

Cloud Computing Data Security-Background & Benefits

Sonia Bassi¹, Anjali Chaudhary²

¹ M.Tech Student, Department Of Computer Science, KITM, Kurukshetra

² Assistant Professor, Department Of Computer Science, KITM, Kurukshetra
sonia_bassiin@yahoo.com

Abstract- In last few years, Cloud computing is rapidly growing area in the IT security space. Because it has been a promising business concept with win-win situation for the users. The users are able to use application as services on the clouds using the internet. Cloud computing has many potential advantages and many enterprise applications and data are migrating to public or hybrid cloud. Even though cloud computing provides compelling benefits and cost effective options for security exploits are introduced.[1] At present, a major concern in cloud adoption is towards its security and privacy. Security and privacy issues are of great concerns to cloud service provider who are actually hosting the services. The security issues are organised into several general categories: - Data portability, Data protection, Trust, Software isolation, Identity management, Reliability, Ownership etc. So that now it is becoming more challenging to secure the digital assets of a company in accordance with the changing demand and growing technologies which were almost fixed earlier.[2]

Keywords: Cloud Computing, Cloud evolution, Cloud models, cloud security.

I. Introduction

Cloud computing is a computing paradigm, where a large pool of systems are connected in private or public networks to provide dynamically scalable infrastructure for application, data and file storage. "Cloud computing is a practical approach to experience direct cost benefits and it has potential to transform a data center from a capital-intensive set up to a variable priced environment.

Cloud Computing is characterised by consumers who use cloud services as needed, who consume shared resources as a service that can rapidly and elastically scale up or down as needed, who pay only for what is used and who access services over a networked infrastructure. Cloud computing is changing the current IT delivery model for services. Benefits for the business and IT include reduced costs, scalability, flexibility, capacity utilization, higher efficiencies and mobility. Cloud computing services providers touted the security and reliability of their services, actual deployment of cloud computing service is not as safe and reliable as they claim. In 2009, the major cloud computing vendors successively appeared several accidents. Amazon's Simple Storage Service was interrupted twice in February and July 2009. This accident resulted in some network sites relying on a single type of storage service were forced to a standstill. March 2009, security vulnerabilities in Google Docs even led to serious leakage of user private information. Google Gmail also appeared a global failure up to 4 hours. It was exposed that there was serious security vulnerability in VMware virtualization software for Mac version in May 2009.

As the mobility has increased, now it is a challenge to secure the increasing boundaries. Now the security focus has began to shift from securing the data centres to protecting the ad hoc endpoints. This was done mainly through many mechanisms including firewalls, confining the end points services, routine changing configurations to restrict access and by other related techniques.

II. The Background of Cloud Computing

Cloud Computing is emerged as the modern technology which developed in last few years, and considered as the next big thing, in the years to come. Since it is new, so it require new security issues and face new challenges as well [3]. In last few years it is grown up from just being a concept to a major part of IT industry. Cloud computing widely accepted as the adoption of virtualization, SOA and utility computing. There are also the architectural security issues which are changing according to various architectural designs functioning over cloud computing [4]. Data security over the cloud is a major concern and various methodologies are proposed [5], also preserving auditing for the data security in cloud computing [6], raising the concern over the privacy related issues in data storage [7], such that no critical information can be intercepted as recently a case happened with Wikileaks, over the security of the data.

Cloud computing works in layers as applying policies on these layers provide better security approach to manage the security concerns [8]. Cloud computing has given a anew horizon to the data hosting and deploying

services. The most important thing of cloud computing is that it enables customers a new way to increase capacity and add capabilities to their machines on the go.

Before we start with cloud computing, three concepts must be clearly understood those are:-

- Cluster Computing
- Grid Computing
- Utility Computing

In Cluster Computing, cluster stands for a group of inter linked local computers, those works together towards a single goal. Instead of Grid computing links a lot of different geographically distributed individual computers to build a single large super infrastructure. Utility computing works pay per use model i.e. paying for what you accessed and used from a shared pool of resources e.g. storage system, software and servers like public utilities e.g. water, electricity and gas etc.

This paper aims to provide some guidelines to assist management with the benefits, types of cloud computing. The process we followed in conducting cloud computing evolution is described in section III, followed by cloud computing benefits (section IV), cloud computing models (section V), types of clouds (section VI), security issues and challenges of cloud computing (section VII) and researches on cloud computing (section VIII) arising from our research.

III. Cloud Computing Evolution

The History begins from the following technologies:

A. Cluster Computing:

This is basically clustering of the coupled computers, to work in a group to accomplish a single computing task by working closely equivalent of forming a single computer. The cluster components are not necessarily, connected to each other through fast local area networks. This grouping of computers improves the performance, speed and availability as well as reduces the overall cost, instead of working over a single computer.

B. Grid Computing:

Grid computing links various geographically distributed individual computers to build a single large infrastructure. It combines the various computer assets from multiple administrative domains to accomplish a single computing task. The main differences between the grids computing from cluster computing are

- a) More loosely coupled
- b) Heterogeneous
- c) Geographically distributed.

The separate grids can be dedicated to single application; but a single grid can also be accessed for a variety of different applications.

C. Utility Computing:

Utility computing works on pay per use basis i.e. paying for what you accessed and used from a shared pool of resources e.g. storage system, software and servers like public utilities e.g. water, electricity and gas etc. So utility computing is the wrapping up of computing resources as a metered service. This concept has the benefit of having negligible or no initial investment to access the various computing resources. Basically in this concept the computational resources are mainly rented as compared to the earlier scenario in which we required to purchase the products to avail the services.

This facility of being served as a utility became the basis of the "On Demand" computing. Cloud computing model further proposed the concept of delivering computing, application and network components as a service. IBM, HP and Microsoft were early giant leaders in the field of utility computing and they have invested a lot on the research work on working of the cloud architecture, payment system and development challenges. Google, Amazon and others started to take the lead in 2008, as they established their own utility services for computing, storage and applications.

D. Cloud Computing:

Cloud computing permits users and organizations to access their applications without any investment and installation and give them the power to access their personal data at any computer by just having internet connection. This technology ensures additional computing power to the user by centralizing storage devices and server which gives them much more processing speed. This technology just uses the internet connection and centralized remote servers.

Yahoo mail, Gmail and other social networks the simplest and widely accepted example of cloud computing. We generally do not care about the implementation of any server to access them. The consumers just need an internet connection and you can start accessing the email inbox. All the management including of servers and emails are done under the supervision of cloud service providers Yahoo, Microsoft, Google etc. The consumer

gets only to use the software interface and all remaining management will be accomplished by the cloud service provider itself. The users simply enjoy the benefits

IV. Benefits of cloud computing

Major growth in cloud computing adoption is expected. Predictions for growth in the cloud services market range between \$46.3 billion reported in 2008 to \$148.8 billion and \$150 billion by 2014 and \$222.5 billion market by 2015 [9-11]. These predictions for growth are based on the realization of the many benefits of cloud computing.

Cloud computing provides compelling savings in IT related costs including lower implementation and maintenance costs; less hardware to purchase and support; the elimination of the cost of power, cooling, floor space and storage as resources are moved to a service provider; a reduction in operational costs; and paying only for what is used (measured service). Cloud computing also enables organisations to become more competitive due to flexible and agile computing platforms, providing for scalability and high-performance resources and highly reliable and available applications and data. Through cloud computing, IT departments save on application development, deployments, security, and maintenance time and costs, while benefiting from economies of scale. 'Going green' and saving costs are a key focus point for organisations. Cloud computing helps organisations to reduce power, cooling, storage and space usage and thereby facilitates more sustainable, environmentally responsible data centres. Moving to the cloud further frees up existing infrastructure and resources that can be allocated to more strategic tasks.

Cloud computing benefits are listed in Fig. 1, arranged from the highest occurrence (therefore cited most in literature) to the lowest.

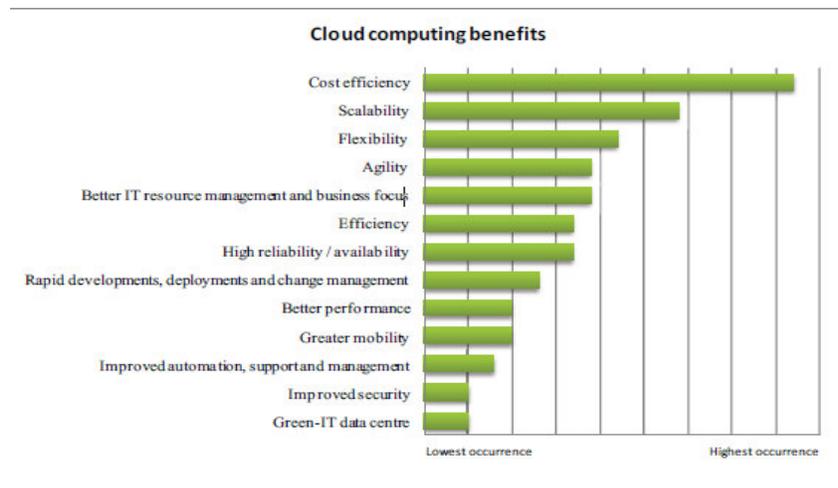


Figure 1. Cloud computing benefits.

Cost efficiency is the main driver for cloud computing adoption. Other primary benefits include scalability, flexibility, agility, better IT resource management and business focus, efficiency, higher reliability and availability, rapid development, deployment and change management, better performance and greater mobility. Improved automation, support and management, improved security, and green-IT data centres were also cited as valuable drivers for moving to the cloud.

V. Cloud Computing Models

The major cloud providers in the current market segment are **Amazon, Google, IBM, Microsoft** etc. Some major challenges that are being faced by cloud computing are to be secured, protect and process the data which is the property of the user.

The users are able to use application as services on the clouds using the internet. User can typically connect to clouds via web browser or web services. It has several security issues. Cloud computing providers services based on three fundamental service delivery models.



Figure 2 Cloud Services and Application

- I. An **Infrastructure-as-a-Service (IaaS)** model provides the capability to provision the computing and storage resources on demand by the users. The users are able to deploy and run the software which includes operating system and other applications and some selected network component, but they don't control the cloud infrastructure. Data security consideration for IaaS includes the management of virtual resources allocation and addressing the virtualization and vulnerabilities and risks that affect the IaaS delivery model.
- II. A **Platform-as-a-Service (PaaS)** model provides the computing platform and solution stack as a service to the users. The users are able to develop their application without purchasing and managing the hardware and software necessary for their application development. The complete life cycle support the delivering application and services are provided by the PaaS model. The user has controlled over the deployed applications and application hosting environment configuration, but they do not manage or control the underlying cloud infrastructure, network, servers, operating systems, or storage. Security consideration for PaaS include access and authorization issues, working with distributed applications, storage and data security.
- III. **Software-as-a-Service (SaaS)** model allow the cloud users to access the applications from cloud providers. This eliminates the cloud users to install and maintain the application that runs on their own local computer. The applications are mostly accessed by users using thin clients via the web browser. The users have control over only their application configuration settings. The underlying cloud resources should be managed and controlled by the cloud providers. SaaS are used as common delivery model for most of the business applications like Enterprise Resources planning (ERP), Customer Relationship Management (CRM), and human Resource Management (HRM) and so on. In effect, there should be more focus provided for access control and identities for accessing the enterprise applications in cloud. SaaS users are billed based on the usage in the monthly or yearly basis.

All these cloud services are accessed via the cloud clients such as desktop, laptop, smart phones, tablets and wireless sensor nodes which are connected to the network.

VI. Types of clouds

A. Public cloud

This is most popular cloud system. In public cloud system a third party data centre provide both disk space and computing power for all the application software. Computing infrastructure is hosted at the vendor's premises. The customer has no visibility over the location of the cloud computing infrastructure [1-3]. The computing infrastructure is shared between organizations. Amazon web and Google apps is the two most popular public cloud computing service providers.

B. Private cloud

Computing architecture is dedicated to the customer and is not shared with other organizations. The cloud infrastructure is operated by an organization. It may be managed by the organization or a third party. They are expensive and are considered more secure than public clouds. Private clouds may be externally hosted ones as well as in premise hosted clouds.

C. Hybrid Cloud

The cloud infrastructure is a composition of two or more clouds (private, public, community). Organizations host some critical, secure applications in private clouds. Cloud bursting (data and application portability) is the term used to define a system where the organization uses its own infrastructure for normal usage, but cloud is used for peak loads.

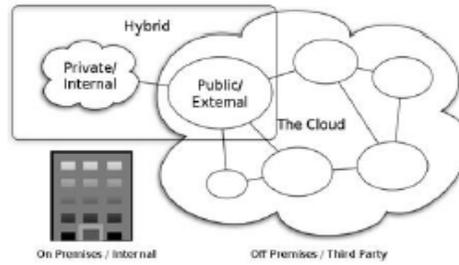


Fig. 3 Deployment Model

D. Community cloud

The cloud infrastructure is shared between the organizations of the same community. For example: all government agencies in a city can share the same cloud but not the non government agencies.

VII. Security Issues of cloud Computing

A. Cloud Computing Security

Wikipedia [12] defines Cloud Computing Security as “Cloud computing security (sometimes referred to simply as “cloud security”) is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing.” Note that cloud computing security referred to here is not cloud-based security software products such as cloud based anti-virus, anti-spam, anti-DDoS, and so on.

B. Security Issues Associated with the Cloud

There are many security issues associated with cloud computing and they can be grouped into any number of dimensions.

According to Gartner [13], before making a choice of cloud vendors, users should ask the vendors for seven specific safety issues: Privileged user access, regulatory compliance, data location, data segregation, recovery, investigative support and long-term viability. In 2009, Forrester Research Inc. [14] evaluated security and privacy practices of some of the leading cloud providers (such as Salesforce.com, Amazon, Google, and Microsoft) in three major aspects: Security and privacy, compliance, and legal and contractual issues. Cloud Security Alliance (CSA) [15] is gathering solution providers, non-profits and individuals to enter into discussion about the current a future best practices for information assurance in the cloud.

The CSA has identified thirteen domains of concerns on cloud computing security [16].

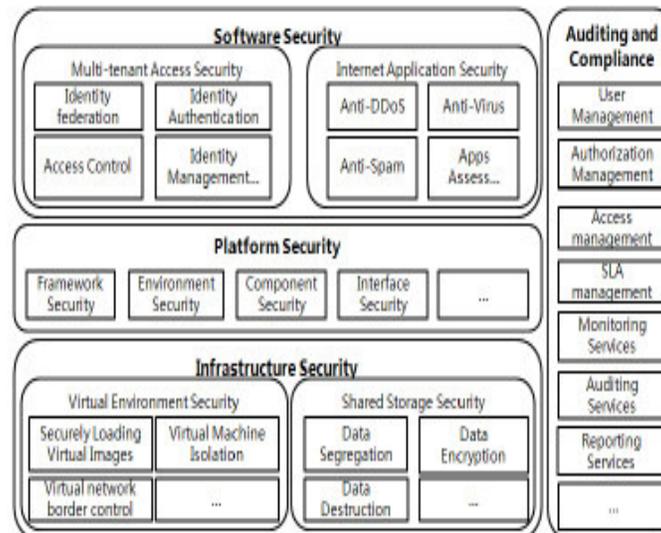


Fig.4: Security Issues of Cloud Computing

VIII. Researches on cloud computing

- IBM/Google has started an academic Cloud Computing initiative.
- HP, Intel Corporation and Yahoo announced the creation of a global, multi-data center, open source test bed, called Open Cirrus.
- Institutes researching on Cloud Computing

The Electronics and Telecommunications Research Institute (ETRI) in Korea, Karlsruhe Institute of Technology, the Malaysian Institute for Microelectronic Systems (MIMOS), the Info comm. Development Authority (IDA) of Singapore, and the Institute for System Programming at the Russian Academy of Sciences.

- Universities researching on Cloud Computing
Boston University, Carnegie Mellon, MIT, Indiana University, North Carolina State, Purdue, University of California, University of Melbourne (Australia), Georgia Tech, University of Massachusetts, Yale, Wayne State, University of Utah, University of Minnesota Virginia Tech, University of Wisconsin Madison, University of Maryland, University of Washington, University of Virginia.

A. *Main Cloud computing service providers*

- Amazon
- Microsoft windows Azure
- Google AppEngine
- Vmware cloud
- Go grid
- Savvis
- Rack space
- Verizon
- AppNexus

B. *Services offered in Cloud Computing*

- Amazon:
Amazon Elastic Compute Cloud (EC2), Amazon SimpleDB, Amazon Relational Database Service (RDS), Amazon Elastic MapReduce, Amazon Virtual Private Cloud (VPC), Auto Scaling, Amazon CloudFront, Amazon Fulfillment Web Service (FWS), Amazon Simple Queue Service (SQS), Amazon Simple Storage Service (S3).

- Google:
Google invests more than \$2 billion a year in data centers for cloud computing.

Google App Engine

AdWords, Maps, Google Places, Base, Google Site Search, AdSense, Analytics, Checkout, Ad Manager, Web Optimizer, Google Apps, Google Friend Connect, Postini services, Webmaster Central, Grow viral traffic to your site, Search company information, Secure your email

- Microsoft "Azure" :
• Internet-scale cloud computing and services platform hosted in Microsoft data centers.
• Provides a range of functionality to build applications that span from consumer web to enterprise scenarios.
• Designed to help developers quickly and easily create, deploy, manage, and distribute web services and applications on the internet.

C. *Widely used Cloud services*

FaceBook , Yahoo, Gmail, Rediff mail , Other email Service providers, Bit Torrent, Skype, LinkedIn, YouTube, Google, Microsoft, Blog-space, Forums, Website Hosting, VPS, WebEx, Groove, Qualys, SecondLife.

IX. Conclusion

Computing clouds is changing the whole IT industry, businesses and global economy. Clearly, cloud computing demands effectiveness, security, and trustworthiness. Cloud computing has now become a common in business [10], government, education, and entertainment which is maintained by the 50 millions of servers globally installed at thousands of data centres today. Private clouds will also become usual in addition to using a few public clouds that are under heavy competition among Google, MS, Amazon, Intel, EMC, IBM, SGI, VMware, Salesforce.com etc.

References

- [1] Rajkumar Buyya et al, Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility, www.scinedirect.com, 2008.
- [2] B. Hay, K. Nance, and M. Bishop, “Storm Clouds Rising: Security Challenges for IaaS Cloud Computing,” Proceedings of the 44th Hawaii International Conference on System Sciences pp. 1–7 (Jan. 2011). nob.cs.ucdavis.edu/bishop/papers/2011-hicss-1/iaas.pdf
- [3] On technical security issues in cloud computing, Meiko Jensen et al, 2009
- [4] Security & Architectural Issues for the national Security cloud computing, Anya Kim et al, 2010
- [5] Ensuring Data Storage security in cloud computing, Cong Wang, et al, 2010
- [6] Privacy reserving, Cong Wang et al, 2010
- [7] Data Security in the world of cloud computing, John Harauz, et al, 2010
- [8] A layered security approach for cloud computing infrastructure, Mehmet Yeldiz et al, 2010
- [9] Deloitte. (2010, 31 August 2010). *Executive Forum – Cloud Computing: risks, mitigation strategies, and the role of Internal Audit*. Available: <http://www.deloitte.com>
- [10] C. Pettey and B. Tudor. (2010, 5 August 2010). *Gartner says worldwide cloud services market to surpass \$68 billion in 2010* Available: <http://www.gartner.com/it/page.jsp?id=1389313>
- [11] Press Office. (2010, 31 August 2010). *Cloud Computing Services - New Market Report Published*. Available: <http://www.companiesandmarkets.com/r.ashx?id=41AETZYHJ289173&prk=ecb8413c602cb89051067456b636c7b9>
- [12] Cloud computing security, http://en.wikipedia.org/wiki/Cloud_computing_security.
- [13] Gartner: Seven cloud-computing security risks. InfoWorld. 2008-07-02. <http://www.infoworld.com/d/security-central/gartner-seven-cloudcomputing-security-risks-853>.
- [14] Cloud Security Front and Center. Forrester Research. 2009-11-18. <http://blogs.forrester.com/srm/2009/11/cloud-security-front-andcenter.html>
- [15] Cloud Security Alliance. <http://www.cloudsecurityalliance.org>.
- [16] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing, V2.1, <http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf>.