International Journal of Computer Science and Informatics

Volume 2 | Issue 2 Article 13

October 2012

Security Analysis of Cloud Computing

Shital P. Adkine
Department Of Computer Application, Sardar Patel College, Chandrapur,Maharashtra, India,
shital_adkine@yahoo.com

Security Analysis of Cloud Computing

Shital P. Adkine

Department Of Computer Application, Sardar Patel College, Chandrapur,Maharashtra, India
E-mail : sadkine@gmail.com , shital_adkine@yahoo.com

Abstract **-** Cloud computing play an important role in IT industry. Cloud computing reshaping the IT industry and in software development process. Cloud computing techniques can offer many facilities like sharing of hardware, availability of software and many more resources as a basic need. Cloud computing effectively reduces the cost, maintenance. As same security is important issue. The security issues also one of the major issues in cloud computing because over data located on the centralized location due to this reliability and avaibility of data not achieve. While dealing with cloud computing loss of control over cloud component is one of the major issues in maintenance. This paper focuses a different issues of risk involved in cloud computing. Also primarily aims to highlight the major security issues existing in current cloud computing environments.

Keywords : *Cloud computing, IaaS, PaaS, SaaS, risk.*

I. INTRODUCTION

The cloud can be described as on-demand computing, for anyone with a network connection. Access to applications and data anywhere, anytime, from any device is the potential outcome. We also need to note a distinction between 'private clouds' (which exist *within* an organization) and 'public clouds' which are used to provide services to users outside an Organization .cloud based on demand web-services such as databases, queues, identity management, data on demand etc. are meeting with browser based thick-client frameworks such as AJAX, Adobe flex, MS Silverlight, etc. to create a new breed paradigm. Cloud computing is Internet based development and use of computer technology. it is emerging computing technology that uses the Internet and central remote servers to maintain data and applications.

In past, task such as word processing were not possible without the installation of software on a local computer. With the development of Local Area Networks and wider bandwidth, multiple CPUs and storage devices could be used to host services like word processing in a remotely managed datacenter.

Cloud computing provides computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services. Cloud computing refers to computing with a pool of virtualized computer resources and is driven by economics of scale. A cloud can host a variety of different workloads, and allow workloads to be deployed and scaled-out quickly on-demand by rapid provisioning of virtual machines or physical machines. Cloud computing allows consumers and business to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing storage, memory, processing and bandwidth.

Cloud computing leverages its low cost and simplicity that benefits both users and the providers through providing cost-effective services and pay-per-use pricing model. In cloud computing, everything including software, platform, and infrastructure is as a service. In cloud computing applications are provided and managed by the cloud server and data is stored remotely in the cloud configuration. Users do not download and install application on their own device or computer; all processing and storage is maintained by the cloud server.

A Cloud can be private or public. A public cloud sells services to anyone on the Internet. A private cloud is a proprietary network or a data center that supplies hosted services to limited number of people. When a service provider uses public cloud resources to create their private cloud, the result is called virtual private cloud. Private or public, the goal of cloud computing is to provide easy scalable access to computing resources and IT services.

These services are broadly divided into three categories:

- Infrastructure-as-a-Service (IaaS)
- Platform-as-a-Service (PaaS) and
- software-as-a-Service (SaaS)

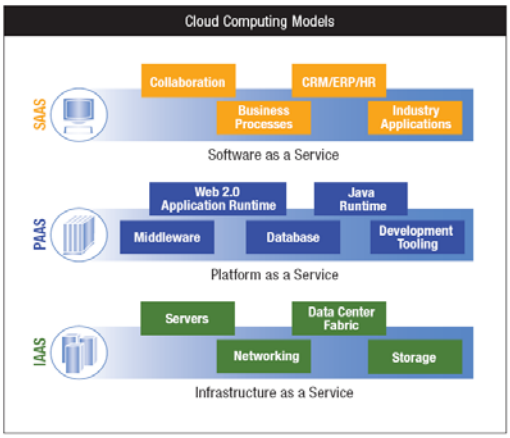


Fig: Cloud computing model [13]

2. Issues in cloud computing

1) To access the cloud servers, it is necessary requirement of constant internet connection, with high bandwidth.
2) Does not work well with low-speed connections.
3) Due to high network traffic on cloud servers, it can be slow.
4) Stored data is not secured because it stored on centralized location,
5) There are some more detailed issues regarding the cloud, and they are in part to do with the nature of the cloud market and its development. Cloud computing is at an early stage in its development, and one of the consequences of this is a lack of definitive market standards. It also means there is a stream of new entrants into the industry, each trying to gain some market power. The lack of market standards leads to issues to do with lock-in (and lack of transferability within the cloud). Once you've committed to a particular cloud provider, an organization is locked in to that provider. This is not a contractual lock-in but a logistical one. Getting data out and moved to a different cloud provider is difficult (but not impossible and third party firms have entered the market to solve this problem). Thus, there are switching costs if you change cloud provider. The issue of lock-in also reflects concerns about reliability. There have been several high profile failures of cloud access, though usually temporary. Both Amazon's and Google's cloud services have been offline a few times, for instance. If you can't move your data or applications to an alternative provider, then your systems are down for the duration. Concerns about security and privacy are frequently mentioned as issues,
6) Confidentiality of data is a potential issue, depending on server location. European servers. One of the most surprising limitations of cloud computing is the data transfer costs. Essentially, the bandwidth required to move large amounts of data in and out of the cloud is just not there.
7) The network connecting clients and servers is a less than secure vehicle that intruders can use to break into computer systems and their various resources. Using publicly available utilities and hardware an attacker can eavesdrop on a network, or "sniff" the network to read packets of information. These packets can contain useful information, E.g. passwords, company details, etc, or reveal weaknesses in the system that can be used to break into the system. Encryption of data can solve the problem of attackers sniffing the network for valuable data. Encryption involves converting the readable data into unreadable data. Only those knowing the decryption key can read the data. A problem here is that some network operating systems don't start encryption until the user has been authenticated (i.e. the password is sent unencrypted But the issues is that how we can encrypt the large volume of data and installation process.

These providers provide their services in all major areas of cloud computing, including SaaS, PaaS and IaaS. Table 1 shows the list of service providers that we studied in this survey. Inorder to analyze the complete state of art of security in cloud computing

Table 1. Major Cloud Service Providers

Service Provider Type	Names
IaaS	Amazon EC2, Amazon S3, GoGrid
PaaS	Google App Engine, Microsoft Azure Services, Amazon Elastic Map Reduce
SaaS	Salesforce, Google Docs

In table 2, we present the results of the survey that depicts the current state of security mechanisms. Information given in table 2 is based on the information available online at the official websites of these providers.

Table 2. Summary of Security Mechanisms by Major Cloud Service Providers

Security Issue	Results
Password Recovery	90% are using standard methods like other common services, while 10% are using sophisticated techniques.
Encryption Mechanism	40% are using standard SSL encryption, while 20% are using encryption mechanism but at an extra cost. 40% are using advance methods like HTTPS access also.
Data Location	70% have their datacenters located in more than one country, while 10% are located at a single location. 20% are not open about this issue.
Availability History	In 40% there is a reported downtime alongwith a result in data loss, while in 60% cases data availability is good.
Proprietary/Open	Only 10% providers have open mechanism.
Monitoring Services	70% are providing extra monitoring services, while 10% are using automatic techniques. 20 % are not open about this issue.

3. Common security requirements

In general the following security point take care of while dealing with cloud computing.

GOAL	DESCRIPTION
CONFIDENTIALITY	Ensuring that information is not disclosed to unauthorized persons.
INTEGRITY	Ensuring that information held in a system is a proper representation of the information intended and that it has not been modified by an unauthorized person.
AVAILABILITY	Ensuring that information processing resources are not made unavailable by malicious action.
NON-REPUDIATION	Ensuring that agreements made electronically can be proven to have been made.

IV. RISK ON CLOUD COMPUTING

Current cloud service providers operate very large systems. They have sophisticated processes and expert personnel for maintaining their systems, but for small enterprises and industries may not have access to like large system. As a result, there are many direct and indirect security advantages for the cloud users. Here we mention some Line of security for cloud computing.

Assets: It includes some question like which assets we are trying to protect?

What properties of these assets must be maintained? The Assets include following data.

- Customer Data
- Customer applications
- Client Computing Devices

Threats: What attacks can be mounted? What other threats are there due to natural, disasters, etc.

Countermeasures: How can we counter those attacks?

Failures in Provider Security: Provider in terms of servers, network, etc. The Customer must trust provider's security, and Many times Failures may violate CIA principles.

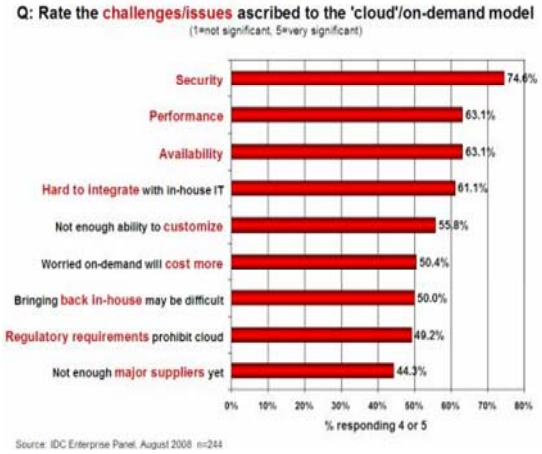
Attacks by Other Customers: It included threats when the provider resources shared with untrusted parties (or customer), uses of different CPU, storage, network, etc. When cloud implemented that time Customer data and applications must be separated. Many of the time failures will violate CIA principles

Availability and Reliability Issues: Clouds may be less available than in-house IT, Due to cloud complexity increases chance of failure, Clouds are prominent attack targets, Internet reliability is spotty Shared resources may provide attack vectors, BUT cloud providers focus on availability

Legal and Regulatory Issues: Laws and regulations may prevent cloud computing, Requirements to retain control, Certification requirements not met by provider. Geographical limitations – EU Data Privacy, New locations may trigger new laws and regulations.

Perimeter Security Model Broken: Including the cloud in your perimeter, Lets attackers inside the perimeter, Prevents mobile users from accessing the cloud directly, not including the cloud in your perimeter, Essential services aren't trusted, No access controls on cloud.

Integrating Provider and Customer Security System: Disconnected provider and customer security systems, Fired employee retains access to cloud, Misbehavior in cloud not reported to customer



V. CLOUD COMPUTING SECURITY ISSUES

According to analyst firm Gartner, customer should consider following seven cloud computing security risks before selecting a cloud computing vendor[7].

Privileged User Access: Sensitive data processed outside the enterprise brings with it an inherent level of risk, because outsourced services bypass the "physical, logical and personnel controls".

Regulatory Compliance: Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider. Traditional service providers are subjected to external audits and security certifications. Cloud computing providers who refuse to undergo this scrutiny are "signaling that customers can only use them for the most trivial functions," according to Gartner [2].

Data Location: When you use the cloud, you probably won't know exactly where your data is hosted. In fact, you might not even know what country it will be stored in. Ask providers if they will commit to storing and processing data in specific jurisdictions, and whether they will make a contractual commitment to obey local privacy requirements on behalf of their customers, Gartner advises.

Data segregation: Data in the cloud is typically in a shared environment alongside data from other customers. Encryption is effective but isn't a cure-all. "Find out what is done to segregate data at rest," Gartner advises. The cloud provider should provide evidence that encryption schemes were designed and tested by experienced specialists. "Encryption accidents can make data totally unusable, and even normal encryption can complicate availability," Gartner says [2].

Recovery: Even if you don't know where your data is, a cloud provider should tell you what will happen to your data and service in case of a disaster. "Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure," Gartner says [2]. Ask your provider if it has "the ability to do a complete restoration, and how long it will take."

Investigative support: Investigating inappropriate or illegal activity may be impossible in cloud computing, Gartner warns. Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers

Long-term viability: Ideally, cloud computing provider will never go broke or get acquired and swallowed up by a larger company. But you must be sure your data will remain available even after such an event. "Ask potential providers how you would get your data back and if it would be in a format that you could import into a replacement application," Gartner says [2].

VI. CONCLUSION

The present paper reveals that, Cloud computing reshaping the IT industry. Cloud computing technology faces lot of issues such as data transfer rate is very low due to heavy traffic network and low bandwidth to transfer 1 terabyte of data it take more time (1 to 2 days) so it is quicker and cheaper to courier external hard drives than to move large volumes of data (i.e. in multiples of terabytes) over the internet due heavy traffic on the network and low bandwidth. The security issues also one of the major issues in cloud computing because over data located on the centralized location due to this reliability and avaibility of data not achieve.

According to research as computing takes a step forward to cloud computing, Cloud security can be delivered as part of the cloud service and also as specific components added in to enhance security. It should not move backward. Users certainly should not accept moving backwards in terms of security. As for the user security is a very prior issueas customer data and program is residing on provider premises. So following two questions arises.

1. At what extent data is secure?
2. At what extent code is secure?

Is cloud computing interrupting the services or we lose privacy of data. At what level our data is damaged, as cloud offers a sharing of information, software and processors at low cost, but we have to gets answer to all security questions regarding in cloud computing.Because security is a key requirement for today's cloud users, it should also be looked upon as a means of way and an opportunity to meet a customer need that may not be well met by the rest of the marketplace.

Our analysis showed that, with careful design and cloud selection, computation in the cloud can be fault-tolerant and reliable. The issue of privacy protection of the client's data and results will be studied as well.

Further on we present some future work ideas that aim to improve the data integrity concept in cloud computing, the issue of privacy protection of the clients data and result will be studied as well ,especially in an open environment (Internet)Improved support for user data security: computation results data can be encrypted and/or signed so that the user of the system can be sure the received data is correct.

REFERENCES

[1]. Hayes, B.: Cloud Computing. Communications ACM 51, 9–11 (2008)

[2] Brodkin, J.: Seven Cloud Computing Security Risks(2008), http://www.gartner.com/DisplayDocument?id=685308

[3] http://en.wikipedia.org/wiki/Cloud_computing

[4]. http://searchcloudcomputing.techtarget.co/

[5]. http://cloudsecurity.org/

[6]. http://www.cloudsecurityalliance.org/

[7]. http://csrc.nist.gov/groups/SNS/cloud-computing/

[8]. http://www.computerweekly.com/ Articles/ 2009/04/ 24/235782/ top-five-cloud-computing-security-issues.htm

[9]. http://webhostinggeeks.com/ blog/2009/08/04/is-cloud-computing-behi

[10] Steve Hanna, Juniper Networks, Cloud Computing: Finding the Silver Lining

[11] John, H.: Security Guidance for Critical Areas of Focus in Cloud Computing (2009), http://www.cloudsecurityalliance.org/guidance/ (Accessed 2 July 2009)

[12]. Gens, F.: IT Cloud Services User Survey, part 2: Top Benefits and Challenges

[13] Cloud computing Whitepaper, November 2009, IBM Point of View: Security and Cloud Computing.