Review on multilayer security on Cloud Server

Preeti[1], Mahesh Kumar[2]

[1]M.Tech. Student ,Computer Science & Engineering

Ganga Institute of Technology and Management Kablana, Jhajjar, Haryana, India

[2] *Associate Professor*, Computer Science & Engineering

Ganga Institute of Technology and Management Kablana, Jhajjar, Haryana, India

[1]ps25194@gmail.com; [2]maheshmalkani@gmail.com

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

***Keywords*— Cross cloud computing, Cloud Server, Client server, Key generation, Security**

I.INTRODUCTION

In computer networking, ***cloud computing*** *is computing that involves a large number of computers connected with a communication network such as Internet, similar to utility computing. In science, cloud computing is a synonym for distributed computing over a network, & means ability to run a program or application on many connected computers at 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 clouds computing. Such virtual servers do not physically exist & could therefore be moved around & scaled up or down on fly without affecting end user, somewhat like a cloud becoming larger or smaller without being a physical object.

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

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

II. LITERATURE REVIEW

Cloud Computing: Security Issues and Research Challenges by Rabi Prasad Padhy

Many industries, such as banking, healthcare and education are moving towards the cloud due to the efficiency of services provided by the pay-per-use pattern based on the resources such as processing power used, transactions carried out, bandwidth consumed, data transferred, or storage space occupied etc. Cloud computing is a completely internet dependent technology where client data is stored and maintain in the data centre of a cloud provider like Google, Amazon, Salesforce.com and Microsoft etc. Limited control over the data may incur various security issues and threats which include data leakage, insecure interface, sharing of resources, data availability and inside attacks. There are various research challenges also there for adopting cloud computing such as well managed service level agreement (SLA), privacy, interoperability and reliability. This research paper outlines what cloud computing is, the various cloud models and the main security risks and issues that are currently present within the cloud computing industry. This research paper also analyses the key research and challenges that presents in cloud computing and offers best practices to service providers as well as enterprises hoping to leverage cloud service to improve their bottom line in this severe economic climate.

Cloud Computing – Research Issues, Challenges, Architecture, Platforms and Applications: A Survey by Santosh Kumar and R. H. Goudar

Cloud computing is the development of parallel computing, distributed computing, grid computing and virtualization technologies which define the shape of a new era. Cloud computing is an emerging model of business computing. In this paper, we explore the concept of cloud architecture and compares cloud computing with grid computing. We also address the characteristics and applications of several popular cloud computing platforms. In this paper, we aim to pinpoint the challenges and issues of cloud computing. We identified several challenges from the cloud computing adoption perspective and we also highlighted the cloud interoperability issue that deserves substantial further research and development. However, security and privacy issues present a strong barrier for users to adapt into cloud computing systems. In this paper, we investigate several cloud computing system providers about their concerns on security and privacy issues.

A Survey on Security Issues and the Existing Solutions in Cloud Computing (2013) by Y. Ghebghoub, S. Oukid, and O. Boussaid

Cloud Computing has been developed to deliver information technologies services on demand to organizations such as well as individual users, this technology is still in its early stages of development because it suffers from different security threats that prevent users trust it In this paper, we identify different security problems existing in the cloud from several research papers and we show suggested solutions.

Security Threats in Cloud Computing Environments by Kangchan Lee

Cloud computing is a model for enabling service user's ubiquitous, convenient and on-demand network access to a shared pool of configurable computing resources. The security for Cloud Computing is emerging area for study and this paper provide security topic in terms of cloud computing based on analysis of Cloud Security treats and Technical Components of Cloud Computing.

III. DEPLOYMENT MODELS

A. Controlled cloud

Controlled cloud services are not publicly available; users are specifically authorized by services vendors. Access to controlled cloud might be through Internet; however, connections would be encrypted. The cloud vendor employs various techniques & 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, & other appropriate technical & organizational measures (TOMs) to protect data are described & demonstrated to customers.

B. Private cloud

Private cloud is cloud infrastructure operated solely for a only one organization, whether managed internally or by a third-party & hosted internally or externally. Undertaking a private cloud project requires a significant level & degree of engagement to virtualized business environment, & requires organization to reevaluate decisions about existing resources. When done right, it could improve business, but every step in 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 hardware, & environmental controls. These assets have to be refreshed periodically, resulting in additional capital expenditures. They had attracted criticism because users "still have to buy, build, & manage them" & thus do not benefit from less hands-on management, essentially "[lacking] economic model that makes cloud computing such as an intriguing concept".

C. Public cloud

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

D. Community cloud

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

IV.**THREATS AND OPPORTUNITIES OF CLOUD**

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

According to *TechInsights Report 2013: Cloud Succeeds* based on a survey, cloud implementations generally meets or exceeds expectations across major service models, such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) & Software as a Service (SaaS).Several deterrents to widespread adoption of cloud computing remain. Among them, are: reliability, availability of services & data, security, complexity, costs, regulations and legal issues, performance, migration, reversion, lack of standards, limited customization and issues of privacy. The *cloud* offers many strong points: infrastructure flexibility, faster deployment of applications & data, cost control, adaptation of cloud resources to real needs, improved productivity, etc. The early 2010s cloud market is dominated by software & services in SaaS mode & IaaS (infrastructure), especially private cloud. PaaS & public cloud are further back.

V.**SECURITY IN CLOUD**

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

Cloud computing are not necessarily reduced. Virtual switches & hypervisor are two examples of points of attack that are not present in traditional data center. The attack surface could be defined as our exposure.Exposures are vulnerabilities that are exploitable by attacker (Northcutt, 2012). Consequently, an increased attack surface might increase security risks of Cloud security providers if risks are not properly managed.Risks could be decreased for small & medium sized business because there might be a lack of staff within specialization in information security whereas Cloud Service Providers (CSP) would have specialized staff that focus on information security. Because of economies scale, it's cheaper to utilize a CSP than to design a high availability data center.

VI.**EXISTING SECURITY MECHANISM**

Much of theoretical work in cryptography concerns cryptographic *primitives*—algorithms within basic cryptographic properties—and their relationship to other cryptographic problems. More complicated cryptographic tools are then built from these basic primitives. These 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 distinction between cryptographic *primitives* & cryptosystems, is quite arbitrary; for example, RSA algorithm is sometimes considered a cryptosystem, & sometimes a primitive. Typical examples of cryptographic primitives include pseudorandom functions, one-way functions, etc.

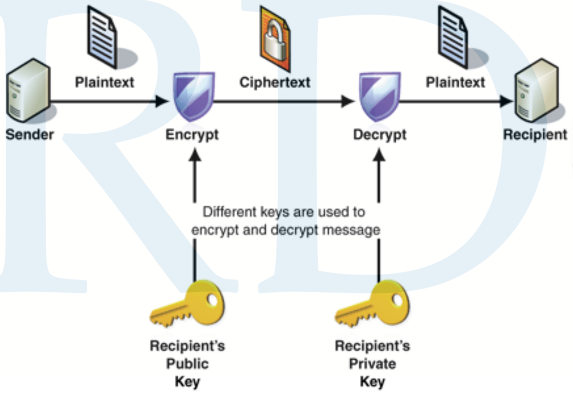


Fig. *1* Encryption mechanism

One or more cryptographic primitives are often used to develop a most complex algorithm, called a cryptographic system, or *cryptosystem*. Cryptosystems are designed to provide particular functionality (exp: -public key encryption) while guaranteeing certain security properties. Of course, as distinction between primitives & cryptosystems is somewhat arbitrary, a sophisticated cryptosystem could be derived from a combination of several more primitive cryptosystems.

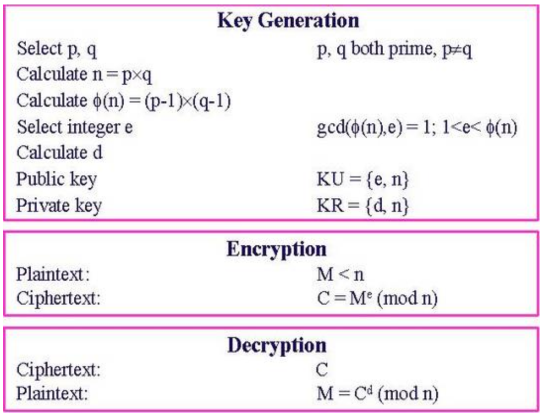
A. Key generation

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

B. Basic Algorithm & Terminology

RSA encryption & decryption are mathematical operations. These are exponentiation, modulo particular number. So RSA keys consist of numbers involved within it calculation, as follows:

1. Public key consists of modulus & public exponent;
2. Private key is consisting same modulus plus private exponent.



Key Generation	
Select p, q	p, q both prime, p≠q
Calculate n = p×q	
Calculate ϕ(n) = (p-1)×(q-1)	
Select integer e	gcd(ϕ(n),e) = 1; 1<e< ϕ(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:	$M = C^d \pmod n$

Fig. 2 Generation of key within encryption and decryption

VII.OBJECTIVE AND METHODOLOGY

Securing Hybrid Cloud server using firewall

A typical approach in an attack on Internet-connected system is:

1. Network enumeration: Discovering information about intended target.
2. Vulnerability analysis: Identifying potential ways of attack.

Exploitation: Attempting to compromise system by employing vulnerabilities found through vulnerability analysis.

VIII.CONCLUSIONS

A **firewall** is a network security system that controls incoming & outgoing network traffic based on an applied rule set. A firewall establishes a barrier b/w a trusted, secure internal network & another network that is assumed not to be secure & trusted. Firewalls exist both as software to run on general purpose hardware & as a hardware appliance. Many hardware-based firewalls also offer another functionality to internal network they protect, such as acting as a DHCP server for that network. The delivery of computing resources in a Cloud environment is elastic, available on demand & convenient for customer. While not mandatory, virtualization of data center is important to achieve economies of scale that enable services to be provided at a low cost than a traditional data center. While virtualization reduces some security risks, others are increased because attack surface in a Cloud service increases. Traditional security methods are still relevant in 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 & port groups add complexity but allow a multi-tenant environment.

REFERENCES

[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. & Dave, S. (2011). To cloud:Cloud powering an enterprise. McGraw-Hill. Buck, K. & Hanf, D. (2009).*

[3] *Mitre cloud computing series, Cloud SLA considerations for 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 & Security Services by Professor Guevara Noubir* *http://www.ccs.neu.edu/home/noubir/Courses/CSU610/S06/cryptography.pdf*