

DIFFERENT ASPECTS OF CLOUD SECURITY

Madhu Chauhan¹, Riidhei Malhotra², Mukul Pathak³ and Uday Pratap
Singh⁴

^{1,3,4}Department of Computer Science & Engineering, Galgotias College of Engineering & Technology, Greater
Noida (U.P.), India

Department of Information Technology & Engineering, Galgotias College of Engineering & Technology, Greater
Noida (U.P.), India

Abstract

Cloud computing is a recent trend in IT that moves computing and data away from desktop and portable PCs into large data centers. It refers to applications delivered as services over the Internet as well as to the actual cloud infrastructure — namely, the hardware and systems software in data centers that provide these services. Organizations use cloud computing as a service infrastructure; critically like to examine the security and confidentiality issues for their business critical insensitive applications. Yet, guaranteeing the security of corporate data in the "cloud" is difficult, if not impossible, as they provide different services like Software as a service (SaaS), Platform as a service (PaaS), and Infrastructure as a service (IaaS). Each service has their own security issues. This paper presents different aspects of security issues related with cloud computing, and its possible solution.

Keywords- cloud computing, w-s security, cloud computing security, virtualization.

1. INTRODUCTION

The new concept of *Cloud Computing* offers dynamically scalable resources provisioned as a service Over the Internet and therefore promises a lot of economic benefits to be distributed among its adopters. Depending on the type of resources provided by the Cloud, distinct layers can be defined (see Figure 1).

The bottom-most layer provides basic infrastructure components such as CPUs, memory, and storage, And is henceforth often denoted as Infrastructure-as-a-Service (IaaS). Amazon's Elastic Compute Cloud (EC2) is a prominent example for an IaaS offer. On top of IaaS, more platform-oriented services allow the usage of hosting environments tailored to a specific need. Google App Engine is an example for a Web platform as service (PaaS) which enables to deploy and dynamically scale Python and Java based Web applications. Finally, the top-most layer provides it users with ready to use applications also known as Software-as-a-Service (SaaS). To access these Cloud services, two main technologies can be currently identified. Web Services are commonly used to provide access to IaaS services and Web browsers are used to access SaaS applications. In PaaS environments both approaches can be found.

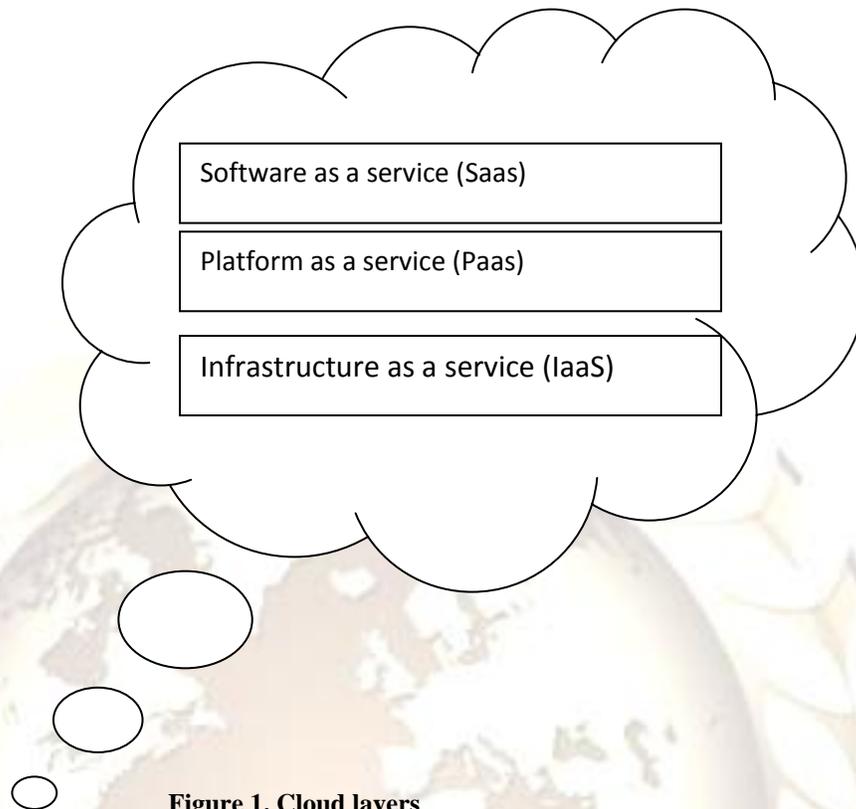


Figure 1. Cloud layers

All of these layers come with the promise to reduce first of all capital expenditures (CapEx). This includes reduced hardware costs in the IaaS layer and reduced license costs in all layers. Especially in the IaaS layer it is not required anymore to engineer the own data center for peak performance cases, which occur in general very seldom and which usually result in a poor utilization of the available resources. Additionally, reductions of the operational expenditures (OpEx) in terms of reduced hardware, license and patch management are promised as well.

Cloud computing is a network-based environment that focuses on sharing computations and resources. Basically, clouds are Internet-based and try to disguise complexity for clients. Cloud providers use virtualization technologies combined with self-service abilities for computing resources via network infrastructure especially the Internet. In cloud environments multiple VMs (VM) hosted on the same physical server as infrastructure. In cloud, costumers only have to pay for what they use. Cloud computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services.

The paper is organized as follows. In the next section, we outline the different virtualization approaches used in the context of Cloud Computing and security. Then, in Section 3, we provide a set of security-related issues that apply to different Cloud Computing scenarios. Each issue is briefly described and complemented with a short sketch on countermeasure approaches that are both sound and applicable in real-world scenarios. The paper then concludes in Section 4, also giving future research directions for Cloud Computing security.

2. VIRTUALIZATION APPROACHES

In the traditional environments which consist of several physical servers that connected by a physical switch, IT organizations can get detailed management information about the traffic that transmits between the servers from the physical switch. Unfortunately, that level of information management is not provided typically by a virtual switch (The virtual switch has links from physical switch via physical NIC that attach to VMs). The resultant is lack of visibility into the traffic flows between and among the VMs on the same physical level that impacts security

performance. There are several common approaches to virtualization with differences in how they have control over the VMs.

2.1 Operating system-based virtualization

In this approach, Virtualization is enabled by a hosting operating system that supports multiple isolated and virtualized guest OS on a single physical server with this characteristic that all are on the same operating system kernel with has control on Hardware infrastructure Exclusively. The hosting operating system has visibility and control over the VMs. This approach is simple but it has vulnerabilities. For example, an attacker can inject kernel scripts in hosting operating system and this can cause all guest OS have to run their OS on this kernel. The result is attacker have control over all VMs that exist or will establish in future.

2.2 Application-based virtualization

An application-based virtualization is hosted on top of the hosting operating system. This virtualization method emulates each VM which contains its own guest operating system and related applications. This virtualization architecture is not commonly used in commercial environments. Security issues of this approach are similar to Operating system-based [1].

2.3 Hypervisor-based virtualization

As mentioned before, a hypervisor is embedded in the hardware infrastructure or the hosting operating system kernel. The Hypervisor is available at the booting time of machine in order to control the sharing of system resources across multiple VMs. Some of these VMs are privileged partitions that they managed the virtualization platform and hosted VMs. In this architecture, the privileged partitions have visibility and control over the VMs. This approach establish most controllable environment and can perform additional security tools such as Intrusion detection systems. But it was vulnerable because of the hypervisor is single point of failure. If hypervisor crashed or attacker gets control over it then all VMs are on the attacker control. However, take control over hypervisor from VM level is difficult but not impossible.

2.4 CLOUD-BASED VIRTUALIZATION CONCERNS

The potential problem also exists for virtualization is provider combine too many VMs onto a physical server. This can result in performance problems caused by impact factors such as limited CPU cycles or I/O bottlenecks. These problems can occur in a traditional physical server, but they are more likely to occur in a virtualized server because of the connection single physical server to multiple VMs that all of them competing for critical resources. Thereby, management tasks such as performance management and capacity planning management are more critical in a virtualized environment than in a similar physical environment. This means that IT organizations must be able to continuously monitor in real time the utilization of both physical servers and VMs. This capability allows IT organizations to avoid both over- and underutilization of server resources such as CPU and memory and to allocate and reallocate resources based on changing business requirements. This capability also enables IT organizations to implement policy-based remediation that helps the organization to ensure that service levels are being met [2].

Another challenge in Virtualization is that cloud organizations now have to manage VMs sprawl. With VM Sprawl, the number of VMs running in a virtualized environment increases because of creating new VMs, not because those VMs are necessary for the business. Worries with VM sprawl are the overuse of the infrastructure. To prevent VM sprawl, VM manager should analyze the need for all new VMs carefully and ensure that unnecessary VMs migrate to other physical server. In addition, an unnecessary

VM will able to move from one physical server to another with high availability and energy efficiency. But be considering the VM destination can be challenging to ensure that the migrated VM keeps the same security, QoS configurations, and needed privacy policies. In the other hand, the destination must be assurance keeping all the required configurations of migrated VM.

3. CLOUD COMPUTING SECURITY ISSUES

In the following, we present a selection of security issues related to Cloud Computing. Each issue is explained briefly and accompanied with a short discussion on potential or real-world measured impacts.

3.1 XML SIGNATURE

A well known type of attacks on protocols using XML Signature for authentication or integrity protection is *XML Signature Element Wrapping* [4] (henceforth denoted shortly as wrapping attack). This of course applies to Web Services and therefore also for Cloud Computing.

Since the discovery of wrapping attacks by McIntosh and Austel in 2005 a number of further variations, Counter measures and again attacks circumventing these countermeasures have been published. For example, in [5] a method – called *inline approach* – was introduced to protect some key properties of the SOAP message structure and thereby hinder wrapping attacks, but shortly later in [6] it was shown how to perform a wrapping attack anyhow.

However, mostly due to the rare usage of WS -Security in business applications these attacks remained theoretical and no real-life wrapping attack became public, until in 2008 it was discovered that Amazon's EC2 services were vulnerable to wrapping attacks [7]. Using a variation of the attack presented before an attacker was able to perform arbitrary EC2 operations on behalf of a legitimate user. In order to exploit the SOAP message security validation vulnerability of EC2, a signed SOAP request of a legitimate, subscribed user needed to be intercepted. Since the vulnerability in the SOAP request validation allows to interfere any kind of operation and have it executed, it does not matter what kind of request the attacker has at its disposal. The instantiation of a multitude of virtual machine to send spam mails is just one example what an attacker can do—using the legitimated user's identity and charging his account.

3.2 BROWSER SECURITY

In a Cloud, computation is done on remote servers. The client PC is used for I/O only, and for authentication and authorization of commands to the Cloud. It thus does not make sense to develop (platform dependent) client software, but to use a universal, platform independent tool for I/O: a standard Web browser. This trend has been observed during the last years, and has been categorized under different names: Web applications, Web 2.0, or Software-as-a-Service (SaaS).

Modern Web browsers with their AJAX techniques (JavaScript, XMLHttpRequest, Plugins) are ideally suited for I/O. But what about security? A partial answer is given in [8], where different browser security policies (with the notable exception of TLS) are compared for the most important browser releases. With a focus on the *Same Origin Policy* (SOP), this document reveals many shortcomings of browser security. If we additionally take into account TLS, which is used for host authentication and data encryption, these shortcomings become even more obvious.

Web browsers can not directly make use of XML Signature or XML Encryption: data can only be encrypted through TLS, and signatures are only used within the TLS handshake. For all other cryptographic data sets within WS-Security, the browser only serves as a passive data store. Some simple workarounds have been proposed to use e.g. TLS encryption instead of XML Encryption, but major security problems with this approach have been described in the literature and working attacks were implemented as proofs-of concept. Our goal is to propose provably secure solutions using TLS, but at the same time encourage the browser community to adapt XML based cryptography for inclusion in the browser core.

3.3. CLOUD INTEGRITY AND BINDING ISSUES

A major responsibility of a Cloud Computing system consists in maintaining and coordinating instances of virtual machines (IaaS) or explicit service implementation modules (PaaS). On request of any user, the Cloud system is responsible for determining and eventually instantiating a free-to-use instance of the requested service implementation type. Then, the address for accessing that new instance is to be communicated back to the requesting user.

Generally, this task requires some metadata on the service implementation modules, at least for identification purposes. For the specific PaaS case of Web Services provided via the Cloud, this metadata may also cover all Web Service description documents related to the specific service implementation. For instance, the Web Service description document itself (the WSDL file) should not only be present within the service implementation instance, but also be provided by the Cloud system in order to deliver it to its users on demand.

Most of these metadata descriptions are usually required by any user prior to service invocation in order to determine the appropriateness of a service for a specific purpose. Additionally, these descriptions also represent some preliminary service identifiers, as assumably service implementations with identical WSDL descriptions provide the same functionality. Thus, these metadata should be stored outside of the Cloud system, resulting in a necessity to maintain the correct association of metadata and service implementation instances.

3.4 FLOODING ATTACKS

A major aspect of Cloud Computing consists in outsourcing basic operational tasks to a Cloud system provider. Among these basic tasks, one of the most important ones is server hardware maintenance. Thus, Instead of operating an own, internal data center, the paradigm of Cloud Computing enables companies(users) to *rent* server hardware on demand (IaaS). This approach provides valuable economic benefits when it comes to dynamics in server load, as for instance day-and-night cycles can be attenuated by having the data traffic of different time zones operated by the same servers. Thus, instead of buying sufficient server hardware for the high workload times, Cloud Computing enables a dynamic adaptation of hardware requirements to the actual workload occurring. Technically, this achievement can be realized by using virtual machines deployed on arbitrary data center servers of the Cloud system. If a company's demand on computational power rises, it simply is provided with more instances of virtual machines for its services.

Under security considerations, this architecture has a serious drawback. Though the feature of providing more computational power on demand is appreciated in the case of valid users, it poses severe troubles in the presence of an attacker. The corresponding threat is that of *flooding attacks*, which basically consist in an attacker sending a huge amount of nonsense requests to a certain service. As each of these requests has to be processed by the service implementation in order to determine its invalidity, this causes a certain amount of workload per attack request, which—in the case of a flood of requests—usually would cause a Denial of Service to the server hardware (cf. [2], [3]).

In the specific case of Cloud Computing systems, the impact of such a flooding attack is expected to be Amplified drastically.

4. CONCLUSION AND FUTURE WORK

In this paper, we presented a selection of issues of Cloud Computing security and approaches of virtualization. We investigated ongoing issues with application of XML Signature and the Web Services security frameworks (attacking the Cloud Computing system itself), discussed the importance and capabilities of browser security in the Cloud Computing context (SaaS), raised concerns about Cloud service integrity and binding issues (PaaS), and sketched the threat of flooding attacks on Cloud systems (IaaS). Cloud computing is defined as a pool of virtualized computer resources. Based on this Virtualization the Cloud Computing paradigm allows workloads to be deployed and scaled-out quickly through the rapid provisioning of VMs or physical machines.

As can be derived from our observations, a first good starting point for improving Cloud Computing security consists in strengthening the security capabilities of both Web browsers and Web Service frameworks, at best integrating the latter into the first. Thus, as part of our ongoing work, we will continue to harden the foundations of Cloud Computing security which are laid by the underlying tools, specifications, and protocols employed in the Cloud Computing scenario.

REFERENCES

- [1] J. Heiser and M. Nicolett, "Assessing the security risks of cloud computing," *Gartner Report*, 2009. [Online]. Available: <http://www.gartner.com/DisplayDocument?id=685308t>.
- [2] M. Jensen, N. Gruschka, and N. Luttenberger, "The Impact of Flooding Attacks on Network-based Services," in *Proceedings of the IEEE International Conference on Availability, Reliability and Security (ARES)*, 2008.
- [3] M. Jensen and N. Gruschka, "Flooding Attack Issues of Web Services and Service-Oriented Architectures," in *Proceedings of the Workshop on Security for Web Services and Service-Oriented Architectures (SWSOA, held at GI Jahrestagung 2008)*, 2008, pp. 117–122.

- [4] Ristenpart and e. ai, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds," 2009.
- [5] N. Gruschka and L. Lo Iacono, "Vulnerable Cloud: SOAP Message Security Validation Revisited," in *ICWS '09: Proceedings of the IEEE International Conference on Web Services*. Los Angeles, USA: IEEE, 2009.
- [6] Google, "Browser security handbook," 2009. [Online]. Available: <http://code.google.com/p/browsersec/>
- [7] M. Jensen, N. Gruschka, and R. Herkenh"oner, "A survey of attacks on web services," *Computer Science - Research and Development (CSR D), Springer Berlin/Heidelberg*, 2009.
- [8] K. K. Fletcher, "Cloud Security requirements analysis and security policy development using a high-order object-oriented modeling," Master of science, Computer Science, Missouri University of Science and Technology, 2010.
- [9] M. Jensen and J. Schwenk, "The accountability problem of flooding attacks in service-oriented architectures," in *Proceedings of the IEEE International Conference on Availability, Reliability and Security (ARES)*, 2009.

Authors:



Madhu Chauhan

The author is pursuing M-Tech in CSE from Galgotias College of Engineering & Technology. She had completed B-Tech from Ideal Institute of Technology; Ghaziabad (U.P) affiliated to Gautam Buddha Technical University in 2010.



Riidhei Malhotra

The author is pursuing M-Tech in CSE from Galgotias College of Engineering & Technology. He had completed B-Tech from Ideal Institute of Technology; Ghaziabad (U.P) affiliated to Gautam Buddha Technical University in 2010.



Mukul Pathak

The author is pursuing M-Tech in CSE from Galgotias College of Engineering & Technology, Greater Noida (U.P.). He had completed B-Tech from College of Engineering & Technology; Moradabad affiliated to Gautam Buddha Technical University in 2010.



Uday Pratap Singh

The author is pursuing M-Tech in CSE from Galgotias College of Engineering & Technology. He had completed B-Tech from Shambhunath Institute of Engineering and Technology; Allahabad (U.P) affiliated to Uttar Pradesh Technical University in 2008.