SECURITY AND PRIVACY ISSUES IN CLOUD COMPUTING

Amina AIT OUAHMAN

Royal Moroccan Armed Forces

Today, cloud computing is defined and talked about across the ICT industry under different contexts and with different definitions attached to it. It is a new paradigm in the evolution of Information Technology, as it is one of the biggest revolutions in this field to have taken place in recent times. According to the National Institute for Standards and Technology (NIST), "cloud computing 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" [1]. The importance of Cloud Computing is increasing and it is receiving a growing attention in the scientific and industrial communities. A study by Gartner [2] considered Cloud Computing as the first among the top 10 most important technologies and with a better prospect in successive years by companies and organizations. Clouds bring out tremendous benefits for both individuals and enterprises. Clouds support economic savings, outsourcing mechanisms, resource sharing, any-where any-time accessibility, on-demand scalability, and service flexibility. Clouds minimize the need for user involvement by masking technical details such as software upgrades, licenses, and maintenance from its customers. Clouds could also offer better security advantages over individual server deployments. Since a cloud aggregates resources, cloud providers charter expert security personnel while typical companies could be limited with a network administrator who might not be well versed in cyber security issues. The new concepts introduced by the clouds, such as computation outsourcing, resource sharing, and external data warehousing, increase the security and privacy concerns and create new security challenges. Moreover, the large scale of the clouds, the proliferation of mobile access devices (e.g., Smartphone and tablets), and the direct access to cloud infrastructure amplify cloud vulnerabilities and threats. As clouds become more and more popular, security concerns grow bigger and bigger as they become more attractive attack targets due to the concentration of digital assets.

Key words: *cloud computing, security, ITC, cloud deployment models, cloud software, cloud platform, cloud infrastructure.*

1. OVERVIEW OF CLOUD COMPUTING

The NIST cloud computing definition [1] is widely accepted as a valuable contribution toward providing a clear understanding of cloud computing technologies and cloud services. It provides a unifying view of five essential characteristics that all cloud services exhibit: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. It also defines three service models available to cloud consumers: cloud software as a service (SaaS), cloud platform as a service (PaaS), and cloud infrastructure as a service (IaaS). This definition also summarizes four deployment models describing how the computing infrastructure that

delivers these services can be shared: private cloud, community cloud, public cloud, and hybrid cloud.

Figure 1 shows cloud deployment models together with their internal infrastructure (IaaS, PaaS and SaaS). Cloud deployment models have similar internal infrastructure, but vary in their policies and user-access levels.

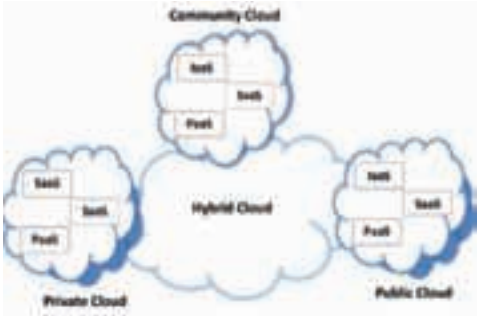

Figure 1: Cloud deployment models and infrastructure

1.1. Essential characteristics

On-demand service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad Network Access: Cloud Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms such as mobile phones, laptops and PDAs.

Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

Rapid Elasticity: Ability to quickly scale in/out service

Measured service: Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

There is also a 6th characteristic of cloud computing advocated by the Cloud Security Alliance which is Multi Tenacity. It refers to the need for policy-driven enforcement, segmentation, isolation, governance, service levels, and chargeback/billing models for different consumer constituencies.

1.2. Cloud Service Models

Software as a Service (SaaS): The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure [3]. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g. web-based email), or a program interface. In other words, in this model, a complete application is offered to the customer as a service on demand.

Platform as a Service (PaaS): In this model, a layer of software or development environment is encapsulated and offered as a service, upon which other higher levels of service are built. The customer has the freedom to build his own applications, which run on the provider's infrastructure. Although the customer does not manage or control the underlying cloud infrastructure, network, servers, operating systems, or storage, but he has the control over the deployed applications.

Infrastructure as a Service (IaaS): also referred as Resource Clouds generally provide resources which are managed and can easily be scaled up, as services to a variety of users. They essentially deliver basic storage and compute capabilities as standardized services over the network. Servers, storage systems, switches, routers, and other systems are pooled and made available to handle workloads that range from application components to high performance computing applications.

1.3. Cloud Deployment Models

Regardless of the delivery model utilized (SaaS, PaaS, IaaS) there are four primary ways in which cloud services are deployed:

Public Cloud: The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Private Cloud: The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them.

Community cloud: The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them.

Hybrid cloud: The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

2. CLOUD SECURITY ISSUES AND CHALLENGES

Security has been one of the most challenging issues for the IT executives particularly in cloud implementation. In fact, numerous security challenges face the cloud as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. Therefore, security issues for many of these systems and technologies are applicable to cloud computing.

2.1. Cloud Security: Categories and Issues

The related security issues that are challenging the cloud can be categorized into five major categories [4] summarized in **Table 1.**

The first Category, "Security standards" (C1), is part of service level agreements (SLA) [5] and legal aspects which define the relationship among parties (provider – recipient) and is extremely important for both parties [6]. It includes identifying/ defining the customer's needs, simplifying complex issues, encouraging dialog in the event of disputes, providing a framework for understanding, reducing/removing areas of conflict, eliminating unrealistic expectations. The user may suffer, in case of data loss, if the above factors are not taken into consideration as he may not be able to put claims on service providers.

Network category related issues are the biggest security challenges in clouds since cloud computing highly depends on network and therefore is more prone to network related attacks compared to the traditional computing paradigms. The clouds can actually be the focus of hackers due to the concentration of valuable "assets" within the clouds. Some of the common issues include unproper installation of network firewalls, Network security configurations, and Internet protocol vulnerabilities. This makes it easier for hackers to access the cloud on behalf of legitimate users [7].

Moreover, migrating to cloud increases the Internet dependency as

a main communication medium for cloud access. Therefore, if, due to some attacks, the Internet is disabled and the cloud services become unavailable, this may cause production to become severely crippled [8].

Table no.1. Security Categories in the cloud

No.	Category	Description
C1	Security Standards	Deals with regulatory authorities and governing bodies that define cloud security policies to ensure secure working environment over the clouds.
C2	Network	Refers to the medium through which the users connect to cloud infrastructure to perform the desired computations. It includes browsers, network connections and information exchange through registration.
C3	Access Control	Covers authentication and access control. It captures issues that affect privacy of user information and data storage.
C4	Cloud Infrastructure	Includes security issues within SaaS, PaaS and IaaS and is particularly related with virtualization environment.
C5	Data	Covers data integrity and confidentiality issues.

Regarding the Access Control category, many security issues and threats are to be considered. Account and service hijacking involves phishing, fraud and software vulnerabilities where attackers steal credentials and gain unauthorized access to servers [9]. This unauthorized access is a threat to integrity, confidentiality and availability of data and services [9]. Unauthorized access can be launched from within or outside the organization. Malicious insiders such as dishonest administrators can severely impact organizations' security.

Furthermore, a single customer may access data and compose services from multiple cloud providers using a mobile application or a browser. This kind of access brings in an inherent level of risk and this risk has been called privileged user access.

Unauthorized access also becomes possible through browser vulnerabilities. Therefore, Internet browser is one of the first stages where security measures should be considered because vulnerabilities in the browser open the door for many follow-on attacks.

As for the cloud infrastructure, the extensive use of virtualization brings unique security concerns for customers or tenants of a cloud service [10]. Virtualization alters the relationship between the OS and underlying hardware - be it computing, storage or even networking. This introduces an additional layer - virtualization - that itself must be properly configured, managed and secured [11]. Specific concerns include the potential to compromise the virtualization software, or "hypervisor". While these concerns are largely theoretical, they do exist. For example, a breach in the administrator workstation with the management software of the virtualization software can cause the whole datacenter to go down or be reconfigured to an attacker's liking.

Regarding the last category, data redundancy [12], data loss and leakage, data location [10], data recovery, data privacy, data protection [13] and data availability [11] have been considered to be the major and important issues in different

case studies which require data to be properly encrypted, transmitted, protected, controlled and available in the time of need.

2.2. Common known attacks on the Cloud

In a regular network, hackers used multiple computers or a botnet to produce a great amount of computing power in order to conduct cyber-attacks on computer systems. This process is complicated and can take months to complete. Nowadays, a powerful computing infrastructure, including both software and hardware components, could be easily created using a simple registration process in a cloud computing service provider. By taking advantage of the prevailing computing power of cloud networks, hackers can fire attacks in a very short time. For example, brute force attacks and DoS attacks can be launched by abusing the power of cloud computing.

A cloud system actually faces a big number of threats. However in this section, we will only cover five of the most common potential attack on the cloud.

2.2.1. Denial of Service (DoS) attacks

Most of the serious attacks in cloud computing come from denial of service (DoS), particularly HTTP, XML and Representational State Transfer (REST)-based DoS attack. The cloud users initiate requests in XML, then send requests over HTTP protocol and usually build their system-interface through REST protocols such as those used in Microsoft Azure and Amazon EC2. Due to vulnerabilities in the system interface, DoS attacks are easier to implement and very difficult for security experts to countermeasure [14]. XML-based distributed denial of service (DDoS) and HTTP-based DDoS attacks are more destructive than traditional DDoS because these protocols are widely used in cloud computing with no strong deterrence mechanisms available to avoid them. HTTP and XML are critical and important elements of cloud computing, so security over these protocols becomes crucial to providing healthy development of a cloud platform.

2.2.2. Cloud Malware Injection Attack

This attack attempt aims at injecting a malicious service implementation or virtual machine into the Cloud system. Such kind of Cloud malware could serve any particular purpose the adversary is interested in, ranging from eavesdropping via subtle data modifications to full functionality changes or blockings. This attack requires the adversary to create its own malicious service implementation module (SaaS or PaaS) or virtual machine instance (IaaS), and add it to the Cloud system. Then, the adversary has to trick the Cloud system so that it treats the new service implementation instance as one of the valid instances for the particular service attacked by the adversary. If this succeeds, the Cloud system automatically redirects valid user requests to the malicious service implementation, and the adversary's code is executed. An attacker can get access to user data through this attack. The incidents of this attack include credential information leakage, user private-data leakage and unauthorized access to cloud resources. The challenge does not only lie in the failure to detect the malware injection attack but also in the inability to determine the particular node on which the attacker has uploaded the malicious instance [15].

2.2.3. Side Channel Attacks

An attacker could attempt to compromise the cloud by placing a malicious virtual machine in close proximity to a target cloud server and then launching a side channel attack.

One incident of side channel attacks is the timing side channel attack [16] which is based on measuring how much time various computations take to perform. Successful modulation of this measured time may lead to leakage of sensitive information about the owner of the computation or even the cloud provider. Timing channels are especially hard to control and pervasive on clouds due to massive parallelism. Another incident of side channel attacks is the energy-consumption side channel attack [17]. Instead of directly attacking the software stack (virtualization layer), attackers can indirectly collect sensitive information about the cloud using energy consumption logs.

2.2.4. Phishing attack

Phishing is an attempt to access personal information from unsuspecting user through social engineering techniques. It is commonly achieved by sending links of WebPages in emails or through instant messages. These links appear to be correct, leading to a legitimate site such as bank account login or credit card information verification but they practically take users to fake locations. Through this deception, the attacker can obtain sensitive information such as passwords and credit card information. Phishing attacks can be classified into two categories: (1) an abusive behavior in which an attacker hosts a phishing attack site on cloud by using one of the cloud services and (2) hijack accounts and services in the cloud through traditional social engineering techniques [16].

Cloud security alliances (CSA) mentioned that cloud service providers do not maintain sufficient control over systems in order to avoid being hacked or spammed. To prevent such attacks, CSA proposes a few precaution measurements such as strict registration process, secure identity check procedure and enhanced monitoring skills [18].

2.2.5. VM Rollback Attack

The virtualization environment in cloud computing is the most vulnerable area to attack. The hypervisor can suspend a VM at any time during execution, take a snapshot of current CPU states, disk and memory and resume a snapshot later without guest VM awareness. This feature has been widely used for fault tolerance and VM maintenance; however, it also provides an open window to an attacker to launch VM rollback attacks. In a rollback attack, a user can take advantage of previous snapshots and run it without the user's awareness and then clean the history and again run the same or different snapshot. By cleaning the history, the attacker will not be caught for his suspicious activities. For example, an attacker can launch a brute force attack to guess a login password for VM, even if the guest

OS has a restriction on the number of attempts such as blocking the user after three failed attempts or erasing all data after 10 times, the attacker can still rollback the VM to its initial state after each try. The attacker will clear the counter inside the VM and bypass the restriction and run the brute-force attack again [19]. Furthermore, rolling back virtual machines can re-expose them to security vulnerabilities that were patched or re-enable previously disabled accounts or passwords. In order to provide rollbacks, we need to make a "copy" (snapshot) of the virtual machine, which can result in the propagation of configuration errors and other vulnerabilities.

3. SECURITY CONTERMEASURES

A cloud computing infrastructure includes a cloud service provider, which provides computing resources

to cloud end users who consume those resources. In order to assure the best quality of service, the providers are responsible for ensuring the cloud environment is secure. This can be done by defining stringent security policies and by applying advanced security technologies.

3.1. Security Policy Enhancement

With a valid credit card, anyone can register to utilize resources offered by cloud service providers. This causes hackers to take advantage of the powerful computing power of clouds to conduct malicious activities, such as spamming and attacking other computing systems. By mitigating such abuse behavior caused by weak registration systems, credit card fraud monitoring and block of public black lists could be applied [20]. Also, implementation of security policies can reduce the risk of abuse use of cloud computational power [21]. Well established rules and regulations can help network administrators manage the clouds more effectively.

3.2. Access Management

The end users' data stored in the cloud is sensitive and private; and access control mechanisms could be applied to ensure only authorized users can have access to their data. Not only do the physical computing systems (where data is stored) have to be continuously monitored, the traffic access to the data should be restricted by security techniques. Firewalls and intrusion detection systems are common tools that are used to restrict access from untrusted resources and to monitor malicious activities. In addition, authentication standards, Security Assertion Markup Language (SAML) and eXtensible Access Control Markup Language (XACML), can be used to control access to cloud applications and data. SAML focuses on the means for transferring authentication and authorization decisions between cooperating entities, while XACML focuses on the mechanism for arriving at authorization decisions [22].

3.3. Data Protection

Data breaches caused by insiders could be either accidental or intentional. Since it is difficult to identify the insiders' behavior, it is better to apply proper security tools to deal with insider threats. The tools include: data loss prevention systems, anomalous behavior pattern detection tools, format preserving and encryption tools, user behavior profiling, decoy technology, and authentication and authorization technologies [23]. These tools provide functions such as real-time detection on monitoring traffic, audit trails recording for future forensics, and trapping malicious activity into decoy documents.

3.4. Security Techniques Implementation

In this section we will discuss some of the possible mitigation solutions available in order to prevent and protect against some of the most common threats discussed earlier.

One of the solution tools is Log inspection. In fact, it collects and analyzes operating system and application logs for security events. Log inspection rules optimize the identification of important security events buried in multiple log entries. These events can be sent to a stand-alone security system, but contribute to maximum visibility when forwarded to a security information and event management (SIEM) system or centralized logging server for correlation, reporting and

archiving. Like integrity monitoring, log inspection capabilities must be applied at the virtual machine level.

Log inspection software on cloud resources enables:

1. Suspicious behavior detection
2. Collection of security-related administrative actions
3. Optimized collection of security events across your datacenter

As discussed earlier in this paper, malware injection attack has become a major security concern in cloud computing systems. It can be prevented by using File Allocation Table (FAT) system architecture [24]. From the FAT table, the instance (code or application) that a customer is going to run can be recognized in advance. By comparing the instance with previous ones that had already been executed from the customer's machine, the validity and integrity of the new instance can therefore be determined. Another way to prevent malware injection attacks is to store a hash value on the original service instance's image file [25]. By performing an integrity check between the original and new service instance's images, malicious instances can be identified. For XML signature wrapping attacks on web services, a variety of techniques have been proposed to fix the vulnerability found in XML-based technologies. For example, XML Schema Hardening technique is used to strengthen XML Schema declarations [26]. A subset of XPath, called FastXPath, is proposed to resist the malicious elements that attackers inject into the SOAP message structure [27].

Furthermore, to prevent phishing attacks, CSA (Cloud security alliances) proposes a few precaution measurements such as strict registration process, secure identity check procedure and enhanced monitoring skills [18]. Privacy laws in cloud computing do not allow cloud service providers to look at what customers are doing, so if a malicious individual or organization is performing something nefarious (phishing attack or uploading malicious code) by using cloud services, it cannot be detected until or unless notified by some security software.

4. CONCLUSION

Cloud computing is in continual development in order to make different levels of on-demand services available to customers. While people enjoy benefits cloud computing brings, security in clouds is a key challenge. Much vulnerability in clouds still exists and hackers continue to exploit these security holes. In order to provide better quality of service to cloud users, security flaws must be identified. Lots of research is going on to address the issues like network security, data protection, virtualization and isolation of resources. Addressing these issues requires getting confidence from user for cloud applications and services. Obtaining user confidence can be achieved by creating trust for cloud resource and applications, which is a crucial issue in cloud computing. Trust management is attracting much attention. Providing secure access to cloud by trusted cloud computing and by using service level agreements, made between the cloud provider and user; requires lots of trust and reputation management. In this paper we gave a telling overview of security threats of cloud computing as well as some effective countermeasures, beside introducing main elements of security in cloud computing.

NOTES AND REFERENCES

[1] The NIST cloud computing definition -- Recommendations of the National Institute of Standards and Technology: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[2] Gartner Hype-Cycle 2012 – Cloud Computing and Big Data (2012). Available at: http://www.gartner.com/technology/research/hype-cycles/.

[3] A cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer.

[4] Cloud Computing – A Classification, Business Models, and Research Directions: http://www.im.uni-karlsruhe.de/Upload/Publications/5416512c-4711-4793-bd42-56e9241cc0a0.pdf.

[5] Cloud Computing Service Level Agreement By the European Union COMMUNICATIONS NETWORKS, CONTENT AND TECHNOLOGY UNIT E2 - SOFTWARE AND SERVICES, CLOUD—June 2013.

[6] A Framework for Auction-based HPC Computing Using Amazon Spot Instances, in Proc. of the International Symposium on Advances of Distributed Computing and Networking (ADCN), 2011.

[7] A quantitative analysis of current security concerns and solutions for cloud computing. http://www.producao.usp.br/bitstream/handle/BDPI/34999/2192-113X-1-11.pdf?sequence=1.

[8] Scheduler vulnerabilities and coordinated attacks in cloud computing: http://arxiv.org/pdf/1103.0759.pdf.

[9] Cloud Computing Security Considerations: http://www.digital.vic.gov.au/wp-content/uploads/2013/06/SEC-GUIDE-06-Cloud-Computing-Security-Considerations-Guideline.pdf.

[10] "Cloud Computing: Virtual Cloud Security Concerns". http://technet.microsoft.com/en-us/magazine/hh641415.aspx.

[11] "Dark Cloud: Study finds security risks in virtualization" http://gcn.com/articles/2010/03/18/dark-cloud-security.aspx.

[12] A survey and analysis of cloud model-based security for computing secure cloud bursting and aggregation in renal environment.

[13] Data Security in the cloud http://www.vormetric.com/sites/default/files/wp-data-security-in-the-cloud.pdf.

[14] A Defense Mechanism to Protect Cloud Computing against Distributed Denial of Service Attacks http://www.ijarcsse.com/docs/papers/Volume_3/5_May2013/V3I5-0202.pdf.

[15] Overview of Attacks on Cloud Computing: http://ijeit.com/vol%201/Issue%204/IJEIT1412201204_57.pdf.

[16] Determinating Timing Channels in Compute Clouds: http://arxiv.org/pdf/1003.5303.pdf.

[17] Energy consumption side-channel attack at virtual machines in a cloud: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6119058&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6119058.

[18] Top Threats to Cloud computing https://cloudsecurityalliance.org/research/top-threats/.

[19] Defending against web application vulnerabilities http://www.infoq.com/articles/defending-against-web-application-vulnerabilities.

[20] “Cloud Computing Security Considerations Interface” http://etherealmind.com/wp-content/uploads/2011/04/Cloud_Computing_Security_Considerations-1.pdf.

[21] Cloud Vulnerability Assessment: https://www.wpi.edu/Pubs/E-project/Available/E-project-042412-130544/unrestricted/Vulnerability_Assessment_Within_The_Cloud_MA_AG.pdf.

[22] Guidelines on Security and Privacy in Public Cloud Computing http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf.

[23] Tackling the Insider Threat http://www.bankinfosecurity.com/blogs.php?postID=140.

[24]Security Attacks and Solutions in Clouds http://salsahpc.indiana.edu/CloudCom2010/Poster/cloudcom2010_submission_98.pdf.

[25]Security Issues in Cloud Computing and Countermeasures http://www.ijest.info/docs/IJEST11-03-04-235.pdf.

[26] On the Effectiveness of XML Schema Validation for Countering XML Signature Wrapping Attacks http://ijircce.com/upload/2013/may/13_A%20Security.pdf.

[27] Analysis of Signature Wrapping Attacks and Countermeasures http://datenschutz.web-schell.de/tl_files/web-datenschutz-schell/Website-Dateien/PDF/wrapping-attacks_and_countermeasures.pdf.