Fatima Badwan[1], Tawfiq Khalil[2]

1 Department of Computer Science, KASIT, The University of Jordan, P.O. Box 13898, Amman 11942, Jordan
2 Department of Computer Science, Oakland University, Michigan, USA
* On Sabbatical leave from The University of Jordan

azzam.sleit@ju.edu.jo, nada.misk@ju.edu.jo, fbadwan@ju.edu.jo, tawfiq_khalil@yahoo.com

## *ABSTRACT*

*Cloud Computing has received much attention by the IT-Business world. As compared to the common computing platforms, cloud computing is more flexible in supporting real-time computation and is considered a more powerful model for hosting and delivering services over the Internet. However, since cloud computing is still at its infancy, it faces many challenges that stand against its growth and spread. This article discusses some challenges facing cloud computing growth and conducts a comparison study between Amazon EC2 and Windows Azure in dealing with such challenges. It concludes that Amazon EC2 generally offers better solutions than Windows Azure. Nevertheless, the selection between them depends on the needs of customers.*

## 1. INTRODUCTION

Cloud Computing is a newly proposed model for hosting and delivering computing services over the web. It refers to the applications delivered as services over the Internet [1] [2] as well as hardware and systems software in the datacenters providing computing services. Cloud Computing is an attractive concept since it eliminates the provisioning planning requirements. It also allows enterprises to start up with fewer resources to serve the existing needs and to grow gradually in response to increasing demands. For example, suppose that an enterprise has an immediate need and the required budget to deploy and maintain an internal application within a short period of time [3] [4]. Although IT hosting teams understand the requirement, deploying applications typically require extensive coordination between hardware, software, operation and support teams. The procurement phase for the required hardware and operating system setup may require several months. Application configuration and testing, building the required operation procedures and moving to production environment are major challenges and may not have the enterprise support and operations quality [5].

The main challenges that an enterprise has in deploying an application are not in the application itself but in the prerequisites and procedures involved in providing the infrastructure required for deployment and maintenance. When cloud computing is implemented, the need for the application hosting team to depend on the hardware team is reduced, because hardware is encapsulated and provided by cloud computing data centers. If the dependencies on servers, load balancers, routers, and switches are eliminated, the application hosting team can focus solely on deploying the application in the cloud service provider of its choice, with business approval [6].

DOI : 10.5121/ijcnc.2013.5503

Cloud computing can be viewed as a scalable, adaptable, and elastic information technology service provisioning to multiple users. End users are usually not interested in any information about the location of resources, data stores, or any technical issues related to infrastructure. On the other hand and since the development of cloud computing technology is currently at its infancy, there are many challenges facing the growth of cloud computing. This article discusses some of these challenges, and offers a comparison between two of the most popular cloud services providers in how they faced these challenges.

Section 2 by provides an overview of cloud computing and its architecture. Section 3 explains a suggested business model for cloud computing. Then, section 4 looks deeper into the challenges and opportunities facing cloud computing provides by highlighting the two main providers: Amazon EC2 and Microsoft Windows Azur. Section 5 concludes this article.

## 2. OVERVIEW OF CLOUD COMPUTING

Cloud computing is a business term for technologies intended to provide application hosting and storage services without requiring the awareness of the end-user for the physical location and configuration of the system providing the services. It refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services. A *Cloud* consists of the datacenter hardware, software and communication which can be public or private. A *Public Cloud* is made available to anyone in a pay-as-you-go manner. However, a *Private Cloud* refers to a datacenter of an enterprise which in not accessible to the public. When part of the service is rendered by a private cloud whereas the remaining part is served by a public cloud, we call this model: a *Hybrid Cloud* [7].

*Grid Computing* and *virtualization* are perhaps the most obvious predecessor technologies that enabled the inception of cloud computing. *Grid computing* is a distributed computing model which manages interconnected computing resources to accomplish a certain computational objective [8]. *Virtualization is* a technology that hides the details of physical hardware including CPU and memory allocation in order to provide abstracted resources for high-level applications. Virtualization is a basic component for establishing low-maintenance platforms for cloud services. This is because a virtualized platform can be portable and scalable without any dependency on the underlying infrastructure. It allows multiple operating systems to be executed on the same machine at the same time and detaches the applications from the operating systems. Virtualization and the dynamic migration of virtual machines allow cloud computing to make the most efficient use of the currently available physical resources. A virtual machine (VM) is typically a virtualized server. Virtualization is the basis of cloud computing since it seamlessly allows applications to dynamically utilize computing resources from pools of servers.

The architecture of a cloud computing environment can be divided into 4 layers; namely, hardware layer, infrastructure layer, platform layer and application layer, as shown in Fig. 1. The Hardware Layer includes the physical resource of the cloud, such as routers, switches, servers, power and cooling systems. Some issues associated to the hardware layer are hardware configurations, fault-tolerance, traffic management, power and cooling resource management.
The Infrastructure Layer is also known as the Virtualization Layer. Using virtualization technologies, the Infrastructure Layer creates a collection of storage and computing resources by partitioning the physical resources [8]. This layer provides the core middleware capabilities like data stores, messaging, etc., as on-demand services [9].

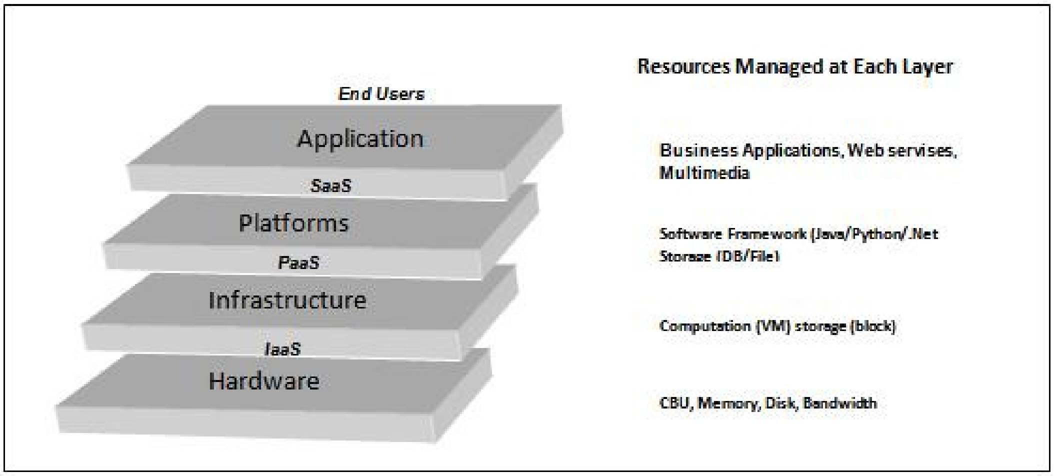
Resources Managed at Each Layer
End Users
Application
SaaS
Platforms
PaaS
Infrastructure
IaaS
Hardware
Business Applications, Web servises, Multimedia
Software Framework (Java/Python/.Net Storaze (DB/File)
Computation (VM) storage (block)
CBU, Memory, Disk, Bandwidth

Figure 1. The layered model of cloud computing

The Platform Layer is built on top of the Infrastructure Layer and consists of operating systems and application frameworks. It facilitates the deployment of applications without the cost and effort of purchasing and managing the underlying hardware and software layers. The purpose of the platform layer is to minimize the trouble of deploying applications into the virtual machines containers. Platforms allow developers to write applications that run in the cloud and/or utilize services provided by the cloud. The Application (Software) Layer is at the highest level of the hierarchy and is the most visible layer to the end-users of the cloud since it consists of the actual cloud applications. Such applications can leverage the automatic-scaling features to realize better availability, performance, and lower operating cost. Users access the services provided by the Application Layer through web-portals which may require fees.

## 3. BUSINESS MODEL

Cloud computing employs a service-driven business model, where hardware and platform-level resources are provided as services on an on-demand basis. A layer of the architecture described in Figure 1 can be implemented as a service to the layer above and may be viewed as a customer of the layer below. Practically, clouds offer services that can be grouped into three categories; namely, software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) [8][10]. IaaS refers to on-demand provisioning of infrastructural resources, usually in terms of VMs. A customer of IaaS is provided storage space, computing, or network resources in order to run and execute platform systems, or applications. Cloud customers are usually unable to control the distribution of software to specific hardware platforms or change parameters of the underlying infrastructure [11]. The cloud owner who offers IaaS is called an IaaS provider.

In the case of PaaS, the cloud provider provides hardware, and other platform layer resources such as operating system support, software development toolkits and selected programming languages to build higher level services. The users of PaaS are typically software developers who host their applications on the platform to provide services for end-users [11].

SaaS refers to providing the services of applications over the web on as needed basis. Customers are end-users of complete applications running on a cloud infrastructure and may only control application parameters for specific user settings [8][10]. The applications are typically accessible through thin-client interfaces, such as web browsers. PaaS and IaaS providers are often called the infrastructure or cloud providers. It is entirely possible that a PaaS provider runs its cloud on top of an IaaS provider's cloud. However, both IaaS and PaaS providers are often part of the same enterprise.

# 4. CHALLENGES AND OPPORTUNITIES OF CLOUD COMPUTING PROVIDERS

Here, we have a closer look into two of the most famous infrastructure providers; namely, Amazon EC2 and Microsoft Windows Azur. Amazon is the largest online retailer in the world which supports its operations through one of the most advanced data centers in the world. Processing millions of transactions daily requires an infrastructure that provides reliability and speed with minimum cost of a transaction. Amazon has established a powerful data center infrastructure supporting virtualized operating systems and storage servers. Amazon utilized its investment in the data centers by renting this platform and storage services to developers for developing and hosting applications [6]. Amazon's cloud services offerings consist of five services: Elastic Compute Cloud (EC2), SimpleDB, Simple Storage Service (S3), CloudFront, Simple Queue Service (SQS) and Elastic MapReduce.

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizable compute capacity in the cloud. It is designed to make web-scale computing easier for developers. Amazon EC2's simple web service interface allows customers to obtain and configure capacity with minimal effort. It provides customers with total control of computing resources and lets them run on Amazon's resilient computing environment. Amazon EC2 reduces the time required to obtain and boot new server instances to minutes, allowing customers to quickly scale capacity, both up and down, as computing requirements change [12]. Amazon EC2 changes the economics of computing by allowing customers to pay only for the resources that customers actually use. Amazon EC2 provides developers the tools to build failure resilient applications and isolate themselves from common failure scenarios.

In 2008, Microsoft announced its official entry into the cloud services business with the Windows Azure platform (previously known as Azure Services Platform). The Windows Azure platform is an attempt to create an end-to-end cloud service offering in the platform, middleware, enterprise services, and consumer services categories. Windows Azure consists of three main components: Windows Azure, SQL Azure, AppFabric (previously known as .NET Services) [6]. Windows Azure is the operating system in the cloud, and it forms the core platform for all the other Azure services. SQL Azure is the database engine in the Windows Azure Platform. AppFabric is the middleware component that consists of services like ServiceBus and Access Control.

The main challenges that face the providers of cloud computing have emerged from different customer worries about the mystery of this concept. Cloud computing is widely recognized as a revolutionary information technology concept and with different offerings that can fit the needs of different kinds of customers. Some enterprises still have fears to move to the cloud computing. According to a survey of more than 500 executives and IT managers of 17 countries, they still trust existing internal systems over cloud-based systems due to the fear about security threats and loss of control of data and systems [11]. In this article, we discuss the challenges identified and recognized in the literature; namely, availability or continuity of service, resource scaling, data deletion, data lock-in and data security [13].

## 4.1 Availability

Organizations worry about whether utility computing services have sufficient availability. Given that the customer management interfaces of public clouds are accessible via the web, there is an increased risk of failure when compared to traditional services. A high degree of availability can be achieved by using multiple cloud computing providers.

Amazon EC2 provides two features to realize availability; namely, *Availability Zones* and *Elastic IP Addresses.* Amazon has thought about ensuring availability despite disastrous failures such as power-cut on data centers or destruction by fire or floods. Copies of the application should be located on separate infrastructures which are physically located in different geographic sites. Thus, Amazon has recently announced Availability Zones. The point of availability zones is the following: if customers launch a server in zone A and a second server in zone B, then the probability that both go down at the same time due to an external event is extremely small [14]. This simple property allows customers to construct highly reliable web services by placing servers into multiple zones such that the failure of one zone doesn't disrupt the service or at the very least, allows customers to rapidly reproduce the service in the second zone.

Amazon EC2 locations are composed of regions and availability zones. Availability zones are distinct locations that are engineered to be insulated from failures in other availability zones and provide inexpensive, low latency network connectivity to other availability zones in the same Region [12]. By launching instances in separate availability zones, customers can secure their applications from failure of a single location. Regions consist of one or more availability zones which are geographically isolated. The Amazon EC2 Service Level Agreement commitment guarantees 99.95% availability for each Amazon EC2 Region [15].

Elastic IP addresses are static IP addresses designed for dynamic cloud computing. Elastic IP addresses are associated with a customer account and allow the customer to perform dynamic mapping of an IP address to a specific instance [14]. Applications can still be reachable even in the presence of failures using the described mapping.

Windows Azure enables users to build and run highly available applications without focusing on the infrastructure. Client libraries are available for multiple programming languages and the storage provides easily accessible storage services that remain highly available and durable. Windows Azure Blobs, Tables and Queues are replicated three times in the same data center to increase resiliency against hardware failure. In order to increase availability, data is replicated over several domains. At no additional cost to the users, Windows Azure Blobs and Tables are also geo-replicated between two data centers hundreds of miles apart from each other on the same continent.

All storage services are accessible via REST APIs. Storage services may be accessible from within a service running in Windows Azure, or directly over the web from any application that can send an HTTP/HTTPS request and receive an HTTP/HTTPS response [16]. In addition to using storage services for customer applications running on Windows Azure, data is accessible from anywhere virtually.

## 4.2 Scaling Resources

The ability of scaling up or down resources to meet workload is one of the most desired cloud computing advantages. A web application developer who hosts services on a cloud may see how the response time gradually increases when the usage of the application also increases because the cloud does not scale up resources quickly enough. On the other hand, scaling must be limited by some threshold [11]. This threshold would stop the continuous increase in the allocation of resources to prevent the cloud provider from suffering a rejection of service attack because the customer's application was malfunctioning. In either case, the customer could be billed for services that they did not want. Existing service level agreements determine quality of service requirements, but not in terms of response time in response to workload variations.

Customers of Amazon EC2 can scale their capacities up or down automatically according to conditions they define which can be done using the auto scaling feature. Auto scaling means to scale-up the system as the load increases and scale-down the system when the load decreases. With auto scaling, customers can ensure that the number of Amazon EC2 instances being used increases seamlessly due increase in demand to maintain performance, and decreases automatically during demand drop to reduce cost. Auto scaling is particularly well suited for applications that experience hourly, daily, or weekly unpredictability in usage [17]. Auto scaling is enabled by Amazon CloudWatch and available at no additional charge beyond Amazon CloudWatch fees. When customer signed up for the Amazon EC2 service, he is automatically registered to use Auto Scaling features via the Auto Scaling APIs or Command Line Tools.

Windows Azure enables customers to easily scale their applications to any size. It is a fully automated self-service platform that allows customers to provision resources within minutes [16]. Elastically grows or shrinks the resource usage based on application demand. Users only pay for the resources their applications use. There are practical limitations on auto scaling in Azure. It takes about 10 minutes to launch an additional instance of a running service and 1-2 minutes to bring an instance down [18]. However, Azure instances are charged by the hour, therefore, it does not make sense to auto scale an Azure service at timescales much less than an hour.

### 4.3 Data Deletion

The user of a public cloud may require data to be deleted; i.e., completely removed from the cloud. This can only be achieved by erasing, repeatedly re-writing the disk sectors with random data, or formatting the server's hard disk which could turn out to be infeasible to perform at the service provider's environment. A malicious user may later take advantage of the remaining data. Even with multiple cycles of re-writing the sectors, which previously held the file, it may be possible to access erased data [11]. This may be quite costly in time and disk I/O and may not be entirely successful.

Amazon Simple Storage Service (S3) is a storage system in which data is accessible to EC2 instances [12]. When an object is deleted from Amazon S3, the mapping from the public name to the object is removed across the distributed system within several seconds. Once the mapping is removed no remote access to the deleted object will be allowed and underlying storage area is reclaimed for use by the system then made available only for write operations. Amazon SimpleDB operates in coordination with EC2 and S3 to allow developers to run queries on structured data [19].

Windows Azure's storage subsystem makes customer data unavailable once delete operations are executed. All storage operations including delete are designed to be immediately reliable. Successful execution of a delete operation removes all references to the associated data item and it cannot be accessed via the storage APIs [20]. All copies of the deleted data item are then garbage collected and the physical bits are overwritten when the associated storage block is reused for storing other data.

### 4.4 Data Lock-in

By using proprietary cloud-based applications, migration off the cloud to another cloud or to an in-house IT environment is not an easy option for customers. Standardizing APIs let the SaaS developer deploy services and data across multiple cloud computing providers in order to avoid propagating the failure of a single company to all copies of customer data. In addition to justifying data lock-in concerns, standardization of APIs enables a new usage model in which the same software infrastructure can be used in a private and public cloud [21]. Such an option mitigates “Surge Computing,” in which the public cloud is utilized to capture the extra tasks that cannot be run in the private cloud due to temporarily intense workloads.

Amazon EC2 has not build a standard API, but it has deployed Gluster, which is a software-only, highly available, scalable, open source NAS file system and provides centrally managed storage pool for public and private cloud environments. GlusterFS is deployed within Amazon Web Services (AWS) Elastic Compute Cloud (EC2) environments via the Gluster Amazon Machine Image (AMI) [22]. Gluster supports customers move to the public cloud or between public, private and hybrid cloud environments with a wide range of automation integration with file and object storage.

As with Amazon EC2, Microsoft has not built a standard API. Windows Azure SDK provides a set of APIs to complement the core services offered by Windows Azure. These APIs are installed as a part of Windows Azure SDK and can be used locally for developing Windows Azure applications [6]. As previously described, these APIs are not a standard in cloud computing and can’t be used by any provider.

## 4.5 Data Security

The distributed nature of the cloud model essentially involves more transits of data over networks, which introduces challenging security risks since service providers typically do not have access to the physical security system of data centers. They must rely on the infrastructure provider to realize full data security. The confidentiality of the data must be assured whether it is at rest (data stored in the cloud) or in transit (to and from the cloud). It is desirable to provide a closed box execution environment where the integrity and confidentiality of the data can be verified by its owner. While encryption is an option to securely store data in the cloud, it does not fit that well with cloud-based processing. In most cases, the data has to be unencrypted at some time when it is inside the cloud. Some operations are impossible to do with encrypted data and performing computations with the encrypted data may consume more computing resources [17].

Cloud users face both internal and external security threats. Many of the security issues involved in protecting clouds from external threats are similar to those facing large data centers. The responsibility to face internal security threats is divided among many parties including cloud users, cloud provider, and third-party vendors providing security-sensitive software or configurations. Cloud users are responsible for application-level security [23]. The cloud provider is responsible for physical security, and enforcing external firewall policies. Security for intermediate layers of the software stack is the responsibility of the user and operator.

Administrators of Amazon EC2 do not have access to customer instances and cannot log into the Guest operating system. EC2 Administrators are required to use their individual cryptographically strong Secure Shell (SSH) keys to obtain access to a host. All accesses are logged and routinely audited [24]. While the data at rest in Simple Storage Service (S3) is not encrypted by default, users can choose to encrypt their data before uploading it to Amazon S3.
Security within Amazon EC2 is provided on multiple levels; namely, the operating system (OS) of the host system, the virtual instance operating system or guest OS, firewall and signed API calls. Each of these levels builds on the capabilities of the others [25]. The objective is to ensure that data stored within Amazon EC2 cannot be retrieved by unauthorized systems or users and that Amazon EC2 instances themselves maximally secured without compromising the flexibility in configuration that customers demand.

As part of securing the data within the application-layer, Microsoft has suggested encryption as part of Azure projects. However, product designers and developers need proper understanding for both encryption and the .NET security model to building on the Windows Azure [26]. In summary, Microsoft applies security mechanisms at different layers of the cloud infrastructure to implement a defense-in-depth approach. These layered mechanisms include:

- Physical security of the data centers (locks, cameras, biometric devices, card readers, alarms)
- Firewalls, application gateways and IDS to protect the network
- Access Control Lists (ACLs) applied to virtual local area networks (VLANs) and applications
- Authentication and authorization of persons or processes that request access to data
- Hardening of the servers and operating system instances
- Redundant internal and external DNS infrastructure with restricted write access
- Securing of virtual machine objects
- Securing static and dynamic storage containers

Security in SQL Azure is very similar to that for an on-site SQL Server [27] [28]. Therefore, SQL administrators find security management a familiar task at the database level. Server-level administration is quit different since databases may cover several physical systems. Table 1 summarizes the previous comparative discussions.

Table 1. Amazon EC2 vs. windows Azure

| Challenge | Amazon EC2 | Windows Azure |
|---|---|---|
| **Availability** | Zones, Regions, Elastic IP Address with<br>Guaranteed Network Availability: 99.95% | Fault-tolerance, Geo Replication, REST and managed API's for storage with<br>Guaranteed Network Availability: 99.9% |
| **Resource Scaling** | Free auto-scaling enabled by CloudWatch | Paid, based on a configuration file specified by the user |
| **Data Deletion** | Delete objects in Amazon S3 and delete Item, and Attributes in Amazon SimpleDB, | Remove all references with garbage collection |
| **Data Lock-in** | Use Gluster to move between public, private and hybrid clouds | No feature to support moving between clouds |
| **Data Security** | Security applied within multiple levels. Encryption can be done by user | Security mechanisms applied at different layers. Security in SQL Azure is similar to that in SQL Server |

## 5. CONCLUSION

Customers of computing services must have a deep study in cloud computing before they decide to make this move. The Service Level Agreement (SLA) covers many issues regarding the services provided by a certain cloud provider such as availability, auto-scaling and security. However, cloud providers normally do not include in their cloud services' SLA any condition to ensure a given level of performance.

When deciding to move to cloud computing, choosing a cloud provider should only be done when the workload of the application to be hosted is completely characterized. This supports the notion that the application type is one of the main parameters for choosing a cloud provider.
From our comparison between Amazon EC2 and Windows Azure platforms, we found that Amazon EC2 wins over Windows Azure in the auto-scaling feature and in solving the situation of data lock-in, since auto-scaling is free in Amazon EC2 and it has deployed specific software (Gluster) to support the move between different types of clouds. Since Amazon EC2 deals with Amazon S3 and Amazon Simple DB, Amazon EC2 guarantee the deletion operation much better than windows Azure, while because it's laid in the platform layer without involving in the infrastructure layer, Windows Azure guarantees the deletion operation within the database level only.

The methodologies of Data Security, the most important issue when moving to cloud computing, is different between Amazon EC2 and Windows Azure. Therefore, choosing between the two providers regarding security depends on the customer desires and controls levels required starting from full security control of data, storage, data center and end-user authentication to let the provider do the job completely.

# ACKNOWLEDGMENT

The authors would like to thank Dr. Mohammad AlHaribat, Middle East University, for his suggestions regarding the editing of this article.

# REFERENCES

[1] A. Sleit, A. L. A. Dalhoum, M. Qatawneh, M. AlSharief, R. Al-Jabaly, and O. Karajeh, Image Clustering using Color, Texture and Shape Features, KSII Transactions on Internet and Information Systems, Vol. 5, No. 1, 2011, pp. 211-227.
[2] A. Sleit, S. Serhan, and L. Nemir, A histogram based speaker identification technique, International Conference on ICADIWT, May 2008, pp. 384-388.
[3] A. Ibrahim and F. Fotouhi, Indexing and retrieving point and region objects, In Proceedings SPIE'96, Storage and Retrieval for Image and video Databases (SPIE), 2670, 1996, pp. 321-336.
[4] A. Ibrahim, F. Fotouhi, and S. Hasan, The SB+-tree: an efficient index structure for join spatial relations, International Journal of Geographical Information Science, Vol. 11, No. 2, 1997, pp. 163-182.
[5] A. Ibrahim, F. Fotouhi, and A. AL-Badarneh, Efficient Processing of Spatial Selection and Join Operations using SB+-tree, International Database Engineering & Applications Symposium, 1997, pp. 279-288.
[6] Tejaswi Redkar, Windows Azure Platform, Apress, 2010, ISBN: 978-1-4302-2479-2.
[7] L. Youseff, M. Butrico, and D. Da Silva, Towards a Unified Ontology of Cloud Computing, Grid Computing Environments Workshop (GCE08), held in conjunction with SC08 (November, 2008), pp. 1-10.
[8] Qi Zhang, Lu Cheng, Raouf Boutaba, Cloud computing: state-of-the-art and research challenges, Journal of Internet Services and Applications, Vol. 1, No. 1. (May 2010), pp. 7-18.
[9] Shyam Kumar Doddavula, Amit Wasudeo Gawande, Adopting Cloud Computing:Enterprise Private Clouds, SETLabs Briefings, Vol. 7, No. 7, 2009, pp. 11-18.
[10] Cloud Computing on Wikipedia, http://en.wikipedia.org/wiki/Cloud_computing, accessed on Dec 4, 2011.
[11] Victor Delgado, Exploring the limits of cloud computing, Masters Thesis, October 4, 2010
[12] Amazon Elastic Computing Cloud, http://aws.amazon.com/ec2, accessed on Mar 3, 2013.
[13] Chadwick et al. My private cloud – granting federated access to cloud resources, Journal of Cloud Computing: Advances, Systems and Applications 2013, 2:3, doi:10.1186/2192-113X-2-3
[14] Afkham Azeez, Autoscaling Web Services on Amazon EC2, http://people.apache.org/~azeez/autoscaling-web-services-azeez.pdf accessed on Mar 16, 2013

[15] Lee Gillam, Bin Li, John O. Loughlin, Anuz Pratap Tomar, Fair Benchmarking for Cloud Computing systems, Journal of Cloud Computing: Advances, Systems and Applications 2013, 2:6 doi:10.1186/2192-113X-2-6, 7 March 2013.

[16] Microsoft windows Azure, http://www.windowsazure.com/en-us/ accessed on Sep 23, 2012.

[17] Amazon Web Services Auto Scaling, http://aws.amazon.com/autoscaling//184-8323629-2376804/ accessed on Mar 19, 2013.

[18] Auto scaling in Windows Azure, http://convective.wordpress.com/2010/10/12/autoscaling-in-windows-azure/ accessed on Jan 10, 2013.

[19] Amazon Web Services: Overview of Security Processes, http://www.utdallas.edu/~muratk/courses/cloud11f_files/AWS_Security_Whitepaper.pdf , accessed on Jan 23, 2012

[20] Charlie Kaufman and Ramanathan Venkatapathy, Windows Security Overview, http://download.microsoft.com/download/6/0/2/6028B1AE-4AEE-46CE-9187-641DA97FC1EE/Windows%20Azure%20Security%20Overview%20v1.01.pdf, accessed on Dec 15, 2012

[21] M. Armbrust et al. Above the clouds: A Berkeley view of cloud computing. EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2009-28, 2009.

[22] Gluster Introduces NAS Virtual Appliances for VMware, Amazon Web Services, http://www.eweek.com/c/a/Midmarket/Gluster-Introduces-NAS-Virtual-Appliances-for-VMware-Amazon-Web-Services-148680/ accessed on Dec 20, 2011.

[23] Michael Armbrust, Armando Fox, A view of Cloud Computing, Communications of the ACM, vol. 53, no. 4, April 2010, pp. 50-58.

[24] S. Subashini, V.Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications, Vol. 34, Issue 1, January, 2011, pp.1–11.

[25] Amazon Web Services: Overview of Security Processes, http://s3.amazonaws.com/aws_blog/AWS_Security_Whitepaper_2008_09.pdf, accessed on Jan 30, 2013.

[26] Jonathan Wiggs, Cloud Security: Crypto Services and Data Security in Windows Azure, MSDN magazine, accessed on January 2013.

[27] Deb Shinder, Microsoft Azure: Security in the Cloud, http://www.redline-software.com/eng/support/articles/security/os/microsoft-azure-security-cloud.php, accessed on Nov 11, 2012.

[28] Shin-ichi Kuribayashi, Improving Quality of Service and Reducing Power Consumption with WAN accelerator in Cloud Computing Environments, International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.1, January 2013, pp. 41-52.