International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-2 Number-4 Issue-7 December-2012

Baseline Requirements and Architecture for Cloud Computing Services

Abdur Rahim Choudhary

Abstract

Government initiatives such as the "Cloud First" policy are bringing the cloud computing services into Federal Agencies. Further, many of the sectors in the Critical Infrastructure of the nation already use cloud computing. Although cloud computing services are slowly coming to age, many issues remain. This paper therefore takes a closer look at the cloud computing services. First it establishes a baseline by specifying high level requirements for cloud computing services. Next it improves upon the current architecture for the cloud computing services by adding new modules to the current architecture. The new modules are gleaned from an analysis of the telecommunications cloud and security in distributed systems. The new modules include a management and control network, a set of trust domains, and a set of proxies. The improved architecture is more ready for primetime use and supports a richer operational model.

Keywords

Cloud computing, cloud computing services, cloud computing security, telecommunications clouds, critical infrastructure, architecture, signaling and control network, security, digital policies.

1. Introduction

Federal Chief Information Officer has required the use of Cloud Computing Services (CCS) in the Federal Agencies via the Cloud First Policy [1]. These CCSs live in the Cyberspace. Security in the Cyberspace has been the focus of a report [2] to the President by the Information Technology Advisory Committee. The report points to the unsatisfactory status of Nation's Cyber Security and a lack of adequate research and development effort.

The CCS is an emerging concept [3] that is promoted mainly by elements in the industry that seek to provide these services. As is usual in such cases, the marketing hype has preceded the necessary research and development work, and even before any precise definitions is available [4]. In the absence of adequate research and development, new concepts introduced by marketing objectives can create hype that obscures the needed transparency and clarity. This seems to be the case for cloud computing services. The clouds are distributed systems, and security in distributed systems is an ongoing and unsolved problem [5]. However, cloud computing security has more challenges than distributed systems security because of additional aspects like virtualization and the roles of multiple providers and multiple consumers. The cloud computing services paradigm requires at least two things: the security of the clouds, and the operational trust between the consumers and providers of the CCSs. Both of these elements are not adequately available at this stage.

The cloud computing promotes *X as a Service* (XaaS) view, where X can be any computing function provided via the cloud computing, such as Software (SaaS), Platform (PaaS), and Infrastructure (IaaS) [6]. However, there is much hype for XaaS approach that remains unsupported by serious research [**Error! Bookmark not defined.**]. This circumstance can lead to a potentially serious impact on the Critical Infrastructure of the Nation [7].

The R&D effort for the XaaS approach is needed not only for the security of the cloud computing but also for the feasibility, detailed functional analysis, and performance specifications of the XaaS approach. With respect to the security of the XaaS approach, an additional caveat comes from the Presidential Report [**Error! Bookmark not defined.**] that clearly emphasizes that the needed research must be in new directions, seeking new security models that paradigm-wise go well beyond the perimeter based security model that currently prevails.

It is with this background in mind that this paper takes a closer look at the cloud computing and XaaS approach. There are two main objectives of this paper. They clarify the provider and consumer relationship by formulating requirements that govern this relationship. These requirements serve a three-fold purpose: to serve as a baseline for an improved CCS architecture, to serve as guidelines for the CCS consumers to make informed outsourcing decisions and to help the CCS providers to better manage the CCS and security.

Section **Error! Reference source not found.** analyzes the current CCS architecture and its underlying operational model. This analysis yields high level requirements, given in section **Error! Reference source not found.**, for the CCS provider and consumer relationship. The requirements are used in section **Error! Reference source not found.** as a baseline to integrate the research results into an improved CCS architecture which is more responsive to the baseline requirements and supports an enhanced operational model. Our conclusions are summarized in section **Error! Reference source not found.**.

2. Current Cloud Computing Architecture

Some marketing oriented cloud computing modalities are described in industry whitepapers [8][9]. The currently prevailing situation is summarized in Figure 1.

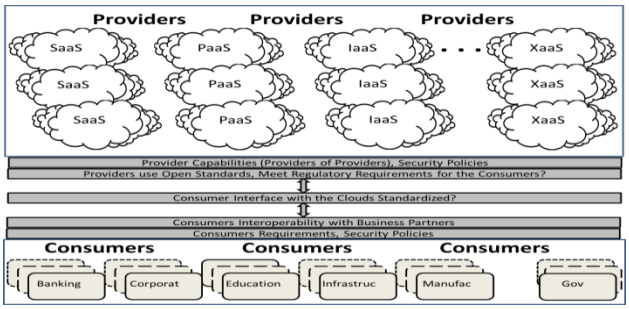


Figure 1: A view of today's cloud computing services architecture

The architecture in Figure 1 has following major components.

2.1 Providers and Consumers Interface

The providers of the XaaS type services are in the forefront of championing and defining what cloud computing is. Since cloud security and service availability are perceived as the major problem, most of the vendor efforts are geared towards assuring the potential customers that cloud services security and availability issues are manageable [6].

From an end to end point of view, what matters most is an analysis of the provider capabilities in the area of service functionality as well as security. Figure 1 shows two aspects of it: (a) the functional capabilities of a provider that would be measured against consumer requirements in the context of the service; and (b) security capabilities and policies of the provider that would be analyzed for compatibility with the security requirements and policies of a consumer. Implicit in the capabilities statement is an analysis of how these capabilities are provided, i.e. are they all provided directly by the provider's own cloud, or some capabilities are acquired from other CCS providers (providers of providers). This is important for the consumer of the CCSs because it implicitly extends the trust model and other considerations like compatibility, standards, and availability to the providers of providers.

In addition, Figure 1 shows the relevance of open standards and regulatory requirements that apply to the business of the consumer. Compliance with the regulatory requirements remains the responsibility of the consumer. Therefore a consumer must ascertain that the CCS provider acquires the capabilities in a manner that is compliant from the regulatory perspective.

The importance of open standards cannot be overstated. The consumer must analyze this point because it can impact the consumer's business productivity and the cost of doing business. For instance, if the business partners of the consumer acquire their CCSs from different providers that have non-standard or proprietary methods, it may result in the operational incompatibility. Such a situation can require additional in-house processing which can partially beat the purpose of outsourcing to the cloud.

The interface that the provider of cloud services extends to the customers is extremely important, as is the consistency, uniformity, and stability of this interface. This is because this interface impacts the training costs and business productivity of the consumers. Further, if a consumer subscribes to multiple providers the customer may need to deal with multiple interfaces. A standard interface that is intuitive and stable can lead to training cost savings and productivity enhancements.

2.2 Service Interface

The interface with the cloud computing service (CCS) is important. The interface is used for communicating content specific to the type of CCS. Other communications between the consumer and the provider are also important. These include identities management, security policies, specification and evaluation of the service level agreements, and feedback on the service adequacy. These may be communicated using the same or a different interface. A consumer may use different providers for different

cloud services. For reasons of training costs and productivity, it is desirable that the interfaces to different CCSs be similar in look and feel. This requirement is facilitated if the interface is standardized. Further, a consumer may need multiple providers for the same service for fault tolerance and business continuity in case of disasters. In such cases it becomes important that different providers use the same look and feel for the interface for seamless operations of the consumer's business across different providers. Failure to pay attention to these considerations can result is higher training costs and reduced productivity for the consumer's business.

2.3 Service Level Agreements

The relationship of providers and consumers is based on the service level agreements (SLA). The existence of an SLA is implicit in **Error! Reference source not found.**. It is important to have a flexible SLA with intuitive metrics to monitor its compliance. The type of SLA that a CCS provider offers is an important consideration in making outsourcing decisions and in selecting a CCS provider.

3. Requirements

The above analysis leads to the following baseline requirements to govern the CCS provider and consumer relationship. We will use these requirements in section **Error! Reference source not found.** to arrive at an improved CCS architecture. Consumers of CCS can use these requirements to assess CCS provider capabilities and to make informed outsourcing decisions. The CCS providers can use these requirements to enhance the capabilities and security of their offerings.

1. The provider capabilities in the area of the service that the consumer is seeking to outsource shall be transparently stated using unambiguous language, and without obscure fine prints.
2. The CCS provider shall clearly state if provider has all the capabilities for the service that the consumer is seeking to outsource, or does it acquire some of the capabilities from other providers, how many other providers, which other providers.
   The answer determines if the trust of the consumer must be extended to the providers of the provider, and the impact analysis on the security and availability of the service.
   Providers using other providers to augment their capabilities may be quite common. Reference [**Error! Bookmark not defined.**] illustrates how even a simple cloud service like the "travel booking" may need to use couple other CCS providers to augment its own capabilities.
3. CCS provider shall transparently disclose its own providers with respect to the particular CCS that the consumer is outsourcing to the provider. Further, the CCS provider shall consult with the consumers when it changes its providers.
4. The CCS provider shall comply with open standards; the provider shall clearly state when it uses nonstandard or proprietary methods.
   The use of nonstandard methods can adversely impact consumers' business efficiency and operational costs.
5. The service that the provider provides shall assist in compliance with the regulatory requirements imposed on the business of the consumer.
   For example, a hospital would need to comply with the Privacy and Security rules of Health Insurance Portability and Accountability Act (HIPAA) even when it uses services from CCS providers. In such a case, the provider assistance is necessary for compliance; otherwise the benefits of outsourcing can be significantly reduced or even eliminated.
6. CCS provider shall make its offerings sufficiently secure. The security shall not be weakened due to providers of provider, and when the providers of provider change.
7. CCS provider security policy and the security capabilities of the provided CCS shall be clearly documented and formally version controlled so that the consumers can assess the commensurability with the consumer service security requirements and organizational security policies.
   Both are important in their own right, namely, the security capabilities requirements of the provided CCS, and the organizational security policies of the provider and consumer. A consumer may find the organizational security policy of the provider acceptable but the security capabilities of the service itself to be unacceptable, or vice versa.
8. CCS provider operations shall be trustable for the business operations of consumers. The issue of trust goes beyond cloud security and provider security policies. Business operations stability is a main component of operational trust.

a. The service environment shall be stable. This includes the reliability, maintainability, and availability of the cloud computing service that the consumer outsources to the provider.
b. The providers of provider shall be stable. This means that the providers that the CCS provider uses are themselves trustworthy and stable.
c. CCS capabilities shall be stable. This means that the service that the provider provides to the consumer shall have a stable capabilities set and a stable interface.
d. Service level agreements shall be stable. This means that there are no unwelcome changes in the service level agreement and the related compliance metrics.
e. CCS security shall be stable. This means that the CCS will remain secure against emerging threats; adequate and timely security patches shall be provided.
f. Provider security policy shall be stable. This means that the security policy of the provider shall remain acceptable to the consumers over the life of the service level agreement.

9. CCS shall have an interface that is intuitive, easy to learn, and stable over time.
   If not, it can impact the consumer's training costs and business productivity.
10. CCS shall support audit capabilities, logging, and operational metrics that the consumer needs for its business practices.
11. CCS provider shall use flexible SLAs to accommodate the consumer specific needs, together with intuitive metrics to monitor SLA compliance.

Despite outsourcing to CCS providers considerable in-house IT capabilities, and the related costs, may still be required. These arise from the hardware and software that is needed to access various CCSs which in general may be provider specific. It becomes more significant when multiple CCS providers are used for multiple business processes, or for business continuity in cases of CCS failure. The client machines or software to access multiple CCSs may be nonstandard and mutually incompatible among different providers. The customer will therefore need to acquire, maintain, and service all the needed machines or software; and train its staff in their use. In addition, special in-house processing may become necessary due to noncompliance with industry standard and non-compatibility among multiple providers. Simple examples of special in-house processing include reformatting, unit conversions, and input and output considerations among business processes.

4. Improved Cloud Computing Architecture

There are many shortcomings of today's CCS architecture and its underlying operational model. The baseline requirements suggest that the chief shortcomings are the cloud computing security and the operational trust between CCS providers and consumers. In this section we will explore ways to improve today's CCS architecture. We will first analyze two other industry areas where similar problems have been successfully resolved. The analysis suggests inclusion of additional architectural components that will remove or greatly diminish the above mentioned shortcomings. Thus we derive an improved architecture, shown in Figure 2, which is more suitable for primetime use.

4.1 Analysis

In this section we present an analysis of related industry areas that have implicitly used cloud computing concepts. The analysis is offered to show how these industries have overcome some of the problems we face today in providing cloud computing services. We analyse the telecommunications cloud and the distributed systems as clouds.

4.1.1 Telecommunications Cloud

Telecommunications sector is a prominent part of the critical infrastructure [7]. The idea of a service cloud is abundantly used in telecommunications to provide "Voice as a Service" [10]. It offers an experience base [11][12] that can be used in XaaS paradigm for secure, robust, and evolvable cloud computing services.

The telecommunications clouds use two-fold network architecture. First, there is the circuit switched network based on the service switching points (SSP) [13] that carry public data. Second, there is a packet switched network for signalling system 7 (SS7) [14] that provide control and management of the cloud. The latter uses signal transfer points (STP) [13] which are like the routers. This network is referred to as the Telecommunications Management Network (TMN) described in ITU-T Recommendation M.3010

[15]. TMN is separated and isolated from the public network infrastructure so that any disruptions due to faults or security threats in the end-user plane in the public network do not spread to TMN. As a result of this separation, it is relatively easy to secure the management network traffic because access to this plane is restricted to authorized network administrators, and traffic is restricted to valid management activities [11].

This two-fold architecture allows the telecommunications clouds to maintain a separation between public data and the signaling data. In analogy, this paper suggests the use of a restricted access signaling network for the control and management of the CCS quality and security. In this paper such network architecture is achieved via the use of a network of policy enforcement points (PEPs) [16].

The analysis of the telecommunication cloud thus leads us to a network of PEPs for the control and management purposes. The control and management network is the new element that our analysis introduces into the current CCS architecture. The PEPs control and manage service security service capabilities, and service quality. This architectural element will be used and further elaborated in section 4.2.

4.1.2 Distributed Systems as Clouds

There is an overload of terminology. The terms Internet, cyberspace, and clouds are roughly equivalent. Further, they are all distributed systems. Hence research results obtained for distributed systems can apply to CCS.

There exist some practices that help secure distributed systems. One set of practices is described as design patterns [17] while another emphasizes a security design that uses trust domains and accompanying digital policies [18]. The analysis of distributed systems therefore leads us to introduce two new architectural elements into the current CCS architecture. These elements are the proxies [17] and the trust domains [18]. Section 4.2 will use these new architectural elements and will elaborate them further.

4.2 Improved Architecture

Synthesizing the analysis results from the previous sections leads to an architecture for the cloud computing services that includes the following three modules in addition to the ones discussed in section 2. An architecture incorporating these improvements is shown in Figure 2.

- **Trust domains** [18] should be included as a module of the cloud computing service and security architecture. Users belong to one or more of these trust domains. Each trust domain is characterized by its own digital policies for security and service capabilities [18]. The trust domain module thus enables different levels of protection and services. Figure 2 implicitly shows 4 trust domains: one domain for the enterprise internal employees, another for the coalition partners (NATO), another level for friends (Taiwan), and yet another for potential adversaries (China). Further, there will generally be subdomains within each domain; for example, the internal enterprise domain may have sub domains for employees, contractors, human resources, financials, and executives. Corresponding to each domain or sub domain, security and service policies are formulated, and its membership is populated [19]. Figure 2 shows the domain policies being enforced using a policy enforcement point (PEP).
- **Signalling Network** consists of the policy enforcement points (PEPs) described above and shown in Figure 2. There are multiple PEPs in the architecture, though only one is shown in Figure 2. In a large cloud like the telecommunications cloud [10] or the global information grid (GIG) [ ] there are a large number of PEPs. The PEPs in an enterprise form a separate network within the cloud, like the telecommunications management network (TMN) [14] [15] within the telecommunications cloud. The purpose of this module is to provide a signaling channel to control and manage the CCSs and the security by placing access control policies, and service level and quality policies in the PEPs. Thus the mediation system shown in Figure 2 enables the application of the policy based management technology to those CCSs that were not designed with this technology in mind. It also permits a mechanism to generate audit and performance metrics, and to automate the management actions in response to operational events.
- **Proxies** [**Error! Bookmark not defined.**] as an architectural component are like simple PEPs that act autonomously without the involvement of Policy Decision Points (PDPs) [**Error! Bookmark not defined.**]. For users that access the CCSs remotely through the networks, for example over the Internet or the Global

Information Grid (GIG), the use of a proxy will further distance them from the CCSs. A proxy can control access, execute simple policies, cut off attacks, and revoke privileges on behalf of the cloud service. The proxies can help contain the damage from an attack; if the attacker brings a proxy down, the cloud service can still go on serving other users that access the service via other proxies (see Figure 2); and an administrator can shut a proxy down in order to disconnect an on-going attack and the attacker.

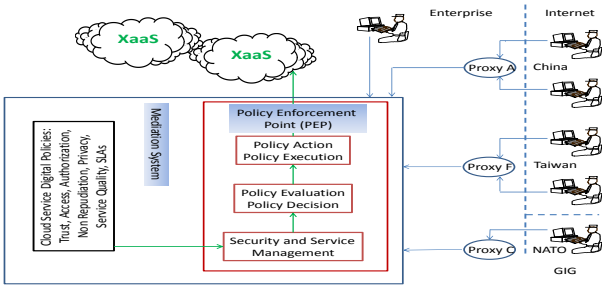


Figure 2: Improved architecture for cloud computing services and operations.

The architecture shown in Figure 2 offers significant improvements over the simple architecture shown in Figure 1. To make the improvements cost affective, the new modules are introduced not as modifications to CCS itself but as mediation systems that are added as adjuncts to the existing deployments. There are in general multiple mediation systems though only one is shown in Figure 2.

The architecture shown in Figure 2 offers the potential for operational efficiencies and cost savings, which take place at multiple levels. Some examples are given below.

- Traditionally the CCS capabilities are managed separately and differently from the management of security. In our architecture there is a unified framework to manage both. The unification takes place through the PEPs, which help enhance efficiency and reduce costs. There are multiple PEPs in this architecture, though only one is shown. In general there is PEP for each managed object which can be a device, an application, or a service. Thus there would be a network of PEPs based on the geographical locations, number of services, number of security devices and applications, as well as network layout. These PEPs together form a management network for CCS and security, not unlike the TMN in telecommunications. This network offers a unified infrastructure for managing services, security, and deployment networks.
- Once the infrastructure of PEPs is in place the CCS capabilities extension can be achieved with a small additional cost involved in connection with the digital policies specific to the capability. For example it can be used to manage additional capabilities such as SLAs, service provisioning, and billing. The agility achieved through this way of managing SLAs, provisioning, and billing can save substantial costs, and at the same time increase customer satisfaction [21]. It also enhances the reliability, maintainability, and availability of the CCS capabilities and its security. The PEPs network offers a policy based management infrastructure [21]. That means the management functions can be automated to save operational costs. No modification is needed to the CCS. The policy based management infrastructure also enables extensibility and evolvability of the CCS capabilities, and hence the provider's business [21]. It means that new CCS capabilities for the existing cloud services as well as new cloud services can be introduced cost effectively.

The proxies shown in Figure 2 can be deployed without changes to the cloud computing services; the PEPs can operate as adjuncts to existing management systems; and mediation systems can be inserted between the users and the service cloud. Hence the improved architecture discussed in this section is minimally disruptive. It adds only a small delta to the overall deployment cost; but it also saves operational costs. Over the lifecycle of a cloud computing service, the suggested improvements are expected to be a net cost saver.

5. Conclusions

Current state of the cloud computing services is not ready for the primetime use. Nevertheless, there is increasing momentum towards using these services, especially in the Government through such initiatives as the Cloud First policy. The research reported in this paper has formulated a set of high level requirements to establish a baseline for the cloud computing services. These requirements are used to formulate a substantially improved architecture for the cloud computing services that supports a rich operational model and is more ready for primetime use. This architecture also saves operational costs,

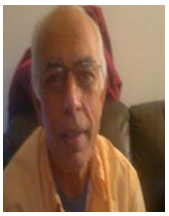
and improves operational agility. The paper offers a set of guidelines. These enable the consumers of the cloud services to make informed decisions to outsource to the cloud. They enable the providers of the cloud services to make their offerings secure, extensible, and evolvable. They also help the consumers and providers to negotiate meaningful service level agreements and compliance metrics.

Acknowledgments

The author acknowledges support from Vahida Inc. He also thanks Yasmeen Sultana for encouragement.

References

[1] Vivek Kundra, U.S. Chief Information Officer, "25 Point Implementation Plan to Reform Federal Information Technology Management", December 9, 2010.
[2] President's Information Technology Advisory Committee, Cyber Security Subcommittee, "Cyber Security: A Crisis in Prioritization", February 2005.
[3] John Rhoton, "Cloud Computing Explained: Implementation Handbook for Enterprises", 2nd Edition, ISBN 978-0-9563556-0-7, Recursive Press, 2011.
[4] National Institute of Standards and Technology, "The NIST Definition of Cloud Computing (Draft)", Special Publication 800-145 (Draft), January 2011.
[5] George Coulouris, Jean Dollimore, Tim Kindberg, and Gordon Blair, "Distributed Systems: Concepts and Design", 5th Edition, ISBN 978-0132143011, Addison Wesley, 2011.
[6] IBM Global Technology Services, technical whitepaper "Security and high availability in cloud computing environments", June 2011.
[7] Homeland Security Presidential Directive 7 (HSPD7): Critical Infrastructure Identification, Prioritization, and Protection. 2003.
[8] The Open Group, "An Architectural View of Security for Cloud – Examining Policy-Based Security Through Scenarios", May 2011.
[9] Intel IT Center, "Planning Guide - Cloud Security: Seven steps for building security in the cloud from the ground up", September 2011.
[10] Gabrielsson, Jan, et al. "Cloud computing in telecommunications." Ericsson Review 1, 29-33, 2010.
[11] ITU-T, "Security in Telecommunications and Information Technology – An overview of issues and deployment of existing ITU-T Recommendations for secure telecommunications", December 2003.
[12] Jim Metzler, Ashton Metzler and Associates, "Planning for Cloud Services from Telecommunications Service Providers", January 2012.
[13] Lorentz G., Moore T., Manes G., Hale J., and Shenoi S., "Securing SS& Telecommunications Networks", Proceedings of 2001 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, 2001.
[14] Dryburgh, Lee and Hewitt, Jeff, "Signaling System No. 7 (SS&/C7): Protocol, Architecture, and Services", ISBN 1-58705-040-4, Indianapolis 2004.
[15] International Telecommunication Union–Telecommunication Standardization Sector (ITU-T), M.3010, "Principles for a Telecommunication management network", February 2000.
[16] Abdur Rahim Choudhary, "Policy Based Management", Bell Labs Technical Journal Vol. 9, pp. 19-29, 2004.
[17] Alan H. Karp and Kevin Smathers, Intelligent Enterprise Technologies Laboratory, HP Laboratories Palo Alto, "Three Design Patterns for Secure Distributed Systems", HPL-2003-40, February 2003.
[18] Abdur Rahim Choudhary and Alan Sekelsky, "Securing IPv6 Network Infrastructure: A New Security Model", Proceedings of the IEEE International Conference on Homeland Security Technologies (HST), pp. 500- 506, held at Waltham, Massachusetts, during 8-10 November, 2010.
[19] Abdur Rahim Choudhary, "Service Intelligence through Agile Information Controls", Bell Labs Technical Journal, Vol. 8, pp. 61-70, 2004.
[20] Department of Defence Chief Information Officer, "Department of Defense Global Information Grid Architecture Vision", Version 1.0, June 2007.
[21] Abdur Rahim Choudhary, "Policy Based Management in the Global Information Grid", J. Internet Protocol Technology, Vol. 3, pp. 72-80, 2008.



Dr. Abdur Rahim Choudhary was born in a small village, Salempur, Jalundhar, Punjab, India. He has a Ph.D. in Theoretical Physics from University of London, UK, and a M.S. in Nuclear Physics from University of Karachi, Pakistan. Dr. Choudhary has published in the area of Theoretical Physics as well as in information and network security, Policy Based Management, Systems Engineering, and Aerospace Engineering. Currently Dr. Choudhary is associated with Vahida Inc. (vahida.org), a not-for-profit corporation registered in the USA under 501 (3) (c). He is interested in philanthropic work for the empowerment of underprivileged masses worldwide.