Cloud Computing Security Threats and Responses

Farzad Sabahi
Faculty of Computer Engineering
Azad University
Iran
f.sabahi@ieee.org

***Abstract*—Cloud computing is one of today's most exciting technologies due to its ability to reduce costs associated with computing while increasing flexibility and scalability for computer processes. During the past few years, cloud computing has grown from being a promising business idea to one of the fastest growing parts of the IT industry. IT organizations have expresses concern about critical issues (such as security) that exist with the widespread implementation of cloud computing. These types of concerns originate from the fact that data is stored remotely from the customer's location; in fact, it can be stored at any location. Security, in particular, is one of the most argued-about issues in the cloud computing field; several enterprises look at cloud computing warily due to projected security risks. The risks of compromised security and privacy may be lower overall, however, with cloud computing than they would be if the data were to be stored on individual machines instead of in a so-called "cloud" (the network of computers used for remote storage and maintenance). Comparison of the benefits and risks of cloud computing with those of the status quo are necessary for a full evaluation of the viability of cloud computing. Consequently, some issues arise that clients need to consider as they contemplate moving to cloud computing for their businesses. In this paper I summarize reliability, availability, and security issues for cloud computing (RAS issues), and propose feasible and available solutions for some of them.**

***Keywords** Cloud Computing; Security; DoS; Countermeasure*

I. Introduction

Cloud computing is a network-based environment that focuses on sharing computations or resources. Actually, clouds are Internet-based and it tries to disguise complexity for clients. Cloud computing refers to both the applications delivered as services over the Internet and the hardware and software in the datacenters that provide those services. Cloud providers use virtualization technologies combined with self-service abilities for computing resources via network infrastructure. In cloud environments, several kinds of virtual machines are hosted on the same physical server as infrastructure. In cloud, costumers must only pay for what they use and have not to pay for local resources which they need to such as storage or infrastructure. Nowadays, we have three types of cloud environments: Public, Private, and Hybrid clouds. A public cloud is standard model which providers make several resources, such as applications and storage, available to the public. Public cloud services may be free or not. In public clouds which they are running applications externally by large service providers and offers some benefits over private clouds. Private Cloud refers to internal services of a business that is not available for ordinary people. Essentially Private clouds are a marketing term for an architecture that provides hosted services to particular group of people behind a firewall. Hybrid cloud is an environment that a company provides and controls some resources internally and has some others for public use. Also there is combination of private and public clouds that called Hybrid cloud. In this type, cloud provider has a service that has private cloud part which only accessible by certified staff and protected by firewalls from outside accessing and a public cloud environment which external users can access to it. There are three major types of service in the cloud environment: SaaS, PaaS, and IaaS [1]. In cloud, similar to every proposed technology, there are some issues which involved it and one of them is RAS factor. For having good and high performance, cloud provider must meet several management features to ensure improving RAS parameters of its service such as:

- Availability management
- Access control management
- Vulnerability and problem management
- Patch and configuration management
- countermeasure
- Cloud system using and access monitoring

II. Information security Policies

In Cloud computing technology there are a set of important policy issues, which include issues of privacy, security, anonymity, telecommunications capacity, government surveillance, reliability, and liability, among others [1]. But the most important between them is security and how cloud provider assures it. Generally, Cloud computing has several customers such as ordinary users, academia, and enterprises who have different motivation to move to cloud. If cloud clients are academia, security effect

978-1-61284-486-2/11/$26.00 ©2011 IEEE

on performance of computing and for them cloud providers have to find a way to combine security and performance. For enterprises the most important problem is also security but with different vision. For them high performance may be not as critical as academia. Well-known Gartner's seven security issues which cloud clients should advert as mentioned below [2]:

- **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 it is held by a service provider [3]. Traditional service providers are subjected to external audits and security certifications.
- **Data location**: When clients use the cloud, they probably won't know exactly where their data are hosted. Distributed data storage is a usual manner of cloud providers that can cause lack of control and this is not good for customers who have their data in local machine before moving from local to cloud.
- **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. Encryption and decryption is a classic way to cover security issues but heretofore it couldn't ensure to provide perfect solution for it.
- **Recovery:** If a cloud provider broke or some problems cause failure in cloud sever what will happen to users' data? Can cloud provider restore data completely? Moreover clients prefer don't get permission to third-party companies to control their data. This issue can cause an impasse in security.
- **Investigative support:** 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 by a larger company with maybe new policies. But clients 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 [4]. Predominantly, the first question is an information security officer must answer to that whether he has adequate transparency from cloud services to manage the governance (shared responsibilities) and implementation of security management processes such as detection and prevention solutions to assure the costumers that the data in the cloud is appropriately protected. Actually, the answer to this question has two parts: what security controls must the customer provide over and above the controls inherent in the cloud platform, and how must an enterprise's security management tools and processes 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 [4].

A. Data Leakage

Innately, when moving to a cloud there is two changes for customer's data. First, the data will store away from the customer's local machine. Second, the data is moving from a single-tenant to a multi-tenant environment. These changes can raise an important concern that called data leakage. Because of them, Data leakage has become one of the greatest organizational risks from security standpoint [5].

Nowadays, for mitigate effects of such problem there has been interested in the use of data leakage prevention (DLP) applications to protect sensitive data. But if data stored in a public cloud because of nature of it, using DLP products is valueless to protect the confidentiality of that data in all types of cloud. Inherently, in SaaS and PaaS discovery of client's data with DLP agents is impossible except when the provider put ability of it to its service. However, it is possible embedding DLP agents into virtual. Unlike the other types of clou, machine in IaaS to achieve some control over data associated.

In private clouds, Costumer has direct control over the whole infrastructure; it is not a policy issue whether DLP agents are deployed in connection with SaaS, PaaS, or IaaS services. However, it may well be a technical issue whether DLP agents interoperate with your SaaS or PaaS services as architected [6]. In hybrid cloud, if service is IaaS, client could set in DLP agents for some control over data.

B. Cloud security issues

Innately, Internet is communication infrastructure for cloud providers that use well-known TCP/IP protocol which users' IP addresses to identify them in the Internet. Similar to physical computer in the Internet that have IP address, a virtual machine in the Internet has an IP address as well. A malicious user, whether internal or external, like a legal user can find this IP addresses as well. In this case, malicious user can find out which physical servers the victim is using then by implanting a malicious virtual machine at that location to launch an attack [7]. Because all of users who use same virtual machine as infrastructure, if a hacker steals a virtual machine or take control over it, he will be able to access to all users' data within it. Therefore, The hacker can copy them into his local machine before cloud provider detect that virtual machine is in out of control then the hacker with analysis the data may be find valuable data afterward[8].

1) *Attacks in cloud*

Nowadays, there are several attacks in the IT world. Basically, as the cloud can give service to legal users it can also service to users that have malicious purposes. A hacker can use a cloud to host a malicious application for achieve his object which may be a DDoS attacks against cloud itself or arranging another user in the cloud. For example, assume an attacker knew that his victim is using typical cloud provider, now attacker by using same cloud provider can sketch an attack against his victim. This situation is similar to this scenario that both attacker and victim are in same network but with this difference that they use virtual machines instead of physical network.

a) DDoS attacks against Cloud

Distributed Denial of Service (DDoS) attacks typically focus high quantity of IP packets at specific network entry elements; usually any form of hardware that operates on a Blacklist pattern is quickly overrun and will become in out-of-service situation. In cloud computing where infrastructure is shared by large number of clients, DDoS attacks make have the potential of having much greater impact than against single tenanted architectures[9]. If cloud has not plenty resource to provide services to its costumers then this is may be cause undesirable DDoS attacks. Solution for this event is a traditional solution that is increase number of such critical resources. But serious problem is when a malicious user deliberately done a DDoS attacks using bot-net[10].

Most network countermeasures cannot protect against DDoS attacks as they cannot stop the deluge of traffic and typically cannot distinguish good traffic from bad traffic. Intrusion Prevention Systems (IPS) are effective if the attacks are identified and have pre-existing signatures but are ineffectual if there is legitimate content with bad intentions[6]. Unfortunately, similar to IPS solutions, firewalls are vulnerable and ineffective against DDoS attacks because attacker can easily bypass firewalls and also IPSs since they are designed to transmit legitimate traffic and attacks generate so much traffic from so many distinct hosts that a server, or for cloud its Internet connection, cannot handle the traffic [6].

It may be more accurate to say that DDoS protection is part of the Network Virtualization layer rather than Server Virtualization. For example, cloud systems use virtual machines can be overcome by ARP spoofing at the network layer and it is really about how to layer security across multivendor networks, firewalls and load balances.

b) Cloud against DDoS attacks

DDoS attacks are one of the powerful threats available in world, especially when launched from a botnet with huge numbers of zombie machines. When a DDoS attack is launched, it sends a heavy flood of packets to a Web server from multiple sources. In this situation, the cloud may be part of the solution. it's interesting to consider that websites experiencing DDoS attacks which have limitation in server resources, can take advantage of using cloud that provides more resource to tolerate such attacks. In the other hand, cloud technology offers the benefit of flexibility, with the ability to provide resources almost instantaneously as necessary to avoid site shutdown.

IV. SOLUTIONS FOR AGAINST CLOUD SECURITY PROBLEMS

There are several traditional solutions to mitigate security problems that exist in the Internet environment, as a cloud infrastructure, but nature of cloud causes some security problem that they are especially exist in cloud environment [11]. In the other hand, there is also traditional countermeasure against popular Internet security problems that may be usable in cloud but some of them must be improved or changed to work effectively in it.

A. Access Control

Access control mechanisms are tools to ensure authorized user can access and to prevent unauthorized access to information systems. Therewith, formal procedures should be in place to control the allocation of access rights to information systems and services. Such mechanisms should cover all stages in the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention should be given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls. The following are the six control statement should be consider to ensure proper access control management [12]:

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

1) *Access control in cloud services*

Generally, in the SaaS model the cloud provider is responsible for managing all aspects of the network, server, and application infrastructure. In this model, since the application is delivered as a service to end users, usually via a web browser, network-based controls are becoming less relevant and are augmented or superseded by user access controls, e.g., authentication using a one-time password [6, 12]. Hence, customers should focus on user access controls (authentication, federation, privilege management, provisioning, etc.) to protect the information hosted by SaaS[13].

In the PaaS delivery model, the Cloud provider is responsible for managing access control to the network, servers, and application platform infrastructure. However, the customer is responsible for access control to the applications placed on a PaaS platform. Access control to applications manifests as end user access management, which includes provisioning and authentication of users[7].

IaaS customers are entirely responsible for managing all aspects of access control to their resources in the cloud. 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. In an IaaS delivery model, access control management falls into one of the following two categories. Access control management to the host, network, and management applications that are owned and managed by the Cloud provider and user must manage access control to his/her virtual server, virtual storage, virtual networks, and applications hosted on virtual servers [12, 13].

B. Incident Countermeasure and response

Basically, one of the important viewpoints in cloud security, similar to other IT fields, is finding problems and vulnerabilities which exist in cloud but more important that finding them is applying appropriate response against all problems that it founds[12]. Generally, the cloud system builds on a collection of specialized storage engines, driven by a custom-built distributed transaction coordinator, which also supports high availability[14]. To achieve flexibility, scalability, and efficiency usage of available resources, cloud providers must face major challenges in the area of adaptability and workload analysis and prototypes lies in these analysis and adaptation components.

1) Partitioning

To allow workloads to scale across multiple computing nodes, it is important to divide their data into partitions that maximize transaction and query performance. The main idea for achieve it, 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. This is particularly challenging in a database environment where there are large amounts of data that may need to be moved in order to reconcile. In migration, available method must be predict adaptation time and try to avoid cloud nodes overload by some procedure such as partitioning and fragment and moving data in smaller pieces of data and maintaining the ability to run 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 be allocate to virtual machines.

V. CONCLUSION

Doubtless, Cloud computing helps IT enterprises use various techniques to optimize and secure application performance in a cost-effective manner. A cloud-based application is based on network appliance software, with its operating system, running in a virtual machine in a virtualized environment. A virtual appliance relieve some of the notable management issues in enterprises because most of the maintenance, software updates, configuration and other management tasks that they are done by cloud provider which responsible for them. But this suggestive way for decentralized application and access every time and everywhere to data, occasion and introduce new set of challenges and security problems that must consider before transfer data to a cloud environment. Additionally, just because the software can run in a Virtual machine does not mean that it performs well in cloud environment necessarily. Thereupon, in cloud there are risks and hidden costs in managing cloud compliance. The key to successful cloud computing initiatives is achieving a balance between the business benefits and the hidden potential risks which can impact efficacy.

Cloud providers often have several powerful servers and resources in order to provide appropriate services for their users but cloud is at risk similar to other Internet-based technology. In the other hand, they are also at risk of attacks such as powerful DDoS attacks similar other Internet-based technology. As a solution, cloud providers can add more resource to protect themselves from such attacks but unfortunately there is no defense against a powerful DDoS attack which has good sapience.

These issues which discussed in this paper are the main reasons that cause many enterprises which have a plane to migrate to cloud prefer using cloud for less sensitive data and store important data in their own local machines.

Eventually, Whilst Cloud computing is an applicable and interesting technology that introduce in the IT industry; it doesn't mean that all business IT needs to move to cloud. In addition, As a result, Moving toward cloud computing require to consider several parameters and most important of them is security.

REFERENCES

[1] S. Roschke, et al., "Intrusion Detection in the Cloud," presented at the Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, Chengdu, China, 2009.

[2] J. Brodkin. (2008). Gartner: Seven cloud-computing security risks. Available: http://www.networkworld.com/news/2008/070208-cloud.html

[3] D. L. Ponemon, "Security of Cloud Computing Users," 2010.

[4] S. K. Tim Mather, and Shahed Latif, Cloud Security and Privacy: O'Reilly Media, Inc., 2009.

[5] C. Almond, "A Practical Guide to Cloud Computing Security," 27 August 2009 2009.

[6] http://cloudsecurity.trendmicro.com/

[7] N. Mead, et al., "Security quality requirements engineering (SQUARE) methodolgy," Carnegie Mellon Software Engineering Institute.

[8] J. W.Rittinghouse and J. F.Ransome, Cloud Computing: Taylor and Francis Group, LLC, 2010.

[9] T. Mather. (2011). Data Leakage Prevention and Cloud Computing. Available: http://www.kpmg.com/Global/Pages/default.aspx

[10] P. Coffee, "Cloud Computing: More Than a Virtual Stack," ed: salesforce.com.

[11] z. Zorz, "Top 7 threats to cloud computing," 2010.

[12] (2010). Security Management in the Cloud. Available: http://mscerts.net/programming/Security%20Management%20in%20the%20Cloud.aspx

[13] (2010). Security Management in the Cloud - Access Control. Available: http://mscerts.net/programming/Security%20Management%20in%20the%20Cloud%20-%20Access%20Control.aspx

[14] P. Sefton, "Privacy and data control in the era of cloud computing."