EMERGING SECURITY CHALLENGES IN CLOUD COMPUTING

Rexhion Qafa, Jozef Bushati

[1]National Agency of Information Society, *rexhion.qafa@akshi.gov.al*
[2]University of Shkoder,"Luigj Gurakuqi, *jozefbushati@gmail.com*,

Abstract

Cloud computing has changed the whole picture that distributed computing used to present e.g. Grid computing, server client computing. Cloud has given a new meaning to distributed, and off-premises computing. Although, Cloud offers great benefits, it also introduces a myriad of security threats to the information and data which is now being ported from on-premises to off-premises. Where cloud computing can help organizations accomplish more by paying less (in the longer run) and breaking the physical boundaries between IT infrastructure and its users, due to openness of accessible information and data relying on trust between cloud provider and customer, heightened security threats must be overcome in order to benefit fully from this new computing exemplar. Breach in the security of any component in the cloud can be both disaster for the organization (the customer) and defacing for the provider. This paper explores the security issues related to the cloud. The paper also discusses the existing security approaches to secure the cloud infrastructure and applications and their drawbacks. Finally, we explore some key research challenges of implementing new cloud-aware security solutions that can provide the likes of pre-emptive protection for complex and ever dynamic Cloud infrastructure, followed by conclusion where we try to entail the whole research and try to formulate a security strategy which will enable the Cloud providers and customers alike to fight against ever emerging security threats.

While it is essential to recognize the fact that there is no silver bullet to counter the threats to distributed or cloud computing model it is however, even more important to appreciate that with right security strategy, multiple layers of security, and implementing well thought after security controls, it is possible to restrain threats.

***Keywords*:** *Cloud, security, cloud computing, security challenges, complex distributed computing, security concerns, security strategy)*

Introduction:

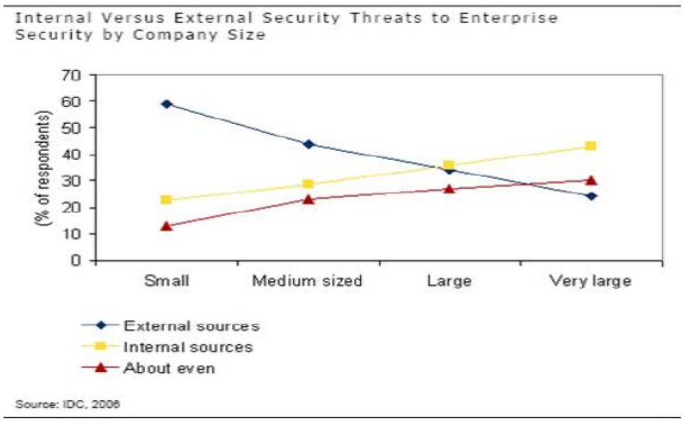
Cloud Computing is a jargon, in other words a new computing model, in which the public Internet is used to connect to provider's hosted network, infrastructure, platform and/or applications to leverage reliable services. Cloud has left all other distributed computing structures/mechanisms far behind both in competition and in terms of popularity and success. The primary reason is that, any service can be scaled up or down as and when required, based on customer's needs. Cloud offers flexibility , quick to production model, and offers capital reduction by enabling organizations to port all their data, information and infrastructure to off-site provider hosted premises. Cloud Computing is essentially a combination of existing technologies that are succeeding in make a paradigm shift in building and maintaining distributed computing systems making use of, multiprocessor, virtualization technology, network based distributed data storage and networking. The cloud providers have Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) and many more services to offer. However, with all that said, one may wonder what happens to the data or information which has been ported to an offsite, out of physical or logical control and possibly unknown premises? As cloud providers do not reveal the location of the data, it is close to impossible to tell, where the data is stored. Moreover, with the cloud model, organizations lose control over physical security. In a public cloud, everyone is sharing resources in a common space, owned by cloud provider i.e. in a shared pool outside the organization's control or boundary where, they do not have any knowledge or control of where the resources are stored. If information is encrypted while transient, who is in control of the encryption/decryption keys, is it the organization (customer) or the provider? These and many more concerns remain to be answered. This paper is organized as follows. Section 2 explores the cloud infrastructure security problems and the different threats that can affect the cloud infrastructure components. In section 3, we will explore the key research challenges of implementing security solutions to protect the cloud infrastructure. Finally, section 4 concludes the paper with a summary of its research contribution.

CLOUD SECURITY ISSUES:

Cloud computing provides organizations with an efficient, flexible and cost effective alternative to hosting their own computing resources. However, hackers, attackers and security researchers have shown that this model can be compromised and is not 100% secure. In a cloud, security is shared between the cloud provider and the cloud user. Both entities need to trust each other and complement wherever there is scope for improving security. There are many security threats which emerge inside or outside of cloud provider’s/consumer’s environment and these can be broadly classified as Insider threats, outsider malicious attacks, data loss, issues related to multi-tenancy, loss of control, and service disruption

a.Insider Threats

It is a well known fact that most security threats arise from within an organization as shown in figure 1. This threat is many folded for consumers of cloud services since; the cloud is based on multi-tenant model, under provider’s single management domain. To top it all, the organizations which subscribe to cloud services, usually lack transparency into provider's processes to hire its employees, for keeping data in different locations and its relationships with third party vendors. There is often no visibility into the hiring standards and practices for cloud employees, by cloud provider to its consumers. This situation and very fact can make space for an adversary from a point of view of corporate espionage, casual hacker or malicious insiders. Without any barring a third party vendor for the provider can tap into the sensitive data and sell it to a competition of the victim organization. The following figure 1 details the results of survey conducted by IDC to reflect the insider threat which is existent everywhere from small to very large size enterprises.



Source: IDC, 2006

Figure 1. Example of insider vs. outsider threats

b.Outside Malicious Attacks

Outside threats are one of the most concerning issues with any organization since, it directly entails release of confidential information out in open or possible defacing of the organization. This is one of the persistent issues in Cloud infrastructure as well since, Clouds are more associable than private networks and have more interfaces to help its legitimate users access information. This very fact is what the hackers and attackers leverage to their advantage by exploiting the API weakness, connection (media or logical channel) tapping or breaking in and by social engineering. The outside attacks may not be as damaging as inside attacks however, they are the most difficult to conceal since, media (wireless being easily and widely accessible) can amplify the attack and the organization and/or cloud provider get to face the heat.

c.Data Loss

When organizations migrate their data to Cloud, they expect to have the same level of data integrity and safety as they would in their premises. The fact is that since, Clouds are multi tenant environment and the access control is not of same level as on premises, unauthorized parties must be prevented from gaining access to sensitive data. This is however, not as easy as it seem and data loss and leakage can cause financial, reputation and customer count loss to the organization. Deletion or alteration of records without a backup of the original content is an obvious example. Insufficient authentication, authorization, and accounting controls, an inconsistent use of encryption and encryption keys, operational failures, political issues and data center reliability are the biggest factors responsible in a direct and indirect way for data loss.

d.Service Disruption

While service hijacking is not new even with Cloud infrastructure, malicious attacks such as phishing, fraud, and exploitation of software vulnerabilities still help hackers score. In case an attacker gains access to an organization's login credentials, he can eavesdrop the data, transactions or manipulate data. Even worse an attacker can replay sessions, and redirect an organization's clients to illegitimate sites or launch a Denial of Service (DoS) or Distributed DoS (DDoS) attack leveraging bot-nets and autodialers. The soft targets are the machines which are connected to outside world and the IP addresses, extensions which are exposed via various publically available internet tools (e.g. WHOIS). The worse part still, these compromised accounts can become a launching base for the attacker from where, he can leverage a legit account to launch subsequent attacks which will go unnoticed and the attacker will be concealed. Service disruptions can cause a business to halt or even loose valuable customer base to competition. Thus, this category of attacks whether internal or external is one of the most impacting.

f.Multitenancy issues

As a Cloud is primarily meant to serve multiple users it directly implies that different users within a cloud share the same applications and the physical hardware to run their Virtual Machines (VMs). Here, the users are the tenants for the provider. While this model seems to be very promising from provider’s perspective, it has some serious limitations in terms of security. The application and hardware sharing can enable information leakage and exploitation and it certainly helps increasing the attack surface. The risk of VM-to-VM attacks or compromised VM becoming a hub for future attacks is greatly enhanced.

g.Loss of Control

When organizations port their data or services to cloud, they are not aware of the location of their data and services since, the provider can host their data or services anywhere within the Cloud. This poses a serious concern as from a user perspective; organizations lose control over their vital data and are not aware of any security mechanisms put in place by the provider. Figure 2 is an indicative of how concerning it is to the organizations is to have their data in an unknown place and with no control over it.

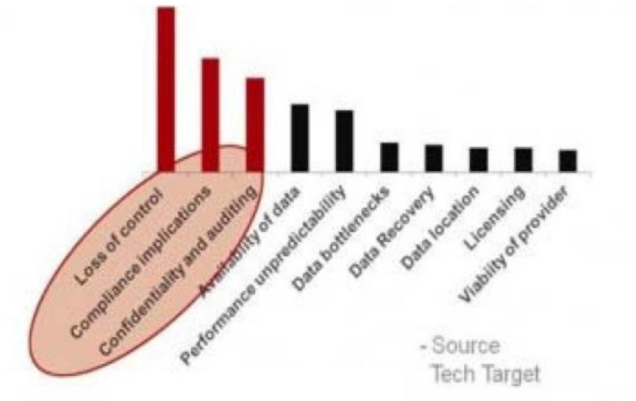


Figure 2. Loss of control over vital data is one of the top concerns

KEY RESEARCH CHALLENGES:

The cloud's 'virtual infrastructure' is very complex and dynamic because of the multi processing, virtual storage, multiple tenants to manage, and multiple applications running at same time. In addition to it, there is huge amount of traffic flowing in and out of each physical server and/or a logical VM. Since, the virtual architecture of the cloud erases many of the physical boundaries that are traditionally used in defining, managing and protecting an organizations' IT assets within a traditional Data Center it leads to a very complex virtual architecture which by itself needs to be protected from all threats whether inside or outside.

Adapting security solutions in a cloud environment to protect cloud virtual infrastructure is a challenge and requires multiple attack vectors and characteristics to be addressed, in order to deliver the accurate and pre-emptive protection.

These key characteristics include:

a.Availability and Perfromance

While vital applications and infrastructure for an organization is an ever required necessity, cloud providers need to address the issues related to availability and performance. One way to achieve these metrics is by defining and adopting a well formed Service Level Agreement (SLA). It acts as a trust relationship between the provider and the customer (any organization in this case) to have a minimum set bar on the time during which the applications and/or infrastructure may not be available. This further leads the organization(s) to have a well defined backup contingency plan to cover the outages. On the other hand, more than just real-time monitoring is needed. Ideally, a cloud security system should have the intelligence to be self-defending, and not just detect but repel threats. To achieve the same, active monitoring should be implemented. This ranges from Network Access Control (NAC) to Intrusion detection systems (IDS) to Intrusion prevention systems (IPS) which enables a network to rely on pre defined yet adaptable attack signatures and profiles to stop an attack before it can launch with full strength and blacklist/block the IP address or source from which it originated (this applies both for inside and outside of the Cloud provider's premises)

b.Malicious Insiders

The threat of malicious insiders has been discussed earlier. However, it still remains a challenge as to how an organization can restrict its internal employees, contractors, vendors and other trusted people who have access to critical resources from within the network, where a soft target exists. This key challenge can be addressed by enforcing strict supply chain management and conducting a comprehensive supplier assessment. This will enable the Cloud provider to ensure that only people who get through pre-defined characteristics and requirements 'testing' or interviewing are hired. This applies equally to contractors and vendors. Also, by specifying human resource requirements as part of legal contracts, resources can be tied to legal action against them in case of any establishment of an espionage or intentional mal-behavior. To complement all of the above, transparency into overall information security and management practices must be in place. A compliance reporting system will help determine security breach notification so that, appropriate action may be taken against a person who has committed a fraud or an intentional sabotage. From a technology perspective, an intrusion prevention system combined with a notification system (SMTP, SNMP) should be deployed to discover any attack attempts and to repel the same.

c.Outside attacks

While insider threats pose a great threat to the Cloud provider and their customer’s alike, the threats evolving from outside pose an even greater impact, not in terms of the damage done directly to the system or processes however, the damage done to the reputation and long term loss of leaving customers. This threat can be mitigated in somewhat similar way to the traditional network Data Center threat mitigation however; a Cloud is not similar to a dedicated Data Center as it has virtual machines and multiple tenants. Henceforth, the perimeter protection using firewalls, ACL’s and intrusion prevention systems is a mandate. On the inside of the perimeter, honey pots should be deployed along with a strong AAA system, which is a challenge in turn to the hackers or attackers to break through. To fortify further the security of the Cloud, a Network Access Control system must be in place to curb any attack attempts as, it will match the OS level (in terms of antivirus, personal firewall) which can be easily made a standard for Cloud employees accessing information remotely as well as the Cloud customers. Virtual machines (VM) should be isolated for each customer and a context based firewall should be implemented such that, even if one machine is compromised, it does not become an attack base for the hacker to launch forth a series of attacks to other VMs. Moreover, the ability to curb zero-day (unknown) threats is a must in the list of Cloud security provider. Since, new security threats arise every day, in numbers, in complexity such that, the hacker behavior can’t be easily predicted. It is most constructive to have an overall logical and topological picture of cloud behavior developed by monitoring different components and activities inside the cloud. This should help the attack vectors to be related to any un-obvious activity hence, correlating attack or hack attempt into a cloud provider's domain. It is however, essential that pre-defined critical objects in the cloud that are targets for hackers are selected (since not all components would attract hackers) and building a correlation will lead to useful monitoring results. Use of honey pots is most recommended for luring casual to professional hackers into a trap.

d.Service Disruptions

Service disruption can land an organization into deep water as, its resources are not available for legit users to use and it will cause not only customer dissatisfaction however, also lowers the morale of the employees. This threat can be mitigated by a many fold process. To begin with, the provider should prohibit the sharing of account credentials between tenants by all means and services should be held valid to each VM or session. Secondly, the provider must employ a strong two-factor authentication technique wherever possible to ensure that its tenants are only getting in after a strong authentication process. Also, this can be complemented by ensuring that these connections come from known IP ranges or DNS names. Proactive monitoring should be leveraged to detect unauthorized activity in a session or in VM. This will help the provider shun the connections deemed unauthorized for a tenant. As discussed earlier, security in a Cloud environment is responsibility of both provider and customer thus, the customer should be ready to use all above mentioned mechanisms to ensure that their data and information is safeguarded. If possible, the provider should be flexible to accept the tenant specific security policies and port them to cloud. Moreover, strict initial customer registration and validation processes can help deter any attacks even before they can emerge. Comprehensive inspection of customer network traffic is a default metric expected from any provider by using Intrusion Prevention System and if possible, by Host Intrusion Prevention System at customer’s endpoints. Hacking attempts to disrupt services can be evaded by monitoring public blacklists and by provider’s own blacklist

f.Mutlitenancy

While multi-tenancy is the concept of Cloud and a boon for the providers, it has its own security relevant limitations. These limitations can be overcome by use of Defense-in-depth approach. Defense-in-depth approach involves defending the cloud virtual infrastructure at different layers with different protection mechanisms, as per the layer requirement and according to the layer characteristics. Applying such a defense strategy ensures that threats have to bypass by more than one defense layer, which in turn gives a degree of assurance that hackers have to do much more work than they anticipate and most of them, if not all will leave the attack mid way. For rest of persistent ones, the multiple layers can present a challenge which is not easily overcome. This strategy enables providers to be able to identify and block a number of threats at early stages, before they propagate into the cloud environment and can do possibly any damage.

g.Loss of Control

Losing control over vital data and critical services can be both disturbing and disrupting for any institution. While this is a reality in the Cloud world, the effect can be minimized by working out a strategy to cope with data integrity and authentication mechanisms, between provider and end user. The organizations must understand cloud provider security policies and SLAs so that, they can point out anything which is not at par with their internal security policies or processes and fix the same before migrating anything vital to the Cloud. This applies both to provider and customer i.e. both parties have to mutually agree on some metrics which enable them to benefit each other. The provider can be accommodating by allowing the customer to port their security processes to customer's virtual domain while, the customer can be specific to what their needs are and ask for the customization of SLAs and processes/policies. In addition to the above two elements, use of strong network authentication, key exchange mechanisms and authorization processes, which are both known to provider and are transparent to the customer are helpful. This way, the customer does not have to worry about loosing control on their critical applications or data and the provider can serve on demand yet, customized services, a perfect case of harmony.

CONCLUSION:

There are numerous security challenges in the cloud of which, this paper has tried to address the most common and critical ones. A secure cloud is impossible unless the virtual environment viz. infrastructure, VM, interfaces, network transmissions are secure. Cloud environment demand much above the traditional security solutions, which do not map well to the virtualized environments, because of the complex and dynamic nature of the cloud computing. As a stepping stone, cloud providers and customers should work together on defining the requirements and the specifics. It is implicit that new virtualization-aware security solutions should be implemented to ensure the preemptive security to the overall system. The cloud security solutions should have the intelligence to be self-defending and have the ability to provide real-time monitoring, detection and prevention of known and unknown threats. Many organizations fail to understand that they are putting their vital information or services in harms way in the rush to take advantage of the benefits of cloud computing, not least of which is significant cost savings. Without a serious consideration of the security implications it is futile to port any information to cloud. To establish zones of trust in the cloud, the virtual machines must be self-defending, effectively moving the perimeter to the virtual machine itself. Enterprise perimeter security i.e., firewalls, network segmentation, intrusion detection and prevention systems [IDS/IPS], monitoring and alarming mechanisms, and the associated security policies.

This research is focused on developing a comprehensive cloud-aware security strategy that can meet the aforesaid research challenges and have the ability to defend the cloud infrastructure and the different layers (including network connections, data at rest, data in transit, applications and VMs) against threats which may arise from within the provider's network or from outside. The security strategy is intended to leverage the existing security (ad-hoc) technologies and employing them in a fluid and dynamic cloud environment. The security strategy to be followed while adopting Cloud computing is a multi step process and involves (not limited to) the following:

- Make sure that the applications have built in security mechanisms to avoid any buffer overflow, SQL injection etc. attacks
- Employ multi-layer security approach to contain the threats and ensure that even if an external/internal layer is breached, there are other layers to back it up .
- For insider attacks ensure that the employees are trained, bound to legal terms and havetechnology elements to curb any threats originating on-premises (e.g. Antivirus, IPS, HIPS, internal firewalls, network segregation, monitoring).
- For 0-day attacks or service disrupting attacks, have security solutions like self-defending networks, Cloud aware security elements (NAC, dot1x etc.) in place. Moreover, usual DataCenter security techniques such as perimeter firewalls, IPS, ACLs can also be leveraged.
- Ensure that multi-tenant systems are well isolated, even when on same hardware, there should be a context based firewall and rules supplementing the individual domain holder’s security processes. This can be further strengthened by introduction of Single Sing On solution to validate sessions.
- The cloud customers (organizations, businesses) should have a sound understanding of security processes and of the SLAs with the provider.This helps remove any discrepancies and creates a symbiotic relationship between provider and customer.
- To counter external threats, have layered security in place, from perimeter to client machine.
- The customers should have a contingency plan in place to counter any outages or service disruptions, at least for the most critical applications or services. This can range from simple notification systems to backup repository of applications on-premises.

To conclude, while it is essential to recognize the fact that there is no silver bullet to counter the threats to distributed or cloud computing model it is however, even more important to appreciate that with right security strategy, multiple layers of security, and implementing well thought after security controls, it is possible to restrain threats.

References:

Luis Vaquero, Luis Rodero-Merino, Juan Caceres, et al, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, pp. 50-55, 2009.

Microsoft Research, "Securing Microsoft's Cloud Infrastructure," in White Paper, 2009, http://www.globalfoundationservices.com/security/documents/SecuringtheMSCloudMay09.pdf.

Wesam Dawoud, Ibrahim Takouna and Christoph Meinel,"Infrastructure as a service security: Challenges and solutions," in 2010 The 7th International Conference on Informatics and Systems, 2010, pp. 1-8.

Cloud Computing – A Practical Approach by Velte, Tata McGraw-Hill Edition (ISBN-13:978-0-07-068351-8)

Cloud Computing Bible by Barrie Sosinsky, Wiley Publishing Inc.(ISBN-13: 978-0470903568)

Wikipedia–Cloud computing security
http://en.wikipedia.org/wiki/Cloud_computing_security

ISACA(auditor’sperspective journal)
http://www.isaca.org/Journal/Past-Issues/2009/Volume-6/Pages/Cloud-Computing-An
Auditor-s-Perspective1.aspx

Research paper – “Private Virtual Infrastructure (PVI) Model for Cloud Computing” International Journal of Software Engineering Research & Practices Vol.1, Issue 1, Jan, 2011

Research paper – “Security Issues and Solutions in Cloud Computing”
http://wolfhalton.info/2010/06/25/security-issues-and-solutions-incloud-computing/

Cloud and Telecom security article
http://sbin.cn/blog/2009/11/10/true-or-false-70-of-security-incidentsare-due-to-insider-threats/

Trusted client to cloud access article
http://soaexpressway.wordpress.com/2011/03/01/trusted-client-tocloud-access/

Cloud computing security forum
http://cloudsecurity.org/