International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)
Volume 3, Issue 3, 2016, PP 12-17
ISSN 2349-4840 (Print) & ISSN 2349-4859 (Online)
DOI: http://dx.doi.org/10.20431/2349-4859.0303002
www.arcjournals.org

Efficient Architecture Cloud Computing Confidentiality

[1]S.Rajasekhar, [2]E. Murali, [3] G. Nagalakshmi

[1]Mtech Student,Dep of Cse, SISTK Puttur
[2]Ass**o**c. Professor, Dep of Cse, SISTK Puttur
[3] Head & Professor, Dep of Cse, SISTK Puttur

Abstract: *Cloud computing is an future paradigm that provides tremendous benefits in economical aspects, like reduced time to market, flexible computing capabilities, and limitless computing power. To use the total potential of cloud computing, data is transferred, processed and stored by external cloud suppliers. However, data owners are very skeptical to place their data outside their own management sphere. This paper discusses to that degree this skepticism is even, by presenting the Cloud Computing Confidentiality design. The Cloud Computing Confidentiality architecture is a step-by-step architecture that makes mapping from data sensitivity onto the most appropriate cloud computing design. The conception is extended by providing a Reference design which incorporates a complete overview of the actors and their roles and the necessary architectural parts for managing and providing cloud services.*

Keywords: Cloud computing, cloud computing confidentiality architecture, Reference architecture.

1. INTRODUCTION

The most thorough security controls required to protect the most sensitive data might not be guaranteed in public cloud computing architectures, whereas they can be completed in private cloud computing architectures. These days, you're frequently process, storing, or transmitting data that's subject to regulatory and compliance necessities. once that data falls underneath restrictive or compliance restrictions, your choice of cloud preparation (whether personal, hybrid or public) hinges on associate degree understanding that the supplier is absolutely compliant. Otherwise, there's the danger of violating privacy, restrictive or different legal necessities. The implications for maintaining the protection of data ar vital once it involves privacy.

Today most computer users have access to the net. additional and additional users ar victimization at least some cloud services, like e-mail, Facebook, Google Docs and so forth. however not solely private users ar change to cloud services, conjointly companies and governments ar adopting them. Cloud computing offers many advantages for its users, e.g. value savings, increased flexibility and present access to the data simply to say some. There are enough privacy violations outside the realm of cloud computing for there to be concern concerning any system—cloud-based or traditional—when storing, process or transmitting sensitive information. The cloud has its own examples further. In 2010, several cloud privacy information exposures occurred with variety of cloud-based services, including Facebook, Twitter and Google.

Privacy concerns inside the cloud model aren't new. As a tenant with legal privacy obligations, your handling of privacy problems is no different if you use the cloud. even as you wouldn't store such info on a server while not adequate controls, you wouldn't choose any cloud supplier without verifying it meets the same benchmarks for how it protects data at rest, in transmission or whereas process.

Your policies may exclude any external provider managing sensitive information for you, including cloud providers. While there may be a perception that the computer on your desk is safer than a public cloud, it's probably not (unless you're taking unusual technical and procedural precautions). Safety and governance are two separate issues, and as part of due diligence, you'll need to fully understand your provider's privacy governance, as well as its security practices and guidelines.

2. ARCHITECTURE DESIGN

Before entering into any commercial agreement, an organization that considers using an outsourcing service shall carry out a specific analysis in order to:

1. Clearly identify the data and processing operations which will be passed to the Cloud;
2. Define its own requirements for technical and legal security;
3. Carry out a risk analysis to identify the security measures essential for the organization;
4. Identify the relevant type of Cloud for the planned processing;
5. Choose a service provider offering sufficient guarantees;
6. Review the internal security policy;
7. Monitor changes over time.

The above steps are followed to guarantee data confidentiality:

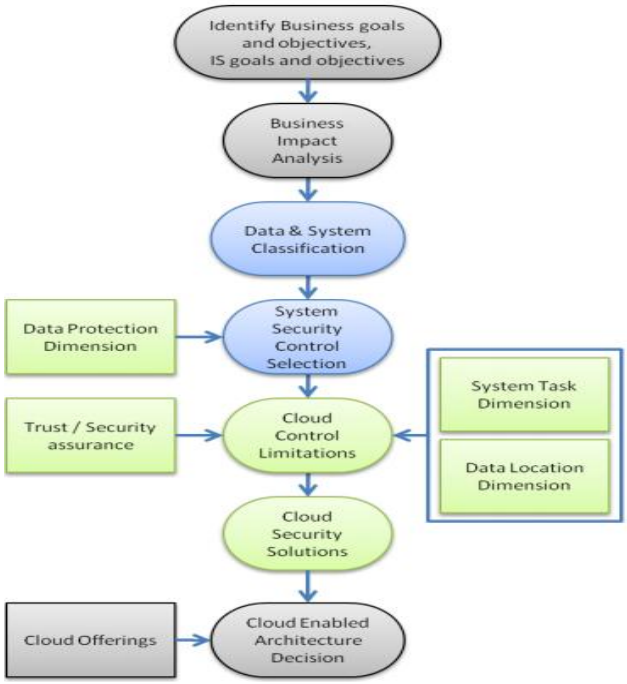

Figure 2-1: *The Cloud Computing Confidentiality Architecture*

3. THE CLOUD COMPUTING CONFIDENTIALITY ARCHITECTURE

The Cloud Computing Confidentiality Architecture will enable companies to review the possibilities to engage in cloud based services, based on the confidentiality of the data used within the company.

The goal of the Architecture is to explain the differences between security in cloud computing environments, and the security in present-day information security practices. This explanation is done by describing the first steps of the IT risk management strategy, and identify which differences will appear when these steps are performed in a cloud computing environment and propose possible solutions to compensate the differences. As it is a good practice for every enterprise to follow such a risk management strategy to secure their data and information systems, the architecture presented here will be relevant to every entity interested to work with cloud based information systems.

Based on the topic of integrated network analysis and design, the architecture is approached from top-down perspective to ensure that security development is consistent with organizational goals and objectives and overall information system goals and objectives.In this top down approach,The explination starts from the need of IT security in the context of strategic goals of the business. From this abstract high level we go down to more concrete parts of the framework. Via a Business Impact Analysis we obtain the business processes and information systems that are deemed important to the business, both in terms of criticality and confidentiality.

With the identified information systems supporting these processes and the information types involved in these information systems, we classify each information type on the topic of confidentiality. When all information types involved in a system have been classified, we can label the confidentiality of an information system by low, moderate or high confidentiality impact level.

With the confidentiality labels associated with the information systems, **we** the risk involved can be ascertained, and define which controls are needed for each confidentiality level.These basic recommendations are adjusted for cloud computing environments, by involving knowledge from our literature review in the form of three dimensions. These dimensions are:

1.Protection mechanisms, which refers to the controls that protect information systems and data.

2.Data location, which refers to the amount of control the data owner can exert over the data itself, depending on where the data is located.

3.System tasks, which refers to whether the data is processed, transferred, stored, or a combination of the three.

Each dimension has its peculiarities in relation to cloud computing, Data protection concerns the layers of protection, from higher abstract level controls to the low technical and physical controls. The Architecture is presented in Figure 2-1. The gray boxes are described to identify goals and objectives at two levels The blue boxes represent the present-day information security practices, in the form of recommendations concerning data classification and control selection. The green rectangles represent important variables in our architecture, in the form of the dimensions from the literature review, and trust related issues. These variables either have their effect on the control selection in above section, or on identification of cloud control limitations.

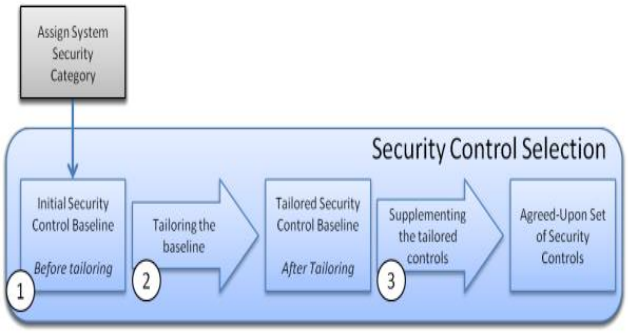

Figure: *The process of security control selection*

4. SECURITY CONTROL SELECTION

In this section, the control selection process is described.The process is started by describing security controls classes and which security control families there are. Then description of the control selection process, presenting a recommended baseline of controls for each impact level of an information system. How this baseline can be refined to match the specific requirements of an organization is also shown. The result will be a list of required technical controls to match the security requirements of an information system given the confidentiality impact level of the system.Security controls, when used correctly, can prevent, limit or determine threat-source damage to organization. Security controls can be placed into three classes:

Technical security controls

Technical controls can be used to protect against specific types of threats. These controls can range from simple to complex measures and consist of a mix of software, hardware and firmware. Next to standalone controls, technical controls also support the management and operational controls described below.

Management security controls

Management security controls are implemented to manage and reduce risks for the organization and to protect an organization's mission. Management security controls can be considered of the highest level of controls, focusing on the stipulation of policies, standards and guidelines, which are carried out by operational procedures to fulfill the organization's goals and missions.

Operational security controls

Operational security controls are used to correct operational deficiencies that might be exploited by potential attackers. These controls are implemented following good industry practices and a base set of requirements in the form of technical controls. Physical protection procedures and mechanisms are examples of operational security controls.

When organizations start the selection process, there are three steps to be executed sequentially:

1. Selecting the initial security control baseline

2. Tailoring the security control baseline

3. Supplementing the tailored security controls

The result of the whole control selection process will be the list of required technical security controls to match the requirements of an information system given the confidentiality impact level of the system.

Composition of system components

Composition of system components to support the Cloud Providers activities in arrangement, coordination and management of computing resources in order to provide cloud services to Cloud Consumers. Figure 3-3 shows a generic stack diagram of this composition that underlies the provisioning of cloud services. A three-layered model is used in this representation, representing the grouping of three types of system components Cloud Providers need to compose to deliver their services. In the model shown in Figure 3-3, the top is the service layer, this is where Cloud Providers define interfaces for Cloud Consumers to access the computing services. Access interfaces of each of the three service models are provided in this layer. It is possible, though not necessary, that SaaS applications can be built on top of PaaS components and PaaS components can be built on top of IaaS components. The optional dependency relationships among SaaS, PaaS, and IaaS components are represented graphically as components stacking on each other; while the angling of the components represents that each of the service component can stand by itself. For example, a SaaS application can be implemented and hosted on virtual machines from an IaaS cloud or it can be implemented directly on top of cloud resources without using IaaS virtual machines.

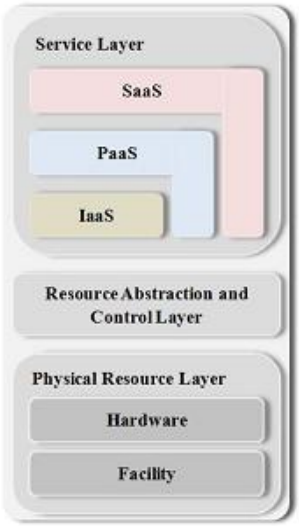

Figure 3-3: *Cloud Provider - composition of system components.*

The middle layer in the model is the resource abstraction and control layer. This layer contains the system components that Cloud Providers use to provide and manage access to the physical computing resources through software abstraction. Examples of resource abstraction components include software elements such as hypervisors, virtual machines, virtual data storage, and other computing resource abstractions. The resource abstraction needs to ensure efficient, secure, and reliable usage of the underlying physical resources. While virtual machine technology is commonly used at this layer, other means of providing the necessary software abstractions are also possible. The control aspect of this layer refers to the software components that

are responsible for resource allocation, access control, and usage monitoring. This is the software fabric that ties together the numerous underlying physical resources and their software abstractions to enable resource pooling, dynamic allocation, and measured service. Various open source and proprietary cloud software are examples of this type of middleware. The lowest layer in the stack is the physical resource layer, which includes all the physical computing resources. This layer includes hardware resources, such as computers, networks,storage components and other physical computing infrastructure elements. It also includes facility resources, such as heating, ventilation and air conditioning, power, communications, and other aspects of the physical plant. Following system architecture conventions, the horizontal positioning, i.e., the layering, in a model represents dependency relationships – the upper layer components are dependent on adjacent lower layer to function. The resource abstraction and control layer exposes virtual cloud resources on top of the physical resource layer and supports the service layer where cloud services interfaces are exposed to Cloud Consumers, while Cloud Consumers do not have direct access to the physical resources.

5. CONCLUSION

The Cloud Computing Confidentiality Architecture presented is a step-by-step Architecture that creates mapping from data sensitivity onto the most suitable cloud computing architecture. The Architectural Components of the Reference Architecture describes the important aspects of service deployment and service composition of system components. This concept can be further enhanced by cloud provider by conducting activities in the areas of service deployment, cloud service management, security, and privacy.

REFERENCES

[1] Amazon. (2009b). Amazon Virtual Private Cloud (Amazon VPC). Retrieved December 28, 2009, from http://aws.amazon.com/vpc/.

[2] Andrzejak, A., Kondo, D. and Anderson, D. (2010). Exploiting Non-Dedicated Resources for Cloud Computing. In Proceedings of 12th IEEE/IFIP Network Operations & Management Symposium (NOMS 2010), Osaka Japan.

[3] Antón, A., Bertino, E., Li, N. and Yu, T. (2007). A roadmap for comprehensive online privacy policy management. *Communications of the ACM, 50*(7): 116.

[4] Armbrust, M., Fox, A., Griffith, R., Joseph, A., Katz, R. et al. (2009). Above the clouds: A Berkeley view of cloud computing. *EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2009-28*.

[5] Baralis, E. and Chiusano, S. (2004). Essential classification rule sets. *ACM Transactions on Database Systems, 29*(4): 635-674.

[6] Bardin, J., Callas, J., Chaput, S., Fusco, P., Gilbert, F. et al. (2009). Security Guidance for Critical Areas of Focus in Cloud Computing v2.1, Retrieved January 28, 2010, from Cloud Security Alliance, from http://www.cloudsecurityalliance.org/guidance/

[7] NIST SP 800-145, "A NIST definition of cloud computing", http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf

[8] NIST SP 800-146, "NIST Cloud Computing Synopsis and Recommendations", http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf

[9] NIST SP 800-53, "Recommended Security Controls for Federal Information Systems and Organizations",http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

[10] Federal Cloud Computing Strategy, http://www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf

[11] Chief Information Officers Council, "Privacy Recommendations for Cloud Computing", http://www.cio.gov/Documents/Privacy-Recommendations-Cloud-Computing-8-19-2010.docx

[12] Office of Management and Budget, Memorandum 07-16, http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf

[13] NIST SP 800-144, "Guidelines on Security and Privacy Issues in Public Cloud Computing", http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf

[14] NIST Cloud Computing Use Cases, http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/UseCaseCopyFromCloud

[15] Gartner, "Gartner Says Cloud Consumers Need Brokerages to Unlock the Potential of Cloud Services", http://www.gartner.com/it/page.jsp?id=1064712.

[16] IETF internet-draft, "Cloud Reference Framework", http://tools.ietf.org/html/draft-khasnabish-cloud-reference-framework-00

[17] IBM, "Cloud Computing Reference Architecture v2.0", http://www.opengroup.org/cloudcomputing/doc.tpl?CALLER=documents.tpl&dcat=15&gdid=23840

[18] GSA, "Cloud Computing Initiative Vision and Strategy Document (DRAFT)", http://info.apps.gov/sites/default/files/Cloud_Computing_Strategy_0.ppt

[19] Cloud Taxonomy, http://cloudtaxonomy.opencrowd.com/

[20] OASIS, the charter for the OASIS Privacy Management Reference Model Technical Committee, http://www.oasis-open.org/committees/pmrm/charter.php

[21] Open Security Architecture (OSA), "Cloud Computing Patterns", http://www.opensecurityarchitecture.org/cms/library/patternlandscape/251-pattern-cloud-computing

[22] Juniper Networks, "Cloud-ready Data Center Reference Architecture", www.juniper.net/us/en/local/pdf/reference-architectures/8030001-en.pdf

[23] Federal Information Security Management Act of 2002 (FISMA), http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

[24] NIST IR-7756, DRAFT "CAESARS Framework Extension: An Enterprise Continuous Monitoring Technical Reference Architecture", http://csrc.nist.gov/publications/drafts/nistir-7756/Draft-nistir-7756_feb2011.pdf .