Is Cloud Secure Enough

Farzad Sabahi

***Abstract*—Cloud computing is a style of computing where scalable IT-related capabilities are provided "as a service" to external customers based on a network such as Internet. Although there are some issues, such as security, that cause cloud clients to worry about, with the growing of cloud computing, data security may become one of the most important concerns for IT governments to move their application and data from local data centers to the cloud environments. For enterprises, it is important to trade off among risks and benefits introduced by cloud technology before deciding to move to the cloud environments. In this paper, I try to summarize cloud computing RAS (Reliability, Availability, and Security) concerns. Additionally, I introduce available solutions for some of those concerns.**

***Index Terms*—Cloud computing, virtualization, security.**

I. Introduction

As defined by the National Institute of Standards and Technology (NIST) , cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of essential characteristics, deployment models, and various service models [1]. Cloud technology tries to disguise complexity for its clients. Generally, Cloud providers use virtualization technologies combined with self-service abilities for computing resources via network infrastructure especially the Internet [2]. Cloud has several noticeable benefits:

- Cloud is useable while it is a money-saver technology. Users do not need to have a local and dedicated data center. This can save more energy and absolutely can reduce costs in enterprises.
- Cloud helps users to implement their application rapidly without involving to the complexity, which exists before using cloud.
- Cloud computing can offer a higher level of reliability and it will be able to respond to emergencies immediately.
- Cloud computing simplifies configuration for users and hides complexity and details from users. Users can focus just on implementing their applications.

A. Cloud Characteristics

In cloud environments, several kinds of virtual machines are hosted on the same physical server as infrastructure. In such environments, a consumer can use computing capability without requiring human interaction with each service's provider. In addition, cloud computing is a pay-as-you-go and one has to only pay for what they use. Users do not have to pay for the local resources they need such as storage or physical infrastructure. Nowadays, we have several types of cloud environments.

- Public cloud: A public cloud is base model which providers provide several resources, such as applications or storage. Such resources are generally available to the public users with pay-as-you-go approach or sometimes they are free to use.
- Private cloud: Private cloud refers to internal services a business offers that are accessible just for users who have permission to use it. We can say that Private cloud is similar to local data center scenario.
- Hybrid cloud: The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds) [3].
- Community cloud: The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns. It may be managed by the organizations or a third party and may exist on premises or off premises [3].

As mentioned in [3] the cloud has several characteristics which make it useful and it is one of the most noticeable technologies for all types of costumers from ordinary people to large enterprises.

- On-demand self-service: A consumer can use service as needed such as server time and network storage automatically.
- Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., cellphones, laptops, and PDAs).
- Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.
- Rapid elasticity: Capabilities can be rapidly and elastically provisioned, in some cases automatically, to scale up quickly.
- 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 (e.g., storage, processing, bandwidth, and active user accounts).

Manuscript received July 25, 2012; revised September 26, 2012.

F. Sabahi is with the Azad University, Zanjan, Iran (e-mail: f.sabahi@ieee.org).

In cloud, similar to every proposed technology, there are some issues and concerns that can worry everyone, which most important of them is RAS factor. In order to achieve the best performance in cloud, providers must meet several management features carefully to ensure about these RAS parameters [4]:

1) Availability management
2) Access control management
3) Vulnerability and problem management
4) Patch and configuration management
5) countermeasure response
6) Circumstance of deployed cloud system
7) access control and event monitoring

There are three major groups of service in cloud and it should be noted that other types of service are derived from these.

- Software as a Service (SaaS): typically accessed by users using a web browser over the Internet.
- Platform as a Service (PaaS): Giving a computing platform or solution stack as a service.
- Infrastructure as a Service (IaaS): The delivery of computer IaaS, typically platform virtualization.

II. Information Security Policies

Cloud computing technology introduces a set of important policy issues, which include issues of privacy, security, anonymity, telecommunications capacity, government surveillance, reliability, and liability, among others [1]. On the other hand, the most important challenge among these issues is security and how cloud providers encounter with it. Cloud computing has several types of customers such as ordinary users, academia, and enterprises who have different motivations to move to cloud. If cloud clients are academia, security has impacts on performance of computing and for them cloud providers have to find a way to combine security and performance. For enterprises, too, the most important problem is security but with different vision. For them high performance may not be as critical as academia. Well-known Gartner's seven security issues which cloud clients should consider are mentioned below [5]:

- 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" IT shops exert over in-house programs.
- Regulatory compliance: Customers are ultimately responsible for the security and integrity of their own data, even when a service provider holds it. Traditional service providers are subjected to external audits and security certifications.
- Data location: When users use the cloud, they probably will not know exactly where their data are hosted.
- Data segregation: Data in the cloud is typically in a shared environment alongside data from other customers. Encryption is effective but is not a cure-all.
- Recovery: If a cloud provider broke or some problems cause failure in cloud, what will happen to users' data? Moreover clients prefer not to let a third party to control their data and this will cause an impasse in security policy to encounter with these challengeable situations.
- Investigative support: Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may be spread across an ever-changing set of hosts and data centers.
- Long-term viability: Ideally, cloud-computing providers will never go broke or get acquired by a larger company with maybe new policies. Nevertheless, users must be sure their data will remain available even after such an event.

III. Cloud RAS Issues

Using Cloud results applications and data will move under third-party control. The cloud services delivery model will create clouds of virtual perimeters as well as a security model with responsibilities shared between the customer and the cloud service provider. This shared responsibility model will bring new security management challenges to the organization's IT operations staff [6]

Generally, the first question from information security officers is whether their company has adequate transparency from cloud services to manage cloud. In addition, how is implementation of security management processes to assure customers about their data that are they appropriately protected from unauthorized access? The answer to these questions has two parts: what security controls policies must the customer perform in the cloud platform, and how must an enterprise's security management tools adapt to manage security in the cloud. Both answers must be continually reevaluated based on the sensitivity of the data and the service-level changes over time [6].

A. Data Leakage

Innately, when moving to a cloud, there are two changes for customer's data. First, the data will host away from the customer's local machine. Second, the data will move from a single-tenant to a multi-tenant environment. These changes can raise probability of data leakage problem. This concern can prevent several enterprises from using cloud if cloud providers are not able to convince and tranquilize them.

Fortunately, there are solutions that are in the use of data leakage prevention (DLP) applications to protect sensitive data. However, if data stored in a public cloud due to its nature, which uses DLP products, have low performance, in order to assure the confidentiality, more considerations are required compared to other types of clouds. In service level, Inherently in SaaS and PaaS, a cloud client does not have control over security management, which is used by cloud provider. Therefore, discovery within clients' data with DLP agents is impossible except when the provider puts this facility in its service. However, if service is IaaS, it is possible to embed DLP agents into a virtual machine to have some control facilities over data.

In private clouds, cloud the costumers and the provider are in the same company. Because of the costumers have direct

control over the whole infrastructure similar to local data center scenario; they can put DLP agents that are deployed in connection with SaaS, PaaS, or IaaS services.

In hybrid cloud, this depends on which service is used by the costumer but if the service is IaaS, the client could set in DLP agents for some control over data. Otherwise, hybrid cloud seems similar to other types of cloud.

B. Cloud Security Issues

As mentioned above, Internet is the communication infrastructure for cloud. As we know, Internet uses TCP/IP protocol that employs IP addresses to identify users. Similar to a physical computer in the Internet that has an IP address, a virtual machine, which is used in cloud and in the Internet as communication infrastructure of cloud, has an IP address as well. An attacker, whether internal or external, similar to legal users can find these IP addresses, too. In this case, a malicious user can find out which physical servers the victim is using and will implant a malicious virtual machine at that location from which an attack is launched [7]. Because all users employ the same infrastructure as virtual machine for their applications, if hackers can take control over a virtual machine, they absolutely inherit all data that exist within it. It means that the hacker can copy them into his local machine in order to analyze them to find valuable data before cloud provider can detect that virtual machine is in an out-of-control situation.

1) Attacks in cloud

Generally, the cloud can give service to malicious users as legal users. Hackers can use a cloud to host his malicious application to gain their target such as DDoS against cloud itself or another user in the cloud. For example, assume an attacker knows the location of his victim cloud provider and virtual machine in that. Thereby the attacker can establish attack against his victim(s). This situation is similar to the scenario in which both the attacker and the victim are in the same physical network except the fact that in cloud environments they use virtual machines instead of physical network.

a) DDoS attacks against cloud

Distributed Denial of Service (DDoS) attacks typically focus flooding high quantity of IP packets at a specific network to victim. In cloud computing where infrastructure is shared by a large number of clients, DDoS attacks may have the potential of having much greater impact than against single tenanted architectures[8]. If cloud has not sufficient resource to provide services to its customers, then this may cause unpredictable DDoS attacks. Solution for this event is a traditional solution that is placing more amounts of such critical resources.

Normally, most network response cannot protect against DDoS attacks as they cannot stop the deluge of traffic and typically cannot distinguish legal traffic from illegal traffic. Intrusion Prevention Systems (IPS) are effective if the attacks are identified and have pre-existing signatures but are ineffective if there is legitimate content with bad intentions[9]. Unfortunately, firewalls are vulnerable and ineffective against DDoS attacks, too. This is because the attacker, similar to IPS solution, can easily bypass firewalls since they are designed to transmit legitimate traffic and attacks. Thus it is difficult and sometimes impossible to determine DDoS attack traffic [9].

b) Cloud against DDoS attacks

As we know, DDoS attacks are one of the most powerful threats available in the network world, especially when launched from a botnet with huge numbers of infected machines. When a DDoS attack is occurred, it tries to send a heavy flood of packets at victim from multiple sources. Fortunately, in this situation the cloud may be part of the solution. If websites, which have limitation in server resources experiencing DDoS attacks, can take advantage of using cloud, that provides more resource to tolerate such attacks [10]. Moreover, cloud technology offers will be able to provide required resources almost real-time to avoid such websites shutdown.

IV. Solution for Cloud Security Problems

There are several traditional solutions to mitigate security problems in the Internet environment as a cloud infrastructure. However, the nature of cloud causes some of these security problems to occur especially in cloud environment. On the other hand, some of the solutions may be inefficient in cloud that may have good performance in the Internet.

A. Access Control

Access control is a method to gain access to an authorized user and prevent unauthorized accessing. In addition, methods to control accessing require some procedures to control the allocation of access permissions to information and services. These procedures should cover all cases in the lifecycle of user access, from establishing the using service to disconnecting from it. More important than access control is the critical situation of managing the allocation of privileged access rights, which can put system in a vulnerable situation. Access control has several parameters but in [11] the following six control statements are introduced. They are important to ensuring proper access control management:

1) Control access to information.
2) Manage user access rights.
3) Encourage good access practices.
4) Control accessing to network services.
5) Control accessing to operating systems.
6) Control accessing to applications and systems.

1) Responsibility

One of most important questions in access control managing is who is responsible for it? It may be customers, Providers or both of them. In addition, what percent of responsibility is for each of them if both of them play a role in access control?

In the SaaS model, the nature of it causes the cloud provider to be responsible for managing all aspects of the network and application infrastructure. In this model, since the application is delivered as a service to end users, usually by using the web browser, network-based controls are of less relevance and are augmented by user access controls [9],[10]. Hence, in this case customers should focus on their clients' access controls such as authentication, privilege management, provisioning to protect the information hosted by SaaS[11].

The PaaS delivery model managing access control is similar to SaaS. However, customers are responsible for access control to their applications placed on a PaaS platform. Access control to applications manifests as end user access management, which includes provisioning and authentication of users[7].

The IaaS has different situations in access control. In the IaaS, cloud customers are entirely responsible for managing all prospects of access control in their infrastructure. Access to the virtual servers, virtual network, virtual storage, and applications hosted on an IaaS platform will have to be designed and managed by the customer [4]. In addition, in the IaaS, access control management to the host, network, and management applications are owned and just managed by the cloud provider and in this case, the user can manage access control to his virtual infrastructure such as virtual server, virtual storage, virtual networks, and also applications hosted on virtual servers [11]

B. Incident Countermeasure and Response

One of the most important issues in cloud security, similar to other type of network-based technology, is finding vulnerabilities that exist in cloud. But more important than finding problems is finding appropriate response against all problems that are detectable [12]. As mentioned above, The cloud builds on a collection of specialized storage engines, driven by a custom-built distributed transaction coordinator, which also supports high availability[13]. To achieve high performance in flexibility, scalability, and efficiency usage of available resources, cloud providers must face major challenges in the area of adaptability and workload analysis.

1) Partitioning

To allow workloads to scale across multiple computing nodes, it is important to divide their data into partitions that maximize transaction performance. The main reason for doing that is to lessen the probability that a given transaction has to access multiple nodes to compute its answer.

2) Migration

One of the main requirements of the cloud is the ability to be flexible. In the context of a cloud service, flexibility means dedicating resources where they are most needed [14]. This is particularly challenging in a database environment where there are large amounts of data that may need to be moved to reconcile. In migration, an available method must predict adaptation time and it has to try to avoid cloud nodes overload. To achieve this, cloud providers can use some procedures such as partitioning, fragmentation, breaking data in smaller pieces of data, and they must be able to launch transactions while movement occurs.

3) Workload analysis and allocation

To collaborate properly workloads on virtual machines, it is necessary to analyze and classify their resource requirements to decide how those can be allocated to virtual machines properly.

4) Backup

Data backup which created by users is one of the most effective and traditional solutions [15]. If users lose their data because of cloud crash or successful attack within cloud, then they can recover the lost data by using backup. Cloud providers also create backup from data within their backup. But data growing in cloud environments is fast and the important question is how much it costs. Are all data is necessary for backup? Who is responsible for it, users or providers? Answers to these questions can improve cloud environments in backup policies.

It is obvious that users must backup their data whether or not the cloud provider may perform backup policies. More important than backup is how many backups would be enough? And it is important that the user and also the provider should do it repeatedly. This assures that the users' data is not lost when unexpected events occur in cloud such as when the cloud provider goes out of business or a physical crash happens. For a better solution, users can store these backup data in a different cloud provider rather than in their local data center.

V. Conclusion

Undoubtedly, cloud computing helps IT enterprises use various techniques to optimize application performance in a cost-effective manner. A cloud-based application is based on network appliance software, which is running in a virtual machine in a virtualized environment. A virtual appliance relieves some of the noticeable management issues and for cloud costumers simplifies issues such as software updates, configuration and other management tasks which cloud costumers have to do before using them. Nevertheless, in the cloud, they are automated and centralized at the data center and the cloud provider is responsible for all of them. Therefore, all applications are decentralized and users can have access to them every time and everywhere. This is good but the bad news is that this benefit creates a new set of challenges and security problems that must be considered. Additionally, just because the software can launch in a virtual machine properly does not mean it can necessarily run in cloud environment.

As shown in this paper, in the cloud, there are risks and hidden costs and this makes it hard to decide on moving to cloud. Cloud providers often have several powerful servers and resources to provide good services for their users. The cloud is internet-based technology and similar to other Internet-based technology is at the risk of attacks such as powerful DDoS attacks. In order to solve DDoS problems, cloud providers can add more resources to protect themselves against such attacks but there is no defense against powerful DDoS attacks with good sagacity. Because of all mentioned issues, many enterprises prefer using cloud for less sensitive data and store important data in their own local data center.

Finally, the following issues are most important to users who think about moving toward cloud computing:

- It should be considered a balance between the business benefits and the hidden potential risks.
- Cloud computing is interesting but it does not mean that all IT related business needs to move to it.

For those users who are newly employ cloud computing, the following notes are vital to be considered:

- Encrypting all sensitive information which is stored in cloud whether in public cloud or private cloud.
- Using detection tools as to find malicious behavior against their data.

- Back up data periodically.
- For some users who can distribute their application, it is useful to run their application on multiple clouds or use another cloud as backup server.

REFERENCES

[1] *The NIST Definition of Cloud Computing*, October 2009.
[2] F. Sabahi, "Security of virtualization level in cloud computing," *ICCSIT*, China, 2011.
[3] V. Kundra, *State of Public Sector Cloud Computing*, vol. 20, May 2010.
[4] F. Sabahi, "Cloud computing security threats and responses," *Presented at the ICCNE*, China, 2011.
[5] J. Brodkin. (2008). *Gartner: Seven Cloud-Computing Security Risks*. [Online]. Available: http://www.networkworld.com/news/2008/070208-cloud.html
[6] S. K. T. Mather and S. Latif, *Cloud Security and Privacy*: O'Reilly Media, Inc., 2009.
[7] N. Mead, *et al.*, "Security quality requirements engineering (SQUARE) methodolgy," *Carnegie Mellon Software Engineering Institute*.
[8] T. Mather. (2011). *Data Leakage Prevention and Cloud Computing*. [Online]. Available: http://www.kpmg.com/Global/Pages/default.aspx
[9] About- Trend Cloud Security Blog – Cloud Computing Experts. [Online]. Available: http://cloudsecurity.trendmicro.com/
[10] Z. Zorz, *Top 7 Threats to Cloud Computing*, 2010.
[11] Security Management in the Cloud - Access Control. (2010). [Online]. Available: http://mscerts.net/programming/Security%20Management%20in%20the%20Cloud%20-%20Access%20Control.aspx
[12] Security Management in the Cloud. (2010). [Online]. Available: http://mscerts.net/programming/Security%20Management%20in%20the%20Cloud.aspx
[13] P. Sefton, *Privacy and Data Control in the Era of Cloud Computing*.
[14] F. Sabahi, "Cloud computing Security threats and responses," *ICCNE*, China, 2011.
[15] R. Ho, *Cloud Security Considerations*, 2009.

Farzad Sabahi received Bachelor of Science and Master of Science degrees in Computer Engineering from Azad University in 2003 and 2007 respectively, specializing in the computer architecture. His research interests include computer architecture, distributed systems, cloud computing, hypervisor-based security and wireless network security. He is a lecturer in the Department of Electrical and Computer Engineering at the Azad University, Zanjan, Iran. He has published several papers in distributed systems, cloud computing, and wireless network security. He has been an invited reviewer for different international conferences. He has been member of The Institute of Electrical and Electronics Engineers (IEEE) since 2006.