RESEARCHERID
THOMSON REUTERS
ISSN: 2277-9655
[ICEMESM-18] Impact Factor: 5.164
IC™ Value: 3.00 CODEN: IJESS7
IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A CRITICAL STUDY OF CHALLENGES IN CLOUD COMPUTING AND RELATED SECURITY PROBLEMS

Prof. Miss Shital P. Adkine[*1] & Prof. Miss Shweta R. Kakde[2]
[*1&2]Department Of Computer Science, K.R.P.M. Nagpur, Maharashtra, India

DOI: 10.5281/zenodo.1220909

ABSTRACT

Cloud computing technology is a new concept of providing reliable, customized and guaranteed computing dynamic environments for end- users; also provide scalable and virtualized resources, bandwidth, software and hardware on demand to consumers. Consumers can typically requests cloud services via a web browser or web service. This paper reviews Cloud Computing, its architecture and Significance, identifies the concepts and characteristics of Clouds. The paper covers the issues that can arise and face in the implementation cloud computing. Using cloud computing, consumers can safe cost of hardware deployment, software licenses and system maintenance. On the other hand, Privacy is an important issue for cloud computing, both in terms of legal compliance and user trust. This paper discusses the issue of cloud computing and outlines its implications for the privacy of personal information as well as its implications for the confidentiality.

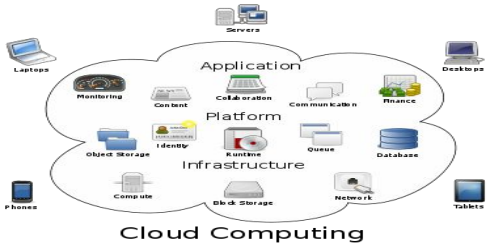
Keywords: Cloud computing,, Security issues, security, cloud security.

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. Cloud computing provides the next generation of internet based, highly scalable distributed computing systems in which computational resources are offered 'as a service'. 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 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. From the cloud providers" perspective, security requires a lot of expenditures (security solutions" licenses), resources (security is a resource consuming task), and is a difficult problem to master (as we discuss later)

There are many companies providing services through private and public clouds .Each has its own requirement and processes for authenticating and authorizing users. As these services connect and share information with each other, each service provider must be sure that it knows the degree to which it can trust the clouds, services and users with which it transacts. The service provider must have the best information security system in the world but it efforts are useless if it"s granting peer-level access to cloud partners with less stringent security standards.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7



II. CLOUD SERVICE MODELS

Cloud computing provides different services rather than a unit of product. These services put forwarded 3 models: software as a service (SAAS), platform as a Service (PAAS), and infrastructure as a Service (IAAS) (Iyer and Henderson, 2010; Han, 2010, Mell and Grance, 2010).

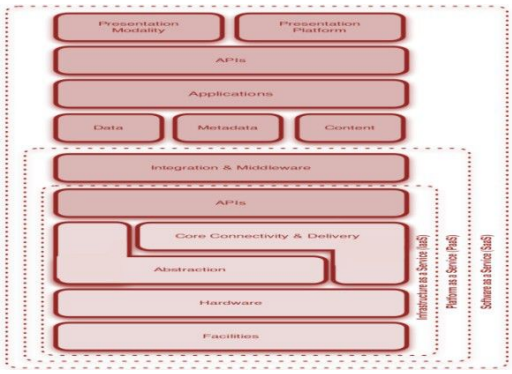


Fig. 1. Cloud Service Model

1) SAAS: it is run by cloud service provider and mostly used by organizations. It is available to users through internet.
2) PAAS: It is a tool (Windows, LINUX) used by developers for developing Websites without installing any software on the system, and can be executed without any administrative expertise.
3) IAAS: It is operated, maintained and control by cloud service providers that support various operations like storage, hardware, servers and networking.

A. Cloud Deployment Models

There are four types of cloud computing models listed by NIST (2009): private cloud, public cloud, hybrid cloud and community cloud.

1) *Public Cloud*: it is for the general public where resources, web applications, web services are provided over the internet and any user can get the services from the cloud,. Public Organizations helps in providing the infrastructure to execute the public cloud.
2) *Private Cloud***:** It is used by the organizations internally and is for a single organization, anyone within the organization can access the data, services and web applications but users outside the organizations cannot access the cloud. Infrastruture of private cloud are completely managed and corporate data are fully maintained by the organization itself.
3) *Hybrid Cloud***:** The Cloud is a combination of two or more clouds (public, private and community). Basically it is an environment in which multiple
4) internal or external suppliers of cloud services are used. It is being used by most of the organizations (IBM and Junipers Network, 2009).
5) *Community Cloud:* The cloud is basically the mixture of one or more public, private or hybrid clouds, which is shared by many organizations for a single cause (mostly security).Infrastructure is to be shared by several organizations within specific community with common security, compliance objectives. It is managed by third party or managed internally. Its cost is lesser then public cloud but more than private cloud.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

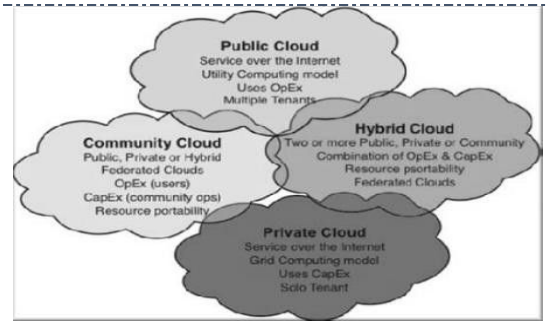


Fig.II Deployment Model for Cloud

B. Characteristics of cloud computing

Cloud computing exhibit five essential characteristics defined by NIST (National Institute of Standards and Technology) [1].

On-demand self-service. A consumer can unilaterally provision computing capabilities.

Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms.

1) *Resource pooling.* The provider"s computing resources are pooled to serve multiple consumers, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.
2) *Rapid elasticity.* Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in.
3) *Measured service.* Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service.

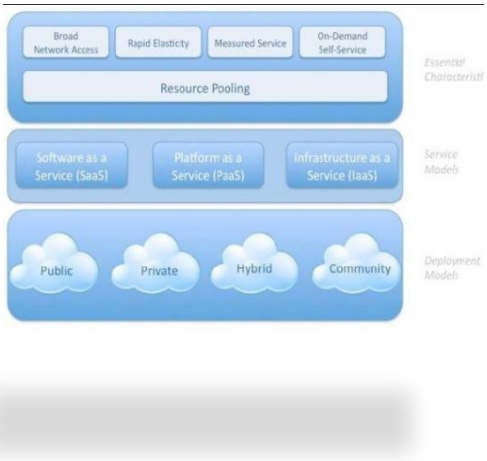


Fig. III. Nist Visual Model of Cloud Computing Definition [3].

III. 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

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

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 he 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. In order to analyze the complete state of art of security in cloud computing

table I. 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 II, 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 II. summary of security mechanisms by major cloud

Security Issue	Results
Password Recovery	90% are using standard methods like other common se vices, while 10% are using sophisticated techniques.
Encryption Mechanism	40% are using standard SSL encryption, while 20% a 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 o 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 resu in data loss, while in 60% cases data availability is goo
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 abo this issue.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

IV. CLOUD COMPUTING SECURITY THREATS

A. Top Seven Security Threats

Top seven security threats to cloud computing discovered by "Cloud Security Alliance" (CSA) are [6]:

1. *Abuse and Nefarious Use of Cloud Computing***.** Abuse and nefarious use of cloud computing is the top threat identified by the CSA. A simple example of this is the use of botnets to spread spam and malware. Attackers can infiltrate a public cloud, for example, and find a way to upload malware to thousands of computers and use the power of the cloud infrastructure to attack other machines. Suggested remedies by the CSA to lessen this threat:
   - Stricter initial registration and validation processes.
   - Enhanced credit card fraud monitoring and coordination.
   - Comprehensive introspection of customer network traffic.
   - Monitoring public blacklists for one"s own network blocks.
2. *Insecure Application Programming Interfaces.* As software interfaces or APIs are what customers use to interact with cloud services, those must have extremely secure authentication, access control, encryption and activity monitoring mechanisms - especially when third parties start to build on them. Suggested remedies by CSA to lessen this threat:
   - Analyze the security model of cloud provider interfaces.
   - Ensure strong authentication and access controls are implemented in concert with encrypted transmission.
   - Understand the dependency chain associated with the API.
3. *Malicious Insiders***.** The malicious insider threat is one that gains in importance as many providers still don't reveal how they hire people, how they grant them access to assets or how they monitor them. Transparency is, in this case, vital to a secure cloud offering, along with compliance reporting and breach notification. Suggested remedies by CSA to lessen this threat:
   - Enforce strict supply chain management and conduct a comprehensive supplier assessment.
   - Specify human resource requirements as part of legal contracts.
   - Require transparency into overall information security and management practices, as well as compliance reporting.
   - Determine security breach notification processes.
4. *Shared Technology Vulnerabilities***.** Sharing infrastructure is a way of life for IaaS providers. Unfortunately, the components on which this infrastructure is based were not designed for that. To ensure that customers don't thread on each other's "territory", monitoring and strong compartmentalization is required. Suggested remedies by CSA to lessen this threat:
   - Implement security best practices for installation/configuration.
   - Monitor environment for unauthorized changes/activity.
   - Promote strong authentication and access control for administrative access and operations.
   - Enforce service level agreements for patching and vulnerability remediation.
   - Conduct vulnerability scanning and configuration audits.
5. *Data Loss/Leakage***.** Be it by deletion without a backup, by loss of the encoding key or by unauthorized access, data is always in danger of being lost or stolen. This is one of the top concerns for businesses, because they not only stand to lose their reputation, but are also obligated by law to keep it safe

   Suggested remedies by CSA to lessen this threat:
   - Implement strong API access control.
   - Encrypt and protect integrity of data in transit.
   - Analyze data protection at both design and run time.
   - Implement strong key generation, storage and management, and destruction practices.
   - Contractually demand providers to wipe persistent media before it is released into the pool.
   - Contractually specify provider backup and retention strategies.
6. *Account, Service & Traffic Hijacking***.** Account service and traffic hijacking is another issue that cloud users need to be aware of. These threats range from man-in-the-middle attacks, to phishing and spam campaigns, to denial-of service attacks.

Suggested remedies by CSA to lessen this threat:

- Prohibit the sharing of account credentials between users and services.
- Leverage strong two-factor authentication techniques where possible.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

- Employ proactive monitoring to detect unauthorized activity.
- Understand cloud provider security policies and SLAs.

7. *Unknown Risk Profile***.** Security should always in the upper portion of the priority list. Code updates, security practices, vulnerability profiles, intrusion attempts – all things that should always be kept in mind.Suggested remedies by CSA to lessen this threat:

- Disclosure of applicable logs and data.
- Partial/full disclosure of infrastructure details (*e.g.,* patch levels, firewalls, etc.).
- Monitoring and alerting on necessary information

V. CONCLUSION

Security as a tool to enable cloud environment remain the same but it changes in the way it is applied to the environment today. Security can have very layered approached and security does not stand alone. We believe that due to the complexity of the cloud, it will be difficult to achieve end-to-end security .Various factor play an important role in cloud security. One of the Major security concerns in cloud computing deals with the confidentiality of operation, integrity of data to be maintained and ensuring availability of application for user. So following are the backup question arises with the confidentiality, data security, recovery of data.

- How many copies of data are being stored?
- At what location data is stored?
- How often is data backed up?
- If 1000 data files uploaded in a day to the cloud but the cloud only backs it up once a week? If this is
- happened , then can it lost 6000 or 7000 files ?can we have to recreate?
- If data is stored as a backup, how is it protected?
- Is it in encrypted format?
- How long will it take to restore lost data?
- Are others ahead?
- Can extra cost for priority service?
- Is data dependent on other data or applications? Can priority given to data recovered first? Cloud security also incorporates with following three key ideas to defending against the threat.
- Data lockdown
- Access policies
- Security intelligence

Cloud Computing has the potential to be way more secure than anything else. The key is that Cloud services must be inherently secure

VI. REFERENCES

[1] Peter Mell, and Tim Grance, "The NIST Definition of Cloud Computing,"2009, http://www.wheresmyserver.co.nz/storage/media/faq- files/clouddef-v15.pdf, Accessed April 2010.
[2] Frank Gens, Robert P Mahowald and Richard L Villars. (2009, IDC Cloud Computing 2010.
[3] IDC, "IDC Ranking of issues of Cloud Computing model," ed, 2009,http://blogs.idc.com/ie/?p=210, Accessed on July 2010.
[4] Cloud Computing Use Case Discussion Group, "Cloud Computing Use Cases Version 3.0," 2010.
[5] ENISA, "Cloud computing: benefits, risks and recommendations for information security," 2009,http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computingrisk-assessment, Accessed On July 2010.
[6] Cloud Security Alliance (CSA). (2010). Available:http://www.cloudsecurityalliance.org/
[7] Balachandra Reddy Kandukuri, Ramakrishna Paturi and Atanu http://www.computerweekly.com/Articles/2009/04/24/235782/top -five-cloud-computing-security-issues.htm
[8] .http://webhostinggeeks.com/blog/2009/08/04/is-cloud- computing-behi
[9] Steve Hanna, Juniper Networks, Cloud Computing: Finding the Silver Lining
[10] John, H.: Security Guidance for Critical Areas of Focus in Cloud Computing (2009),
[11] Hayes, B.: Cloud Computing. Communications ACM 51, 9– 11 (2008)
[12] Brodkin, J.: Seven Cloud Computing Security Risks(2008),

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

http://www.gartner.com/DisplayDocument?id=685308
[13] http://en.wikipedia.org/wiki/Cloud_computing
[14] .http://searchcloudcomputing.techtarget.co/ [16]. http://cloudsecurity.org/
[15] http://www.cloudsecurityalliance.org/
[16] http://csrc.nist.gov/groups/SNS/cloud-computing/

CITE AN ARTICLE

It will get done by IJESRT Team