Available online at www.elixirpublishers.com (Elixir International Journal)

Computer Engineering

Elixir Comp. Engg. 74 (2014) 26767-26770

ISSN: 2229-712X

Security issues in cloud computing

Sumit Kumar*, Ashutosh Bhatt and Gaurav Singh Rawat\

Computer Science and Engineering Department, Maharishi Dayanand University, Rohtak, Haryana, India.

ARTICLE INFO

Article history:

Received: 15 April 2014;

Received in revised form:

21 August 2014;

Accepted: 29 August 2014;

Keywords

Cloud,

Internet,

Flexibility.

ABSTRACT

Cloud computing has quickly become one of the most prominent buzzwords in the IT world due to its revolutionary model of computing as a utility. It promises increased flexibility, scalability, and reliability, while promising decreased operational and support costs. It is much more than simple internet. It is a construct that allows user to access applications that actually reside at location other than user's own computer or other Internet-connected devices. In this paper, we have discussed security risks and concerns in cloud computing and enlightened steps that an enterprise can take to reduce security risks and protect their resources. We have also explained cloud computing strengths/benefits, weaknesses, and applicable areas in information risk management. Cloud computing is continuously evolving and there are several major cloud computing providers such as Amazon, Google, Microsoft, Yahoo and several others who are providing services such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Storage-as-aService and Infastructure-as-a-Service (IaaS) and this paper has discussed some of the services being provided.

Introduction

Clouds are large pools of easily usable and accessible virtualized resources. These resources can be dynamically reconfigured to adjust to a variable load (scale), allowing optimum resource utilization. There have been publicized attacks on cloud computing providers and this paper discusses recommended steps to handle cloud security, issues to clarify before adopting cloud computing, the need for a governance strategy and good governance technology, cloud computing strengths, weaknesses, analyzes the benefits and costs of cloud computing in information security management.

One of the most appealing factors of cloud computing is its pay-as-you-go model of computing as a resource. This revolutionary model of computing has allowed businesses and organizations in need of computing power to purchase as many resources as they need without having to put forth a large capital investment in the IT infrastructure. Other advantages of cloud computing are massive scalability and increased flexibility for a relatively constant price. For example, a cloud user can provision 1000 hours of computational power on a single cloud instance for the same price as 1 hour of computational power on 1000 cloud instances.

Cloud computing is continuously evolving and there are several major cloud computing providers such as Amazon, Google, Microsoft, Yahoo and several others who are providing services such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Storage-as-aService and Infastructure-as-a-Service (IaaS) and this paper has discussed some of the services being provided.

Cloud computing can be classified based on the services offered and deployment models. According to the different types of services offered, cloud computing can be considered to consist of three layers. considered to consist of three layers.

Infrastructure as a Service (IaaS) is the lowest layer that provides basic infrastructure support service.

Platform as a Service (PaaS) layer is the middle layer, which offers platform oriented services, besides providing the environment for hosting user's applications.

Software as a Service (SaaS) is the topmost layer which features a complete application offered as service on demand.

Characteristics and components of IaaS include:

1. Utility computing service and billing model.
2. Automation of administrative tasks.
3. Dynamic scaling.
4. Desktop virtualization.
5. Policy-based services.
6. Internet connective.

Security issues in cloud computing.

1. DoS attacks comes into play when a malicious computer bombards the web server of a particular service with so many requests that the bandwidth is totally consumed with these fake requests and because of that attack the genuine user who has areal requests is denied the possibility of getting the request completed. This is done with the help of IP spoofing and zombie computers, it works in such way that request generated by the malicious host is send to all zombie computers and which in turn send it to a particular web server hence consuming all the bandwidth since the web server will try to answer all the request and wait for the response since there is no one on the other side hence the server will wait with the open channel for the response, hence resulting in a DoS attack Countermeasure: IP traceback and group filtering are some of the countermeasures for the DOS attack , in IP traceback , the IP of the suspected Router of client is traced back to check its origin, if not verified then the channel is blocked for it. In group filtering the packet TTL is checked along with the benchmark of the group if the TTL is more than the expected value the filtering for that IP is done.

Internet connections can be attacked in various ways.

A general type of attack is called ―Man-in–the-middle‖ . The idea behind this attack is to get in between the sender and the recipient, access the traffic, modify it and forward it to the

Tele:

E-mail addresses: anshu.rocks93@gmail.com

recipient. The term ―Man-in-the-middle‖ have been used in the context of computer security since at least 1994, some different variants of this kind of attack exist, but a general definition of a man-in-the-middle attack may be described as a ― Computer security breach in which a malicious user intercepts — and possibly alters — data travelling along a network. This is another issue of network security that will happen if secure socket layer (SSL) is not properly configured. For example if two parties are communicating with each other and SSL is not properly installed then all the data communication between two parties could be hack by the middle party. Countermeasure: The proper installation of secure socket layer(SSL) is required and the secured channel should always be checked before the trusted parties are going to start the communication.

Network Sniffing:

Another type of attack is network sniffer, it is a more critical issue of network security in which unencrypted data are hacked through network for example an attacker can hack passwords that are not properly encrypted during communication. If the communication parties not used encryption techniques for data security then attacker can capture the data during transmission as a third party. Countermeasure: The user should the encrypted method such as AES 128bit and triple DES to secure the data been transferred.

SQL Injection Attack:

SQL injection attacks are the attacks where a hackers uses the special characters to return the data for example in SQL scripting the query end up with where clause that may be modified by adding more information in it. For example an argument value of variable y or 1==1 may cause the return of full table because 1==1is always seems to be true.

Browser Security:

The next issue is Browser Security. As a client sent the request to the server by web browser the web browser have to make use of SSL to encrypt the credentials to authenticate the user.SSL support point to point communication means if there is third party, intermediary host can decrypt the data. If hacker installs sniffing packages on intermediary host, the attacker may get the credentials of the user and use in these credentials in the cloud system as a valid user. Counter measure: countermeasure for this attack is Vendor should use WS-security concept on web browsers because WS security works in message level that use XML encryption for continuous encryption of SOAP messages which does not have to be decrypted at mediator hosts. 4.8 Bad Integration Migrating to the cloud implies moving large amounts of data and major configuration changes (e.g., network addressing). Migration of a part of an IT infrastructure to an external cloud service provider requires profound changes in the infrastructure design (e.g. network and security policies). A bad integration caused by incompatible interfaces or inconsistent policy enforcement may evoke both functional and non-functional impacts.

Unsecure Administration:

API The administration middleware standing between the cloud infrastructure and the cloud service user may be not sure with insufficient attention devoted to sanitation of cloud service user inputs and authentication. Non-protected APIs, mostly administration APIs becomes a target of choice for attackers. This is not specific to cloud environment. However, the service-oriented approach makes APIs a basic building block for a cloud infrastructure. Their protection becomes a main concern of the cloud security.

Shared Environment Cloud resources are virtualized:

Different cloud service users (possibly competitors) share the same infrastructure. One key concern is related to architecture compartmentalization, resource isolation, and data segregation. Any unauthorized and violent access to cloud service user's sensitive data may compromise both the integrity and confidentiality.

Hypervisor Isolation Failure :

The hypervisor technology is considered as the basis of cloud infrastructure. Multiple virtual machines co-hosted on one physical server share both CPU and memory resources which are virtualized by the hypervisor. This threat covers the failure of mechanisms isolating attack" could be launched on a hypervisor to gain illegal access to other virtual machines' memory.

Service Unavailability Availability is not specific to cloud environment

However, because of the service oriented design principle, service delivery may be impacted while the cloud infrastructure in not available. Moreover, the dynamic dependency of cloud computing offers much more possibilities for an attacker. A typical Denial of Service attack on one service may clog the whole cloud system.

Cloud Malware Injection Attack:

The third issue is Cloud Malware Injection Attack, which tries to damage a spiteful service, application or virtual machine. An interloper is obligatory to generate his personal spiteful application, service or virtual machine request and put it into the cloud structure (Booth, 2004). Once the spiteful software is entered into the cloud structure, the attacker care for the spiteful software as legitimate request. If successful user ask for the spiteful service then malicious is implemented. Attacker upload virus program in to the cloud structure. Once cloud structure care for as a legitimate service the virus is implemented which spoils the cloud structure. In this case hardware damages and attacker aim is to damage the user. Once user asks for the spiteful program request the cloud throws the virus to the client over the internet. The client machine is infected by virus.

Threats Cloud computing faces just as much security threats that are currently found in the existing computing platforms, networks, intranets, internets in enterprises. These threats, risk vulnerabilities come in various forms. The Cloud Security Alliance (Cloud Computing Alliance, 2010) did a research on the threats facing cloud computing and it identified the flowing seven major threats:

- ♦ Abuse and Nefarious Use of Cloud Computing
- ♦ Insecure Application Programming Interfaces
- ♦ Malicious Insiders
- ♦ Shared Technology Vulnerabilities
- ♦ Data Loss/Leakage
- ♦ Account, Service & Traffic Hijacking
- ♦ Unknown Risk Profile

Risks

Risk according to SAN Institute "is the potential harm that may arise from some current process or from some future event." In IT security, risk management is the process in which we understand and respond to factors that may lead to a failure in the confidentiality, integrity or availability of an information system (SAN Institute); the IT security risk is the harm to a process or the related information resulting from some purposeful or accidental event that negatively impacts the process or the related information (SANS Institute).

Moving to the cloud presents the enterprise with a number of risks and that include securing critical information like the protection of intellectual property, trade secrets, personally

identifiable information that could fall into the wrong hands. Making sensitive information available on the internet requires a considerable investment in security controls and monitoring of access to the contents. In the cloud environment, the enterprise may have little or no visibility to storage and backup processes and little or no physical access to storage devices by the cloud computing provider. And, because the data from multiple customers may be stored in a single repository, forensic inspection of the storage media and a proper understanding of file access and deletion will be a significant challenge (Information Security Magazine, 2009).

Steps to Cloud Security

Edwards (2009) stated that, with the security risk and vulnerability in the enterprise cloud computing that are being discovered enterprises that want to proceed with cloud computing should, use the following steps to verify and understand cloud security provided by a cloud provider:

♦ Understand the cloud by realizing how the cloud's uniquely loose structure affects the security of data sent into it. This can be done by having an in-depth understanding of how cloud computing transmit and handles data.

♦ Demand Transparency by making sure that the cloud provider can supply detailed information on its security architecture and is willing to accept regular security audit. The regular security audit should be from an independent body or federal agency.

♦ Reinforce Internal Security by making sure that the cloud provider's internal security technologies and practices including firewalls and user access controls are very strong and can mesh very well with the cloud security measures.

♦ Consider the Legal Implications by knowing how the laws and regulations will affect what you send into the cloud.

♦ Pay attention by constantly monitoring any development or changes in the cloud technologies and practices that may impact your data's security.

Issues to Clarify Before Adopting Cloud Computing

Gartner, Inc., the world's leading information technology research and advisory company, has identified seven security concerns that an enterprise cloud computing user should address with cloud computing providers (Edwards, 2009) before adopting:

♦ User Access. Ask providers for specific information on the hiring and oversight of privileged administrators and the controls over their access to information. Major companies should demand and enforce their own hiring criteria for personnel that will operate their cloud computing environments.

♦ Regulatory Compliance. Make sure your provider is willing to submit to external audits and security certifications.

♦ Data location. Enterprises should require that the cloud computing provider store and process data in specific jurisdictions and should obey the privacy rules of those jurisdictions.

♦ Data Segregation. Find out what is done to segregate your data, and ask for proof that encryption schemes are deployed and are effective.

♦ Disaster Recovery Verification. Know what will happen if disaster strikes by asking whether your provider will be able to completely restore your data and service, and find out how long it will take.

♦ Disaster Recovery. Ask the provider for a contractual commitment to support specific types of investigations, such as the research involved in the discovery phase of a lawsuit, and verify that the provider has successfully supported such activities in the past. Without evidence, don't assume that it can do so.

♦ Long-term Viability. Ask prospective providers how you would get your data back if they were to fail or be acquired, and find out if the data would be in a format that you could easily import into a replacement application.

Cloud Computing And Cost

The economic appeal of Cloud Computing is often mentioned as converting capital expenses to operating expenses. Enterprises using Cloud Computing pay differently depending on the agreement between them and the Cloud Computing providers. Usually Cloud Computing providers have detailed costing models which are used to bill users on pay per use basis. There are different cost models available in the market for Cloud Computing. However, the most used model is discussed by Armbrust, which is a short term billing model. The short term billing model as one of the most interesting and novel feature of Cloud Computing. Researchers have discussed the economics of Cloud Computing in two respects i.e. Consumer Perspective and Provider Perspective. Both the perspectives have different cost/price models.

Solution integrity

Within the realm of cloud computing, solution integrity refers to the ability of the cloud provider to ensure the reliable and correct operation of the cloud system in support of meeting its legal obligations, e.g., SLAs, and any technical standards to which it conforms. This encompasses protecting data while it is on the cloud premises, both cryptographically and physically; preventing intrusion and attack and responding swiftly to attacks such that damage is limited; preventing faults and failures of the system and recovering from them quickly to prevent extended periods of service outage; and protection of cloud tenants from the activities of other cloud tenants, both direct and indirect.

(1)Incident response and remediation Even though solutions are run by the cloud provider, cloud providers have an obligation to both their customers and to regulators in the event of a breach or other incident. In the cloud environment, the cloud consumer must have enough information and visibility into the cloud provider’s system to be able to provide reports to regulators and to their own customers. The CSA suggests that cloud customers clearly define and indicate to cloud providers what they consider serious events, and what they simply consider incidents [5]. For example, a cloud consumer may consider a data breach to be a serious incident, whereas an intrusion detection alert may just be an event that should be investigated.

(2)Fault tolerance and failure recovery For a CSP, one of the most devastating occurrences can be an outage of service due to a failure of the cloud system. For example, Amazon’s EC2 service went down in April 2011, taking with it a multitude of other popular websites that use EC2 to host their services. Amazon Web Services suffered a huge blow from this outage. CSPs must ensure that zones of service are isolated to prevent mass outages, and have rapid failure recovery mechanisms in place to counteract outages. The CSA recommends that cloud customers inspect cloud provider disaster recovery and business continuity plans to ensure that they are sufficient for the cloud customer’s fault tolerance level [5].

Conclusion

Cloud computing is a combination of several key technologies that have evolved and matured over the years. Cloud computing has a potential for cost savings to the enterprises but the security risk are also enormous. Enterprise looking into cloud computing technology as a way to cut down on cost and increase profitability should seriously analyze the security risk of cloud computing.

Enterprise should verify and understand cloud security, carefully analyze the security issues involved and plan for ways to resolve it before implementing the technology. Pilot projects should be setup and good governance should be put in place to effectively deal with security issues and concerns. We believe the move into the cloud computing should be planned and it should be gradual over a period of time. Cloud providers exist in the market today, so the cloud paradigm has already overcome its initial security hurdles and moved from theory into reality. However, current cloud providers have provided extremely proprietary solutions for dealing with security issues.

In this Paper we also discuss the Security holes associated with Iaas implementation. The security issues presented here concern the security of each IaaS component in addition to recent proposed solutions. We carried out a systematic review and identified security requirements from previous publications that we classified in nine sub-areas: Access Control, Attack/Harm Detection, Non-repudiation, Integrity, Security Auditing, Physical Protection, Privacy, Recovery, and Prosecution.

Reference

References Armbrust, M. Fox, A, Griffith, R. Joseph, D. A. Katz, R. Konwinski, A. et al. (2009, February). Above the clouds: A Berkeley View of cloud computing. Retrieved on March 10, 2010 from http://d1smfj0g31qzek.cloudfront.net/abovetheclouds.pdf) security.

Bendandi, S. (2009). scribd.com. Cloud computing: Benefits, risks and recommendations for information Retrieved on March 15, from http://www.scribd.com/doc/23185511/Cloud-Computing-benefits-risks-and-recommendationsfor-information-security 2010

Brandl D. (2010, January). Don't cloud your compliance data. Control Engineering, 57(1), 23. CloudTweeks. (2010, January). Plugging into the cloud. Retrieved from http://www.cloudtweaks.com/cloud-diagrams

“Sampling issues we are addressing”, http://cloudsecurityalliance.org/issues.html#15, accessed on April 09, 2009. [8].

MikeKavis,”Real time transactions in the cloud”, http://www.kavistechnology.com/ blog/?p=789, accessed on April 12, 2009.

D Kyriazis, A Menychtas, G Kousiouris, K Oberle, T Voith, M Boniface, E Oliveros, T Cucinotta, S Berger, "A Real-time Service Oriented Infrastructure", International Conference on Real-Time and Embedded Systems (RTES 2010), Singapore, November 2010 [12]

Keep an eye on cloud computing, Amy Schurr, Network World, 2008-07-08, citing the Gartner report, "Cloud Computing Confusion Leads to Opportunity". Retrieved 2009-09-11.

IBM Corporation, Enterprise Security Architecture Using IBM Tivoli Security Solutions, Aug 2007.

Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, 2009.

“Federated identity management.” Internet: http://en.wikipedia.org/wiki/Federated_identity_management, [Dec. 16, 2011].

Shigang Chen, Meongchul Song, Sartaj Sahni, Two Techniques for Fast Computation of Constrained Shortest Paths, IEEE/ACM Transactions on Networking, vol. 16, no. 1, pp. 105-115, February 2008.

King-Shan Lui, Klara Nahrstedt, Shigang Chen, Hierarchical QoS Routing in Delay-Bandwidth Sensitive Networks, in Proc. of IEEE Conference on Local Area Networks (LCN’2000), pp. 579-588, Tampa, FL, November 2000.

ZHANG, L. and ZHOU, Q. 2009. CCOA: Cloud Computing Open Architecture. In Web Services, 2009. ICWS 2009. IEEE International Conference on, 607-616.

NAPPER, J. and BIENTINESI, P. 2009. Can cloud computing reach the top500? In UCHPC-MAW '09: Proceedings of the combined workshops on UnConventional high performance computing workshop plus memory access workshop, 17-20.

Birman, K., Chockler, G., and van Renesse, R. 2009. Toward a cloud computing research agenda. SIGACT News, 40, 2, 68-80.

KEAHEY, K., TSUGAWA, M., MATSUNAGA, A. and FORTES, J. 2009. Sky Computing. Internet Computing, IEEE 13, 5, 43-51.

NURMI, D., WOLSKI, R., GRZEGORCZYK, C., OBERTELLI, G., SOMAN, S., YOUSEFF, L. and ZAGORODNOV, D. 2008. The Eucalyptus Open-source Cloud-computing System. Proceedings of Cloud Computing and Its Applications.