Security Issues and Challenges in Cloud Computing

K. Lakshmi

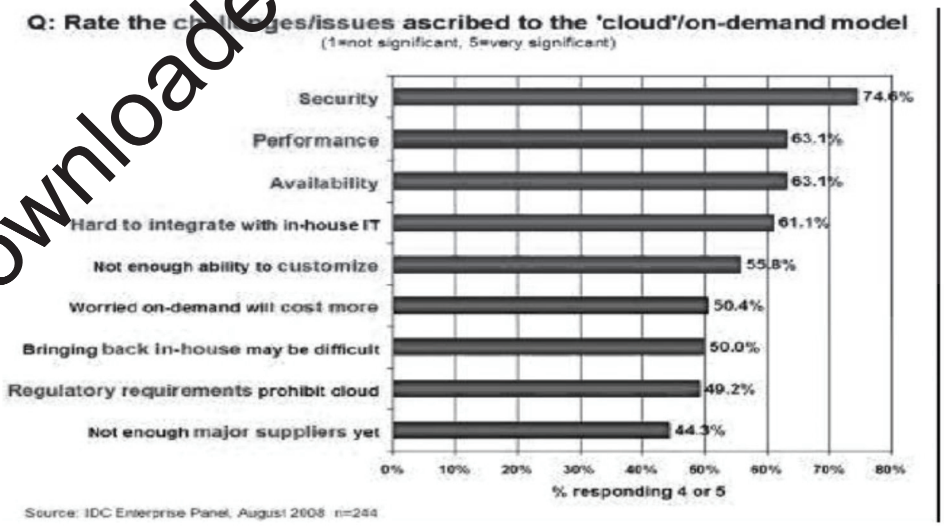
Assistant Professor, ChristuJyothi Institute of Technology & Science,
Warangal, Telangana, India

Abstract: Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources such as networks, servers, storage, applications, and services that can be rapidly provisioned and released with minimal management effort or service provider Interaction. Despite the potential gains achieved from the cloud computing, the organizations are slow in accepting it due to security issues and challenges associated with it. Security is one of the major issues which hamper the growth of cloud. The idea of handing over important data to another company is worrisome; such that the consumers need to be vigilant in understanding the risks of data breaches in this new environment. This paper introduces a detailed analysis of the cloud computing security issues and challenges focusing on the cloud computing types and the service delivery types.

Keywords: Cloud computing, on-demand network access, security.

1. Introduction

The "Cloud" is the default symbol of the internet in diagrams. The broader term of "Computing" encompasses Computation, Coordination logic and Storage. Cloud computing is a way to increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software. It extends Information Technology's (IT) existing capabilities. Cloud computing is the delivery of computing services over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications.



Source: IDC Enterprise Panel, August 2008 n=244

FIGURE 1: Results of IDC survey ranking security challenges, 2008 [1]

Despite of all the hype surrounding the cloud, customers are still reluctant to deploy their business in the cloud. Security issues in cloud computing has played a major role in slowing down its acceptance, in fact security ranked first as the greatest challenge issue of cloud computing as depicted in figure1

From one point of view, security could improve due to centralization of data and increased security-focused resources. On the other hand concerns persist about loss of control over certain sensitive data, and the lack of security for stored kernels entrusted to cloud providers. If those providers have not done good jobs securing their own environments, the consumers could be in trouble. Measuring the quality of cloud providers' approach to security is difficult because many cloud providers will not expose their infrastructure to customers. This work is a survey more specific to the different security issues and the associated challenges that has emanated in the cloud computing system.

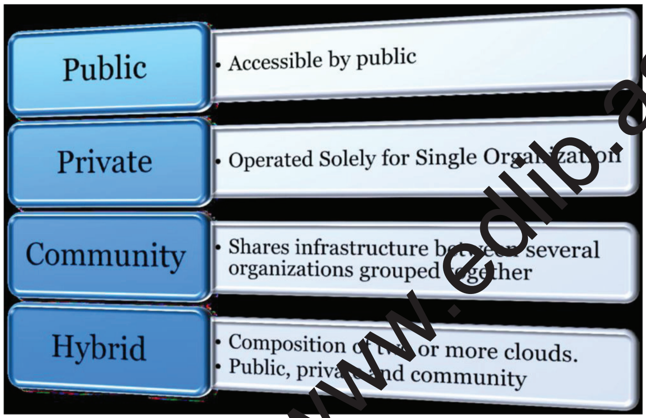
2. Related Works

Gartner 2008 identified seven security issues that need to be addressed before enterprises consider switching to the cloud computing model. They are as follows: (1) privileged user access - information transmitted from the client through the Internet poses a certain degree of risk, because of issues of data ownership; enterprises should spend time getting to know their providers and their regulations as much as possible before assigning some trivial applications first to test the water, (2) regulatory compliance - clients are accountable for the security of their solution, as they can choose between providers that allow to be audited by 3rd party organizations that check levels of security and providers that don't (3) data location – depending on contracts, some clients might never know what country or what jurisdiction their data is located (4) data segregation - encrypted information from multiple companies may be stored on the same hard disk, so a mechanism to separate data should be deployed by the provider. (5) recovery - every provider should have a disaster recovery protocol to protect user data (6) investigative support - if a client suspects faulty activity from the provider, it may not have many legal ways pursue an investigation (7) long-term viability - refers to the ability to retract a contract and all data if the current provider is bought out by another firm.[2] The Cloud Computing Use Case Discussion Group discusses the different Use Case scenarios and related requirements that may exist in the cloud model. They consider use cases from different perspectives including customers, developers and security engineers.[3] ENISA investigated the different security risks related to adopting cloud computing along with the affected assets, the risks likelihood, impacts, and vulnerabilities in the cloud computing may lead to such risks.[4] Balachandra et al, 2009 discussed the security SLA's specification and objectives related to data locations, segregation and data recovery.[5] Kresimir et al, 2010 discussed high level security concerns in the cloud computing model such as data integrity, payment and privacy of sensitive information.[6] Bernd et al, 2010 discuss the security vulnerabilities existing in the cloud platform. The authors grouped the possible vulnerabilities into technology-related, cloud characteristics-related, security controls related.[7] Subashini et al discuss the security challenges of the cloud service delivery model, focusing on the SaaS model.[8] Ragovind et al, (2010) discussed the management of security in Cloud computing focusing on Gartner's list on cloud security issues and the findings from the International Data Corporation enterprise.[9] Morsy et al, 2010 investigated cloud computing problems from the cloud architecture, cloud offered characteristics, cloud stakeholders, and cloud service delivery models perspectives.[10] A recent survey by Cloud Security Alliance (CSA)&IEEE indicates that enterprises across sectors are eager to adopt cloud computing but that security are needed both to accelerate cloud adoption on a wide scale and to respond to regulatory drivers. It also details that cloud computing is shaping the future of IT but the absence of a compliance environment is having dramatic impact on cloud computing growth.[11] Several studies have been carried out relating to security issues in cloud computing but this work presents a detailed analysis of the cloud computing security issues and challenges focusing on the cloud computing deployment types and the service delivery types.

3. Security Issues in Cloud Computing

A. Deployment of cloud services:

Cloud services are typically made available via a private cloud, community cloud, public cloud or hybrid cloud as shown fig2.



Public	• Accessible by public
Private	• Operated Solely for Single Organization
Community	• Shares infrastructure between several organizations grouped together
Hybrid	• Composition of two or more clouds. • Public, private and community

Figure 2: Cloud deployment model [13]

B. Private cloud

It is set up within an organization's internal enterprise datacenter. In the private cloud, scalable resources and virtual applications provided by the cloud vendor are pooled together and available for cloud users to share and use. Utilization on the private cloud can be much more secure than that of the public cloud because of its specified internal exposure. Only the Organization and designated stakeholders may have access to operate on a specific Private cloud.

C. Public cloud

The deployment of a public cloud computing system is characterized on the one hand by the public availability of the cloud service offering and on the other hand by the public network that is used to communicate with the cloud service. In addition, public cloud portfolios employ techniques for resource optimization; however, these are transparent for end users and represent a potential threat to the security of the system.

D. Hybrid cloud

A hybrid cloud service deployment model implements the required processes by combining the cloud services of different cloud computing systems, e.g. private and public cloud services. The hybrid model is also suitable for enterprises in which the transition to full outsourcing has already been completed, for instance, to combine community cloud services with public cloud services.

E. Cloud Service Models

Following on the cloud deployment models, the next security consideration relates to the various Cloud computing service delivery models. The three main cloud service delivery models are: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS).

(i) Infrastructure as a Service (IaaS)

Infrastructure as a Service is a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis.IaaS has many characteristics and components such as Utility service and billing model, Automation of administrative tasks, Dynamic scaling, Desktop, policy-based services, Internet connectivity.

(ii) Platform as a Service (PaaS)

Platform as a Service (PaaS) is a way to rent hardware, operating systems, storage and network capacity over the Internet. The service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones.

Platform as a Service (PaaS) is an outgrowth of Software as a Service (SaaS), a software distribution model in which hosted software applications are made available to customers over the Internet. PaaS has several advantages for developers. With PaaS, operating system features can be changed and upgraded frequently.

(iii) Software as a Service

Software as a Service (SaaS) is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet.SaaS is becoming an increasingly prevalent delivery model as underlying technologies that support Web services and service-oriented architecture (SOA) mature and new developmental approaches, such as Ajax, become popular. Meanwhile, broadband service has become increasingly available to support user access from more areas around the world.

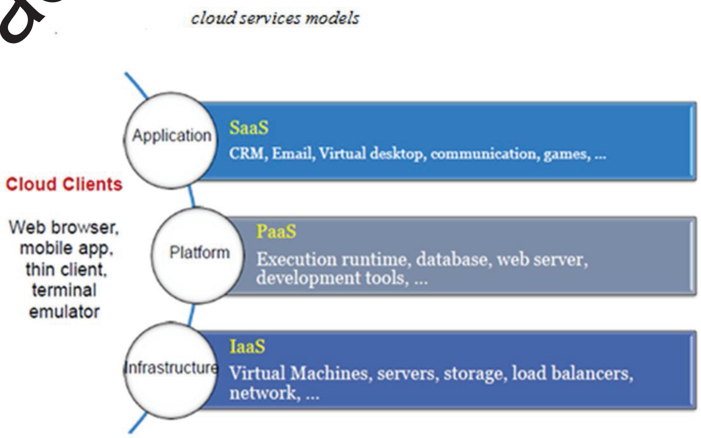

cloud services models
Application
SaaS
CRM, Email, Virtual desktop, communication, games, ...
Cloud Clients
Web browser, mobile app, thin client, terminal emulator
Platform
PaaS
Execution runtime, database, web server, development tools, ...
Infrastructure
IaaS
Virtual Machines, servers, storage, load balancers, network, ...

Fig.2 The following are the additional services provided by the cloud.

4. Computing Challenges in Cloud

A. Security: The current adoption of cloud computing is associated with numerous challenges because users are still skeptical about its authenticity. The cloud acts as a big black box, nothing inside the cloud is visible to the clients and Clients have no idea or control over what happens inside a cloud Even if the cloud provider is honest, it can have malicious system admins who can tamper with the VMs and violate confidentiality and integrity Clouds are still subject to traditional data confidentiality, integrity, availability, and privacy issues, plus some additional attacks.

B. Costing Model: Pricing is the process of determining what a service provider will receive from an end user in exchange for their services. The pricing process can be as follows: fixed in which the customer is charged the same amount all the time dynamic, in which the price charged changes dynamically or market dependent in which the customer is charged based on the real time market conditions.

C. Service Level Agreement (SLA): Although cloud consumers do not have control Over the underlying computing resources, they do need to ensure the quality, availability, reliability, and performance of these resources when consumers have migrated their core business functions onto their entrusted cloud. In other words, it is vital for consumers to obtain guarantees from providers on service delivery. Typically, these are provided through Service Level Agreements (SLAs) negotiated between the providers and consumers. The very first issue is the definition of SLA specifications in such a way that has an appropriate level of granularity, namely the tradeoffs between expressiveness and complicatedness, so that they can cover most of the consumer expectations and is relatively simple to be weighted, verified, evaluated, and enforced by the resource allocation mechanism on the cloud. In addition, different cloud offerings (IaaS, PaaS, and SaaS) will need to define different SLA meta specifications. This also raises a number of implementation problems for the cloud providers. Furthermore, advanced SLA mechanisms need to constantly incorporate user feedback and customization features into the SLA evaluation framework.

D. What to migrate: Based on a survey (Sample size = 244) conducted by IDC in 2008, the seven IT systems/applications being migrated to the cloud are: IT Management Applications (26.2%),Collaborative Applications (25.4%), Personal Applications (25%), Business Applications (23.4%),Applications Development and Deployment (16.8%), Server Capacity (15.6%), and Storage Capacity (15.5%). This result reveals that organizations still have security/privacy concerns in moving their data on to the Cloud. Currently, peripheral functions such as IT management and personal applications are the easiest IT systems to move. Organizations are conservative in employing IaaS compared to SaaS. This is partly because marginal functions are often outsourced to the Cloud, and core activities are kept in-house. The survey also shows that in three years' time, 31.5% of the organization will move their Storage Capacity to the cloud. However this number is still relatively low compared to Collaborative Applications (46.3%) at that time.

Conclusion

Although Cloud computing can be seen as a new phenomenon which is set to revolutionize the way we use the Internet, there is much to be cautious about. There are many new technologies emerging at a rapid rate, each with technological advancements and with the potential of making human's lives easier. However, one must be very careful to understand the security risks and challenges posed in utilizing these technologies. Cloud computing is no exception. In this paper key security considerations and challenges which are currently faced in the Cloud computing are highlighted. Cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution in the future.

References

1. Gens. (2009, Feb.). “New IDC IT Cloud Services Survey: Top Benefits and Challenges”,*IDC eXchange*, Available: <http://blogs.idc.com/ie/?p=730> [Feb. 18, 2010].
2. J. Brodkin. (2008, Jun.). “Gartner: Seven cloud-computing security risks.” *InfoWorld*, Available: <http://www.infoworld.com/d/security-central/gartner-seven-cloudcomputingsecurityrisks-853?page=0,1> [Mar. 13, 2009].
3. Cloud Computing Use Case Discussion Group. "Cloud Computing UseCases Version 3.0,"2010.
4. ENISA. (2009, Feb) "Cloud computing: benefits, risks and recommendations for information security." Available: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computingriskassessment [Jul. 10, 2010].
5. R. K. Balachandra, P. V. Ramakrishna and A. Rakshit.“Cloud Security Issues.”In PROC‘09 IEEE International Conference on Services Computing, 2009, pp 517-520.
6. P. Kresimir and H. Zeljko "Cloud computing security issues and challenges." In PROCThird International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, 2010, pp. 344-349.
7. B. Grobauer, T. Walloschek and E. Stöcker, "Understanding Cloud Computing Vulnerabilities," *IEEE Security and Privacy*, vol. 99, 2010.
8. S. Subashini, and V. Kavitha. (2010) “A survey on security issues in service delivery models of cloud computing.” *J Network ComputAppl*doi:10.1016/j.jnca.2010.07.006. Jul. 2010.
9. S. Ramgovind, M. M. Eloff, E. Smith. “The Management of Security in Cloud Computing” InPROC 2010 IEEE International Conference on Cloud Computing 2010.
10. A. Morsy, J. Grundy and Müller I. “An Analysis of the Cloud Computing Security Problem” In PROC APSEC 2010 Cloud Workshop. 2010.
11. Cloud Security Alliance (CSA). Available: http://www.cloudsecurityalliance.org [Mar.19,2010]