Volume 3, Issue 6, June 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Security: A Key Requirement of Cloud

Anupma Sehrawat[1], Neha Bishnoi[2]
Computer Science and Engineering
Amity University Haryana
Amity Education Valley, Panchgaon, Manesar, Gurgaon.
INDIA

Abstract: Cloud computing is becoming a well-known buzzword nowadays due to its ability to reduce costs associated with computing while increasing scalability and flexibility for computer processes. Cloud manages a variety of different workloads, including the batch of back-end operations and user-oriented interactive applications. Cloud computing is a highly discussed topic in the technical world. The software industry is entering in the development of cloud services at a faster pace. Now many corporations have involved in the cloud computing related techniques and many cloud computing platforms have been put forward. This is a favorable situation to study the applications of cloud computing related techniques. Cloud computing platforms provide easy access to a company's high-performance computing and storage infrastructure through web services. With cloud computing, the aim is to hide the complexity of IT infrastructure management from its users. This paper discusses various issues related to security of cloud and their solutions. Security frameworks provided by some organizations have also been briefly discussed in this paper.

Keywords: Cloud Computing, User-oriented, Interactive, Cloud Computing Platforms, Security Solutions, Security Framework

1. INTRODUCTION

Cloud computing is a network-based scenario that emphasize on using the resources on sharing basis. Basically, clouds are Internet-based and it tries to counterfeit the ramification for users. Cloud computing ascribe to both the applications delivered as services over the Internet and the hardware and software in the datacenters that provide those services. Cloud computing providers use virtualization technologies combined with self-service abilities for computing resources via network infrastructure. In cloud computing scenario, there are many types of virtual machines that are hosted on the same server as infrastructure. Cloud computing is essentially a combination of existing technologies that are succeeding in make a paradigm shift in building and maintaining distributed computing systems making use of, multiprocessor, virtualization technology, network based distributed data storage and networking. Cloud computing is much economic because of its zero maintenance cost, as its service provider is completely responsible for the availability of services and clients are free from maintenance and management problems of the resources. Due to this feature, cloud computing is also known as utility computing, or IT on demand [1]. Scalability is another key attribute of cloud computing and this can be accomplished only by server virtualization. Today's web-based generation of computing mainly uses remote servers placed in extremely safe and secure data centers for storage of data and management, so organizations do not need to pay for and look after their internal IT solutions. Security is considered a key feature for cloud computing consolidation as a robust and feasible multi-purpose solution. The main goal of this article is to identify, classify, organize and quantify the main security concerns and solutions associated to cloud computing.

2. CLOUD: A 3 LAYER ARCHITECTURE

Different layers can be defined based on the resources provided by the cloud as shown in Fig.1. The top layer provides users with ready to use applications and is also known as Software-as-a-Service (SaaS) such as Salesforce.com's CRM (Customer Relationship Management) product, and Google Apps such as Docs and Calendar. It is the capability provided to the consumer 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 provider-defined user-specific application configuration settings. The middle layer provides platform-oriented service, satisfying specific needs and is also known as Platform-as-a-Service (PaaS). PaaS delivers cloud-based application development tools, in addition to services for testing, deploying, collaborating on, hosting, and maintaining applications. For example, a PaaS service may enable to deploy and dynamically scale python and Java based web applications. It is the capability provided to the consumer 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. The bottom layer provides infrastructure services such as CPUs, memory, and storage and is also known as Infrastructure-as-a-service (IaaS). It is the capability provided to the consumer 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 physical infrastructure but the consumer has control over operating systems, storage, deployed applications, and possibly limited control of selecting networking components.

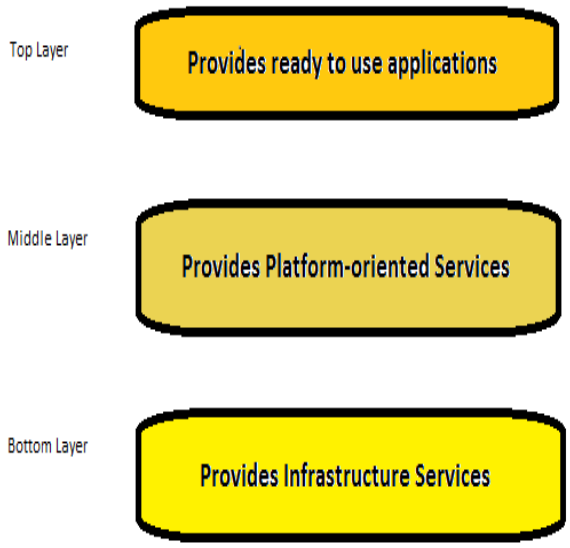

Fig.1. Three Layer Architecture of Cloud

3. CLOUD COMPUTING ISSUES

Cloud computing has several customers such as ordinary users, academia, and enterprises who have different motivations to move to cloud. If cloud clients are academia, security effects on performance of computing and for them cloud providers have to find a way to combine security and performance. For enterprises the most important problem is also security but with different vision. For them high performance may not be as critical as academia. Well-known Gartner's seven security issues which cloud clients should consider as mentioned below [2]:

- **Favored user access**: Sensitive data processed outside the enterprise brings with it an inherent level of risk because outsourced services bypass the "physical, logical and personnel controls".
- **Administrative compliance**: Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider [3]. Traditional service providers are subjected to external audits and security certification.
- **Data location**: When clients use the cloud, they probably won't know exactly where their data are hosted. Distributed data storage is a usual manner of cloud providers that can cause lack of control and this is not good for customers who have their data in local machine before moving from local to cloud.
- **Data dissociation**: Data in the cloud is typically in a shared environment alongside data from other customers. Encryption is effective but isn't a cure all. Encryption and decryption is a classic way to cover security issues but heretofore it couldn't ensure to provide perfect solution for it.
- **Recovery**: If a cloud provider broke or some problems cause failure in cloud sever what will happen to users' data? Can cloud provider restore data completely? Moreover clients prefer don't get permission to third-party companies to control their data. This issue can cause an impasse in security.
- **Analytical support**: Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers.
- **Continual essence**: Ideally, cloud computing provider will never go broke or get acquired by a larger company with maybe new policies. But clients must be sure their data will remain available even after such an event.

4. CLOUD COMPUTING SECURITY

Here, in this section we identify the main problems in Cloud Computing. It is classified in seven categories: network security, interfaces, data security, virtualization, governance, compliance and legal issues. Each category includes several potential

security problems, resulting in the classification with subdivisions that highlight the main issues identified by the aforementioned references:

1) **Network security**: Network security risks include the increased risk of hacking and intrusion, enterprise, perimeter evaporation and mobile device attacks. In case of security provider must include customer's existing internal networks and providing them security in such a way that could extend local strategies to any remote resources or process [2]. It could be done by providing transfer security, firewall and security configuration.

2) **Data security**: It constitutes the risk of data leakage leading to confidentiality and privacy risk, the lack of control over hosted data and applications, availability concerns of cloud services and data, the risk of data integrity impairment, and ineffective protection of data in transit, in rest or in backup due to inadequate encryption. This could be achieved by cryptography, redundancy, and disposal.

3) **Compliance**: Organizations need to ensure the security and integrity of their data, even when it is held by service provider in the cloud. They also need to prove conformity with security standards regardless of the locations of their data and applications. This could be achieved by Service Level Agreements (SLA), Loss of service, Audit, and service conformity.

4) **Interfaces**: The main focus is on issues related to user, administrative and programming interfaces for using and controlling clouds. It includes API, Administrative interface, User interface and Authentication.

5) **Legal issues**: Placing large amounts of data in globally accessible clouds leaves the organization open to large distributed threats as attackers can gain access at one virtual location rather than a secured on-site location. It is related to judicial requirements and law. This includes Data location, E-discovery, Provider privilege, Legislation.

6) **Virtualization**: This includes some controls which can be considered for the mitigation of virtualization security risks. These controls include those related to security administration and control, logical access, network security, physical security, change control, and management and monitoring. This could be achieved by Isolation, Hypervisor vulnerabilities, Data Leakage, Virtual Machine Identification, and Cross Virtual Machine Attacks.

7) **Governance**: Access via a public network and hosted services means increased exposure and subsequently more risks. Privileged access rights should be assigned carefully to authorize users only, and reviewed for adequacy on a frequent basis. The implementation of security tools and techniques are required to ensure authorized user access to data and applications. This could be achieved by Data control, Security control, and Lock-in.

5. SECURITY SOLUTIONS

The number of citations for security problems related to administrative aspects is high; they correspond to 70% (27% of legal issues, 29% of compliance, and 14% of governance). The references to solutions show a total of 30%.The results are presented in figure 2.

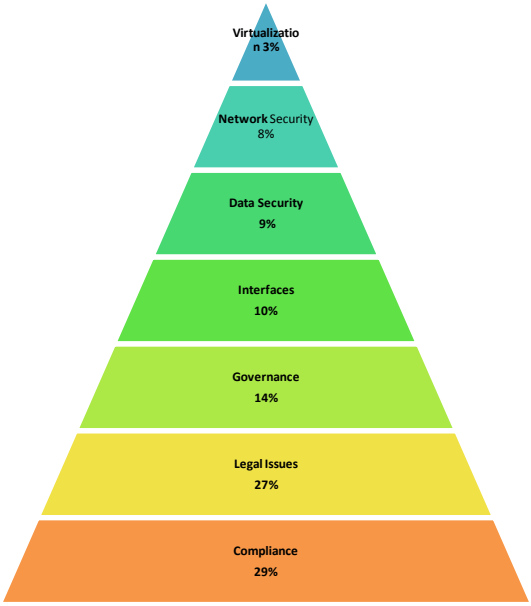

Fig.2. Chart for Solutions Citations

The situation is completely different when analyzing technical aspects of security. In case of data privacy information should be identified and classified appropriately. The cloud service provider's security and information personal should have adequate knowledge and skills to prevent, detect and react to security breaches in a timely manner. Third party audits should be performed on regular basis[3-4]. To provide data control third party audits should be performed on regular basis to monitor the cloud service provider's conformity to agreed terms, and the effective implementation of and adherence to security policies, procedures and standards. It is the responsibility of cloud service provider to provide customer transparency around controls, security and operations [6-9]. Cloud service provider should have adequate backup and data replication policies and should keep auditable proof of the adequacy of restore procedures including accurate, complete and timely recovery of data [10]. Network services and management should provide for adequate provisioning of bandwidth speed and network capabilities. To maintain data integrity patch management policies and procedures should be implemented [11]. Service providers should keep auditable proof that no unauthorized changes occurred during the specified period [6]. Data segregation should be enforced through correctly defined security parameters and adequate and secure configuration of virtual machines and hypervisors [12]. To maintain data encryption controls and management of cryptographic material and methods, whether in transit or at rest, should be implemented [9]. Cloud service providers should ensure that all access or changes to cloud services, resources and data produce auditable records regardless of success or failure. Formal approval should be obtained and kept for new or changed rights to privileged accounts. Administrator access should be encrypted and extra secured by using one-time password protection or multi-factor authentication [12]. Network level controls should be implemented to secure systems and data and prevent unauthorized use, disclosure, damage, or loss of data [12]. Adequate security controls should be enforced between mobile users and cloud based services[20]. Cloud service providers should prove that data, including all copies and back-ups, are stored in geographic locations permitted by a formal contract, SLA, or regulation [12].

6. SECURITY FRAMEWORKS PROVIDED BY DIFFERENT ORGANIZATIONS

CSA

CSA is an organization led by a collision of industry practitioners, corporations, associations and other stake holders [13], such as Dell, HP, Ebay. The architecture defined by CSA includes various features. It enables trust in the cloud based on well known standards and specifications allied to security framework another open resource. It uses widely adopted frameworks in order to achieve standardization of policies and best practices based on already accepted security principles. It gives a tridimensional structure based on premises of cloud delivery, trust and operations.

NIST

Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life[14]. It studied the benefits and risks of adopting cloud solutions for business operations. It provided information for security assessments and decision making.

ENISA

ENISA is an agency responsible for achieving high and effective level of network and information security within the European Union [62]. It defines what cloud services should provide rather than how to design and implement solutions. It has made the understanding of cloud internal operations and mechanisms easy.

7. CONCLUSION

This paper focuses on security issues related to cloud and their solutions. It also emphasize on the solution frameworks provided by various organizations. In future we tend to develop new techniques or solutions which will contribute in making cloud more secure.

REFERENCES

[1] IDC, "Cloud computing 2010 – an IDC update," slideshare.net/JorFigOr/cloud-computing-2010-an-idc-update, September 2009.

[2] D. Tompkins, "Security for cloud-based enterprise applications,"http://blog.dt.org/index.php/2009/02/security-for-cloud-basedenterprise- applications/, February 2009.

[3] B. Robertson. (2009, 1 December 2009). *Top Five Cloud Computing Adoption Inhibitors*. Available: http://www.gartner.com/it/initiatives/pdf/KeyInitiativeOverview_CloudComputing.pdf

[4] M. Vael. (2010, 24 July 2010). *Cloud Computing: An insight in the Governance & Security aspects*. Available:http://www.isaca.org/Groups/Professional-English/informationsecuirtymanagement/GroupDocuments/Across%20Cloud%20Computing%20governance%20and%20risks%20May%202010.pdf

[5] M. Gregg. (2010, 14 May 2010). *10 Security Concerns for Cloud Computing*. Available: www.globalknowledge.com

[6] C. Weitz, *et al.* (2010, 31 August 2010). *A balancing act: What cloud computing means for business, and how to capitalize on it*. Available: www.deloitte.com

[7] L. Ponemon. (2010, 29 September 2010). *Security of Cloud Computing Users: A Study of Practitioners in the US & Europe*. Available:http://www.ca.com/~/media/Files/IndustryResearch/security-cloudcomputing-users_235659.pdf
[8] V. Raval, "Risk Landscape of Cloud Computing," *ISACA Journal* vol. 1, 2010.
[9] Distributed Management Task Force. (2010, 17 March 2011). *Architecture for Managing Clouds*. Available: http://www.dmtf.org/about/policies/disclosures.php.
[10] Cloud Security Alliance. (2009, 20 May 2010). *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1*. Available:www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf
[11] J. W. Rittinghouse and J. F. Ransome, *Cloud Computing:Implementation, Management, and Security*. Florida: CRC Press, 2010.
[12] Centre for the Protection of National Infrastructure (CPNI). (2010, 20 June 2010). *Information Security Briefing 01/2010: Cloud Computing*. Available: http://www.cpni.gov.uk/Docs/cloudcomputing-briefing.pdf
[13] CSA, "Interoperability and portability," July 2011.
[14] NIST, "Draft cloud taxonomy," http://collaborate.nist.gov/twiki-cloudcomputing/bin/view/CloudComputing/ReferenceArchitectureTaxonomy,March 2011.
[15] Communications of the ACM, vol. 53, pp. 62-69, 2010.
[16] M. Gregg. (2010, 14 May 2010). *10 Security Concerns for Cloud Computing*. Available: www.globalknowledge.com
[17] J. Hagel and J. S. Brown. (2010, 15 April 2010). *Cloud Computing:Storms on the Horizon*. Available: http://www.deloitte.com/assets/Dcom-nitedStates/Local%20Assets/Documents/TMT_us_tmt/us_tmt/ce/CloudsStormsonHorizon_102210.pdf
[18] J. Hurwitz, *et al.*, *Cloud Computing for Dummies, HP Special Edition*. Indianapolis, Indiana: Wiley Publishing, Inc, 2010.
[19] N. Kelson. (2010, 2 September 2010). *Cloud Computing Management Audit/Assurance Program*. Available: www.isaca.org

