

UNISYS

Security in Cloud Computing



Hasmukh Goswami College of Engineering, Ahmedabad
Gujarat Technological University, Ahmedabad

Amar Gondaliya
Information Technology
Hasmukh Goswami College of Engineering, Ahmedabad
E-mail: amar.hgce@gmail.com Phone :+919725787644

ABSTRACT

Cloud computing service providers take advantage of virtualization technologies, combined with self-service capabilities, to offer cost-effective access to computing resources via the internet. But major issue in cloud computing is security. Several concerns which identify security requirements in cloud computing.

This paper identifies security concerns arising in cloud computing environments and outlines methods to maintain compliance integrity and preserve security protection as virtual resources move from on-premise to public cloud environments. Many organizations that are providing security software that provides security control for cloud computing, but this paper provides the checklist of key questions for enterprise and service provider for cloud computing deployment.

Overview

1. Introduction
 - 1.1 The cloud computing opportunity
 - 1.2 Essential characteristics
 - 1.3 What, When, How, to move on Cloud
2. Security Concerns
3. Security in cloud computing
 - 3.1 Security Stack in cloud computing
 - 3.2 Security Issues in SaaS
 - 3.3 Security Issues in PaaS
 - 3.4 Security Issues in IaaS
 - 3.5 Security Attacks in Cloud
4. Cloud security challenges
 - 4.1 Administrative access
 - 4.2 Dynamic Virtual machines: VM-state and sprawl
 - 4.3 Vulnerability Exploits and VM-to-VM Attacks
 - 4.4 Data Integrity: Co-Location, Compromise and Theft
5. Research Issues
6. Solution approaches
 - 6.1 Firewall
 - 6.2 Intrusion Detection and Prevention (IDS/IPS)
 - 6.3 Integrity Monitoring
 - 6.4 Log Inspection
7. Conclusion

1.INTRODUCTION

Cloud computing represents significant opportunity for service providers and enterprises. Relying on the cloud computing, enterprises can achieve cost savings, flexibility, and choice for computing resources. They are looking to expand their on-premise infrastructure, by adding capacity on demand. Cloud computing, most, simply, extends an enterprise's ability to meet the computing demands of its everyday operation. Offering flexibility and choice, mobility and scalability, all coupled with potential cost savings, there is significant benefit to leveraging cloud computing. However, the area is causing organizations to hesitate most when it comes to moving business workloads into public cloud is **security**.

This paper covers the variation of cloud computing that is also called **Infrastructure as a Service (IaaS)**. It looks at the security implications and challenges that IaaS represents and offers best practices to service providers and enterprises.

1.1 The cloud computing opportunity

Several points that attract enterprises and organization to move to the cloud computing that's why the following opportunities in the cloud computing is considered.

Industrial momentum: industry analysts and companies like Amazon, Citrix, Dell, Google, HP, IBM, Microsoft, Sun, VMware and many others appears greatly in support of cloud computing. In September 2008, the VMware vCloud was the first example of a technology vendor bringing service providers, applications and technologies together to increase the availability and opportunity for enterprises to leverage cloud computing.

Flexibility: Enterprises can choose to outsource hardware while maintaining control of their IT infrastructure; they can fully-outsource all aspects of their infrastructure; or, often driven by departmental initiatives, enterprises are deploying both fully and partially-outsourced segments of their infrastructures.

Cost Savings: Infrastructure on demand leads to more efficient IT spending. Restriction on headcount and capital expenditures often back innovation. Seasonal demands spike capacity requirements and require a robust infrastructure that is frequently unutilized. Cloud computing is a cost-effective alternative.

Mobility and Choice: technology is leading the evolution. Virtualization technologies like VMware enables applications and services to be moved from internal environments to public clouds, or from one cloud service provider to another.

Scalability: Infrastructure as a Service (IaaS) synonymous with scalability. Failover and redundancy are also high-impact opportunities to leverage cloud computing.

1.2 Essential characteristics

On-demand service: Get computing capabilities as needed automatically

Broad Network Access: Services available over the net using desktop, laptop, PDA, mobile phone

Resource pooling: Provider resources pooled to server multiple clients

Rapid Elasticity: Ability to quickly scale in/out service

Measured service: control, optimize services based on metering

1.3 What, When, How, to move on Cloud

Identify the asset(s) for cloud deployment: it is essential to identify the assets in the cloud computing and their importance. Following are the assets of cloud computing

1. Data
2. Applications/Functions/Process

Evaluate the asset: Determine how important the data or function is to the organization

How would we, be harmed if... :

1. The asset became widely public and widely distributed?
2. An employee of our cloud provider accessed the asset?
3. The process of function was manipulated by an outsider?
4. The process or function failed to provide expected results?
5. The info/data was unexpectedly changed?
6. The assets were unavailable for a period of time?

Security Pitfalls

1. User is not aware with how cloud services are provided
2. There is no well demarcated network security border
3. Cloud computing implies loss of control

2. Security Concerns

However the cloud computing is attracting the enterprises and organizations to move, but the some concerns for the enterprises and organization has to keep in mind for their virtual infrastructure. These concerns which identify the security issues in cloud computing are as follows:

Where's the data? : Deferent countries have deferent requirements and controls placed on access.

Who has access? : Access control is a key concern, because insider attacks are a huge risk. A potential hacker is someone who has been interested with approved access to the cloud.

What are your regulatory requirements? : Organizations operating in the US, Canada, or the European Union have many regulatory requirements that they must abide by (e.g., ISO 27002, Safe Harbor, ITIL, and COBIT).

Do you have the right to audit? : This particular item is no small matter; the cloud provider should agree in writing to the terms of audit.

What type of training does the provider over their employees? : This is actually a rather important item, because people will always be the weakest link in security. Knowing how your provider trains their employees is an important item to review.

What type of data classification system does the provider use? : Is the data classified? How is your data separated from other users? Encryption should also be discussed. Is it being used while the data is at rest or in transit?

What are the service level agreement (SLA) terms?: The SLA serves as a contracted level of guaranteed service between the cloud provider and the customer that specifies what level of services will be provided.

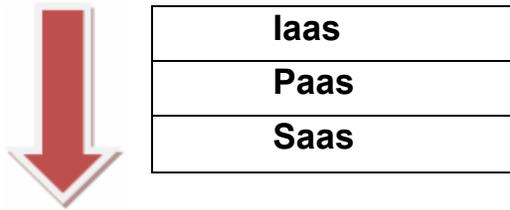
What is the long-term viability of the provider? : How long has the cloud provider been in business and what is their track record. If they go out of business, what happens to your data? Will your data be returned, and if so, in what format?

What happens if there is a security breach? : While many providers promote their services as being unhackable, cloud based services are an attractive target to hackers.

What is the disaster recovery/business continuity plan (DR/BCP)? : All physical locations face threats such as fire, storms, natural disasters, and loss of power. In case of any of these events, how will the cloud provider respond, and what guarantee of continued services are they promising?

3. Security and compliance in cloud computing

3.1 Security Stack in cloud computing



Lower down the stack the cloud vendor provides, the more security issues the consumer has to address or provide.

3.2 Security Issues in SaaS

Following key security element should be carefully considered as an Integral part of the SaaS deployment process:

1. Data Security
2. Network Security
3. Data locality
4. Data integrity
5. Data access
6. Data Segregation
7. Authorization and Authentication
8. Data Confidentiality
9. web Application security
10. Data Breaches
11. Virtualization vulnerability
12. Availability
13. Backup
14. Identity Management on sign-on process

3.3 Security Issues in PaaS

1. In PaaS, the provider might give some control to the people to build applications on top of the platform. But any security below the application level such as host and network intrusion prevention will still be in the scope of the provider.
2. Applications sufficiently complex to leverage an Enterprise Service Bus (ESB) need to secure the ESB directly, leveraging a protocol such as Web Service (WS) Security (Oracle, 2009). The ability to segment ESBs is not available in PaaS environments. Metrics should be in place to assess the effectiveness of the application security programs.
3. Hackers are likely to attack visible code, including but not limited to code running in user context. They are likely to attack the infrastructure and perform extensive black box testing. The vulnerabilities of cloud are not only associated with the web applications but also vulnerabilities associated with the machine-to-machine Service Oriented Architecture (SOA) applications.

3.4 Security Issues in IaaS

Taking virtual machines, which contain critical applications and sensitive data, off premise to public and shared cloud environments creates security challenges for organizations that have relied on network perimeter defense as the main method to protect their datacenter. It may also revoke compliance and breach security policies. OS Security issues also alive in IaaS. Following are the points which are considered in IaaS.

3.5 Security Attacks in Cloud

1. Denial of Service (DoS) attacks: Some security professionals have argued that the cloud is more vulnerable to DoS attacks, because it is shared by many users, which makes DoS attacks much more damaging. Twitter suffered a devastating DoS attack during 2009.

2. 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.

3. Authentication attacks: Authentication is a weak point in hosted and virtual services and is frequently targeted. There are many different ways to authenticate users; for example, based on what a person knows, has, or is. The mechanisms used to secure the authentication process and the methods used are a frequent target of attackers.

4. Man-in-the-middle cryptographic attacks: This attack is carried out when an attacker places himself between two users. Anytime attackers can place themselves in the communication's path, there is the possibility that they can intercept and modify communications.

5. Network Security:
 1. Network penetration and packet analysis
 2. Session management weaknesses
 3. Insecure SSL trust configuration.

6. Web Application Security:
 1. Injection flaws like SQL, OS and LDAP injection
 2. Cross-site scripting
 3. Broken authentication and session management
 4. Insecure direct object references
 5. Cross-site request forgery
 6. Insecure cryptographic storage
 7. Failure to restrict URL access
 8. Insufficient transport layer protection
 9. Un-validated redirects and forwards

4. Cloud security challenges

4.1 Administrative Access to Servers and Applications

One of the most important characteristics of cloud computing is that it offer “self-service” access to computing power, most likely via internet. In traditional datacenters, administrative access to servers is controlled and restricted to direct or on-premise connections. In cloud computing, this administrative access must now be conducted via internet, increasing exposure and risk. It is extremely important to restrict administrative access and monitor this access to maintain visibility of changes in the system control

4.2 Dynamic Virtual Machines: VM State and Sprawl

Virtual machines are dynamic. They can quickly be reverted to previous instances, paused and restarted, relatively easily. They can also readily clone and seamlessly moved between physical servers. This dynamic nature and potential for VM sprawl makes it difficult to achieve and maintain consistent security. Vulnerabilities or configuration errors may be unknowingly propagated. Also, it is difficult to maintain an auditable record of the security state of a virtual machine at any given point in time. In the cloud computing environments, it will be necessary to be able to prove the security state of a system, regardless of its location or proximity to other, potentially insecure virtual machines.

4.3 Vulnerability Exploits and VM-to-VM attacks

Cloud computing servers use the same operating systems. Enterprise and web applications as localized virtual machines and physical servers. The ability for an attacker or malware to remotely exploit vulnerabilities in these systems and applications is a significant threat to virtualized cloud computing environments. In addition co-location of multiple virtual machines increases the attack surface and risk of VM-to-VM compromise. Intrusion detection and prevention system need to be able to detect malicious activity at the VM level regardless of the location of the VM within the virtualized cloud environment.

4.4 Data Integrity: Co-location, Compromise and Theft

According to the 2008 Data breach Investigation Report conducted by Version Business Risk Team, 59% of data breaches resulted from hacking and intrusions. Dedicated resources are expected to be more secure than shared resources. The attack surface in fully or partially shared cloud environments would be expected to be greater and cause increased risk. Enterprises need confidence and auditable proof that cloud resources are not being tampered with nor compromised, particularly when residing on shared physical infrastructure. Operating system and application files and activities need to be monitored.

5. Research Issues

Following are the points which give the vision to researcher to research more in cloud computing security.

1. How to secure the cloud while maintaining availability?
2. How to provide secure key assignment schemes for cloud users?
3. How to make browser secure against various type of attacks?
4. It would be desirable to add XML Encryption and XML Signature functionality to the browser.
5. How to develop secure API for Cloud users?
6. We should be careful about the security concerns while putting our business on Cloud
7. There are open research challenges in cloud computing security which demand intensive Research
8. The security model should be provably secure Security as a Service should be provided to the Cloud users

6. Solution approaches

The following outlines four distinct security technologies –firewall, intrusion detection and prevention, integrity monitoring and log inspection- that can be deployed as software on virtual machines to increase protection and maintain compliance integrity of servers and applications as virtual resources move from on-premise to public cloud environment

6.1 Firewall

Decreasing the attack surface of virtualized servers in cloud computing environments. A bi-directional firewall, deployed on individual virtual machines can provide centralized management of server firewall policy. It should include pre-defined templates for common enterprise server types and enable the following:

1. Virtual machine isolation
2. Fine-grained filtering(Source and Destination Address, Ports)
3. Coverage of all IP-based protocols (TCP, UDP, ICMP, ...)
4. Coverage of all frame types (IP, ARP, ...)
5. Prevention of Denial of Service (DoS) attacks
6. Ability to design policies per network interface
7. Location awareness to enable tightened policy and the flexibility to move the virtual machine from on-premise to cloud resources

6.2 Intrusion Detection and Prevention (IDS/IPS)

Shield vulnerabilities in operating system and enterprise applications until they can be patched, to achieve timely protection against known and zero-day attacks. As previously noted, virtual machines and cloud computing servers use the same operating systems, enterprise and web applications as physical servers. Deploying intrusion detection and prevention as software on virtual machines shields newly

discovered vulnerabilities these applications and OSs to provide protection against exploits attempting to compromise virtual machines.

6.3 Integrity Monitoring

Integrity monitoring of critical operating system and application files (files, directories, registry keys and values, etc.) is necessary for detecting malicious and unexpected changes which could signal compromise of cloud computing resources. Integrity monitoring software must be applied at the virtual machine level.

6.4 Log Inspection

Log inspection 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

7. Conclusion

After discussing the security issues this paper conclude that we should be careful about the security concerns while putting our business on Cloud. There are open research challenges in cloud computing security which demand intensive research. The security model should be probably secure. Security as a Service should be provided to the cloud users.

Acknowledgement

I am very much thankful to organizers of the **Cloud 20/20 Version 3.0, Unisys Confidential** contest to provide the great opportunity to create this paper and describe the ideas in cloud computing technology.

I take great pleasure in expressing our profound sense of gratitude to my esteemed guide Mr. Ramani Shankar for his invaluable guidance, keen interest and constant encouragement for this whitepaper.

Lastly, I wish to acknowledge all the respondents, well wishers and those who directly or indirectly helped us in completing this paper.

Amar Gondaliya

References

1. www.cloudreadyscurity.com
2. www.cloudsecurityalliance.org/guidance
3. www.malwaredomainlist.com/
4. blogs.zdnet.com/security
5. www.programmableweb.com
6. securitylabs.websense.com/content/Blogs