Third Asia Pacific Conference on Advanced Research (APCAR, Melbourne, July, 2016)
ISBN:978 0 9943656 20
www.apiar.org.au

ENHANCING CLOUD COMPUTING WITH SECURITY TRUST MODEL

John Ayoade (PhD, SMIEEE)
Southern Institute of Technology, New Zealand
Email: john.ayoade@sit.ac.nz

Abstract

Cloud computing is a framework that allows the implementation and accessibility of computing resources such as networks, servers, storage, applications and services over the internet. Cloud Computing is a concept that presents a good number of benefits for its users; however, it also raises some security challenges which may slow down its use. In this paper, we will discuss some of those security issues that can stand as barriers to realizing the full benefits that cloud computing can bring and we are proposing a security trust model that could enhance the confidence that users need to fully trust the use of cloud computing and maximize the potential benefits that it offers.

***Keywords*:** Cloud Computing, Security, Certificate Authority, PKI.

1. Introduction

Cloud Computing Services

Cloud computing can be categorized into three models, Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

SaaS is the service provision to the consumer to use the provider's applications running on a cloud infrastructure. These applications could be accessed through different devices by the consumers. SaaS is such a service provision model that does not require the consumer attention or effort in regards to management or control of the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings.

PaaS is the service provision to the consumer to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services and tools supported by the provider. Just as the SaaS consumer does need to manage or control the underlying cloud infrastructure, so does PaaS. These include networks, servers, operating systems and storage, but they have control over the deployed applications and possibly configuration settings for the application-hosting environment.

IaaS is the service provision to the consumer for processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. IaaS is such a service provision model that does not require the consumer attention or effort in regards to the management or control the underlying cloud infrastructure but has control over operating systems, storage and deployed applications; and possibly limited control of selected networking components (e.g., host firewalls) (Mell & Grance, 2011).
This paper is organized as follows:

Section I briefly describes the cloud computing services. Section II describes cloud computing deployment models. In Section III, the author describes the benefits and challenges of deploying cloud computing. Section IV describes mobile cloud computing. Section V explores security challenges in cloud computing. Section VI describes the certificate authority trust model. In Section VII, the author

proposed a security trust model that instils confidence in cloud computing deployments and in users based on the mutual trust that exist amongst the internetworks devices, application and infrastructures.

2. Cloud Computing Development Models

In this section, the three types of cloud computing deployment models will be discussed. These are public, private and hybrid clouds.

Public clouds are service provision by organizations that use such services to offer rapid access to affordable computing resources to other organizations or individuals. With public cloud services, users don't need to purchase hardware, software or supporting infrastructure, which is owned and managed by the service providers (http://www.ibm.com/cloud-computing). Public clouds are services that are made available to the general public by a service provider who hosts the cloud infrastructure. Generally, public cloud providers like Amazon AWS, Microsoft and Google provide the infrastructure and offer access over the Internet. With this kind of model, customers have no visibility or control over where the infrastructure is located. It is important to note that all customers on public clouds share the same infrastructure pool with limited configuration, security protections and availability variances (http://blog.appcore.com).

A Private cloud is a service provision by a service provider that controls the way virtualized resources and automated services are customized and used by various lines of business and constituent groups.
Private clouds exist to take advantage of many of cloud's efficiencies, while providing more control of resources and steering clear of multi-tenancy (http://www.ibm.com/cloud-computing). Private cloud is cloud infrastructure dedicated to a particular organization. Private clouds allow businesses to host applications in the cloud, while addressing concerns regarding data security and control, which is often lacking in a public cloud environment. It is not shared with other organizations, whether managed internally or by a third-party, and it can be hosted internally or externally.
Hybrid clouds are service provision of combination of two or more clouds (private, community or public) that remain unique entities but are bound together offering the advantages of multiple deployment models. The reality is a private cloud cannot exist in isolation from the rest of a company's IT resources and its public cloud. Most companies with private clouds will evolve managing workloads across data centers, private clouds and public clouds – thereby creating hybrid clouds (http://www.ibm.com/cloud-computing).

There are two variations of private clouds:

1. On-Premise Private Cloud: This is a cloud computing service provision service that is hosted within an organization's own facility. A business IT department would incur the capital and operational costs for the physical resources with this model. On-Premise Private Clouds are best used for applications that require complete control and configurability of the infrastructure and security. This kind of model is highly recommended for organizations or individual that are worried and concerned about security and privacy issues revolving around cloud computing.

2. Externally Hosted Private Cloud: Externally hosted private clouds are also exclusively used by one organization, but are hosted by a third party specializing in cloud infrastructure. The service provider facilitates an exclusive cloud environment with full guarantee of privacy. This format is recommended for organizations that prefer not to use a public cloud infrastructure due to the risks associated with the sharing of physical resources (http://blog.appcore.com). However, since the cloud infrastructure is externally hosted, there are still security and privacy concerns in this model.

3. Benefits and Challenges of Cloud Types

Public Cloud customers benefit from economies of scale, because infrastructure costs are spread across all users, allowing each individual client to operate on a low-cost, "pay-as-you-go" model. Another advantage of public cloud infrastructures is that they are typically larger in scale than an in-house enterprise cloud, which provides clients with seamless, on-demand scalability. These clouds offer the greatest level of efficiency in shared resources; however, they are also more vulnerable than private clouds.

A public cloud is the obvious choice when an organization's workload for applications is used by lots of people, such as e-mail or a situation an organization need to test and develop application code or need incremental capacity (the ability to add computer resources for peak times) or doing collaborative projects (http://blog.appcore.com). Comparatively Private clouds are more expensive, but also more secure when compared to public clouds. An Info-Tech survey shows that 76% of IT decision-makers will focus exclusively on the private cloud as these clouds offer the greatest level of security and control.
Private Clouds could be a better model to choose when you need data sovereignty, cloud efficiencies, consistency across services and more server capacity (http://blog.appcore.com).

On the other hand, hybrid cloud model requires both on-premise resources and off-site server based cloud infrastructure. One of the benefits of hybrid cloud model is that by spreading things out over a hybrid cloud, you keep each aspect of your business in the most efficient environment possible. The downside is that you have to keep track of multiple cloud security platforms and ensure that all aspects of your business can communicate with each other.

There are a couple of situations where a hybrid environment is regarded as a best. For example, a situation where an organization wants to use a SaaS application, but they are concerned about their security. Another example is an organization which offers services that are tailored for different vertical markets. You can use a public cloud to interact with the clients, but keep their data secured within a private cloud. Furthermore, where you can provide public cloud to your customers while using a private cloud for internal IT (http://blog.appcore.com).

4. Mobile Cloud Computing

Mobile Cloud Computing is a paradigm for mobile applications whereby most of the processing and data storage associated with the applications is moved off the mobile device to powerful, centralized computing platforms located in the Cloud. These centralized applications are then accessed over the mobile Internet, using either a thin native client or web browser on the device (Prasad, Gyani & Murti, 2012).
Mobile Cloud Computing was introduced after the concept of Cloud Computing was launched in mid-2007. It has been attracting the attention of entrepreneurs as a profitable business option that reduces the development and running cost of mobile applications and mobile users as a new technology to achieve rich experience of a variety of mobile services at low cost and of researchers as a promising solution for green core IT (Ali, 2009). Fig.1 below describes the mobile cloud computing architecture.

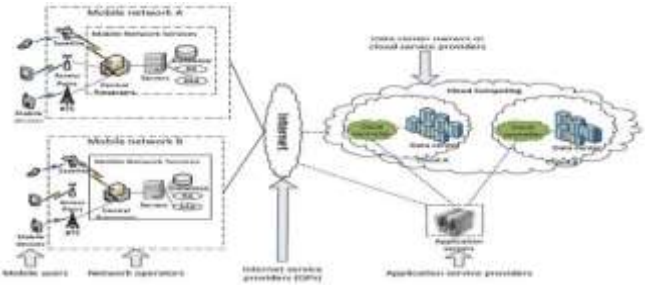

Fig. 1 Mobile Cloud Computing Architecture

Fig. 1 was proposed by (Dinh et al., 2011) and it shows that the mobile devices are connected to the mobile networks through the base stations, access points or satellite. The mobile networks (mobile networks A and B) can be connected to clouds (cloud A and B) via the internet through their ISPs. From this simple overview of the mobile cloud computing, it is glaring that there are many different internetworks of devices, platforms and infrastructures. As a result of this security, authentication of all these infrastructures are very important in order to ensure that the security of data and applications used, exchanged and stored in the cloud are protected and secured.

Prasad, Gyani & Murti (2012) mentioned that the mobile network operators can provide services to mobile users as AAA (Authentication, Authorization and Accounting) based on the Home Agent (HA) and subscriber's data stored in databases. After that, the subscriber's requests are delivered to a cloud through the Internet.

In cloud, the cloud controllers process the requests to provide mobile users with the corresponding cloud services. These services are developed with the concepts of utility computing, virtualization and service oriented architecture (e.g. web application and database servers).

5. Security Challenges in Cloud Computing

Cloud Computing is a concept that presents a good number of benefits for its users as described above; however, it also raises some security issues and challenges which may slow down its use. Understanding what vulnerabilities exist in Cloud Computing will help organizations make the shift towards the Cloud due to its efficiency and cost benefits. Since Cloud Computing leverages many technologies, it also inherits their security issues and challenges (Hashizume et al., 2013).

Although adopting cloud computing attracts many benefits, there are also some significant barriers to adoption. One of the most significant barriers to adoption is security, followed by issues regarding compliance, privacy and legal matters (KPMG, 2010).
Cloud Computing represents a computing model and there is a great deal of uncertainty about how security at all levels (e.g., network, host, application, and data levels) can be achieved (Rosado et al., 2012). That uncertainty has consistently led information executives to state that security is their number one concern with Cloud Computing (Mather, Kumaraswamy & Latif, 2009).
The cloud system is running in the internet and the security problems in the internet also can be found in the cloud system. The cloud system is not different from the traditional system in the PC and it can meet other special and new security problems. The biggest concerns about the cloud computing are security and privacy (Liu, 2012). The same thing is applicable to mobile cloud computing. Actually, more concerns are expressed towards mobile cloud computing because of wireless connectivity is prone to more security and privacy vulnerabilities.

There are several aspects of mobile cloud security, including antivirus, authentication, data protection and digital rights management. Security vulnerability can cause serious problems, including property damage, cloud vendor economic loss, and user distrust. There are many instances of malware attempting to steal personal information or intercept mobile transactions. Since mobile devices are resource-constrained, locally executed antivirus software can hardly protect them efficiently from threats. A current solution is to offload the threat detection functionality to the cloud. Nevertheless, since a pure cloud antivirus relies on cloud resources, it is difficult to deal with malware that can block the device's Internet connection. Besides, authentication is critical for access to sensitive information such as bank accounts and confidential files. With constrained text input on mobile devices, users tend to use simple passwords, making mobile applications more vulnerable to authentication threats (Liu et al., 2013).

6. Certificate Authority Trust Models

Trust is one of the fundamental solutions to the security issues in cloud and mobile cloud computing. Trust may be defined as a confidence in or reliance on another person or entity. One of the principle foundations of PKI is that of trust. For example, Alice must trust that the public key in Bob's digital certificate actually belongs to him. A trust model refers to the type of trusting relationship that can exist between individuals or entities. A third party trust refers to a situation in which two entities trust each other because each trusts a third party (Ciampa, 2012).

Public Key Infrastructure supports a number of security-related services, including data confidentiality, data integrity and end-entity authentication. Fundamentally, these services are based on public/private key pairs. The public component of this key is issued in the form of a public key certificate and in association with the appropriate algorithms. In order for an authority to communicate with principals and verifiers in a cost-effective and reliable way, there must be an existing close relationship between them.

A hierarchical trust model is one in which all of the end entities and relying parties use a single root Certificate Authority (CA) or multiple root CAs as their trust anchor. If the hierarchy has multiple levels, the Root CA certifies the public keys of intermediate CAs (or substituted CAs). In this model, certificates are issued in only one direction, and a CA never certifies another CA "Superior" to itself (Li et al., 2006). Mesh or distributed trust models use another style of trust model. In a typical mesh style, each end entity trusts the CA that issued their own certificates. Thus, there is no root CA for the entire PKI. The all CAs in this environment have peer relationships; they are neither superior nor subordinate to one another (Li et al., 2006). In the bridge trust model there is no single CA that signs digital certificates. However, with the bridge trust model, there is one CA that acts as a facilitator to interconnect all other CAs. This facilitator CA does not issue a digital certificate; instead, it acts as the hub between hierarchical trust models and distributed trust models (Ciampa, 2012).
In the bridge trust, the PKI domain trusts each other through a bridge CA (BCA) by cross-certification process. In this model, trust relationship is not established between a subscriber domain and a relying party domain directly, but established through the bridge CA (Copper et al., 2005; Shimaoka, Hastings & Nielsen, 2008).

7. Proposed Model

It was proposed that a mutual trust between different internetworks devices, platforms and infrastructures across different models should be deployed. Mutual authentication means two parties authenticating each other suitably. This means that the client authenticates itself to a server and that server authenticates itself to the client in such a way that both parties (client and server) have the assurance of the other's identity. This is the goal and importance of this proposed model. The author believes this model is very important in cloud computing in order to enhance users' trust in the implementation and use of cloud computing.

One of the ways to provide this trust is for different internetworks devices, platforms and infrastructure to mutually authenticate each other prior to exchanging communications.
For example, with cloud computing, data and applications do not need to reside in the same location and one can choose to shift only parts of functions to the cloud. For example, you can host your application and data in your own data centre, while still outsourcing a portion of its functionality to the cloud through a Platform as a service (https://cloudsecurityalliance.org). This shows that a high level of trust needs to be established amongst internetworks devices, platforms and infrastructures in order to realise security.

In Fig. 2, we proposed that there should be a mutual trust between the subscriber domains (for example internetworks devices/entities). Fig. 2 shows a mutual trust between BCA' and CAs. This means that there should be a bridge CA' (BCA') for every domain and BCA' certifies the CAs. The BCAs' are the certificate authorities that certify all internetworks devices/entities within their domains. In a nutshell, instead of having just one bridge CA for the whole PKI domain trusts a BCA' for every domain should be established in order to alleviate heavy workload for the BCA. Also, having just one BCA is identified as a risk because the BCA could be compromised and once the BCA is compromised, the whole mechanism is forfeited. In other words, if the adversary can clone the BCA, it can act as the authentic BCA and impersonate any member of the CAs. As a result, all the authentic devices or entities security will be compromised. However, having a BCA' for every trust domain will overcome this kind of impersonation because each entity and the BCA' will have mutual authentication. In case any of the devices is compromised the BCA' will be aware of this and flag such an issue notifying other BCA's through the BCA.

The BCA' will be instituted like this:

One BCA will certify all BCAs' and every BCA' in a domain will certify every CA in that domain. Now, in order to ensure mutual authentication between the entities, the BCA' in one domain can trust each other and check on the authenticity of each other from the BCA. Also, in order to avoid impersonation of compromised BCA, BCA' and CA; every CA can confirm the authenticity of its BCA' with any other BCA' from other domain or even from the root BCA. Fig. 2, depicts the procedure and mechanism of the operation used in our proposed model.

Table 1: Notation Table

Notation	Meaning	Representation in Cloud Computing System
CA	Certificate Authority	Devices/entities
BCA	Bridge Certificate Authority	Root Server
BCA'	Domain Bridge Certificate Authority	Domain Server

Table 1 shows the notation used in the paper and what each notation means and what kind of representation those notations have in the cloud computing system. These notations are used in the trust model described in Fig. 2.

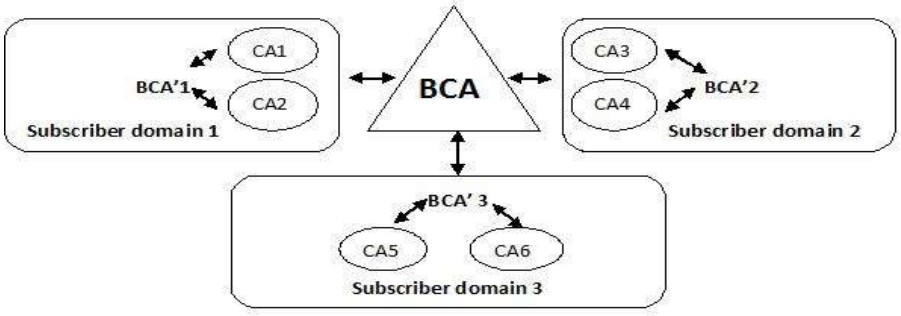

Fig. 2:

Fig. 2 shows that BCA certifies subscriber domains 1, 2 and 3. Subscriber domain 1 (BCA'1) certifies CA1 and CA2. Also, subscriber domain 2 (BCA'2) certifies CA3 and CA4 and subscriber domain 3 (BCA'3) certifies CA5 and CA6. There will be mutual authentication between BCA and BCA'1, BCA and BCA'2 and BCA and BCA'3. As a result of mutual authentication amongst the BCA and BCA'1, BCA'2 and BCA'3, it will be difficult for the systems to be compromised and any of the bridged BCA's can authenticate each other and check on any mistrust going on in the system. For example, if the BCA is compromised, easily the bridge BCA's will be aware and inform each other. In a nutshell, there is a mutual trust amongst the devices, platforms and internetworks in cloud computing and as a result cloud computing users will be confident to deploy and use cloud computing comfortably.

8. Conclusion

Cloud computing domain bridge trust (BCA') will be more suitable in order to assure security confidence in the mind of users planning to deploy different services in the cloud. Furthermore, adopting BCA' in cloud computing will ensure mutual authentication between different devices and application and assurance of mutual trust will be realized.

Another important step is to identify risks available among the internetworks devices, platforms and infrastructures across different models. This identification is not a once in a while procedure, but it has to be continuously identified in order to detect such risks. Once the risks are identified, they need to be evaluated and adequate research should be carried out on how such risks should be mitigated or totally eradicated in order to provide security.

9. References

i. Ali, M., 2009. *Green Cloud on Horizon*. In Proceedings of the 1st International Conference on Cloud Computing (CloudCom), pp. 451- 459.

ii. Ciampa, M., 2012. *Security Guide to Network Security Fundamental Course Technology*.

iii. Copper, M., Dsambasow, Y., Hesse, P., Joseph, S. & Nicholas, R., 2005. *Internet X.509 Public Key Infrastructure: Certification Path Building*. RFC.

iv. Dinh, H., Lee, C., Niyato, D. & Wang, P., 2011. *A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches*. Available at: http://onlinelibrary.wiley.com

v. Hashizume, K., Rosado, D., Fernández-Medina, E. & Fernandez, E., 2013. An Analysis of Security Issue for Cloud Computing. *Journal of Internet Services and Applications – A Springer Open Journal*, doi:10.1186/1869-0238-4-5

vi. KPMG. 2010. *From Hype to Future: KPMG's 2010 Cloud Computing Survey*. Available at: http://www.techrepublic.com/whitepapers/from-hype-to-future-kpmgs-2010-cloud-computing-survey/2384291

vii. Li, M., Ren, Y., Wang, Z., Xie, J. & Yao, H., 2006. *A New Modified Bridge Certification Authority PKI Trust Model*. 1st International Symposium on Pervasive Computing and Application.

viii. Liu, W., 2012. *Research on Cloud Computing Security Problem and Strategy*. Published in Consumer Electronics, Communications and Networks (CECNet), 2nd International Conference. Available at: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?&arnumber=6202020

ix. Liu, F., Shu, P., Jin, H., Ding, L., Yu, J., Niu, D. & Li, B., 2013. *Gearing Resource- Poor Mobile Devices with Powerful clouds – Architectures, Challenges, and Applications*. IEEE Digital Library.

x. Mell, P. & Grance, T., 2011. *The NIST Definition of Cloud Computing*. National Institute of Standards and Technology Special Publication Special Publication, pp. 800-145. Available at: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf 2011

xi. Prasad, M., Gyani, J. & Murti, P., 2012. Mobile Cloud Computing: Implications and Challenges. *Journal of Information Engineering and Applications*, 2(7), pp. 2224-5782.

xii. Rosado, D. G., Gómez, R., Mellado, D., Fernández-Medina, E., 2012. Security Analysis in the Migration to Cloud Environments. *Future Internet*, 4(2), pp. 469-487.

xiii. Shimaoka, M., Hastings, N. & Nielsen, R., 2008. *Memorandum for multi-domain Public Key Infrastructure (PKI) Interoperability*. Network Working Group Request for Comments.

Other Resources:

xiv. A Smarter Planet - Smart Cloud. Available at: http://www.ibm.com/cloud-computing/in/en/what-is-cloud-computing.html [Accessed Dec 2013]

xv. Cloud Security Alliance. Available at: https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

xvi. Types of Cloud Computing: Private, Public and Hybrid Clouds. Available at: http://blog.appcore.com/blog/bid/167543/Types-of-Cloud-Computing-Private-Public-and-Hybrid-Clouds