Cloud Computing Security Concerns

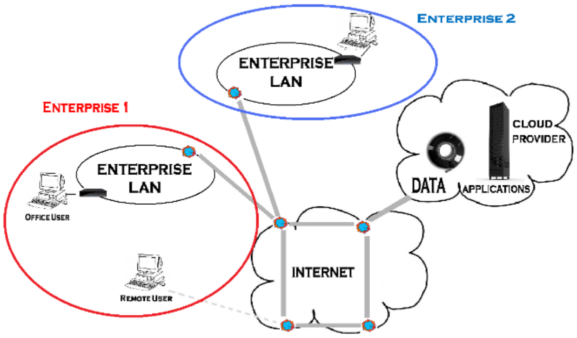
Christina Ruby
New Horizon College, Kasturi Nagar, Bangalore
christinaruby2012@gmail.com

Abstract : The increased degree of connectivity and the increasing amount of data has led many providers and in particular data centers to employ larger infrastructures with dynamic load and access balancing. By distributing and replicating data across servers on demand, resource utilization has significantly improved. The coming shift to cloud computing is a major change in the IT industry nowadays. As the name suggests, cloud computing lets developers write applications and use services that run in the cloud. Even though it has many characteristic features such as Elasticity, Reliability, Quality of Service, Agility and adaptability, Availability of services, Cost reduction, Pay per use, Improved time to market, Return of investment, etc.There are also a lot of security concerns about its privacy, security, data integrity, intellectual property management, audit trails, and several other issues. Security and privacy continue to be the top concerns in adopting cloud computing. Security risks are often more pronounced on the cloud because the company turns over custody of their data to the provider such as sensitive customer data and mission critical systems. Data, application and network back-up and redundancy will become very essential in these cases.

Keywords: Cloud, cloud computing, cloud model, service, risk, security, privacy.

SERVICES OFFERED BY CLOUD

The diagrammatic representation of the cloud computing model is shown below:



A cloud service has three distinct characteristics that differentiate it from traditional hosting. It is sold on demand, typically by the minute or the hour; it is elastic, a user can have as much or as little of a service as they want at any given time; and the service is fully managed by the cloud provider. Cloud computing is a general term for anything that involves delivering hosted services over the Internet. Some of these services are shown in the next section.

The following contains some of the services offered in cloud computing:

1. Software as a service (SaaS): A SaaS application runs entirely in the cloud

2. Infrastructure as a Service (IaaS): These provide scalable resources as services to the user.

3. Platform as a Service (PaaS): They provide computational resources using which applications and services can be developed and hosted.

FUTURE OF CLOUD COMPUTING

➢ Cloud Computing is being used by the organizations dealing in smaller projects. For large organizations, Security is the biggest concern. There are few crucial details like license, security, privacy that needs to be worked upon soon.

➢ Educational Purposes: Cloud Computing can be used for expanding the education in the entire world. This is possible by sharing an important information, article or project details with all the stakeholders (like students, professors and researchers etc.) working on the same. Cloud Computing can prove to be a 'Budgeted Technology Training' in the future.

➢ For Personal Usage: Using the Cloud Computing concepts, the end user is not required to take a back up of his files and documents on his system. He/she can keep his system free from all kinds of data backups.

TYPES OF RISKS

The different types of risks encountered in cloud computing are:-

1. Location - Storing data in certain regions may not be acceptable to your customers, especially the government.

2. Operational - Whether we can transfer data and applications to and from the cloud. Or whether we are bound to a certain application or platform or OS.

3. Third party contractual limitations on use of cloud
Privileged user access i.e. who has access to data and their backgrounds.
- Data location i.e. whether you control the physical location of your data?

4. Security

- Physical security i.e. Physical location of data centers; protection of data centers against disaster and intrusion.
- Operational security i.e. who has access to facilities/applications/data?

4. PRIVACY AND SECURITY CONCERNS

Some questions that arise due to privacy and security concerns in Cloud Computing:

USUAL SECURITY THREATS

The typical security threats associated with cloud computing are:-

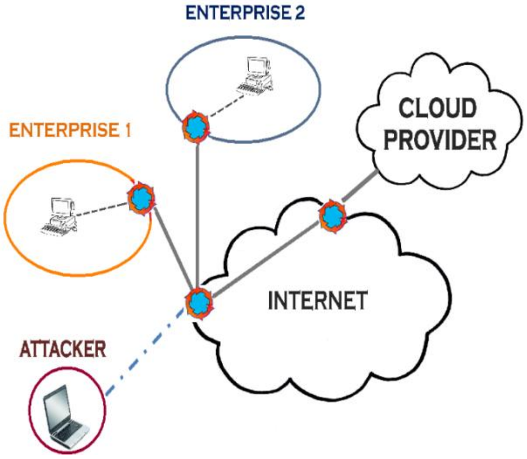
1. Spoofing Identity - In this way, an attacker can fool a victim into believing that he has proper authorization which results in accessing confidential data.

2. Data tampering – The attacker can delete or modify the data which results in unreliable data.

3. Information disclosure - In this way, an attacker can fool a victim into disclosing confidential information

4. Denial of service – This type of attack consumes excess bandwidth and uses unwanted resources, which causes network traffic.

5. Repudiation – Refuses to check the origin and integrity of the data.



Once an attacker gains access to the network, any of the above threats may occur.

TYPES OF CLOUD MODELS

Based on the cloud model which is being used we need to control and eliminate any security risks.

There are four cloud models:

1. Are hosted data and applications within the cloud protected by suitably robust privacy policies?

2. Are the cloud computing provider's technical infrastructure, applications, and processes secure?

3. Are processes in place to support appropriate action in the event of an incident that affects privacy or security?

1. Private cloud - The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party.

2. Community cloud - The cloud infrastructure is shared by several organizations.

3. Public cloud - The cloud infrastructure is made available to the general public and is owned by an organization selling cloud services.

4. Hybrid cloud - The cloud infrastructure is a composition of two or more clouds (private, community, or public).

STEPS TO TACKLE SECURITY ISSUES

1. Selecting a Vendor and Ensuring Proper Security

- Select an appropriate cloud model based on the type of information that will be moved to the cloud.

- Look for a cloud model that contains redundancy. Though data loss could occur and result in lost profits.

- Thoroughly investigate not only the vendor's encryption and access security, but also the security of the physical location of the servers.

2. Entering into a Service Agreement

The service agreement should address:

- Records management – require the cloud vendor to follow the company's destruction and retention policies, including retention, rotation and destruction of backup tapes.

- Accessibility – include a timeliness provision stating how long the cloud vendor has to deliver the company's data.

- Customer support – include a service guarantee to ensure there is adequate support, particularly when executing preservation or collection obligations or data transfer.

- Legal policies – specify how the cloud vendor will respond to a subpoena requiring production of the company's data.

- Confidentiality – require a privacy provision that contractually obligates the cloud vendor to keep the company's data private.

- Length of Agreement – try not to commit to a multi-year contract and include a severability clause. If any vendor issues arise, the company's data may be locked.

- Termination – detail how and when data will be transferred if there is a breach or termination of the contract.

3. Executing a Coordinated eDiscovery Plan

- Develop a comprehensive preservation plan, identifying key contacts at the vendor who will be responsible for receiving the preservation notice and fulfilling the vendor's obligations under the notice.

- When a duty to preserve triggers, send a preservation notice to the identified contacts at the cloud vendor.

- Determine in advance how the electronically stored information will be collected, the format it will be provided in, and the best format for production.

- To the extent practical, ensure naming conventions, folder structures and other organizational tools are used in the platform in the cloud. Know the data destruction procedures and policies of the cloud provider.

- Data that is improperly destroyed may be located and accessed by an unauthorized user or otherwise result in a data breach.

4. Contemplate an Exit Strategy

- Software as a Service and Platform as Service providers often use unique proprietary applications and interfaces for their databases. Reformatting the data to be accessible by another provider may be costly and complex.

- Find a back-up vendor that utilizes the same on-premise systems as your current cloud provider in case the need arises for a quick move.

CONCLUSION

Cloud platforms aren't yet at the center of most people's attention. The odds are good, though, that this won't be true in the near future. To take full advantage of the benefits, users must be given reliable assurances regarding the privacy and security of their online data. The attractions of cloud-based computing, including scalability and lower costs, are very real. If you work in application development, whether for a software vendor or an end user, expect the cloud to play an increasing role in your future. The next generation of application platforms is here.

REFERENCES

i. Tim Mather, SubraKumaraswamy, ShahedLatif, "Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance", 1st Edition, O'Reilly Media, Inc, September 2009.

ii. *Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1", -* ***http://www.cloudsecurityalliance.org/csaguide.pdf, December 2009***

iii. Te-Shun Chou, Department of Technology Systems, East Carolina University, Greenville, NC, U.S.A."Security Threats On Cloud Computing Vulnerabilities" International Journal of Computer Science & Information Technology (IJCSIT) Vol 5, No 3, June 2013, pp. 80-81.

iv. .ParikshitPrasad,BadrinathOjha,RajeevRanjanshahi,RatanLal." 3 Dimensional Security in Cloud Computing",Indian Institute of Information Technology, Allahabad U.P India.

v. .Sagar Tirodkar1, Yazad Baldawala1, Sagar Ulane1, Ashok Jori1 "Improved 3-Dimensional Security inCloud Computing", International Journal of Computer Trends and Technology (IJCTT) – volume 9, 5– Mar 2014

vi. .S.Sajithabanu and E.George Prakash Raj, "Data Storage Security in Cloud," International Journal of Computer Science and Technology, ISSN: 0976-8491 (Online)| ISSN: 2229-4333 (Print), IJCST Vol. 2, Issue 4, Oct. -Dec. 2011.

vii. Sean Convery," Network Authentication, Authorization, and Accounting: Part One" The Internet Protocol Journal - Volume 10, No. 1,March 2007.

viii. P. Mell and T. Grance, "The NIST Definition of Cloud Computing" Computer Security Division, IT Laboratory, National Institute of Standards and Technology,Gaithersburg,2011.http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf ,pp.2-3.

ix. CloudServices<https://www.wikipedia.org/wiki/cloud_computing>