ISSN 2278-8808
An International Peer Reviewed
SCHOLARLY RESEARCH JOURNAL
FOR INTERDISCIPLINARY STUDIES

SECURITY ISSUES IN CLOUD COMPUTING

Keyan Abdul Aziz Mutlaq
Republic of Iraq, University of Basrah
College of Education Department of Computer Science

Received: 20 August 2012
Accepted: 28 August 2012

Abstract

Cloud computing is an emerging technology now a days. All the organization whether small or large are moving towards it. Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation.Since data is a valuable entity for any organization and ensuring security for it is very important therefore security is a major Issue in cloud computing these days. This paper focuses on the security issue. It gives idea of cloud computing, risk involved and security concerns in brief.

Key words: *security , cloud computing*

Introduction

In simple terms, cloud computing is a way to enhance computing experience by enabling users to access software applications and data that are stored at off site data centres rather than on the user's own device or PC or at an organization's on-site data centre.

Cloud computing is a new concept of computing technology that uses the internet and remote servers in order to maintain data and applications. It provides dramatically scalable and virtualised resources, bandwidth, software and hardware on demand to consumers. This allows the consumers to safe cost of hardware deployment, software licenses and system maintenance. The consumers are able to use applications or services on the clouds using the internet. Users can typically connect to clouds via web

browsers or web services. Although cloud computing offers many advantages to the consumers, it also has several security issues. This paper illustrates the issues in cloud computing concept.

What is cloud computing?

A cloud is a pool of virtualized computer resources. A cloud can

- ➔ Host a variety of different workloads. Including batch style back end jobs and interactive user facing application.
- ➔ Allow workloads to be deployed and scaled out quickly through the rapid provisioning of virtual machines or physical machines.
- ➔ Support redundant self recovering highly scalable programming models that allow workloads to recover from many unavoidable hardware/ software failures.
- ➔ Monitor resource use in real time to enable rebalancing of allocations when needed[11].

Cloud computing Architectural Framework

The use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation.

There are many types of public cloud computing:[1]

- Infrastructure as a service (IaaS)
- Platform as a service (PaaS)
- Software as a service (SaaS)
- Storage as a service (STaaS)
- Security as a service (SECaaS)
- Data as a service (DaaS)
- Test environment as a service (TEaaS)
- Desktop as a service (DaaS)
- API as a service (APIaaS)
- Backend as a service (Baas)

There are five principal chracterstics of cloud computing

1. Abstraction of infrastructure
2. Resource democratization
3. Service oriented archichture
4. Elasticity / Dynamism of resource
5. Utility model of consumption and allocation

There are three cloud services delivery models

2.1. Infrastructure as a service (IaaS)

In this most basic cloud service model, cloud providers offer computers, as physical or more often as virtual machines, and other resources. The virtual machines are run as guests by a hypervisor, such as Xen or KVM. Management of pools of hypervisors by the cloud operational support system leads to the ability to scale to support a large number of virtual machines[2].

Platform as a service (PaaS)

In the PaaS model, cloud providers deliver a computing platform typically including operating system, programming language execution environment, database, and web server. Application developers can develop and run their software solutions on a cloud platform without the cost and complexity of buying and managing the underlying hardware and software layers. With some PaaS offers, the underlying computer and storage resources scale automatically to match application demand such that cloud user does not have to allocate resources manually.

Software as a service (SaaS)

In this model, cloud providers install and operate application software in the cloud and cloud users access the software from cloud clients. The cloud users do not manage the cloud infrastructure and platform on which the application is running. This eliminates the need to install and run the application on the cloud user's own computers simplifying maintenance and support. What makes a cloud application different from other applications is its scalability. This can be achieved by cloning tasks onto multiple virtual machines at run-time to meet the changing work demand[3].

There are four cloud service deployment and consumption modalities

Public cloud

Public cloud applications, storage, and other resources are made available to the general public by a service provider. These services are free or offered on a pay-per-use model[4].

2.5. Community cloud

Community cloud shares infrastructure between several organizations from a specific community with common concerns (security, compliance, jurisdiction, etc.), whether managed internally or by a third-party and hosted internally or externally[5].

Hybrid cloud

Hybrid cloud is a composition of two or more clouds (private, community or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models[5].

Private cloud

Private cloud is cloud infrastructure operated solely for a single organization, whether managed internally or by a third-party and hosted internally or externally[5]. Undertaking a private cloud project requires a

significant level and degree of engagement to virtualize the business environment, and it will require the organization to reevaluate decisions about existing resources.

Risk In Cloud Computing:

1. Security:

   For many organization security of information is the most critical risk. This may be driven by a need to protect intellectual property, trade secrets, personally identifiable information, or other sensitive information. Making that sensitive information available on the internet requires a significant investment in security controls and monitoring of access to the content and pathways to the information. The logging and auditing controls provided by some vendors are not yet as robust as the logging provided within enterprises an applications. The organization has visibility to anyone who had access to the document and what might have been done to the document.

2. E- Discovery:

   The current climate for E-discovery assumes for the most part that an enterprise knows specifically where its information is being stored how it is being backed up and how it is secured. The rules also assume that an enterprise will be able to phtysically examine storage devices and when required, exmine storage media for evidence of erased and or deleted files. In the cloud environment the enterprise may have little or no visibility to storage and backup processes and little or not physical access to storage dvices, and because the data from multiple customers may be stored in a single repository, forensic inspection of the storage media and a proper understanding of file access and deletion will be a significant challenge.

3. Computer forensics:

   For may organization, computer forensics is a ciritical componenet of e-discovery efforts and internal investigations and often requires physical access to the storage device or computing resource. Much can be learned from information stored by a computer's operating system in physical and volatile storage: information that is retained in a computer's random access memeory that disappears almost immediately after a computer is turned off. When data and applications are moved off the local personal computer the forensics investigator may lose the ability to access very critical information for the case. The provenance of a particular file or the time the file was last accessed can often the crucial in determining how the file was used and who had access to it. If the data storage shifts to the cloud, the ability to obtain uncontaminated copies of evidentiary data may be reduced if not eliminated [6].

Privacy Question In Cloud Computing

Cloud computing does raise a number of important policy questions concerning how people, organizations, and governments handle information and interactions in this environment.

The properties of client plus cloud computing raise valid questions about security and privacy such as:

- Are hosted data and applications within the cloud protected by suitably robust privacy policies?
- Are the cloud computing provider's technical infrastructure, applications, and processes secure?
- Are processes in place to support appropriate action in the event of an incident that affects privacy or security?

Security is an essential component of strong privacy safeguards in all online computing environments, but security alone is not sufficient. Consumers and businesses are willing to use online computing only if they trust that their data will remain private and secure. The ability of cloud computing providers to live up to these expectations is critical not only for the future of cloud computing but also for protecting fundamental rights of privacy and freedom of expression[7].

Security Issues Related to Cloud Computing:

As cloud computing is achieving increased popularity, concerns are being voiced about the security issues introduced through adoption of this new model. The effectiveness and efficiency of traditional protection mechanisms are being reconsidered as the characteristics of this innovative deployment model can differ widely from those of traditional architectures.[9] An alternative perspective on the topic of cloud security is that this is but another, although quite broad, case of "applied security" and that similar security principles that apply in shared multi-user mainframe security models apply with cloud security.[10]

I. Confidentiality and segregation: This is a concern anytime there is a shared infrastructure and is particularly a concern in the cloud.

II. Compliance**:** In order to obtain compliance with regulations including FISMA, HIPAA, and SOX in the United States, the Data Protection Directive in the EU and the credit card industry's PCI DSS, users may have to adopt *community* or *hybrid* deployment modes that are typically more expensive and may offer restricted benefits. This is how Google is able to "manage and meet additional government policy requirements beyond FISMA

III. Privacy: The cloud model has been criticised by privacy advocates for the greater ease in which the companies hosting the cloud services control, thus, can monitor at will, lawfully or unlawfully, the communication and data stored between the user and the host company. Instances such as the secret NSA program, working with AT&T, and Verizon, which recorded over 10 million phone calls between American citizens, causes uncertainty among privacy advocates, and the greater powers it gives to telecommunication companies to monitor user activity

IV. Trust: The site to which the data will be sent in order to process or maintain should be trustworthy

V. Portability and interoperability: There are issues and complexities associated with moving and sharing data.

VI. Reliability and resiliency: An organization loses control and is vulnerable if a vendor lacks resiliency and goes down[8].

Conclusion:

Cloud computing reduces the cost of infrastructure. It increases the profitability of an organization by increasing resource utilization. Cloud computing is an innovative technology used by small and large business organizations. Google is a popular application which provides email, word processing and spreadsheet applications to any computer with a browser and an internet connection to achieve this client must be ensure of the security of his data. Security is an important issue these days. It is a major disadvantage. Security in cloud computing is a challenge of this era.

References:

1. ^ Monaco, Ania (7 June 2012 [last update]). "A View Inside the Cloud". *theinstitute.ieee.org* (IEEE). Retrieved August 21, 2012.
2. ^ Amies, Alex; Sluiman, Harm; Tong, Qiang Guo; Liu, Guo Ning (July 2012). "Infrastructure as a Service Cloud Concepts". *Developing and Hosting Applications on the Cloud*. IBM Press. ISBN 978-0-13-306684-5.
3. ^ Hamdaqa, Mohammad. *A Reference Model for Developing Cloud Applications*.
4. ^ [a b c d] "Defining "Cloud Services" and "Cloud Computing"". IDC. 2008-09-23. Retrieved 2010-08-22.
5. ^ [a b c d e] "The NIST Definition of Cloud Computing". National Institute of Science and Technology. Retrieved 24 July 2011.
6. Three cloud computing risks to consider, information security Magzine Issue: June 2009
7. Privacy in the cloud computing Era a Microsoft Perspective, November 2009, Microsoft.com/download/3/…/cloud_privacy_wp_102809.pdf.
8. Chris Hoff IANS. Disruptive Innovation and security implications of Cloud Computing, Multimedia User Briefing February 2009.
9. ^ [a b] Zissis, Dimitrios; Lekkas (2010). "Addressing cloud computing security issues". *Future Generation Computer Systems*. doi:10.1016/j.future.2010.12.006.
10. ^ Winkler, Vic (2011). *Securing the Cloud: Cloud Computer Security Techniques and Tactics*. Waltham, MA USA: Syngress. pp. 187, 189. ISBN 978-1-59749-592-9.
11. John Salmon, Clouded in uncertainity – the legal pitfalls of cloud computing, 24 Sept 2008.