Critical issues in Cloud Computing services & its Solutions

Satinder Kaur
Department of Computer Science & Engineering, GNDU, RC, Sathiala.

Simmi Bagga
Department of Computer Science &IT, Sant Hira Dass Kanya MahaVidyalaya, Kala Sanghian.

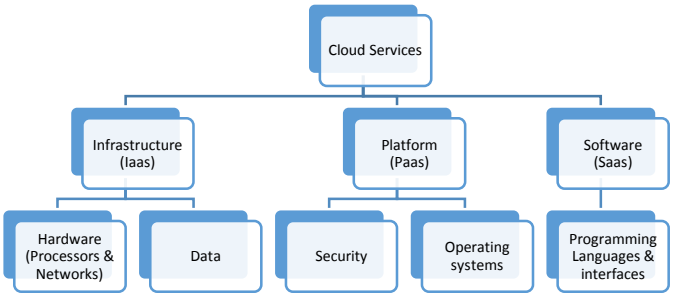
Hardeep Singh
Department of Computer Science & Engineering, GNDU, RC, Sathiala.

Abstract – Cloud computing deals with the branch of distributed data processing in which computer resources and capacities are provided to the user as an Internet service on payment basis. There are various problematic issues of cloud computing which needs special intentions for proper solutions so that cloud services can be used securely and safely. As these are many faults yet to be fully solved so, it becomes a new challenging area for the researchers. This paper introduces the services architecture of cloud and its supporting modules, critical issues in cloud computing with their solutions which can be implemented yet.

Index Terms – Anonymity, Network Reconnaissance, Port Scanning, Attacks, Brute-force.

1. INTRODUCTION

Cloud Computing represents one of the most significant and recent shifts in information technology which many of us are likely to see in our lifetimes. Reaching the point where computing functions as a utility has great potential, promising innovations we cannot yet imagine. Customers are both excited and nervous at the prospects of Cloud Computing. They are excited by the opportunities to reduce capital costs. They are excited for a chance to divest themselves of infrastructure management and focus on core competencies [3]. Most of all, they are excited by the agility offered by the on-demand provisioning of computing and the ability to align information technology with business strategies and needs more readily. However, customers are also very concerned about the risks of Cloud computing if not properly secured, and the loss of direct control over systems for which they are nonetheless accountable [1]. Cloud computing services are presented to the user in the figure 1.



1.1. Cloud Service Models & Internet

To implement the above hierarchy, three different models are employed. All these models are dependent on today's mother of everything i.e. internet which makes cloud services a different terms i.e. Internet of Things (IoT) as shown in figure 2. It is only the heterogeneity in Internet that makes possible this new shifting i.e. providing remote service on a cloud. For success customer as well as provider or vendor both need internet connectivity.

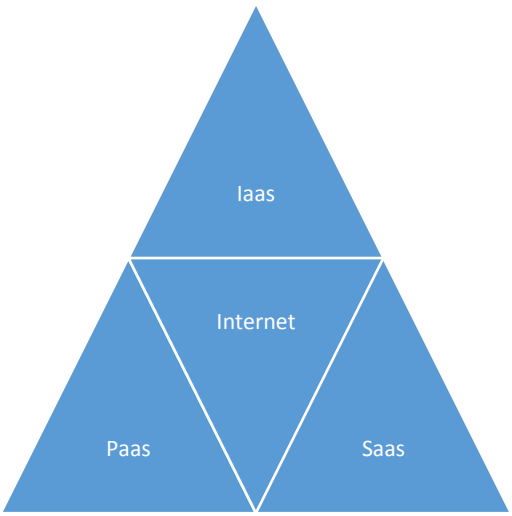


Figure 2: Relationship Between Internet & Cloud services

IaaS. First of all, we are interested in IaaS, because this service is the most needed and "realistic" environment for pentesters today. IaaS allows users to create a virtual server using the equipment of a cloud computing provider. The most evident advantage of this service consists in almost unlimited computing power, which may be used by a pentester as necessary, e.g. for password decryption. What is IaaS for a pentester? It is a unique opportunity to use dozens of servers of equal power to follow a realistic approach to implementation of such techniques as IPS fraud in the course of various attacks, such as remote port scanning, distributed password brute-forcing, denial of service attacks, network perimeter scanning and automated vulnerability detection in the Customer infrastructure. These services hardly have any peculiar features as such, except for the possibility to use resources limited only by a financial ceiling.

The list below shows the pioneer providers of cloud computing services:

- Amazon Compute Cloud [4]
- Sun Cloud Computing [5]
- Oracle Cloud Computing [6]
- IBM cloud [7]
- Windows Azure [8]
- Google App Engine [9]

PaaS. PaaS provides to companies different programming languages and tools to develop applications more quickly and efficiently in a cloud environment. The defining factor that makes PaaS unique is that it lets developers build and deploy web applications on a hosted cloud infrastructure. It consumes cloud infrastructure. Every centralized system requires new and different security measures. So, platform services are expected to provide full security. Common examples of platforms include Windows™, Apple Mac OS X, and Linux for operating systems; Google Android, Windows Mobile, and Apple iOS for mobile computing; and Adobe AIR or the Microsoft .NET Framework for software frameworks.

SaaS. SaaS is a software model provided by the vendor through an online service. It provides network-based access to commercially available software. User interface powered by "thin client" applications; cloud components; communication via (Application Program Interfaces (APIs); stateless; loosely coupled; modular; semantic interoperability [11]. This will avoid capital expenditure on software and development resources; reduced Return On Investment (ROI) risk; streamlined and iterative updates. On the contrary, Centralization of data requires new/different security measures. Examples of SaaS include Netflix, Intuit QuickBooks Online, Gmail, and Google Docs.

2. ABUSE TYPE[2]

The purposes of applying any innovative technology can be both good and bad. Similarly, cloud computing concludes with two ends. Advantages of cloud are manifold:

- Increased speed of deployment
- Increased user adoption
- Reduced support requirements
- Lowered cost of implementation and upgrades
- Lowered wastage of resources
- Increased interactivity, reliability and interoperability

But what are the threats in availing cloud services? How can a misuse be made of the service? This section is an attempt to consider this question in terms of the most widespread abuses by malicious Internet users. The following are the abuses which are mostly occur while using cloud computing services [10].

- Anonymity

Anonymity of operations with cloud computing services presents a highly urgent problem. Primarily, all information necessary to access such services is at best confined to a credit card number and a cell phone number, which are used to authenticate the person (e.g. by the Amazon service). To sell the services at a profit, providers readily offer promotional programs that allow users to enjoy the services free of charge within a certain time period and the only available information about a user who has accessed the service is the email and the IP address used to control the provided cloud computing services. However, there are a lot of ways to use cloud computing anonymously. The most elaborate verification at the registration stage is performed by Amazon: they request not only the debit card number, but also the telephone number of the account owner-to-be. A robot verifies this telephone number by making a call and giving the user-to-be a secret code necessary to complete registration. This peculiarity is quite inconvenient for a potential attacker; however, it does nothing towards registering anonymously.

- Network Reconnaissance

Network reconnaissance includes activities aimed at automated data-gathering for further analysis. Cloud computing presents a great platform for such operations as it provides everything needed for automatic data-gathering, namely: various IP addresses to gather the information from, broad bandwidth, and computing power high enough to process the gathered data and store it in the required format. When an IP address is blocked, it may be automatically changed using APIs which are present in most services. The possibility to change an IP address promptly allows one to organize effective distribution of letters using large databases of e-mail addresses.

- Port Scanning

Cloud computing services (e.g. IaaS) are a good choice for an attacker to use for network perimeter scanning and automated vulnerability search. Success is almost guaranteed, as an IaaS service allows attackers to bypass protection means such as IPS/IDS. Port scanning can be hidden from IPS/IDS if it is done from more than ten different IP addresses at time intervals and step by step. So, even well-configured IPS/IDS is unable to detect the port scanning event, otherwise the system will block only one IP address from all of the scanning servers. Naturally, this task requires special software that allows remotely managed server processes to run on the cloud provider site.

- Attack Implementation

A Cloud IaaS service site is ideal to attack remote services, carry out password bruteforcing and perform various client-site attacks. First, it is by no means complicated to deploy any utility, for example Metasploit Framework or Immunity Canvas. Second, password bruteforce can be distributed as in remote host port scanning to prevent the attacker IP address from being blocked. Third, an IaaS site can be an agent between an attacker and its target host as it helps to delete the entire IaaS action history if the server is shut down.

- Brute-force

Conditionally unlimited cloud resources enable attackers to successfully perform hash bruteforce and rainbow table generation and then to restore encrypted data. The main advantage that clouds provide for rainbow table generation is their huge data storage capacity. In practice, rainbow table generation for ntlm algorithm (mixalpha-numeric-all-space, 8 symbols) is just a matter of time and money. It would take 1290 years for a top home computer to generate such a table. Cloud computing is akin to a time machine that takes 18 months and 320,000 dollars to be created. Thus, clouds can generate such a table in just 18 months.

It is time to modify password policy: an NTLM hash of an 8-symbol password can easily be decrypted. Moreover, the 8-symbol requirement is hardly on the list of most corporate policies. A typical password security policy is less strict and allows users to have shorter passwords. According to the statistics collected by Dmitry Evteev of Positive Technologies, and presented in his report (http://www.ptsecurity.ru/download/PT-Metrics-Passwords-2009.pdf, available in Russian only), most users try to bypass password policy restrictions and use simple passwords.

Is it takes much time and considerable financial resources to generate such tables even by means of cloud computing? Yes, it does take a millennium and about 80 million dollars to generate a rainbow table for passwords consisting of English letters and figures (lower case, 1-12 symbols), which borders on fantasy even for an average national budget. However, if we were to set our mind to it and use 20,000 servers instead of 20, we could generate the table in a year.

- DDoS via Clouds

The success of a DDoS (Distributed Denial of Service) attack has the following preconditions:

- a great number of attacking machines

- an “intelligent” loading of the system under attack

The IaaS service together with specially developed software for DDoS attacks ensures successful DDoS against target systems. The IaaS service supports a multitude of attacking machines. Specialized software should be responsible for “intelligent” loading of systems under attack for the purpose of causing a denial of service. The specialists have developed a requirements specification for such software.

- Operability under various platforms (Linux/Windows)

- Several modules

- centralized control (client<->server)

- Trojan Horses in Instance

Another advantage of cloud computing services is that they allow one to select an OS and its components easily through a useful web interface. The user can apply both standard solutions from the provider and OS images created by users of the provider. For example, the Amazon service uses the latter scheme actively. However, this is the scheme that hides a hazard: providers do not guarantee that system images shared by users do not perform any hidden actions (i.e. do not log events, copy personal data, operate as a botnet part, distribute malicious software, etc.).

The performed testing indeed proved that most providers do not control such activities. The testing required:

- creating an image of a popular OS in the AMI format and publish it with open access to the Amazon interface;

- compiling a good description of the configured system (installed software, useful features, etc.).

At the same time, it was not mentioned that it is necessary to read the fine-print text informing users that every time they start this OS image, an HTTP GET message is sent to a server collecting statistical data. This fact could even be left unmentioned in the image description. As a result, 1000 messages were received during one month.

What is the amount of sensitive data that could have been gathered if it were more than just an innocuous collection of statistical information on the number of messages?

What stops a malicious user from uploading an image of a system with a pre-installed rootkit in it and use it once a day to

scan determined IP address ranges, thus gathering sensitive data? Hardly anything. It should be pointed out that providers assign a separate IP address from a given range for each image. Thus, one IP address can change owners several times a day. Just a couple of clicks in the web interface, and the IP address is changed, enabling attackers to perform phishing attacks and redirect users to so-called "exploit packs". Changing too fast, a malicious IP address gives users no time to spot it.

How Is Abuse Actually Treated? An immediate reaction on abuse should be part of the security policy of any provider, since it puts their reputation as a serious company at stake. But what is the reality? A little research has revealed that even such major cloud computing providers as Amazon are in no hurry to deal with various violations and investigate incidents. In fact, it doesn't go further than an incident entry. First of all, to look into an incident, a provider requires not only the attacker's IP address, but the exact date and time of the attack, which is a bit frustrating: if the time in your server is misconfigured, the investigation of your incident, even if conducted, will be unsuccessful.

After the required information about the attacker has been submitted to the provider, the correspondence will carry on. However, it will be quite a one-way correspondence: the provider will be happy to get your answers to their questions, while you, with some exceptions, will get a polite silence in response to yours.

3. PROPOSED SOLUTIONS: WHAT TO DO UNDER ATTACK?

When addressing your provider for the first time about the attack, you will be asked to provide the following information:

- Attacker's IP address;

- Victim's IP address;

- The port under attack and the protocol used for the attack;

- Exact date, time and victim's time zone;

- Logs from the victim's machine that evince the fact of the attack (not more than 4 Kb);

- Contact details.

It should be mentioned straightaway that the exact date, time and the victim's time zone of the attack are of extreme importance because the attacker's IP address can be changed several times a day, thus making it more difficult to trace the violator. For such cases we recommend identifying the IP address at the moment of the attack and then checking its availability within several hours. This information can be of significant help to the provider in investigating the incident. Try to identify the exact type of the attack also, then make a copy of the log files from the service being attacked. This copy is to be submitted to the security service later.

Other Security Measures that must be there are:

- Privacy measures-One-Time password (OTP), a digital certificate and biometric Verification
- Trusted third party involvement-Low and high level confidentiality, Server and client authentication, Creation of security domains, Cryptographic separation of data Certificate based authorization
- Legal measures-security metrics and standards in Service Level Agreements (SLA) and contracts.
- Machine security-Firewalls & Anti-virus software

4. CONCLUSION

Cloud computing technology has provided users with high-power computing, but at the same time it has provided some with an opportunity to apply this power for their selfish ends. There is no remedy for this problem. However, if you know possible attack vectors that use cloud computing, you can protect your information resources from possible incidents (e.g. caused by applying weak encryption algorithms). As regards users applying cloud computing services, we would like to say in conclusion that even when they use advanced services from top providers, they should always remember basic information security principles.

REFERENCES

[1] Yury Goltsev, "{AB}USE Their Clouds.Cloud Computing as Viewed by Pentester" Copyright © 2012 Positive Technologies.
[2] http://www.cloudsecurityalliance.org/topthreats
[3] Cloud Security Alliance, "Top Threats to Cloud Computing V1.0" © 2010 Cloud Security Alliance.
[4] Amazon Compute Cloud (http://aws.amazon.com/).
[5] Sun Cloud Computing (http://www.sun.com).
[6] Oracle Cloud Computing (http://www.oracle.com/us/technologies/cloud/).
[7] IBM cloud (http://www.ibm.com/ibm/cloud).
[8] Windows Azure (http://www.microsoft.com/windowsazure/windowsazure/).
[9] Google App Engine (http://code.google.com/appengine).
[10] Kaur S, Kaur P. Challenges in Cloud Computing : Need Solutions Yet ISTE faculty section convention 2013 organized by Ravat Bahra College of Engineering & Nano Technology for Women, Hoshiarpur 26th-27th July, 2013.
[11] Anjum Asma et al., Cloud Computing Security Issues *International Journal of Application or Innovation in Engineering & Management (IJAIEM)* Volume 1, Issue 2, October 2012, ISSN 2319 – 4847
[12] http://www.irishtimes.com/business-services/cloud-computing-ireland/getting-clear- about- cloud-computing.
[13] http://www.datacenterknowledge.com/archives/2008
[14] "Defining and Measuring Cloud Elasticity". KIT Software QualityDepartment.http://digbib.ubka.uni-karlsruhe.de/volltexte/1000023476