ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 8, August 2013

SECURITY CONCERNS IN MEDIUM SIZE ENTERPRISE CLOUD COMPUTING

SHAIK.SAIDHBIMCA,M.TECH(CSE),(Ph.D)
Department of Information System
UNIVERSITY OF GONDAR

IBRAHIM GASHAW
Department of information system
University of Gondar

Abstract

Cloud computing in an small size enterprise infrastructure bring significant security concerns. Successful implementation of cloud computing in a small size enterprise requires proper planning and understanding of emerging risks, threats, vulnerabilities, and possible countermeasures. We believe small size enterprise should analyze the company/organization security risks, threats, and available countermeasures before adopting this technology. In this paper, we have discussed security risks and concerns in cloud computing and enlightened steps that a small size enterprise can take to reduce security risks and protect their resources. We have also explained cloud computing strengths/benefits, weaknesses, and applicable areas in information risk management.

1.0 Introduction

This paper discusses recommended steps to handle cloud security, issues to clarify before adopting cloud computing, the need for a governance strategy and good governance technology, cloud computing strengths, weaknesses, analyzes the benefits and costs of cloud computing in information security management.

Cloud computing is continuously evolving and there are several major cloud computing providers such as Amazon, Google, Microsoft, Yahoo and several others who are providing services such as Software-as-a-Service (SaaS), Platform-as-a-Service(PaaS), Storage-as-a-Service and Infrastructure-as-a-Service (IaaS) and this paper has discussed some of the services Being provided.

Small Size Enterprises are starting to look into cloud computing technology as a way to cut down on cost and increase profitability, because across all industries "CIOs are under continuous pressure to reduce capital assets, headcounts, and support costs, and cloud systems give them a way to meet those goals" There are many definitions of cloud computing and the most comprehensive definition available ,who defined cloud computing as "collections of IT resources (servers, databases, and applications) which are available on an on-demand basis, provided by a service company, available through the internet, and provide resource pooling among multiple users."

Figure 1. shows what is available to enterprises in the cloud.

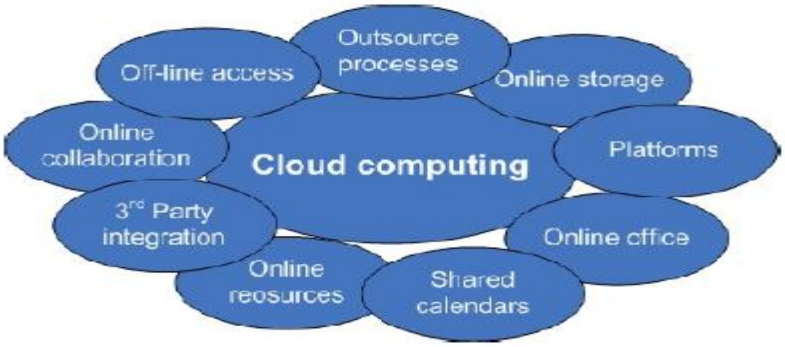


Figure 1. Cloud Computing Resources (Cloud Tweaks, 2013)

2.0. Cloud Computing Growth

The "cost associatively" formulae as shown in Formula 1. (Armbrust, Fox, Griffith, Joseph, Katz, Konwinski and et al., 2009) can be used to compute the profitability of cloud computing. For example using 1000 Amazon EC2 machines for 1 hour costs the same as using 1 traditional non cloud machine for 1000 hours.

The Profitability of cloud computing can be explained in the "cost associatively" formulae shown in Formula 1., the left-hand side multiplies the net revenue per user hour by the number of user-hours, giving the expected profit from using cloud computing while the right-hand side performs the same calculation for a fixed-capacity datacenter by factoring in the average utilization, including nonpeak workloads, of the datacenter; whichever side is greater represents the opportunity for higher profit gave example on elasticity with calculations on the potentials of cloud computing savings and cost reduction:

$$\text{UserHours}_{\text{cloud}} \times (\text{revenue} - \text{Cost}_{\text{cloud}}) \geq \text{UserHours}_{\text{datacenter}} \times \left(\text{revenue} - \frac{\text{Cost}_{\text{datacenter}}}{\text{Utilization}}\right)$$

2.1. Cloud Computing Example

Cloud computing providers provide a variety of services to the customers and these services Include e-mails, storage, software-as-a-services, infrastructure-as-a-services etc.

The attractiveness of cloud computing is not only to small size enterprises but also entrepreneurs, startups, medium companies and small companies would benefit greatly and they will have a new alternative and opportunities that is not available to them in the past that would save them cores of rupees because with cloud computing they will have the choice to only rent the necessary computing power, storage space and communication capacity from a large cloud computing provider that has all of these assets connected to the Internet.

Companies "can pay only for the volume of these services that they use, they can quickly add or Subtract resources from their order, and they never have to take possession of the hardware and all of the technical support headaches associated with it".

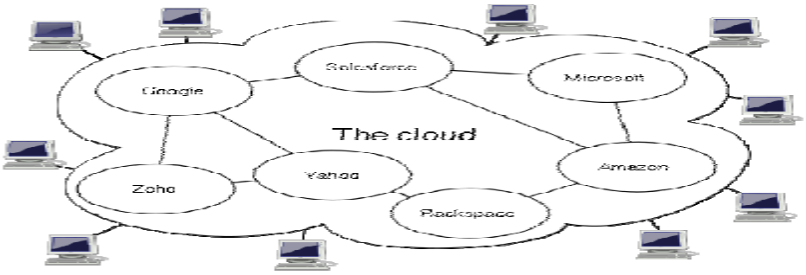
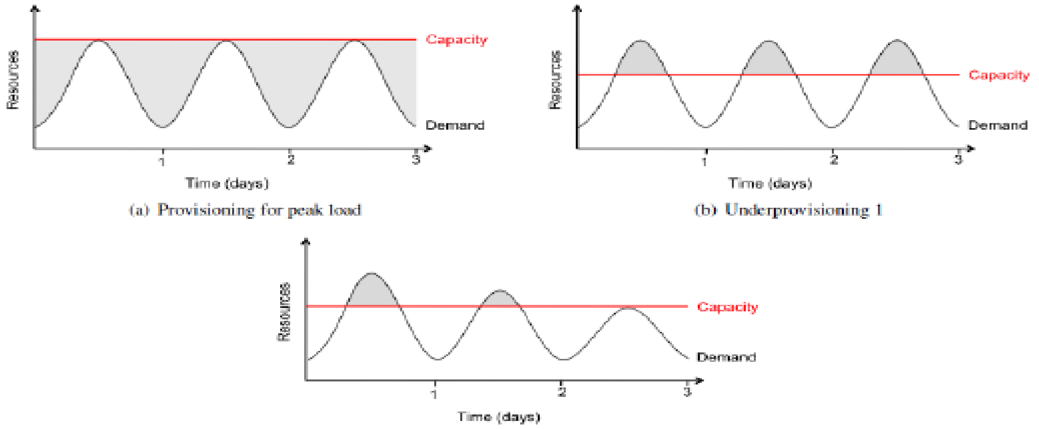


Figure 2. Cloud Computing Overview (CloudTweaks, 2010)

2.3 Cost Minimization

Cost minimization of cloud computing to enterprises can be explained in cloud computing Elasticity capability. Assume our service has a predictable daily demand where the peak requires 500 servers at noon but the trough requires only 100 servers at midnight, as shown in Figure 2(a). As long as the average utilization over a whole day is 300 servers, the actual utilization over the whole day (shaded area under the curve) is 300 x 24 = 7200 server-hours; but since we must provision to the peak of 500 servers, we pay for 500 x 24 = 12000 server hours, a factor of 1.7 more than what is needed. Therefore, as long as the pay-as-you-go cost per server-hour over 3 years is less than 1.7 times the cost of buying the server, we can save money using utility computing.



(a) Provisioning for peak load

(b) Underprovisioning 1

In Figure 3: (a) Even if peak load can be correctly anticipated, without elasticity we waste resources (shaded area) during nonpeak times. (b) Underprovisioning case 1: potential revenue from users not served (shaded area) is sacrificed. (c) Underprovisioning case 2: some users desert the site permanently after experiencing poor service; this attrition and possible negative press result in a permanent loss of a portion of the revenue stream.

3.0 Security Threats, Risks, and Vulnerabilities

With the increasing popularity of small sized enterprise cloud computing and its public connectivity via the internet it is the next frontier for viruses, worms, hackers and cyber-terrorists to start probing and attacking. Many enterprises are seriously looking into cloud computing to save cost, in the not too distance future cloud computing adoption rate will skyrocket and cloud computing vulnerability to viruses, worms, hackers and cyber attacks will increase because organized criminals, terrorist and hostile nations would see this as a new frontier to try to steal private information, disrupt services and course harm to the enterprise cloud computing network. Cloud computing security risk incident has happened when Google a major cloud computing and Software as a Service (SaaS) provider had its systems attacked and hacked.

With cloud computing, physical location of data are spread across geographic area that could span over continents, countries or regions. One of the top security concerns of enterprises are the physical location of the data that are being stored in the cloud especially if they are located in another country because the laws of the host country of the equipment apply to the data on the machines and that could be a big issue if the host country does not have adequate laws to protect sensitive data or if the host nation becomes hostile or when the government of the hosting nation changes and become unfriendly. There have been instances where there has been a complete blackout of entire cloud services and making it unavailable for hours and even days due to bugs. Google's Gmail went down for two hours, Ctrix's GoToMeeting and GoToWebinar were temporarily unavailable, Amazon.com's Simple Storage Service was "out of commission for excruciating eight hours". Imagine an enterprise that completely depends on a cloud computing service provider whose system had been disrupted for hours or days, the lost of business could be catastrophic.

3.1 Threats

Cloud computing faces just as much security threats that are currently found in the existing computing platforms, networks, intranets, internets in enterprises. These threats, risk Vulnerabilities come in various forms. The Cloud Security Alliance did a research on the threats facing cloud computing and it identified the flowing seven major threats:

- Abuse and Nefarious Use of Cloud Computing
- Insecure Application Programming Interfaces
- Malicious Insiders
- Shared Technology Vulnerabilities
- Data Loss/Leakage
- Account, Service & Traffic Hijacking
- Unknown Risk Profile

3.2 Risks

Moving to the cloud presents the small size enterprise with a number of risks and that include securing critical information like the protection of intellectual property, trade secrets, personally Identifiable information that could fall into the wrong hands. Making sensitive information available on the internet requires a considerable investment in security controls and monitoring of access to the contents. In the cloud environment, the enterprise may have little or no visibility to storage and backup processes and little or no physical access to storage devices by the cloud computing provider. 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 .

3.3 Vulnerability

Small size Enterprise cloud computing is just as vulnerable as any other technology that uses the public internet for connectivity. The vulnerability includes eavesdropping, hacking, cracking, malicious attacks and outages.

Research has shown that it is possible for attackers to precisely map where a target's data is physically located within the "cloud" and use various tricks to gather intelligence. Another vulnerability to an attack is the use of denial-of-service attack and it has been found out that if an attacker is on the same cloud servers as his victim, a conventional denial-of service attack can be initiated by am ping up his resource usage all at once.

The researchers went on to say that a way around the weakness they found in Amazon's EC2 is for customers to insist that their cloud machines are placed on physical machines that only they can access or that they and trusted third parties can access. This solution will likely be at a price premium because part of the economy of cloud services is maximizing use of physical servers by efficiently loading them up with cloud machines and locating the cloud datacenter where the utility price is the cheapest.

The work by the researchers highlights that clouds and the virtual environments they employ are relatively new; as a result they still draw the attention of attackers bent on finding and Exploiting unexplored vulnerabilities.

There will be more efficient security software because with cloud computing software vendors will be driven to fix inefficient security approaches that burn up resources The cloud will be a better anti-virus detection and the University of Michigan researchers has found out that if anti-virus software tools were moved from a PC to the cloud they could detect 35 percent more recent viruses than a single anti-virus program on a personal computer. The bottom line is that businesses should treat clouds with a certain amount of suspicion; they should assess the risk the cloud service represents and only commit data to such services that can tolerate that risk" .

4. Cloud Computation Implementation Guidelines

4.1 Steps to Cloud Security

Understand the cloud by realizing how the cloud's uniquely loose structure affects the security of data sent into it. This can be done by having an in-depth understanding of how cloud computing transmit and handles data.

Demand Transparency by making sure that the cloud provider can supply detailed information on its security architecture and is willing to accept regular security audit. The regular security audit should be from an independent body or federal agency.

Reinforce Internal Security by making sure that the cloud provider's internal security technologies and practices including firewalls and user access controls are very strong and can mesh very well with the cloud security measures.

Consider the Legal Implications by knowing how the laws and regulations will affect what you send into the cloud.

Pay attention by constantly monitoring any development or changes in the cloud technologies and practices that may impact your data's security.

4.2 Issues to Clarify Before Adopting Cloud Computing

Gartner, Inc., the world's leading information technology research and advisory company, has identified seven security concerns that an enterprise cloud computing user should address with cloud computing providers (Edwards, 2009) before adopting:

User Access. Ask providers for specific information on the hiring and oversight of privileged administrators and the controls over their access to information. Major companies should demand and enforce their own hiring criteria for personnel that will operate their cloud computing environments.

Regulatory Compliance. Make sure your provider is willing to submit to external audits and security certifications.

Data location. Enterprises should require that the cloud computing provider store and process data in specific jurisdictions and should obey the privacy rules of those jurisdictions.

Data Segregation. Find out what is done to segregate your data, and ask for proof that encryption schemes are deployed and are effective.

Disaster Recovery Verification. Know what will happen if disaster strikes by asking whether your provider will be able to completely restore your data and service, and find out how long it will take.

Disaster Recovery. Ask the provider for a contractual commitment to support specific types of investigations, such as the research involved in the discovery phase of a lawsuit, and verify that the provider has successfully supported such activities in the past. Without evidence, don't assume that it can do so.

Long-term Viability. Ask prospective providers how you would get your data back if they were to fail or be acquired, and find out if the data would be in a format that you could easily import into a replacement application.

5.0 Cloud Computing Strengths, weaknesses, and Application Areas in Information Risk Management

5.1 Cloud Computing Strengths/Benefits

The strength of cloud computing in information risk management is the ability to manage risk more effectively from a centralize point. Security updates and new patches can be applied more effectively thereby allowing business continuity in an event of a security hole.

5.2 Weaknesses

Cloud computing weakness include list of issues such as the security and privacy of business data being hosted in remote 3rd party data centers, being lock-in to a platform, reliability/ performance concerns, and the fears of making the wrong decision before the industry begins to mature.

5.3 The benefits and costs of Cloud Computing in information security management

The top security benefits of cloud computing includes:

- The security and benefits of scale that all kinds of security measures are cheaper when

Implemented on a large scale including all kinds of defensive measures such as filtering, patch management, hardening of virtual machine instances and hypersivors, etc. The benefits of scale also include multiple locations, edge networks, timeliness of response to incidents and centralized threat management.

- Security as a market differentiator that give cloud providers a strong driver to improve

security practices and many cloud customers will buy on the basis of the reputation for confidentiality, integrity and resilient of and the security services offered by a provider

- Large cloud providers will offer a standardized, opened interface to manage security

thereby opening a market for security services.

- Rapid and smart scaling of resources where cloud provider dynamically reallocate resources for filtering, traffic shaping, authentication, encryption and defensive

measures such as distributed denial-of-service (DDoS) attack

- Audit and evidence-gathering where dedicated pay-per-use forensic images of virtual machines are accessible without taking infrastructure offline and it provide cost effective storage for logs allowing comprehensive logging without compromising performance. The cost of cloud computing in information security management includes the costs of migrating, implementing, integrating, training, and redesigning. Also it includes the cost of training supporting people in the new processes. The new architecture could generate new security holes and issues during redesigning and deploying the implementation thereby driving cost up. In the application areas in information risk management, cloud computing is commercially viable alternative for enterprises in search of a cost-effective storage and server solution.

6.0 Conclusion

Cloud computing is a combination of several key technologies that have evolved and matured over the years. Cloud computing has a potential for cost savings to the enterprises but the security risk are also enormous. Enterprise looking into cloud computing technology as a way to cut down on cost and increase profitability should seriously analyze the security risk of cloud computing.

The strength of cloud computing in information risk management is the ability to manage risk More effectively from a centralize point. Security updates and new patches can be applied more effectively thereby allowing business continuity in an event of a security hole.

Enterprise should verify and understand cloud security, carefully analyze the security issues involved and plan for ways to resolve it before implementing the technology. Pilot projects Should be setup and good governance should be put in place to effectively deal with security issues and concerns.

References

1. Armbrust, M. Fox, A, Griffith, R. Joseph, D. A. Katz, R. Konwinski, A. et al. (2009, February). Above the clouds: A Berkeley View of cloud computing

2. Bendandi, S. (2009). scribd.com. Cloud computing: Benefits, risks and recommendations for information security. Retrieved on March 15, 2010 from http://www.scribd.com/doc/23185511/Cloud-Computing-benefits-risks-and-recommendationsfor-information-security

3. Brandl D. (2010, January). Don't cloud your compliance data. Control Engineering, 57(1), 23. CloudTweeks. (2010, January). Plugging into the cloud. Retrieved from http://www.cloudtweaks.com/cloud-diagrams

4. Cloud Security Alliance (2010). Top Threats to Cloud Computing. Cloud Security Alliance. Retrieved from http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

5.CloudTweeks. (2010, January). Posts tagged cloud computing graph. Retrieved from http://www.cloudtweaks.com/tag/cloud-computing-graph/

6. Cohen, D. Farber, M. Fontecilla, R. (2008). Cloud computing a transition methodology. Booz Allen Hamilton. Retrieved from http://www.boozallen.com/media/file/cloud-computingtransition-methodology.pdf

First Author:
Sk.saidhbi MCA,M.TECH(CSE),(Ph.D) ,lecturer ,university of Gondar now she is doing phd with cloud computing security , she have 6 international publications.

Second Author:
Ibrahim Gashaw , B.A degree in Business Administration and information system (Information system) MSC degree in Information Technology at University of Gondar.