Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 6, June 2015, pg.398 – 404

RESEARCH ARTICLE

Need of Multi-Layer Security in Cloud Computing for on Demand Network Access

Asst. Prof. Rajiv Mishra[1], Meenaxi Kumari[2]

[1] Department of Computer Science & Engineering, MDU, Rohtak University, India
[2] Department of Computer Science & Engineering, MDU, Rohtak University, India
[1] mishrarajiv99@gmail.com; [2] meenaxikdn@gmail.com

Abstract: Cloud computing security or, more simply, 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.

[1] Introduction

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. This cloud model promotes availability and is composed of five essential **characteristics,** three **service models**, and four **deployment models**.

[2]Characteristics

On-demand self-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's provider.

Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., 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. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

Rapid elasticity. Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

Measured Service. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

[3]Service Models:

Cloud Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Cloud Platform as a Service (PaaS)**.** The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Cloud Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

[4] Deployment Models:

Private cloud. The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.
Community cloud. The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

Public cloud. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

Hybrid cloud**.** The cloud infrastructure is a composition of two or more clouds (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).
Note: Cloud software takes full advantage of the cloud paradigm by being service oriented with a focus on statelessness, low coupling, modularity, and semantic interoperability.

[5]Security issues associated with the cloud

Organizations use the Cloud in a variety of different service models (SaaS, PaaS, and IaaS) and deployment models (Private, Public, Hybrid, and Community).[1] There are a number of security issues/concerns 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 (companies or organizations who host applications or store data on the cloud). The responsibility goes both ways, however: the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the user must take measures to fortify their application and use strong passwords and authentication measures.

When an organization elects to store data or host applications on the public cloud, it loses its ability to have physical access to the servers hosting its information. As a result, potentially business sensitive and confidential data is at risk from insider attacks. According to a recent Cloud Security Alliance Report, insider attacks are the third biggest threat in cloud computing. Therefore, Cloud Service providers must ensure that thorough background checks are conducted for employees who have physical access to the servers in the data center. Additionally, data centers must be frequently monitored for suspicious activity.

In order to conserve resources, cut costs, and maintain efficiency, Cloud Service Providers often store more than one customer's data on the same server. As a result, there is a chance that one user's private data can be viewed by other users (possibly even competitors). To handle such sensitive situations, cloud service providers should ensure proper data isolation and logical storage segregation.

The extensive use of virtualization in implementing cloud infrastructure brings unique security concerns for customers or tenants of a public cloud service. 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. 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.

[6] Cloud security controls

Cloud security architecture is effective only if the correct defensive implementations are in place. An efficient cloud security architecture should recognize the issues that will arise with security management. The security management addresses these issues with security controls. These controls are put in place to safeguard any weaknesses in the system and reduce the effect of an attack. While there are many types of controls behind a cloud security architecture, they can usually be found in one of the following categories:

Deterrent controls

These controls are intended to reduce attacks on a cloud system. Much like a warning sign on a fence or a property, deterrent controls typically reduce the threat level by informing potential attackers that there will be adverse consequences for them if they proceed. [Some consider them a subset of preventive controls.]

Preventive controls

Preventive controls strengthen the system against incidents, generally by reducing if not actually eliminating vulnerabilities. Strong authentication of cloud users, for instance, makes it less likely that unauthorized users can access cloud systems, and more likely that cloud users are positively identified.

Detective controls

Detective controls are intended to detect and react appropriately to any incidents that occur. In the event of an attack, a detective control will signal the preventative or corrective controls to address the issue. System and network security monitoring, including intrusion detection and prevention arrangements, are typically employed to detect attacks on cloud systems and the supporting communications infrastructure.

Corrective controls

Corrective controls reduce the consequences of an incident, normally by limiting the damage. They come into effect during or after an incident. Restoring system backups in order to rebuild a compromised system is an example of a corrective control.

[7]Cloud security requires multiple layers

The digital universe containing our photos, videos, movies, banking data, health data, tax statements and more is doubling roughly every two years.

Securing this data is a concern. The proportion of sensitive data in the digital universe that requires protection is growing faster than the universe itself. What's more, by 2020 nearly 40% of the information in the digital universe will be touched by cloud computing providers.

As we collectively put more and more business as well as personal data in the cloud, we expect cloud providers to fully secure the data. However, that's rarely the case today. Hardly a day goes by without headlines about another significant data breach.

Cloud providers must adopt a defense-in-depth strategy for data security. This means using layers of security technologies and business practices to make sure that data is protected in multiple ways. A good cloud security plan starts with data encryption but certainly doesn't end there. In fact, there are five keys to cloud data security.

The first tactic that IT security professionals deploy is data encryption, which uses mathematical algorithms to hide the real values of the data. If the data is stolen, it is meaningless without access to the algorithm, or key, to unlock it. Encryption is a tried-and-true technology that can be used on structured data (e.g., numbers) as well as unstructured data (e.g., text). Today's encryption schemes can preserve the format of the data and maintain critical user functionality like searching and sorting within applications.

The next layer of defense is contextual access control. Security policies dictate who can access data from what device and where (geographic location). For example, a doctor can access patient records using his iPad while in the hospital but not during off-hours at home.

Data loss prevention (DLP) technology ensures that specific data is not sent to the cloud in clear text. DLP can protect very sensitive data like social security numbers, credit card numbers and patient records by ensuring that it is not stored in the cloud in general but if it has to be then it is first encrypted.

Application auditing creates a detailed audit trail of user actions within enterprise applications—a list of who did what, and when. This helps administrators detect unusual activities that might indicate a data breach and it is a fundamental pillar of all data compliance, privacy, and governance regulations.

[8]Conclusion

And finally, cloud providers must enforce all of the security policies mentioned above (e.g., encryption, access control) as data moves from one application to another; for example, as financial data moves from credit scoring applications to a mortgage origination application.

Data security in the cloud is critical and can't be left to chance. Cyber criminals are good at attacking weak defenses. Only a thoughtful, multi-layered, defense-in-depth approach to security will protect our growing digital universe.

References

1. IDC (2009) Cloud Computing 2010 – An IDC Update.slideshare.net/JorFigOr/cloud-computing-2010-an-idc-update

2. Armbrust M, Fox A, Griffith R, Joseph AD, Katz RH, Konwinski A, Lee G,Patterson DA, Rabkin A, Stoica I, Zaharia M (2009) Above the Clouds: Gonzalezet al. Journal of Cloud Computing: Advances, Systems and Applications2012,1:11 Page 17 of 18

http://www.journalofcloudcomputing.com/content/1/1/11 A Berkeley View of Cloud Computing. Technical Report UCB/EECS-2009-28, University of California at Berkeley, eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html

3. Rimal BP, Choi E, Lumb I (2009) A Taxonomy and, Survey of Cloud Computing Systems. In: Fifth International Joint Conference on INC, IMS and IDC, NCM '09, CPS. pp 44–51

4. Shankland S (2009) HP's Hurd dings cloud computing, IBM.CNET News

5. Catteddu D, Hogben G (2009) Benefits, risks and recommendations for information security. Tech. rep., European Network and Information Security Agency, enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

6. CSA (2009) Security Guidance for Critical Areas of Focus in Cloud Computing. Tech. rep., Cloud Security Alliance

7. Mather T, Kumaraswamy S (2009) Cloud Security and privacy: An Enterprise Perspective on Risks and Compliance. 1st edition. O'Reilly Media

8. Chen Y, Paxson V, Katz RH (2010) What's New About Cloud Computing Security? Technical Report UCB/EECS-2010-5, University of California at Berkeley, eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html

9. Mell P, Grance T (2009) The NIST Definition of Cloud Computing. Technical Report 15, National Institute of Standards and Technology, www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf

10. Ibrahim AS, Hamlyn-Harris J, Grundy J (2010) Emerging Security Challenges of Cloud Virtual Infrastructure. In: Proceedings of APSEC 2010 Cloud Workshop, APSEC '10

11. Gonzalez N, Miers C, Redıgolo F, Carvalho T, Simplıcio M, Naslund M,Pourzandi M (2011) A quantitative analysis of current security concerns and solutions for cloud computing. In: Proceedings of 3rd IEEE CloudCom. Athens/Greece: IEEE Computer Society

12. Hubbard D, Jr LJH, Sutton M (2010) Top Threats to Cloud Computing. Tech. rep., Cloud Security Alliance. cloudsecurityalliance.org/research/projects/top-threats-to-cloud-computing/

13. Tompkins D (2009) Security for Cloud-based Enterprise Applications. http://blog.dt.org/index.php/2009/02/security-for-cloud-based-enterprise-applications/

14. Jensen M, Schwenk J, Gruschka N, Iacono LL (2009) On Technical Security Issues in Cloud Computing. In: IEEE Internation Conference on Cloud Computing. pp 109–116

15. TrendMicro (2010) Cloud Computing Security - Making Virtual Machines Cloud-Ready. Trend Micro White Paper

16. Genovese S (2009) Akamai Introduces Cloud-Based Firewall. http://cloudcomputing.sys-con.com/node/1219023

17. Hulme GV (2011) CloudPassage aims to ease cloud server security management. http://www.csoonline.com/article/658121/cloudpassage-aims-to-ease-cloud-server-security-management

18. Oleshchuk VA, Køien GM (2011) Security and Privacy in the Cloud – A Long-Term View. In: 2nd International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology (Wireless VITAE), WIRELESS VITAE '11. pp 1–5, http://dx.doi.org/10.1109/WIRELESSVITAE.2011.5940876

19. Google (2011) Google App Engine. code.google.com/appengine/

20. Google (2011) Google Query Language (GQL). code.google.com/intl/en/appengine/docs/python/overview.html

21. StackOverflow (2011) Does using non-SQL databases obviate the need for guarding against SQL injection? stackoverflow.com/questions/1823536/does-using-non-sql-databases-obviate-the-need-for-guarding-against-sql-injection

22. Rose J (2011) Cloudy with a chance of zero day. www.owasp.org/images/1/12/Cloudy with a chance of 0 day Jon Rose-Tom Leavey.pdf

23. Balkan A (2011) Why Google App Engine is broken and what Google must do to fix it. aralbalkan.com/1504

24. Salesforce (2011) Salesforce Security Statement. salesforce.com/company/privacy/security.jsp

25. Espiner T (2007) Salesforce tight-lipped after phishing attack. zdnet.co.uk/news/security-threats/2007/11/07/salesforce-tight-lipped-after-phishing-attack-39290616/

26. Yee A (2007) Implications of Salesforce Phishing Incident.ebizq.net/blogs/securityinsider/2007/11/-implications of salesforcephi.php

27. Salesforce (2011) Security Implementation Guide. login.salesforce.com/help/doc/en/salesforcesecurity implguide.pdf

28. Li H, Dai Y, Tian L, Yang H (2009) Identity-Based Authentication for Cloud Computing. In: Proceedings of the 1st International Conference on Cloud Computing, CloudCom '09

29. Amazon (2011) Elastic Compute Cloud (EC2). aws.amazon.com/ec2/

30. Kaufman C, Venkatapathy R (2010) Windows Azure Security Overview.go.microsoft.com/?linkid=9740388, [August]

31. McMillan R (2010) Google Attack Part of Widespread Spying Effort.PCWorld

32. Mills E (2010) Behind the China attacks on Google. CNET News

33. Arrington M (2010) Google Defends Against Large Scale Chinese CyberAttack: May Cease Chinese Operations. TechCrunch

34. Bosch J (2009) Google Accounts Attacked by Phishing Scam. BrickHouse Security Blog

35. Telegraph T (2009) Facebook Users Targeted By Phishing Attack. The Telegraph

36. Pearson S (2009) Taking account of privacy when designing cloud computing services. In: Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing, CLOUD '09

37. Musthaler L (2009) Cost-effective data encryption in the cloud. Network World

38. Yan L, Rong C, Zhao G (2009) Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-Based Cryptography. In: Proceedings of the 1st International Conference on Cloud Computing, CloudCom '09

39. Tech C (2010) Examining Redundancy in the Data Center Powered by the Cloud and Disaster Recovery. Consonus Tech

40. Lyle M (2011) Redundancy in Data Storage. Define the Cloud

41. Dorion P (2010) Data destruction services: When data deletion is not enough. SearchDataBackup.com

42. Mogull R (2009) Cloud Data Security: Archive and Delete (Rough Cut). securosis.com/blog/cloud-data-security-archive-and-delete-rough-cut/

43. Messmer E (2011) Gartner: New security demands arising for virtualization, cloud computing. http://www.networkworld.com/news/2011/062311-security-summit.html

44. Ristenpart T, Tromer E, Shacham H, Savage S (2009) Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In: Proceedings of the 16th ACM conference on Computer and communications security, CCS '09. New York, NY, USA, ACM, pp 199–212, doi.acm.org/10.1145/1653662.1653687

45. Chow R, Golle P, Jakobsson M, Shi E, Staddon J, Masuoka R, Molina J (2009) Controlling data in the cloud: outsourcing computation without outsourcing control. In: Proceedings of the 2009 ACM workshop on, Cloud computing security, CCSW '09. New York, NY, USA, ACM, pp 85–90, http://doi.acm.org/10.1145/1655008.1655020