Research Paper on Cloud Security

Annu Devi

Abstract

This paper reviews the best practices to secure Cloud services and data, including conventional security techniques and working with vendors to ensure proper Service Level Agreements exist.
While Cloud services offer flexibility, scalability and economies of scale, there have been commensurate concerns about security. Cloud services such as Software as a service, Platform as a service or Infrastructure as a service will each have their own security concerns that need to be addressed. As more data moves from centrally located server storage to the Cloud, the potential for personal and private data to be compromised will increase. Confidentiality, availability and integrity of data are at risk if appropriate measures are not put in place prior to selecting a Cloud vendor or implementing your own cloud and migrating to Cloud services.

Introduction

In computer networking, **cloud computing** is computing that involves a large number of computers connected through a communication network such as the Internet, similar to utility computing. In science, cloud computing is a synonym for distributed computing over a network, and means the ability to run a program or application on many connected computers at the same time.

Network-based services, which appear to be provided by real server hardware and are in fact served up by virtual hardware simulated by software running on one or more real machines, are often called cloud computing. Such virtual servers do not physically exist and can therefore be moved around and scaled up or down on the fly without affecting the end user, somewhat like a cloud becoming larger or smaller without being a physical object.

Benefits of Cloud Computing [8]

Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a utility (like the electricity grid) over a network. At the foundation of cloud computing is the broader concept of converged infrastructure and shared services.

The cloud also focuses on maximizing the effectiveness of the shared resources. Cloud resources are usually not only shared by multiple users but are also dynamically reallocated per demand. This can work for allocating resources to users. For example, a cloud computer facility that serves European users during European business hours with a specific application (e.g., email) may reallocate the same resources to serve North American users during North America's business hours with a different application (e.g., a web server). This approach should maximize the use of computing power thus reducing environmental damage as well since less power, air conditioning, rackspace, etc. are required for a variety of functions.

Deployment models

Controlled cloud

Controlled cloud services are not publicly available; users are specifically authorized by services vendors. Access to the controlled cloud may be through the Internet; however, connections would be encrypted. The cloud vendor employs various techniques and technologies to prevent unauthorized access. The services vendor discloses to customers its processes for managing customer data. Any sub processors used in processing customer data are identified to customers. Data protection schemes such as administrative controls, encryption methods, and other appropriate technical and organizational measures (TOMs) to protect data are described and demonstrated to customers.

Private cloud

Private cloud is cloud infrastructure operated solely for a single organization, whether managed internally or by a third-party and hosted internally or externally. Undertaking a private cloud project requires a significant level and degree of engagement to virtualize the business environment, and requires the organization to reevaluate decisions about existing resources. When done right, it can improve business, but every step in the project raises security issues that must be addressed to prevent serious vulnerabilities. Self-run data centers are generally capital intensive. They have a significant physical footprint, requiring allocations of space, hardware, and environmental controls. These assets have to be refreshed periodically, resulting in additional capital expenditures. They have attracted criticism because users "still have to buy, build, and manage them" and thus do not benefit from less hands-on management, essentially "[lacking] the economic model that makes cloud computing such an intriguing concept".

Public cloud

A cloud is called a "public cloud" when the services are rendered over a network that is open for public use. Technically there may be little or no difference between public and private cloud architecture, however, security consideration may be substantially different for services (applications, storage, and other resources) that are made available by a service provider for a public audience and when communication is effected over a non-trusted network. Generally, public cloud service providers like Amazon AWS, Microsoft and Google own and operate the infrastructure and offer access only via Internet (direct connectivity is not offered).

Community cloud

Community cloud shares infrastructure between several organizations from a specific community with common concerns (security, compliance, jurisdiction, etc.), whether managed internally or by a third-party and hosted internally or externally. The costs are spread over fewer users than a public cloud (but more than a private cloud), so only some of the cost savings potential of cloud computing are realized.

Hybrid cloud

Hybrid cloud is a composition of two or more clouds (private, community or public) that remain distinct entities but are bound together, offering the benefits of multiple deployment models. Hybrid cloud can also mean the ability to connect collocation, managed and/or dedicated services with cloud resources.

By utilizing "hybrid cloud" architecture, companies and individuals are able to obtain degrees of fault tolerance combined with locally immediate usability without dependency on internet connectivity. Hybrid cloud architecture requires both on-premises resources and off-site (remote) server-based cloud infrastructure.

Threats to Security of Cloud server

However, cloud computing continues to gain steam with 56% of the major European technology decision-makers estimate that the cloud is a priority in 2013 and 2014, and the cloud budget may reach 30% of the overall IT budget.

According to the *TechInsights Report 2013: Cloud Succeeds* based on a survey, the cloud implementations generally meets or exceedes expectations across major service models, such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

Several deterrents to the widespread adoption of cloud computing remain. Among them, are: reliability, availability of services and data, security, complexity, costs, regulations and legal issues, performance, migration, reversion, the lack of standards, limited customization and issues of privacy. The *cloud* offers many strong points: infrastructure flexibility, faster deployment of applications and data, cost control, adaptation of cloud resources to real needs, improved productivity, etc. The early 2010s cloud market is dominated by software and services in SaaS mode and IaaS (infrastructure), especially the private cloud. PaaS and the public cloud are further back.

Cloud server security

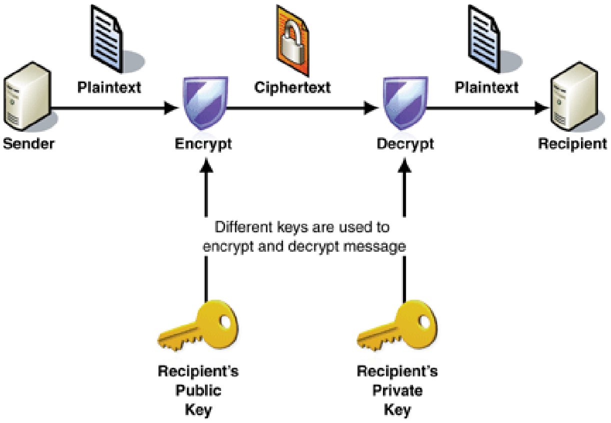
Security in the world of information technology has become a popular topic within the industry and within the media. It is not uncommon to read about successful hacker exploits against consumers, business or government. As witnessed by the July, 2012 Dropbox security breach (Strauss, 2012) or the 6 million passwords that were stolen from eHarmony and LinkedIn, risks associated with Cloud computing are not necessarily reduced.

Virtual switches and the hypervisor are two examples of points of attack that are not present in the traditional data center. The attack surface can be defined as our exposure.
Exposures are the vulnerabilities that are exploitable by the attacker (Northcutt, 2012).
Consequently, an increased attack surface may increase security risks of Cloud security [7] providers if the risks are not properly managed.

Risks can be decreased for small and medium sized business because there may be a lack of staff with specialization in information security whereas Cloud Service Providers (CSP) will have specialized staff that focus on information security. Because of economies of scale, it is cheaper to utilize a CSP than to design a high availability data center.

Previous security Mechanism

Much of the theoretical work in cryptography[4] concerns cryptographic *primitives*—algorithms with basic cryptographic properties—and their relationship to other cryptographic problems. More complicated cryptographic tools are then built from these basic primitives. These primitives provide fundamental properties, which are used to develop more complex tools called *cryptosystems* or *cryptographic protocols*, which guarantee one or more high-level security properties. Note however, that the distinction between cryptographic *primitives* and cryptosystems, is quite arbitrary; for example, the RSA algorithm is sometimes considered a cryptosystem, and sometimes a primitive. Typical examples of cryptographic primitives include pseudorandom functions, one-way functions, etc.



One or more cryptographic primitives are often used to develop a more complex algorithm, called a cryptographic system, or *cryptosystem*. Cryptosystems are designed to provide particular functionality (e.g. public key encryption) while guaranteeing certain security properties. Cryptosystems use the properties of the underlying cryptographic primitives to support the system's security properties. Of course, as the distinction between primitives and cryptosystems is somewhat arbitrary, a sophisticated cryptosystem can be derived from a combination of several more primitive cryptosystems.

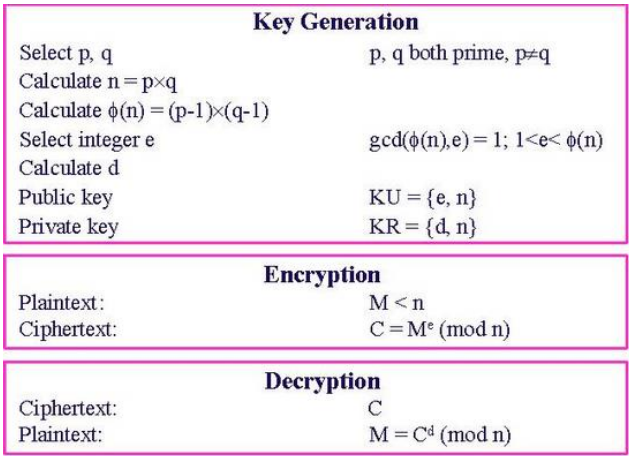
Key generation

When used with asymmetric ciphers for key transfer, pseudorandom key generators are nearly always used to generate the symmetric cipher session keys. However, lack of randomness in those generators or in their initialization vectors is disastrous and has led to cryptanalytic breaks in the past. Therefore, it is essential that an implementation uses a source of high entropy for its initialization.

Basic algorithm and terminology

RSA encryption and decryption are essentially mathematical operations. They are what are termed *exponentiation*, *modulo* a particular number. Because of this, RSA keys actually consist of numbers involved in this calculation, as follows:

- the public key consists of the modulus and a public exponent;
- the private key consists of that same modulus plus a private exponent.



Key Generation

Select p, q	p, q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1) \times (q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Encryption

Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod n$

Decryption

Ciphertext:	C
Plaintext:	$M = C^d \pmod n$

Challenges

- ➢ Intruders: those who capture the packet and alter the information
- ➢ Users with limited privileges should not be able to access unauthorized information
- ➢ Crypto analyst: those who decrypt cipher text into plain text without key

Objective of research

There are multiple enhancements in security mechanism.

1. The presence of intruder should be detected to prevent an unauthorized access of information by adding some delimiter at the end of encrypted text and same delimiter should be used during decryption.

2. Some time information to be sent are multiple and merged using delimiter into plain text then at the time of decryption plain text is split again in multiple pieces of information.

3. Allow authentic access to the information on the basis of privilege levels of user.

4. To protect information from cryptanalyst IP Filter would be attached in decryption odule

Future scope and Conclusion

Traditional security methods are still relevant in the Cloud but are implemented in a virtual means. In a virtualized Cloud environment customers are segregated into separate security zones called multi-tenancy. Virtual NICs, virtual switches and port groups add complexity but allow a multi-tenant environment.

Business and government will continue to move a Cloud environment in an effort to reduce costs, improve efficiencies and reduce administrative overhead. Delivering IT services via the Cloud portends to be a time saver, a money saver and allow for better efficiencies. This new paradigm of computing offers many benefits but it also increases security risks.

The delivery of computing resources in a Cloud environment is elastic, available on demand and convenient for the customer. While not mandatory, virtualization of the data center is important to achieve economies of scale that enable services to be provided at a lower cost than a traditional data center. While virtualization reduces some security risks, others are increased because the attack surface in a Cloud service increases.

Reference

[1]Amazon. (2011). Amazon Web Services: Overview of Security Processes. Retrieved from http://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf

[2]Arora, P., Biyani, R. and Dave, S. (2011). To the cloud:Cloud powering an enterprise. McGraw-Hill. Buck, K. and Hanf, D. (2009).

[3]Mitre cloud computing series, Cloud SLA considerations for the government consumer. Retrieved from http://www.mitre.org/work/tech_papers/2010/10_2902/cloud_sla_considerations_government.pdf

[4] Introduction to Cryptography
http://en.wikipedia.org/wiki/Cryptography

[5]Traditional Cloud server security

http://cloudsecuritythreats.blogspot.in/2011/11/traditional-security.html

[6] Fundamentals of Cryptography: Algorithm and Security Services by Professor Guevara Noubir

http://www.ccs.neu.edu/home/noubir/Courses/CSU610/S06/cryptography.pdf