SECURITY VULNERABILITIES IN CLOUD COMPUTING

Abstract

Cloud computing is a relatively new computing paradigm that implements pay per use model to give the clients on demand access to computing requirements. It has redefined computing resources as utility rather than a significant capital consideration and has gathered immense popularity. However, the data and services are prone to many security threats that can cause severe damage to the client. Therefore, the clients should be aware of those risks before moving to the cloud environment.

Sagar Aryal
Sagar.aryal3@metropolia.fi

Sushil Bastola
Sushil.bastola@metropolia.fi

Contents

1. Introduction

Cloud computing is a computing model that enables convenient and ubiquitous pay per use access to shared and configurable computing resources over the network [1]. It is the result of convergence and evolution of Grid computing, Utility Computing and SaaS. Cloud computing models provide IT resources like storage and deployment of business applications with reduced efforts and minimal communication the service provider [2]. The NIST definition of cloud computing (2011) requires cloud computing models to have the following characteristics.

1. The consumer can access the required computing resources automatically without the requirement of any human interaction with the service provider.
2. The resources provided can be accessed from devices of all form factors independent of the software platform and operating systems used.
3. The provider's resources can be shared among multiple consumers using multi-tenant model, with dynamic assignment and reassignment of computing resources.
4. The provider's resources can be elastically provisioned and released.
5. The cloud system can monitor, control and report the use of resources in order to provide transparency to both the consumer and the provider. [1]

The above guidelines ensure the accessibility and availability of the data and elasticity of the cloud computing system.

As a result of their hassle free and convenient deployment, medium to big size operations are attracted to the use of cloud computing. The pay-per use and on demand model of cloud computing has made computing resources a utility rather than capital consideration. As it enables the corporations to use the resources without having to buy, setup and maintain computers, it has been gathering immense popularity over the years. This popularity is further aided by big corporations like Netflix and Dropbox moving to Amazon Cloud Services. [3]

2. Security Threats in Cloud Computing

Security of organizational and personal data is of prime importance to corporations and individuals alike as the loss or theft of confidential data may result in enormous loss in terms of economy or reputation. Virtualization technologies used at the core of cloud computing, it's over the network deployment and the need to trust the service provider for the integrity and availability of data exposes a wider attack domain for the attackers to exploit [3;4]. The paradigm of cloud computing has summoned several threats to the integrity and confidentiality of data as providers may have complete control over the underlying software and hardware infrastructure used to deploy the services [5] .The major security threats of cloud computing as identified by The Cloud Security Alliance(CSA) (2010) are described below.

2.1. Abuse and Nefarious use of Cloud

Abuse and nefarious use of cloud is the top threat identified by the CSA. As the cloud providers do not have strict registration and monitoring policies, it is easier for cyber criminals to improve their reach and effectiveness and avoid detection.[6;7;8] The potential threats arising from abuse and nefarious use of cloud are described below:

2.1.1. VM Escape and VM Hopping

Cloud computing is based on virtualization, which involves creating 'virtual machines' that share the physical resource of the host system. When the cloud provider does not deploy strict means to ensure the isolation of virtual machines, the virtual machine can allow the attackers malicious code to escape its VM and attack other VMs or the hypervisor itself. This is known as VM escape. VM escape gives the attacker the access to the host operating system and all the virtual machines running in it, hence compromising both the host and the guests. [7; 9]

VM hopping is similar to VM escape however in this case, the attacker can 'hop' from one virtual machine to the other virtual machine running on the same physical hardware but not to the underlying hypervisor. This kind of attack compromises the guests who are using different VMs on the same physical hardware.

2.1.2. Hyper jacking

Hyper jacking is an attack in which an attacker installs a rouge hypervisor to take complete control of the VM server. This gives the attacker control of everything running on the machine and presents the attacker with the opportunity to compromise the integrity of the system. Regular security measures are ineffective against this type of attacks as the operating system is not aware that the system is not aware that the machine is being compromised. This method of attack does not only compromise data but also maintains the persistence so that the attacker can view the data repetitively. [9]

2.1.3. Abuse of Privileges

The shared nature of cloud computing also opens possibilities for privilege abuse to get costumer information or other sensitive data. The system administrators have highest level of privileges in the cloud computing environment. These privileges can be misused to get and exploit the sensitive and confidential data of the customers with the possibility of selling the information to parties interested. System administrators may also be forced by the government or spy agencies to reveal the information of the customers. [7]

2.1.4. Identity Theft

Attackers have used different attacks to steal the identity of internet users. As most cloud providers do not have regulatory policies to set up the account, malicious users can easily set up an account and use it without any restrictions from the vendors. They can exploit this to gain critical customer data.

Furthermore, the attackers can also set up fake clouds and offer discounts to lure the users to use their services like email-applications. After an individual provides confidential data to the rouge cloud providers, they can use that information to further violate the digital privacy of that individual. These privacy violations can cause financial, social or moral loss to the individual concerned. [7]

2.1.4. Service Engine Attacks

The service engine is the platform that sits atop physical hardware and defines the architecture of the cloud. Service engine is usually reserved for the service providers but in case of IaaS (Infrastructure as a Service) model, the customer may have the access to the service engine. An attacker may subscribe to IaaS and use the virtual machine to compromise the service engine and potentially gain access to customer resources. This allows the attacker to escape the isolation boundaries and exploit their freedom to compromise data across multiple VMs potentially from multiple providers. [7]

2.1.5. VM theft

VM theft is the ability to steal the virtual machine file from the host and mount it to run it elsewhere. VM theft is equivalent to cloning the customer's physical server without having to break into data center and remove computing equipment.

2.1.6. Other vulnerabilities

In addition to the attack forms mentioned above, the power of cloud and all the resources it offers can also be used to perform attacks on other systems and break encryptions. Some of the vulnerabilities are listed below.

1. The attackers may use the resources offered by cloud computing to perform DDOS (Distributed Denial of Service) attacks on sensitive websites and data servers and hence deny users from getting the information they require.
2. The malicious users can use cloud environment to host malicious data.
3. The computing resources offered by the cloud may be misused to brute force into passwords and encryption keys.
4. The cloud resources can also be used as captcha solving farms to solve the captchas and hence break in or brute force into so called 'anti-robot' websites and services.
5. Cloud computing environments can also be used to host botnets. Botnets are internet connected programs that communicate with other botnets to perform an operation. Botnets can be used by the attackers to launch DDOS attacks.

2.2. Insecure Interfaces and APIs

Cloud computing service providers use a set of APIs and software interfaces to provide services to the customers and manage their interaction with the cloud services. The overall security and the availability of cloud services depends on this APIs and interfaces. Unknown services or API dependencies in the cloud environment can lead to the compromise in critical interfaces like login and access control. Accidental or malicious attempts to bypass these policies may reveal access control information or the encryption algorithm to the attacker, hence compromising the overall security and integrity of the cloud environment. Hence, the service provider's reliance on weak set of interfaces and insecure third party APIs can cause the compromise of confidentiality, integrity and accountability of the whole cloud computing environment. [8]

2.3. Malicious Insiders

Almost every organization has malicious individuals working for them. The impact malicious insiders can have in an organization is considerable, provided their access level and the ability to infiltrate. They can cause harms to the economy and repute of the organization. In cloud environment the threat of malicious insiders is further amplified by the lack of communication and transparency between the service provider and the customer. The attack domain is also widened in cloud environment as it mostly converges all the IT services into single management domain. [8; 10]

In cloud environment the customer's organization is susceptible to malicious individuals both inside own organization and inside the provider's organization. The susceptibility is further aided by the fact that the provider does not have to reveal the backgrounds of the employees and the access they have to provider's resources. This practice makes it easier for the adversaries of an organization, ranging from hobbyists to organized or nation-funded criminals to infiltrate the service provider to gain access and harvest the confidential data of the customer, with almost no risk of detection.

2.4. Shared Technology Issues

Cloud computing environments use virtualization technologies to share physical resources among users. Even if the virtual machines are isolated by hypervisors, they run on the same physical hardware. Most of the hardware used in cloud computing data centers use hardware that were not designed for virtualization (e.g. Graphics card). These hardware act as a weak link between the hypervisor and the cloud architecture and allow attackers to target those hardware to perform cross VM side-channel attacks on other user's virtual machines. Attackers may monitor the data like time consumed per computation and even use it to obtain encryption keys. [10]

Kortchinsky (2009) exploited bugs in the VMware emulated video device to host memory leak into the guest and even perform arbitrary memory writes from the guest VM. With admin rights in the VM, he was able to write his own driver on top VMware video driver to map the framebuffer and FIFO to gain direct and unrestricted access to perform memory leaks. [11] This exploitation by Kortchinsky exposes the vulnerabilities present in virtualization, the underlying technology in the implementation of cloud computing.

2.5. Data Loss and Leakage

Data loss refers to the condition in which the information stored in a digital storage media is destroyed because of various reasons including malicious deletion, errors in transmission and drive failures. Similarly, data leakage means the unauthorized transfer of data from the storage media to the outside world. Both data loss and leakage can be disastrous to organizations. The leakage of trade secrets or other confidential data may damage the repute and profit of the organization. Likewise, the loss of trade data or financial documents can have similar consequences. If appropriate backups are not made, the loss of data can be further devastating.

The data stored in cloud is accessible to the service provider at all the time and they possess the right to monitor the data for transparency purposes. This makes it easier for the service provider to leak the data. Likewise, problems in connection to the cloud provider's storage servers or the problems in the provider's storage media may corrupt the data and render it unusable. In addition to these cloud storage also exposes the data to a wider array of attacks. Furthermore, the cloud storage provider may also be forced by government or law enforcement agencies to reveal some of the customer's data without the consent from the customer. Likewise, the loss of encoding key can also destroy the data stored in cloud storage. Thus, the risk of loss or leakage of data is significantly greater in cloud environment due to the number of factors like insufficient authentication, auditing and authorization controls; trivial encryption; operational failures and persistence challenges; data center reliability and jurisdiction and political issues [8].

2.6. Account or Service Hijacking

Service or account hijacking is the process by which the attacker hijacks the account information or the service traffic of the user to eavesdrop on the activities and transactions performed by the user. It is one of the most common techniques used by the attackers to gain control of the target system. Means like social engineering or phishing can be deployed to steal the usage credentials, which can in turn be used to compromise the reputation of the organization or use it to influence their clients and probably launch attacks on their organizations. These attacks can have a domain larger than one online platform as most of the passwords and other security credentials are typically reused. The attackers can manipulate organizational data thus obtained or redirect the customers to illegitimate websites to further damage the reputation of the organization.

In April 2010, the attackers capitalized on a Cross-Site Scripting (XSS) bug in Amazon to hijack the session ids of its users and hence gain access to their accounts. This also compromised the login credentials of Amazon customers. Even if the bug was shortly removed, many Amazon users suffered from the attack. Hence, the ever-present threat of account and service hijacking is also existent in modern cloud computing environments, but this attack is more potent in cloud computing environments, as the clouds may hold extremely sensitive individual or corporate data.

2.7. Unknown Risk Profile

Cloud computing reduces the cost of ownership and maintenance of hardware and software to allow companies to invest in their core business ideas. This has made cloud computing popular as it has clear financial benefits to the organizations. The cloud service providers have capitalized on the financial and organizational benefits of cloud computing to advertise their services to the corporations. During advertising the providers publicize the features and functionalities about their platform but they do not reveal the security procedures they use in their systems. Along with security procedures, the version of the software they use and the last update of their systems is also usually kept secret. In addition to those, the vendors of the services do not mention who in their organization can have access to customer's data and if there have been any attempts to breach into their environment.

Most often, the clients overlook these fundamental questions as they are lured by the prospect of financial benefits and the vendors do not put any effort to explain their infrastructure and the means used to secure that. Likewise, the clients also do not have information about other clients sharing the environment with them. All of the issues mentioned above and the minimal efforts made by both the vendor and the clients to know or explain about the details of the environment and security measures in it leaves the clients in an unknown state of risk, which may include some serious threats to their organization.

3. Conclusion and Discussion

Cloud computing has amassed heaps of popularity in recent times, in both development and usage fronts. Cloud vendors like Amazon and Microsoft are constantly working to improve their features and offer more and more applications to their customers. In addition to offering more applications, they have also succeeded to mitigate the boundaries of platform and form factor. However, the key issue of protecting client data has often been overlooked.

The data online has never been secure because of large number of hobbyists, organized criminals and most recently hacktivists that are trying to compromise data for various reasons ranging from personal satisfaction to activism. The realm of cloud computing adds more security threats to already insecure data as it provides attackers with an increased surface area for launching their attacks. The attackers may capitalize on cloud explicit techniques like hyper jacking and service channel attacks or rely on the classical techniques like phishing and service hijacking to compromise corporate data. These kinds of attacks can lead an organization to a state of total downfall.

Therefore, the clients of cloud computing should be more careful when uploading sensitive data to the cloud. They should be well informed about the security threats of the cloud computing environment and the security measures implemented by their providers. The providers, in addition to working for better security measures and improved isolation in the virtual machines, should also inform their clients about their platform, their security techniques and the previous attacks to their platform if any. The vendors should also focus more on increasing security of their systems rather than advertising their other features. They should also perform strong background check of their employees and maintain strong access control systems to keep the malicious insiders at check. In addition to that, the vendors and the clients both should back up their data to prevent potential losses.

In a nutshell, cloud computing is a growing market and has the potential to become a very well used service in the internet. However, it has its fair share of vulnerabilities and threats which are mostly overlooked by both the clients and the vendors. Therefore, both should take measures to maintain the confidentiality, integrity and availability of the data in the cloud.

4. References

1. Mell P, Grance T. The NIST definition of cloud computing. Communications of the ACM. 2010 Dec; 53(6):50
2. Zissis D, Lekkas D. Addressing cloud computing security issues. Future Generation computer systems. 2012 Mar; 28(3):583-592.
3. Nanavati M, Colp P, Aiello B, Warfield A. Cloud security: A gathering storm. Communications of the ACM. 2014 May; 57(5):70-79.
4. Singh A, Shrivastava M. Overview of attacks on cloud computing. International Journal of Engineering and Innovative Technology (IJEIT). 2012 Apr;1(4):321-323
5. Kumar P, Sehgal VK, Chauhan DS, Gupta PK, Diwakar M. Effective ways of Secure, Private and Trusted Cloud Computing. International Journal of Computer Science Issues. 2011 May; 8(3):412-421
6. Srinivasamurthy S, Liu DQ. Survey on cloud computing security. Proceedings of Conference on Cloud Computing, CloudCom 2010
7. Hamza YA, Omar MD. Cloud computing security: Abuse and nefarious use of cloud computing. International Journal of Computational Engineering Research 2013 Jun; 3(6): 22-27.
8. Cloud Security Alliance. Top Threats to Cloud Computing. March 2010. cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf. Last accessed 21.04.2016 11:02
9. Carbone M, Lee W, Zamboni D. Taming virtualization. Security & Privacy, IEEE. 2008 Jan; 6(1): 65-67.
10. Bamiah MA, Brohi SN. Seven deadly threats and vulnerabilities in cloud computing. Int. J. Adv. Eng. Sci. & Techs. 2011(9):87-90.
11. Kortchinsky K. Cloudburst: A VMware guest to host escape story. Black Hat USA. 2009 Jun.