Cloud Computing Security, Privacy Improvements Using Virtualized High Trust Zone

Ashish Patel, Prabhakar Tiwari

Computer Science And Engineering Department SGBAU Amravati University, India.
Computer Science And Engineering Department SGBAU Amravati University ,India.

Abstract -

The benefits of cloud computing are clearly well known which include rapid deployment, ease of customization, reduce cost and low risks. However, some high profile security breaches confuse organizations as they attempt to deploy cloud services in their businesses. Although, the cloud service providers pitch the security of their services. Enhancements in existing security measures and advanced solutions are needed to ensure high level security and privacy of data on cloud. This paper provides a holistic overview of cloud security issues by encompassing unique threats in cloud computing and presents findings of a survey of practitioners view on cloud security. A Virtualized High Trust Zone (VHTZ) is then presented as a solution, especially for infrastructure based cloud services to tackle the attacks and network monitoring in a virtualized infrastructure.

Key words: **Cloud security, high trust zone, network monitoring.**

1. INTRODUCTION

Due to increasing connectivity and virtualization cloud computing has become mainstream venture for today's technology savvy enterprises. This leads to an increase adoption of cloud computing. However, still many organizations approach cloud computing skeptically. This is primarily because of the security issues associated with allowing a third party to manage data access and storage. To visualize the cloud's security issues, cloud fundamentals need to be understood. In cloud computing, information is stored in centralized servers and cached temporarily on clients that can include desktop computers, notebooks, handhelds and other networked devices. Typically, a cloud utilizes a set of virtualized computers that enable users to start and stop servers or use compute cycles only when needed. By design, cloud computing is scalable, flexible and elastic – offering IT staffs a way to easily increase capacity or add additional capabilities on demand without investing in new and expensive infrastructure, training new personnel or licensing more software. There are three key elements or delivery platforms of cloud computing. This paper extends our earlier studies 'an empirical study of challenges in managing the security in cloud computing' and 'Security challenges and countermeasures in cloud computing' and provides our holistic approach in securing cloud computing using a High Trust Zone (HTZ) virtual environment. The HTZ emphasizes on virtual environment in IaaS due to its extensible delivery model which allows abstract infrastructure and resources to be made available to clients as isolated Virtual Machines (VMs) .

2. SECURITY AND PRIVACY ISSUES IN CLOUD COMPUTING

Cloud computing and its service platforms are exposed to security and privacy issues, mainly due to the fact that the users do not have a control over the data. This raises several questions such as (1) trust, can users trust a cloud service which is open to various vulnerabilities (2) data uncertainty, what happens of the cloud sever crashes, how the data is recovered and what are the disaster recovery procedures, and (3) control over data, how much control a user has over their data which might be stored in an unidentified location. The privacy issue in cloud computing are growing but specifically in the public cloud architecture and exclusively in "on-demand" and "pay-as-you-go" model, which is a shared cloud computing platform and is opted by various enterprises for further cost reduction while opting for cloud computing, most of the providers opt for virtualization being a part of public cloud, as it enables them to share multiple resources with various users in an independent environment.

A. Minimum User Control

The cloud does offer variety of services and platforms to its users but when it comes to data control the cloud seriously falls flat. Due to very basic reasons that the providers and the users hardly have a control over the data being stored and transmitted as its happening over the cloud and without any strong formed policies at both ends.

B.Unauthorized Usage of Data

There is possibility that the data stored on the cloud service provider end may be used by third party agencies (besides law enforcement agencies) for advertising purposes, this way the providers can earn extra revenue while sharing the data of the user with the advertising agencies or companies. However there is no such guarantee provided by some service providers that they would not share the user data with third parties but it should be in the best practices of the user/enterprise to bind the providers in a legal contract agreement clearly mentioning the said point. This will ensure trust between the providers and users and will allow restrained access to their data by third party or advertisers.

C. Data Redundancy

Data duplication is one of the benefits of the cloud but is also a point of concern. To protect the data and to take necessary disaster recovery steps the data of the user is replicated over various data centers of the providers, it is difficult to find out genuinely whether all data has been wiped out from the multiple storage locations of the providers.

E. Multi Tenancy

Cloud computing users share physical resources with others through common software: virtualization layers. These shared environments introduce unique risks into a user's resource stack. For example, the cloud consumer is completely unaware of a neighbor's identity, security profile or intentions. The virtual machine running next to the consumer's environment could be malicious, looking to attack the others or sniff communications moving throughout the system.

F. Data Privacy

The public nature of cloud computing poses significant implications to data privacy and confidentiality; Cloud data is often stored in plain text, and only few companies have an absolute understanding of the sensitivity levels their data stores hold. Data breaches are embarrassing and costly . Recent laws, regulations and compliance frameworks compound the risks; offending companies can be held responsible for the loss of sensitive data and may face heavy fines over data breaches. Business impacts aside, loose data security practices also harm on at personal level. Lost or stolen medical records, credit card numbers or bank information may cause emotional and financial ruin, the repercussions of which could take years to repair.

The risks to cloud computing are further categorized as below:

Unauthorized access – It is always a risk that the data being stored in the cloud can be used by unauthorized personnel's or the third party users especially in "pay-as- you-go" and "on-demand" cloud models where the security of these models are of a least concern to the cloud providers. For instance a virtual machine (VM) on a PaaS service model hosted for a client by a service provider will hardly carry any security checks or security policy updates as that would incur cost and that would be added to the client costs and the service provider might loose the client in added costs to the whole "pay-as-you-go" model and this way they open doors to the attackers. VM threats – VM threats or virtual machine threats are the most complicated and destructive threats, any loophole or vulnerability in VM can lead the attacker straight to the physical host and thus compromising the physical host. VM threats are on rise these days because the enterprises/users and the cloud service providers do not pay enough attention in updating the VM security policies this can open doors to the attackers inviting them to use the vulnerability and putting everything in the cloud model and the physical host at stake.

a. Threat Model -The virtualized architecture of cloud computing offers various benefits to the cloud user however security of the cloud is the responsibility that is shared between the cloud user and cloud provider. The users of cloud computing are not aware of the security policies through which their VMs are protected. On the other side, cloud providers running VMs are not aware of the contents of the VMs. Thus, there is no complete trust between cloud customers and providers. From a cloud provider perspective, the VMs of the user cannot be trusted. For instance, a hacker can be either a cloud user that may be already hosting a service or a non-cloud user. In either of these models the victim is the cloud provider who runs the service to host the VMs of the users. In case of a security breach, the responsibility and infrastructure that is compromised belongs to the provider. In the former threat model, hackers have more chances of success due to the fact that they have more access to the cloud computing virtual infrastructure and have the ability to run various malware to gain access on the system.

b. Security Threats - It is evident that breaching any component of the virtualized cloud infrastructure greatly

impacts on the security of the other components and affects the overall security of the cloud computing virtualized infrastructure. investigated several vulnerabilities and threats to the security of the cloud computing especially focusing on the virtualized cloud computing security. These threats can be broadly categorized in three categories.

3. VIRTUALIZED HIGH TRUST ZONE(VHTZ)

A High Trust Zone (HTZ) is proposed by to safeguard virtual cloud computing on IaaS platform, and virtual environment. Creating a high trust zone establishes a high degree of trust between the data, users, providers and the systems. following the security in proposed two phases.

Phase -1 - Configuring the Virtualized Infrastructure

Step -1 -Securing the Virtual Cloud

The first step to protect the virtual cloud is to protect the virtualization infrastructure by isolating the infrastructure (virtualized) from the servers that are going to be virtualized, also by protecting accounts that will be used to control virtualization, securing applications by moving them to the High trust zone and by hardening the Operating System (OS). By hardening the OS, the unnecessary applications or features of the OS will be removed and only the required ones will be kept. The most important factor of this process is to isolate the virtualization infrastructure, this means that the customer VMs will not impact any of the system or data center VMs of the cloud provider.

Step -2 - Securing applications and moving them to High Trust zone

Before moving applications to High Trust Zone it is necessary to build a preproduction virtualized environment, this will be used to test the application (to be moved) for testing, compatibility, application review and some testing on the security perspective of the application [7]. The goal for application testing from security perspective is to ensure that existing policies of the application or the VM is carried over from the physical world to the virtual world. For instance whether to allow the GPO (group policy objects) objects in the application such as remote deployment of application updates etc.

Step – 3 - Risk Assessments of Applications

Risk assessment of application is mandatory to find out the risks associated with the applications before moving them to the High Trust Zone. This assessment is required to ensure that applications or the system being added to the high trust zones do not have any additional risks associated with them or add to the security risks of the High Trust[8].

Phase - 2 Network Monitoring

To secure the High Trust Zone and to provide the High Trust Zones with the capability of prevention and protection environment, there is a strong need of implementing a mix of network attack and intrusion detection capabilities. At first, the network intrusion monitoring has to be implemented that will analyze and monitor all traffic coming into and going out of the high trust zone. Additionally, there is a strong need of implementing network traffic analysis behavior, this process would ensure the normal traffic patterns and shall enable abnormal traffic activity, with a facility of sending appropriate alerts[9]. Besides the aforesaid the authors also suggest implementing Host Based Intrusion Prevention System and Host Based Intrusion Detection System specifically on the VMs deployed on the High Trust zones, this would help to have a broader and wide coverage of the attacks specifically to the VMs.

4. CONCLUSION

In this paper we have presented the unique security and privacy issues in cloud computing. This paper provides a thorough overview of security issues Enhancements are needed in current security solutions to fully realize the benefits of cloud computing. For a safer Infrastructure as a Service (IaaS) a Virtualized High Trust Zone (VHTZ) is presented to secure the virtual machines in IaaS environment. The two phases VHTZ ensures the cloud security by configuring the virtualized infrastructure and ensuring network monitoring to detect and prevent network attacks. The VHTZ increases the monitoring of incoming and outgoing network traffic by providing extra host level security protection to the individual.

REFERENCES

[1] Cloud Security Alliance. Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, http://www.cloudsecurityalliance.org/csaguide.pdf [2] Gellman, R. (2009). Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing. Retrieved August 18, 2012, from World Privacy Forum: http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf

[3] Tadapaneni, N. R. (2017). Different Types of Cloud Service Models. Available at SSRN 3614630.

[4] Mansukhani, B., and Zia, T. A. (2011). An Empirical Study of Challenges in Managing the Security in Cloud Computing. 9th Australian Information Security Management Conference (secau Security Congress 2011). December 5 – 7, 2011, Perth, Australia.

[5] Tadapaneni, N. R. (2018). Cloud Computing: Opportunities And Challenges. International Journal of Technical Research and Applications.

[6] Brodkin, J. (2018). Gatrner: Seven Cloud computing security risks. Retrieved 06 07, 2011, from http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853

[7] Winkler, V. (. (2011). Securing the Cloud - Cloud Computing Security Techniques and Tactics (1st Edition ed.). Oxford: Syngress

[8] Pearson S, e. a. (2009). Scalable, Accountable Privacy Management for Large Organizations. (pp. 168-174). INSPEC: IEEE.

[9] Chauhan, S., & Vermani, S. (2016). Shift from Cloud Computing to Fog Computing. Journal of Applied Computing, 1(1), 25-29.