Survey on Security Issues and Solutions in Cloud Computing

D.Gnanavelu[1] (Research Scholars),

Computer Science, Meenakshi University, K.K Nagar, Chennai-78, Tamil Nadu, India

Dr. G.Gunasekaran[2], *Principal,*

Meenakshi College of Engineering, K.K Nagar, Chennai-78, Tamil Nadu, India

ABSTRACT

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. Cloud computing weakness include list of issues such as the security and privacy of business data being hosted in remote 3rd party data centers, being lock-in to a platform, reliability/performance concerns, and the fears of making the wrong decision before the industry begins to mature. We show Successful implementation of cloud computing in an enterprise requires proper planning and understanding of emerging risks, threats and possible countermeasures. This paper show how we secure the cloud security, privacy and reliability when a third party is processing sensitive data. 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.

Keywords - *Cloud Computing, Risk, IaaS, PaaS, SaaS, Security, Quality Assurance.*

1. INTRODUCTION

Cloud computing is the collection of virtualized and scalable resources, capable of hosting application and providing required services to the users with the "pay only for use" strategy where the users pay only for the number of service units they consume. It is the development of parallel computing, distributed computing grid computing, and is the combination and evolution of Virtualization, Utility computing, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS). Cloud is a metaphor to describe web as a space where computing has been pre installed and exist as a service; data, operating systems, applications, storage and processing power exist on the web ready to be shared. Where the IT resources include network, server, storage, application, service and so on and they can be deployed with much quick and easy manner and least management and also interactions with service providers. Cloud computing can much improve the availability of IT resources and owns many advantages over other computing techniques.

2. ARCHITECTURAL COMPONENTS

Cloud service models are commonly divided into SaaS, PaaS, and IaaS that exhibited by a given cloud infrastructure.

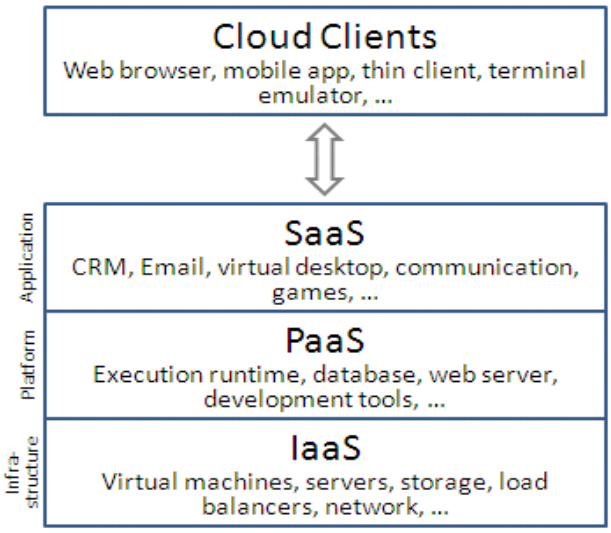

Figure 1. Cloud computing infrastructure

2.1 Software as a Service (SaaS)

Cloud consumers release their applications in 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 multi-tenancy system architecture, namely, different cloud consumers' applications are organized in a single logical environment in the SaaS cloud to achieve economies of scale and optimization in terms of speed, security, availability, disaster recovery and maintenance(1). Examples of SaaS include

SalesForce.com, Google Mail, Google Docs, and so forth.

2.2 Platform as a service (PaaS)

Platform as a Service approach (PaaS), the offering also includes a software execution environment. For example, there could be a PaaS application server that enables the lone developer to deploy web-based applications without buying actual servers and setting them up. PaaS model aims to protect data, which is especially important in case of storage as a service. In case of congestion, there is the problem of outage from a cloud environment. Thus the need for security against outage is important to ensure load balanced service. The data needs to be encrypted when hosted on a platform for security reasons. Cloud computing architectures making use of multiple cryptographic techniques towards providing cryptographic cloud storage have been proposed in (2).

2.3 Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS) refers to the sharing of hardware resources for executing services, typically using Corresponding Author virtualization technology. Potentially, with IaaS approach, multiple users use available resources. The resources can easily be scaled up depending on the demand from user and they are typically charged on a pay-per-use basis (3). They are all virtual machines, which need to be managed. Thus a governance framework is required to control the creation and usage of virtual machines

3. CHALLENGES ON CLOUD ADOPTION PERSPECTIVE

3.1 Security: Well-known security issues such as data loss, phishing, botnet (running remotely on a collection of machines) serious threats to an organization's data and software. The multi - tenancy model and the pooled computing resources on cloud computing has introduced new security challenges such as shared resources (hard disk, data, VM) on the same physical machine invites unexpected side channels between a malicious resource and a regular resource. And, the issue of “reputation fate-sharing” will severely damage the reputation of many good Cloud “citizens” who happen to, unfortunately, share the computing resources with their fellow tenant – a notorious user with a criminal mind.

3.2 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.

3.3 Costing Model: Cloud consumers must consider the tradeoffs amongst computation, communication, and integration. While Migrating to the Cloud can significantly reduce the infrastructure cost, it does raise the cost of data communication.

3.4 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.

3.5 Charging Model: From a cloud provider's perspective, the elastic resource pool has made the cost analysis a lot more complicated than regular data centers, which often calculates their cost based on consumptions on static computing

3.6 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.

3.7 Service Level Agreement: It is vital for consumers to obtain guarantees from providers on service delivery. Typically , these are provided through Service Level Agreements (SLAs) negotiated between the providers and consumers.

4. ISSUES IN CLOUD COMPUTING

More and more information on individuals and companies is placed in the cloud; concerns are beginning to grow about just how safe an environment it is? Issues of cloud computing (4) can summarize as follows:

4.1 Privacy: Cloud computing utilizes the virtual computing technology, users personal data may be scattered in various virtual data centers rather than stay in the same physical location, users may leak hidden information when they are accessed cloud computing services. Attackers can analyze the critical task depend on the computing task submitted by the users.

4.2 Reliability: The cloud servers also experience downtimes and slowdowns as our local server.

4.3 Legal Issues: Worries stick with safety measures and confidentiality of individual all the way through legislative levels.

4.4 Compliance: Numerous regulations pertain to the storage and use of data requires regular reporting and audit trails. In addition to the requirements to which customers are subject , the data centers maintained by cloud providers may also be subject to compliance requirements.

4.5 Freedom: Cloud computing does not allow users to physically possess the storage of the data, leaving the data storage and control in the hands of cloud providers.

5. SOLUTION OF SECURITY ISSUES

5.1 Audit and compliance: Cloud computing raises issues regarding compliance with existing IT laws and regulations and with the division of compliance responsibilities.

5.1.1 Compliance with laws and regulations:
Regulations written for IT security require that an organization using IT solutions provide certain audit functionality. However, with cloud computing, organizations use services provided by a third-party. Existing regulations do not take into account the audit responsibility of a third-party service provider (5).

5.2 Access control: Access management is one of the toughest issues facing cloud computing security (5). One of the fundamental differences between traditional computing and cloud computing is the distributed nature of cloud computing. Within cloud computing, access management must therefore be considered from a federated sense, where an identity and access management solution is utilized across multiple cloud services and potentially multiple CSPs.

Access control can be separated into the following functions:

5.2.1 Authentication: An organization can utilize cloud services across multiple CSPs, and can use these services as an extension of its internal, potentially non-cloud services. It is possible for different cloud services to use different identity and credential providers, which are likely different from the providers used by the organization for its internal applications. The credential management system used by the organization must be consolidated or integrated with those used by the cloud services (5).

5.2.2 Authorization: Requirements for user profile and access control policy vary depending on whether the cloud user is a member of an organization, such as an enterprise, or as an individual. Access control requirements include establishing trusted user profile and policy information, using it to control access within the cloud service, and doing this in an auditable way (5).
Once authentication is done, resources can be authorized locally within the CSP. Many of the authorization mechanisms that are used in traditional computing environments can be utilized in a cloud setting.

5.3 Flow control : Information flow control is central to interactions between the CSP and cloud consumer, since in most cases, information is exchanged over the Internet, an unsecured and uncontrollable medium. Flow control also deals with the security of data as it travels through the data lifecycle within the CSP – creation, storage, use, sharing, archiving, and destruction.

5.3.1 Secure exchange of data**:** Since most cloud services are accessed over the Internet, an unsecured domain, there is the utmost need to encrypt credentials while they are in transit (5). Even within the cloud provider's internal network, encryption and secure communication are essential, as the information passes between countless, disparate components through network domains with unknown security, and these network domains are shared with other organizations of unknown reputability.

5.4 Identity/credentials (management):
Within cloud computing, identity and credential management entails provisioning, de-provisioning, and management of identity objects and the ability to define an identity provider that accepts a user's credentials (a user ID and password, a certificate, etc.) and returns a signed security token that identifies that user. Service providers that trust the identity provider can use that token to grant appropriate access to the user, even though the service provider has no knowledge of the user (7).
An organization may use multiple cloud services from multiple cloud providers. Identity must be managed at all of these services, which may use different identity objects and identity management systems.

5.5 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.

5.5.1 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.

5.5.2 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.

6. CONCLUSION

Cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution in the future. We tried to solve many issues. In our future work, we will include the developing of testing of data flow and security in cloud computing.

Although cloud computing has revolutionized the computing world, it is prone to a number of security threats varying from network level threats to application level threats. In order to keep the Cloud secure, these security threats need to be controlled. Moreover data residing in the cloud is also prone to a number of threats and various issues like: confidentiality and integrity of data should be considered while buying storage services from a cloud service provider. Auditing of the cloud at regular intervals needs to be done to safeguard the cloud against external threats. In addition to this, cloud service providers must ensure that all the SLA's are met and human errors on their part should be minimized, enabling smooth functioning.

7. REFERENCES

[1] Wang, Lizhe; von Laszewski, Gregor; Kunze, Marcel; Tao, Jie. Cloud computing: A Perspective study, *Proceedings of the Grid Computing Environments (GCE) workshop. Held at the Austin Civic Center: Austin, Texas:* 16 November 2008.

[2] Seny Kamara, Kristin Lauter, "Cryptographic cloud storage", Lecture Notes in Computer Science, Financial Cryptography and Data Security, pp. 136- 149, vol. 6054, 2010. DOI: 10.1007/978-3-642-14992-4_13

[3] S. Bhardwaj, L. Jain, and S. Jain, "Cloud computing: A study of infrastructure as a service (IAAS)", International Journal of engineering and information Technology, 2(1):60–63, 2010.

[4] J. F. Yang and Z. B. Chen, "Cloud Computing Research and Security Issues," *2010 IEEE International Conference on Computational Intelligence and Software Engineering (CiSE)*, Wuhan pp. 1-3, DOI= 10-12 Dec. 2010.

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

[6] Xiaojun Yu; Qiaoyan Wen, "A View about Cloud Data Security from Data Life Cycle," *Computational Intelligence and Software Engineering (CiSE), 2010 International Conference on* , vol., no., pp.1-4, 10-12 Dec. 2010.

[7] Cloud Computing Use Case Discussion Group, *Cloud Computing Use Cases Whitepaper v4.0*, July 2010.

[8] Smith, S., & Weingart, S. (1999). Building a high performance, programmable secure coprocessor [Special Issue on Computer Network Security] Computer Networks, 31, 831–860. doi:10.1016 S1389-1286(98)00019-X

[9] Teswanich, W., & Chittayasothorn, S. (2007). A Transformation of RDF Documents and Schemas to Relational Databases. IEEE Pacific Rim Conferences on Communications, Computers, and Signal Processing, 38-41.

[10] Krishna Chaitanya.Y, Bhavani Shankar.Y, Kali Rama Krishna.V andV Srinivasa Rao, Study of security issues in Cloud Computing, *International Journal of Computer Science and Technology ,Vol. 2, No. 3*, Sept 2011

[11] Aderemi A. Atayero, Oluwaseyi Feyisetan , Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption, *Journal of Emerging Trends in Computing and Information Sciences, Vol. 2, No. 10*, October 2011

[12] Kuyoro S. O, Ibikunle.F and Awodele O, Challenges and Security Issues in Cloud Computing *International Journal of Computer Networks, Vol. 3, No. 5*, pp. 247-255, 2011

[13] Armbrust, M. et. al., (2009), "Above the clouds: A Berkeley view of Cloud Computing", *UC Berkeley EECS*, Feb 2010.

[14] Ramgovind, S.; Eloff, M.M.; Smith, E., "The management of security in Cloud computing," *Information Security for South Africa, 2010*, vol., no., pp.1-7, 2-4 Aug. 2010.

[15] Pradeep Kumar Tiwari, Dr. Bharat Mishra. " Cloud Computing Security Issues, Challenges and Solution" International Journal of Emerging Technology and Advanced Engineering ,ISSN 2250-2459, Volume 2, Issue 8, August 2012

[16] Buyya R, Chee Shin Y, Venugopal S, Broberg J, Brandic I. Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems; 2009; 25(6):599–616.

[17]Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing. Journal of Network and computer Applications; 2011; 4(1):1–11.

[18] Takabi H, Joshi J B D, Ahn G. Security and privacy challenges in cloud computing environments. IEEE Security & Privacy; 2010;8(6) :24–31.

[19] Sangroya A, Kumar S, Dhok J, Varma V. Towards analyzing data security risks in cloud computing environments. Communications in Computer and Information Science; 2010; 54:255–265.

Author Profile

D.GNANAVELU is a research scholar working in Meenakshi College of Engineering, Chennai under the supervision of Principal Dr. G. Gunasekaran. He Received M.Phil(Computer Science) Degree in 2008 from Alagappa University India.