Security Challenges Of Cloud Computing

Anuradha Thilakarathne, Janaka I Wijayanayake

Abstract: In today's ICT service industry, there are many changes that promote technology services in many markets. Cloud Computing is a comprehensive solution that delivers IT as a service. Different Cloud Services enable an organization to operate its IT applications on an OPEX model rather than the traditional CAPEX model. The cloud computing significantly impacts shifting of both IT paradigm and Telecom platform. Telecommunication services, especially the Internet service have flooded the world with huge volume of information and posing challenges to the organizations and telecommunication operators on keeping up expanding the network in order to provide the good quality of services while providing higher level of security on service deliverables. In this paper, we examine the types of security risks been glued on to the cloud computing and the importance of refrain from those vulnerabilities in mass scale.

Index Terms: Cloud, Malware, Network, Security, Spyware, Virtualization, Zombie

1 Introduction

Enterprises continuously seek innovative approaches to reduce operational computing costs while getting the most from their resources. Recent developments in Cloud Computing technology play a major role in helping organizations to reduce the operational cost. It is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Fig. 1 presents an overview of the NIST Cloud Computing reference architecture [1], which identifies the major actors, their activities and functions in Cloud Computing.

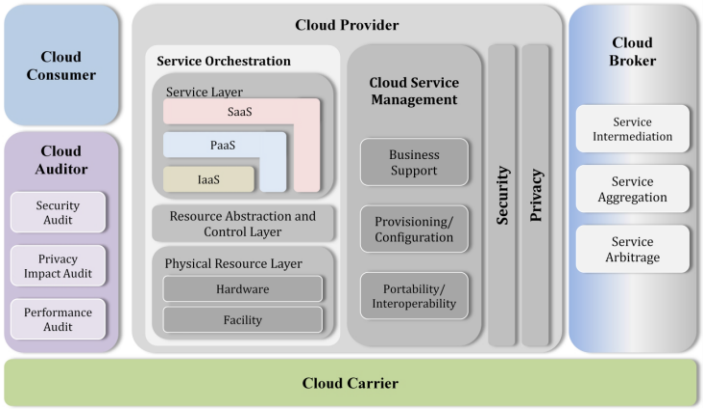

Fig. 1. *The Conceptual Reference Model [1]*

IT experts have classified Cloud Computing vendors into three broad categories based on the fundamental nature of the Cloud-based solution they provide: Infrastructure-as-a-Service (IaaS) [2], Platform-as-a-Service (PaaS) [3] and Software-as-a-Service (SaaS) [4]. The main difference between these service models lies in how responsibilities are divided between Cloud Service Provider (CSP) and Cloud Consumer. For example, in IaaS offering, the Cloud consumer has extensive control over his servers and the installed operating systems and applications; the virtualization infrastructure and at least parts of the network infrastructure. With SaaS, in contrast, the Cloud consumer usually controls only certain configuration parameters of the contracted service the application and all underlying infrastructure is under control of the CSP. PaaS lies between these two extremes in that the customer controls the application as a whole (including the code), while the CSP controls the runtime environment and supporting infrastructure.

2 Towards Cloud Security

The new paradigm of Cloud Computing possesses severe security risks to its adopters due to the distributed nature of Cloud Computing environments which make them a rich target for malicious individuals. Cloud resides with an entirely virtual infrastructure which is, invisible to the user [5, 6]. This inherent abstraction ensures that an application or business service is not directly tied to the underlying hardware infrastructure such as servers, storage or networks. This allows business services to move dynamically across virtualized infrastructure resources in a very efficient manner. However, the virtualization techniques used in Cloud possess numerous security threats and attacks. A fully or partially shared Cloud environment is expected to have a greater attack surface and therefore, can be considered to have a greater risk than a dedicated resource environment [7]. Cloud Instances (CIs) are vulnerable as they move between the private Cloud and the public Cloud. Moreover, the easiness of cloning a virtual machine instance leads to propagation of security vulnerabilities and configuration errors. In addition to this, the co-location of multiple CIs increases the attack surface and risk of CI to another instance compromise [7]. Cloud Consumers run numerous applications/scripts in order to complete their computing tasks. Most of them are too complex and complicated to trust. Even with access to the source code, it is difficult to reason about the security of these applications. They might harbor malicious code such as computer viruses, worms, bots, Trojan horses and spyware or contain bugs that are exploitable [8] by carefully crafted input. It is essential that

- *Anuradha Thilakarathne, M.Sc. IT (UK), Division of Information Technology, Telecommunications Regulatory Commission of Sri Lanka, Colombo. E-mail: anuradha@trc.gov.lk*
- *Janaka I Wijayanayake, PhD (Japan), Department of Industrial Management, University of Kelaniya. E-mail: janaka@kln.ac.lk*

instead of just relying on conventional defense techniques, the next generation of system software must be designed from the ground up to provide stronger isolation of services running on computer systems.

3 Existing Security Threats & Attacks

3.1 VM Escaping & VM Monitoring

Cloud infrastructure is benefited with co-location of multiple CIs. This benefit, if not carefully deployed, become a threat to the environment. Moreover, current virtual machine monitors (VMMs) do not offer the perfect solution for VM instance monitoring. Many security vulnerabilities, which an attacker can exploit, have been discovered in all popular VMMs [9]. In ideal world administrator and users of virtualization expect 100% isolation of VM instances. Unfortunately, architectural limitations, the VM vendor's approach to isolation, or bugs in the virtualization software may limit the ability of isolation. VM escape is such a scenario which in the worst case, a program running inside a VM would be able to completely bypass the VM layer, getting full access to the hosting environment [10]. For example, successful exploitation of VMWare remote arbitrary code execution vulnerability may allow an attacker to execute arbitrary code on the vulnerable computer hosting VMWare resulting a complete compromise [10]. Sometimes one VM can monitor another VM, resides on same physical resources. This is done through CPU, memory or network traffic or some other means of intervention. The Hypervisor is responsible for memory isolation and it can use the built in memory protection feature of modern CPUs, which prevents one VM seeing the other VM's memory resources [11]. Network traffic isolation completely depends on the configuration of the virtual networking environment. VMs are linked to the host machine by means of virtual hub" or by a virtual switch [11]. This enables the guest machines to sniff packets into the network or even worse that the guest machines can use Address Resolution Protocol (ARP) poisoning to redirect the packets going to and coming from another guest [12]. When virtualization technology differs, there are different implications for the host machine to influence the VMs up and running in the system. Once the host machine got compromised, the security of the VMs is under question. Always care should be taken when configuring the VM environment so that enough isolation should be provided which avoids the host being a gateway for attacking the virtual machine [12].

3.2 Zombies in the Cloud

Botnets are one of the fastest growing threats among malware today. A zombie is a computer connected to the Internet that has been compromised by a hacker, computer virus or Trojan horse and can be used to perform malicious tasks of one sort or another under remote direction. A Zombie essentially needs not to be a physical computer. A zombie can be a VM instance in the Cloud. Jiang et al [13], provide an estimate that 40% of the 800 million computers that connect to the internet on a daily basis are Zombies that are part of a botnet [13]. For an example, Amazon's Cloud-based EC2 service was attacked by a botnet in late 2009 [14]. This attack was triggered by a compromised internal service. Analysis of the incident yielded information detailing how a variation of the password-stealing Zeus banking Trojan had infected client computers within the EC2 Cloud. The infection was a direct result of malicious intruders compromising a site within EC2, and transforming it into a Botnet Command and Control (C&C) system. The attack was further aggravated by a power outage at one of Amazon's data centers in Virginia [14]. William Moss and Brian Richardson, in their research presented a hypo that if an attacker wished to turn a Cloud environment into a large botnet, they could begin by establishing and verifying co-residency on a cluster within a Cloud such as EC2. Once this was established, they would have free region to upload their malicious code to their own co-resident CI. They further state that within a short amount of time, due to the fact that EC2 does not allow more than one machine per user on any given cluster [15], the attacker could establish zombies that had co-residency with several targets in a short amount of time, provided they had no preference as to who their targets were.

3.3 Cloud Malware Injections

Cloud malware injection is an attempt of injecting a malicious service implementation or virtual machine into the Cloud system [16]. Once a malicious VM instance is planted in the Cloud or there is a malware infected CI available on the Cloud, it could serve any particular purpose the adversary is interested in, ranging from eavesdropping to full functionality changes or blockings. The Cloud administrators need to pay special attention on this type of attack that will look to penetrate the security perimeters of these titanic data pools in the Cloud. Once compromised, vast quantities of personal data will become available to cyber-criminals. For an example a report by CNN [17] highlighted that in January 2010, Google announced its web-based Gmail system had been compromised by a malware attack originating in China. This incident proves that malware is already finding its way into these titanic data pools [18] of the major players of Cloud resources.

3.4 Flooding Attacks

Cloud Computing enables a dynamic adaptation of hardware requirements to the actual workload requirements. Though this feature of providing more computing power on demand is appreciated in the case of valid users, it poses severe issues in the presence of an attacker. Once such attacking scenario is “flooding attacks” [16]. To elaborate flooding attacks on Cloud, two security experts David Bryan and Michael Anderson conducted a research and they warned that "Cloud-based denial-of-service attacks are looming on the horizon with $6 and a homemade Thunder Clap" program, they managed to take down their client's server by using the Amazon's EC2 Cloud infrastructure itself [19]. In a Direct Denial of Service attack (DOS), the attacker only needs to flood a single Cloud-based address in order to perform a full loss of availability of the intended service. In the worst case scenario, if an attacker manages to utilize another different Cloud Computing infrastructure or the same Cloud infrastructure, where the victim resides, as the attack launching pad. It will lead towards a race in the processing power between two different Cloud infrastructures, or between the victim and the attacker within the same Cloud infrastructure [20]. In a situation where the attacker and the victim reside in same Cloud infrastructure, the race for processor power would play both Cloud systems against each other. Both the parties would be provided more and more computational resources for creating, respectively fending, the flood, until one of them eventually reaches full loss of availability.

3.5 Side Channel Attacks

"I might find out all kind of business intelligence with things that these `side-channels' might leak," said Radu Sion, a computer scientist at Stony Brook University who was chairing a Cloud security workshop at CCSW 2009 conference at which a paper was presented [21]. Because Cloud Computing introduces a shared resource environment, unexpected side channels (passively observing information) and covert channels (actively sending data) can arise. Sharing of resources means that an activity of one Cloud user might be visible to other Cloud users that use the same resources; potentially leading to the construction of covert and side channels. Utilization of side channels to learn information about co-residency of VM instances inside the Cloud is one of the usable scenarios of side channel attacks. In [22], they have shown that (time-shared) caches allow an attacker to measure when other instances are experiencing computational load. Leaking such information might seem not harmful, but in fact it can already be quite useful to clever attackers. They introduce several novel applications of this side channel: robust co-residence detection and timing keystrokes by an honest user (via SSH) of a co-resident instance. Although side channel attacks are said to be possible in carefully controlled environments, Cloud service providers claim that the side-channel method is not seeming reasonable or probable. Further, they explain that the side channel techniques presented are based on test results from a carefully controlled lab environment with configurations that do not match the actual commercial Cloud environment. As the researchers point out, there are a number of factors that would make such an attack significantly more difficult in practice.

3.6 Malicious Insiders

Although it is less likely, the damage that may be caused by malicious insiders is often far greater. This threat clearly identifies that there is no security mechanisms which will provide a 100% secure environment. In [23] Stephen Biggs and Stilianos Vidalis believe that time will ultimately see Cloud infrastructures, resources and physical domains been compromised by insider attacks. Even though certain roles like Cloud service providers, system administrators and managed security service providers are essential to manage Cloud service infrastructure, these roles sometimes may lead to a role of a malicious insider [24].

3.7 Insecure APIs and Interfaces

The era of cloud has realized the inconsistency of attempting to make services accessible to millions while restricting any harm to a great extent unnamed clients may do to the service. The response has been an open confronting application programming interface, or API, that characterizes how an outsider associate an application to the administration and giving confirmation that the outsider delivering the application is who he says he is. Heading web engineers, including Twitter and Google, teamed up on pointing out Oauth [25], an open approval administration for web benefits that controls outsider access. Oauth turned into a web designing team standard in 2010 and form 2.0 is utilized for a few administrations by real multi-occupant associations such of Facebook, Microsoft and Google. Anyway security masters caution that there is no superbly secure open API, and Oauth, in spite of its insurance and controls, is liable to break [26]. Execution of Oauth-supporting APIs by outsider engineers could be defective too. From authorization and access control to encryption and action checking, these interfaces must be intended to ensure against both inadvertent and pernicious endeavors to bypass different strategies. Such strategies keep unapproved clients from arriving at parts of uses that are not piece of the general population benefit or confine clients to operations that match their benefit level. Dependence on a powerless set of interfaces and APIs exposes organizations to a mixture of security issues identified with privacy, integrity, accessibility and accountability.

3.8 Shared Technology

In a multi nature's turf, the tradeoff of a solitary segment, for example, the hypervisor, uncovered more than simply the compromised client rather it uncovered the whole environment to a capability of compromise and rupture. The same could be said other imparted services, including CPU reserves, a shared database benefit, or shared storage. The cloud is about shared foundation, and a misconfigured working framework or application can prompt compromises beyond their immediate surroundings. In a shared infrastructure, the security experts acclaimed an in-profundity defensive system [27]. Protections ought to apply to the utilization of compute, storage, networking, applications and client access. Further the observing ought to look for dangerous moves and practices.

4 Conclusion

Since the concept of Cloud Computing was proposed Cloud Security has inevitably become a significant business differentiator. Much of cloud computing targets customers who have extensive business reasons (and scars from the past) leading them to treat security as an elevated priority. Although emerging technologies and architectures, used in Cloud Computing, introduce new features, they bring their own security concerns and challenges to the Cloud environment. Cloud Security Alliance (CSA) states that the lowest common denominator of security will be shared by all tenants in the multi-tenant virtual environment unless a new security architecture can be achieved that does not wire in any network dependency for protection". New robust security measurements are essential in order to assure proper security. Although there are many security concerns, just as the Internet made information universally accessible, affordable, and useful, Cloud Computing also has the potential to bring about the computation revolution, in which large-scale computations become universally accessible, affordable, and useful.

Acknowledgment

I would like to sincerely thank to Dr. Janaka Wijayanayake and Ms. K.V.S. Perera for the discussion on some important points and their precious time.

References

[1] Albus J., 2002. A reference model architecture for intelligent unmanned ground vehicles. In Proceedings of SPIE Aerosense Conference. Pp. 303-310.

[2] Ghosh R., Naik V.K, Trivedi K.S. 2011. Power-performance trade-offs in IaaS cloud: A scalable analytic approach. In IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops (DSN-W). Hong Kong, 27-30 June. China: IEEE. 152 - 157.

[3] Qayyum J., et al. 2011. Implementing and Managing framework for PaaS in Cloud Computing. IJCSI International Journal of Computer Science, 8 (5), pp. 474-479.

[4] Banerjee S., Jain S., 2014. A survey on Software as a service (SaaS) using quality model in cloud computing. International Journal of Engineering and Computer Science, 3 (1), pp. 3598-3602.

[5] Gurav U. and Shaikh R., 2010. Virtualization: a key feature of cloud computing, In Proceedings of the International Conference and Workshop on Emerging Trends in Technology. Mumbai, 26-27 February. 227-229.

[6] Lombardi F. and Pietro R.De. 2011. 'Secure virtualization for cloud computing'. Journal of Network and Computer Applications, 34(4), pp. 1113–1122.

[7] Pal S., Kumar P., 2012. 'Efficient Architectural Framework for Cloud Computing ', International Journal of Cloud Computing and Services Science (IJ-CLOSER), 1(2), pp. 66-73.

[8] Yinqian Zhang, Ari Juels, Michael K. Reiter, and Thomas Ristenpart., 2012. Cross-VM side channels and their use to extract private keys. In Proceedings of the 2012 ACM conference on Computer and communications security (CCS '12). USA, 16-18 Oct. New York: ACM. 305-316.

[9] Sharif M., Lee W., Cui W., and Lanzi A., 2009. Secure in-vm monitoring using hardware virtualization. In Proceedings of the 16th ACM Conference on Computer and Communications Security. Chicago, 9-13 November. New York: ACM. 477-487.

[10] Kuyoro S.O., Ibikunle F., Awodele O. 2011. Cloud Computing Security Issues and Challenges. International Journal of Computer Networks (IJCN), 3(5), 247-255.

[11] Padhy R.P., Patra M.R. 2012. 'An Enterprise Cloud Model for Optimizing IT Infrastructure ', International Journal of Cloud Computing and Services Science (IJ-CLOSER), 1(3), pp. 123-133.

[12] Nimje A.R, Gaikwad V.T, Datir H.N., 2013. Green Cloud Computing: A Virtualized Security Framework for Green Cloud Computing. International Journal of Advanced Research in Computer Science and Software Engineering, 3 (4), pp. 642-646.

[13] Li C., Jiang W., and Zou X., 2009 Botnet: Survey and Case Study. In Fourth International Conference on Innovative Computing, Information and Control (ICICIC). Kaohsiung, 7-9 Dec. Kaohsiung: IEEE. 1184 - 1187.

[14] Jansen W. and Grance T., 2011. SP 800-144. Guidelines on Security and Privacy in Public Cloud Computing. Technical Report. NIST, Gaithersburg, MD, United States.

[15] Buyya R. et al. 2009. 'Future Generation Computer Systems'. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility, 25(2009), pp. 599-616.

[16] Jensen M., Schwenk J., Gruschka N., and Iacono L., 2009. On Technical Security Issues in Cloud Computing. In IEEE International Conference on Cloud Computing, 2009. CLOUD '09. Bangalore, 21-25 September. Bangalore: IEEE. 109 - 116.

[17] Wang X., Ting-lei H., Zhi-jian R., 2010. Notice of Retraction Research on the anti-virus system of military network based on cloud security. In International Conference on Intelligent Computing and Integrated Systems (ICISS). Guilin, 22-24 Oct. New York: IEEE. 656 - 659.

[18] Balduzzi M., Zaddach J., Balzarotti D., Kirda E., Loureiro S., 2012. A security analysis of amazon's elastic compute cloud service. In SAC '12 Proceedings of the 27th Annual ACM Symposium on Applied Computing. Italy, 26-30 March. New York: ACM. 1427-1434.

[19] Ristenpart T., Tromer e., Shacham H., Savage S., 2009. Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds. In Proceedings of Computer and Communications Security -- CCS '09. USA, 9–13 November. New York: ACM. 199-212.

[20] Jensen M., Gruschka N., and Luttenberger N., 2008. The Impact of Flooding Attacks on Network-based Services. In third International Conference on Availability, Reliability and Security, 2008. ARES 08. Barcelona, 4-7 March. Barcelona: IEEE. 509-513.

[21] David T., 2009. Cloud Security Is Not (Just) Virtualization Security. CCSW 2009: The ACM Cloud Computing Security Workshop. Chicago, 13 November.

[22] Shacham H., Ristenpart T., Tromer E. and Savage S., 2009. Hey, you, get out of my cloud: Exploring information leakage in third-party compute clouds. Proc. 16th ACM Conf. Computer and Communications Security. Chicago, 9-13 November. New York: ACM. 199-212.

[23] Biggs S., Vidalis S., 2010. 'Cloud Computing Storms', International Journal of Intelligent Computing Research (IJICR), 1(1/2), pp. 61-68.

[24] Duncan A.J., Creese S., Goldsmith M., 2012. Insider Attacks in Cloud Computing. In IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). Liverpool, 25-27 June. California: IEEE. 857-862.

[25] Pai S., et al., 2011. Formal Verification of OAuth 2.0 using Alloy Framework. In International Conference on Communication Systems and Network Technologies (CSNT). India, 3-5 June. USA: IEEE. 655-659.

[26] Georgiev M., et al., 2012. The most dangerous code in the world: validating SSL certificates in non-browser software. In ACM Conference on Computer and Communications Security. Raleigh, 16-18 October. USA: ACM. 38-49.

[27] Padhy R., Patra M., Satapathy S., 2011. Cloud Computing: Security Issues and Research Challenges. International Journal of Computer Science and Information Technology & Security (IJCSITS), 1(2), 136-146.