ISSN: 0975-833X

Available online at http://www.journalcra.com

International Journal of Current Research
Vol.3, Issue, 6, pp.208-210, June, 2011

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

REVIEW ARTICLE

PERSPECTIVE ISSUES ON SAFEGUARDING MECHANISMS OF DATA CENTERS INVIRTUALIZED CLOUD COMPUTING

[1]Arunakumari, G.L. and [2]Renu Nekkanti

MCA Department, GITAM University, Visakhapatnam, INDIA

ARTICLE INFO

Article History:
Received 13th March, 2011
Received in revised form
1st April, 2011
Accepted 29th May, 2011
Published online 2nd June 2011

Key words:
Cloud computing,
Security,
Safeguard mechanisms,
Hypervisor,
Vulnerabilities.

ABSTRACT

Cloud computing is evolving as a key computing platform for sharing resources that include infrastructures, software, applications and business processes. This new approach to computing allows users to avoid upfront hardware and software investments, gain flexibility, collaborate with others, and take advantage of the sophisticated services that cloud providers offer. Security is a huge concern for cloud users. In this paper, we analyze some security requirements in cloud computing environment. One of the major threats to virtualization and cloud computing is malicious software that enables computer viruses or other malware that have compromised one customer's system to spread to the underlying hypervisor and ultimately, to the systems of other customers. This paper is concerned with discovery of the vulnerabilities in the landscape of clouds, discovery of security solutions, safeguard mechanisms by behavioral patterns and finding evidence that early-adopters or developers have grown more concerned with security

INTRODUCTION

In 2008, the term ‘‘cloud computing’’ entered mainstream discussions about data protection and privacy. In cloud computing, resources are provided as a service over the Internet to customers who use them on an as-needed basis. Computing services are available through data centers and accessible anywhere, so that the cloud is a single point of access for tools that address the entire customer’s computing needs. This approach to delivering computing power and processing has prompted questions about the security and privacyof information in the cloud, as privacy professionals and information technology experts must ensure that data is protected, even in this new environment. Cloud computing provides Internet-based services, computing and storage for users in all markets including financial, healthcare, and Government. Security is a huge concern for cloud users. Cloud providers have recognized the cloud security concern and are working hard to address it. In fact, cloud security is becoming a key differentiator and competitive edge between cloud providers. By applying the strongest security techniques and practices, cloud security may soon be raised far above the level that IT departments achieve using their own hardware and software.

Cloud Architecture

Most of the current clouds are built on top of modern datacenters. It incorporates Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) and provides these services like utilities so the end users are billed by how much they used. Figure **1** shows a hierarchical view for cloud computing.

Hierarchical view for cloud computing

- Software as a service(saas)
- Platform as a service(PaaS)
- Developers implementing cloud applications
- Infrastructure as a service(IaaS
- [(Virtualization ,storage network) as a service]• Hardware as a service
- Hardware as a service

Software as a Service **(SaaS)**

Cloud consumers release their applications on a hosting environment, which can be accessed through networks from various clients (e.g. web browser, PDA, etc.) by application users. Cloud consumers do not have control over the Cloud infrastructure that often employs a multi-tenancy system architecture, namely, different cloud consumers' applications are organized in a single logical environment on the SaaS cloud to achieve economies of scale and optimization in terms

***Corresponding author:** chandran.aruna@gmail.com*

of speed, security, availability, disaster recovery, and maintenance.

***Platform as a Service* (PaaS)**

PaaS is a development platform supporting the full "Software Lifecycle" which allows cloud consumers to develop cloud services and applications (e.g. SaaS) directly on the PaaS cloud. Hence the difference between SaaS and PaaS is that SaaS only hosts completed cloud applications whereas PaaS offers a development platform that hosts both completed and in-progress cloud applications.This requires PaaS, in addition to supporting application hosting environment, to possess development infrastructure including programming environment, tools, configurationmanagement, and so forth.

***Infrastructure as a Service* (IaaS)**

Cloud consumers directly use IT infrastructures (processing, storage, networks, and other fundamental computing resources) provided in the IaaS cloud. Virtualization is extensively used in IaaS cloud in order to integrate/decompose physical resources in an ad-hoc manner to meet growing or shrinking resource demand from cloud consumers. The basic strategy of virtualization is to set up independent virtual machines (VM) that are isolated from both the underlying hardware and other VMs. Notice that thisstrategy is different from the multi-tenancy model, which aims to transform the application software architecture so that multiple instances (from multiple cloud consumers) can run ona single application (i.e. the same logic machine).

Security Issues

Cloud computing security (sometimes referred to simply as "cloud security") is an evolving sub-domain of computer security, network security and more broadly, information security. It refers to a broad set of policies, technologies and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. There are number of security issues associated with cloud computing but these issues fall into two broad categories: Security issues faced by cloud providers (organizations providing Software, Platform, or Infrastructure-as-a-Service via the cloud) and security issues faced by their customers. In most cases, the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect their information.In order to ensure that data is secure (that it cannot be accessed by unauthorized users or simply lost) and that data privacy is maintained.Cloud providers attend to the following areas:

A. Securing data at rest

Cryptographic encryption is certainly the best practice and in many U.S. states and countries worldwide, it's the law for securing data at rest at the cloud provider. Fortunately, hard drive manufacturers are now shipping self encrypting drives that implement the TCG's Trusted Storage standards. Self-encrypting drives build encryption hardware into the drive, providing automated encryption with minimal cost or performance impact. Software encryption can also be used, but it is slower and less secure since the encryption key can be copied off the machine without detection.

B. Securing data in transit

Encryption techniques should also be used for data in transit. In addition, authentication and integrity protection ensure that data only goes where the customer wants it to go and is not modified in transit. Well-established protocols such as SSL/TLS should be used here. The tricky part is strong authentication, as described next.

C. Authentication

User authentication is often the primary basis for access control, keeping the bad guys out while allowing authorized users in with a minimum of fuss. In the cloud environment, authentication and access control are more important than ever since the cloud and all of its data are accessible to anyone over the Internet.

D. Separation between customers

One of the more obvious cloud concerns is separation between a cloud provider's users (who may be competing companies or even hackers) to avoid inadvertent or intentional access to sensitive information. Typically a cloud provider would use virtual machines (VMs) and a hypervisor to separate customers.

E. Cloud legal and regulatory issues

To verify that a cloud provider has strong policies and practices that address legal and regulatory issues, each customer must have its legal and regulatory experts inspect cloud provider policies and practices to ensure their adequacy. The issues to be considered include data security and export, compliance, auditing, data retention and destruction, and legal discovery. In the areas of data retention and deletion, efficient storage techniques can play a key role in limiting access to data.

F. *Incident response*

As part of expecting the unexpected, customers need to plan for the possibility of cloud provider securitybreaches or user misbehavior. An automated response or at least automated notification is the best solution.

EXISTING METHODOLOGY

There are several groups interested in developing standards and security for clouds and cloud security. Some of the security solutions are briefly discussed here.

A. Web Application Solutions

The best security solution for web applications is to develop a development framework that shows and teaches a respect for security.

B. Accessibility Solutions

An often-ignored solution to accessibility vulnerabilities is to shut down unused services, keep patches updated, and reduce permissions and access rights of applications and users.

C. Authentication Solutions

Data Verification, Tampering, Loss and Theft Solutions.Resource isolation to ensure security of data during processing, by isolating the processor caches in virtual machines, and isolating those virtual caches from the Hypervisor cache.

D. Privacy and Control Solutions

The issues of privacy and control cannot be solved, but merely assured with tight service-level agreements (SLAs) or by keeping the cloud itself private.

E. Physical access solutions

One simple solution is to simply use in-house "private clouds"eg. "The Eucalyptus Open-Source Cloud-Computing System". Cloud computing providers have setup several data centers atdifferent geographical locations over the Internet in order to optimally serve needs of their customers around the world. However, existing systems do not support mechanisms and policies

PROPOSED METHODOLOGY

My research framework is to discover how the vulnerabilities are exploited and what must be done to close the vulnerabilities. One of the pieces of the framework might be developing a way to monitor the cloud's management software and another might be development of isolated processing for specific clients' applications. Having a way to tell whether the virtual machines in the cloud are patched properly would also be a useful part of the framework. People's behavior can be tracked and monitored; for instance whether people allow the automated patching software to run, or updating anti-virus software definitions (on virtual machines running operating systems that are susceptible to viruses, worms and other such malware), or whether people understand how to harden their virtual machines in the cloud.

Conclusion

The main purpose of this paper is to investigate some security requirements in cloud computing environment. Computing services are available through data centers and accessible anywhere, so that the cloud is a single point of access for tools that address the entire customer's computing needs.

Security issues fall into two broad categories: Security issues faced by cloud providers (organizations providing Software, Platform, or Infrastructure-as-a-Service via the cloud) and security issues faced by their customers. We discover how the vulnerabilities are exploited and what must be done to close the vulnerabilities and to a broad set of policies, technologies and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. Future work includes monitoring and tracking people's behavior or whether people understand how to harden their virtual machines in the cloud.

REFERENCES

[1] Wikipedia - Cloud Computing. [Online]. http://en. wikipedia.org/wiki/Cloud computing

[2] Bhaskar Prasad Rimal, Eumni Choi, Ian Lumb, A Taxonomy and Survey of Cloud Computing Systems, 2009 Fifth International Joint Conference on INC, IMS, and IDC, IEEE Computer Society.

[3] Wei-Tek Tsai, Xin Sun, JanakaBalasooriya, Service-orientedCloud Computing Architecture, 2010 Seventh International Conference on Information Tecnology, IEEE Computer Society.

[4] RajkumarBuyya and Chee Shin Yeo, "Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility," *Future Generation Computer Systems*, pp. 599-616, 2009.

[5] C. Yeo and R. Buyya.*Integrated Risk Analysis for a Commercial Computing Service*. Proc. of the 21st IEEE International Parallel and Distributed Processing Symposium, Long Beach, California, USA, March 2007.

[6] IBM. IBM virtualization. 2009. http://www.ibm.com /virtualization

[7] Cloud Security Alliance (CSA): http://cloudsecurity alliance.org/

[8] A Security Analysis of Cloud Computing: (http://cloud computing.sys-con.com/node/1203943)

[9] Cloud Security Questions? Here are some answers (http://cloudcomputing.sys-con.com/node/1330353)

****