Proceedings of Informing Science & IT Education Conference (InSITE) 2014

Cite as: Srinivasan, S. (2014). Building trust in cloud computing: Challenges in the midst of outages. *Proceedings of Informing Science & IT Education Conference (InSITE) 2014* (pp. 305-312). Retrieved from http://Proceedings.InformingScience.org/InSITE2014/InSITE14p305-312Srinivasan0544.pdf

Building Trust in Cloud Computing: Challenges in the Midst of Outages

S. Srinivasan
Jesse H. Jones School of Business, Texas Southern University, Houston, TX, USA

srinis@tsu.edu

Abstract

Cloud computing is evolving rapidly as a global technology solution for cost-effective Information Systems deployment. By its design the cloud computing concept requires the businesses to operate over the internet by subscribing to services as needed. Internet was not designed for secure communication. Moreover, businesses feel that they lose control over the infrastructure and data when they use cloud services. The cloud service providers offer assurances to the customers on the safe handling of their data and access to unlimited computing resources on demand. Moreover, cloud service offers users the ability to pay for what they use only. These positive features have attracted several businesses to the cloud but concern remains about the reliability and security of cloud service usage. Our hypothesis is that cloud computing will continue to grow in popularity and service providers will benefit by enhancing trust among their customers. The importance of building trust is essential because there have been several high profile cloud outages. In this overview paper we focus on the various steps that the cloud service provider could take to earn customer trust and build on it further. Also, we look at the major cloud outages over the past five years.

Keywords: Cloud computing, Trust, Outages, AWS, Security, Privacy, e-commerce, SLA

Introduction

Cloud computing adoption is growing rapidly worldwide. Its economic impact both in terms of job creation and commerce are significant. Cloud computing's attraction to the businesses is its ability to transfer the capital expenditure to operational expenditure whereby businesses could allocate resources in a continuous manner rather than tie up resources. Businesses get access to high-end computing services on the cloud while at the same time paying only for what they use. Moreover, cloud computing is able to make available unlimited computing resources to businesses through the concept of virtualization. Virtualization means that the same physical device is capable of hosting multiple servers. From the business perspective they have dedicated virtual servers as needed and from the cloud service provider perspective multiple clients share the same physical infrastructure. This is called multi-tenancy. The cloud service provider is able to benefit from economies of scale and pass on the cost savings to the customer.

The three main types of cloud services available are SaaS, PaaS and IaaS. SaaS stands for Software as a Service and is

the widely used of the three cloud services. SaaS provides the customer the ability to run an application of their choice such as Office Productivity Suite, Inventory Management and Customer Relations Management. The Office Productivity Suite could be used by all employees in the business for collaboration and document creation, spreadsheet analysis and slide presentations. The leading SaaS provider in this area is Microsoft through its Office 365 Suite. On the Customer Relations Management application the global leader is Salesforce. Most small and medium sized businesses depend on SaaS. The cloud service removes the need for the business to worry about all the details in managing an information system. Instead, the business is able to enjoy the benefits of all computing features and the cloud service provider has the responsibility to make the computing infrastructure available to the business. This model is suited for any business that does not have computing expertise to manage a network and associated services. SaaS accounts for a significant portion of the cloud services revenue. Forrester Research study (O'Neill, 2011) points out the SaaS revenue will grow from $21 billion in 2011 to $93 billion by 2016. At that time the SassS market is expected to be saturated with all the important applications for the customer. Major SaaS providers are Amazon Web Services (AWS), Microsoft, Google and Salesforce. The small and medium sized businesses embrace SaaS.

PaaS stands for Platform as a Service. In order to use this service a business needs to have people with sufficient computing expertise. Unlike SaaS, a PaaS customer has slightly better control over the service platform they use in the cloud. This type of service is popular with developers who need to test their services across multiple platforms such as various versions of Windows, Mac, Linux and Unix operating systems. The cloud service provider makes available the infrastructure and the PaaS customer decides on what service platform they would need and the service provider makes that available. The customer is responsible for the types of applications that they run in these platforms. Once again the service provider will be able to offer the necessary applications on demand. Since the cloud computing model uses the pay-as-you-go model the customer pays only for what they use and they could increase or decrease their usage level because cloud service supports demand elasticity. Major PaaS providers are Microsoft Windows Azure, Amazon Web Services and Google. According to a Forrester Research study (O'Neill, 2011) the global PaaS market is expected to grow from $4 billion in 2013 to $12 billion in 2018 when it will reach its peak demand.

IaaS stands for Infrastructure as a Service. This service is most suited for large businesses only as the customer is expected to manage both the hardware and the software that run on these hardware. Large businesses manage their own information systems and may need additional infrastructure to test some of their applications in a controlled environment. In such situations they have the necessary computing expertise but lack the infrastructure. This is the kind of need that IaaS fills for large businesses. Once again the business is able to take advantage of using only what they need and paying only for what they use. The IaaS customer has full control of the hardware and the applications that run on them. Major IaaS providers are Amazon Web Services, IBM Softlayer, Rackspace and Verizon Terremark. The Forrester Research study (O'Neill, 2011) shows that IaaS is second in the revenue generation for global cloud service. IaaS is projected to peak in 2014 at $6 billion and then drop in demand. The overall annual global cloud computing market was worth $41 billion in 2011 and is expected to grow to $241 billion by 2020.

In addition to these three types of cloud services there are also four cloud deployment models. These are classified as public cloud, private cloud, hybrid cloud and community cloud. By very definition, in public cloud the customer will share the resources with other users. In other words, multi-tenancy is a standard feature of public cloud. This naturally raises the customer's concern about the security of their data. In a well-publicized paper Zhang et al showed that using side channel attack one could recover the encryption key stored in a different VM on the same physical server (Zhang, 2012). This was done in a laboratory setting but the concern is that multi-

tenancy is a cause for concern for many businesses. It is important to note that the public cloud is the largest of the deployment models with a market share of 70% followed by the private cloud at 24% (Greenbook, 2011). Private clouds allay customer concern about possible loss of data as the service is dedicated a single user and there is no multi-tenancy involved. However, private clouds are more expensive compared to public clouds and so many small and medium sized businesses may not be able to afford private clouds. An EMC^2 analyst points out that in the long run private clouds are cheaper than public clouds as the cost savings advantage of public clouds last only two years (Hollis, 2013). Major public and private cloud providers are Amazon Web Services, Microsoft, Google, Rackspace and Salesforce.

Literature Review for Trust in Cloud

Trust in cloud means that a customer is willing to use the services of an unknown third party to handle all their computing needs. This means that the customer is willing to let their sensitive data reside on a remote server that they do not own. Ever since cloud computing started growing many researchers have addressed the issue of trust in the cloud. A brief look at ten different papers shows that customers are willing to use the cloud for all its benefits in spite of some reservations that they may have about security and trust the service provider to take adequate steps to protect their data. Habib et al considered various aspects of trust and concluded that trust has to be earned (Habib, 2012). Josang et al. study the impact of trust and reputation for online provisioning (Josang, 2007). One of the major concerns in cloud computing is the information leakage because of multi-tenancy and many customers using the same SaaS application. Ristenpart et al looked into the impact of multi-tenancy and how information leakage could occur in such an environment (Ristenpart, 2009). This work is often cited as one of the major reasons for concern for public cloud customers.

One of the organizations that is working hard to make the cloud service succeed in its goal is Cloud Security Alliance (CSA), a non-profit organization. CSA has produced several position papers that explain the steps that a customer could take to address their security concerns. One such position paper deals with the concept of Controls Matrix (Cloud Security Alliance, 2011). This concept is widely used by the major cloud service providers so that customers could verify for themselves the security features that are built-in the cloud service for enhancing their trust. Another important contribution of Cloud Security Alliance is its Security, Trust and Assurance Registry. The primary goal of this Registry is to record the security practices of the cloud service providers that customers could visit and check prior to subscribing to the cloud service with that vendor (CSA STAR, 2011). Major cloud service providers Amazon Web Services, Google, Microsoft, Intel, and Verizon all submit their security control practices to the STAR registry, thus enhancing its value for the potential cloud customers to look at the trust aspects of a service provider.

One of the things that a customer would want to know prior to subscribing for a cloud service is the quality of their web service. To measure this aspect Wang et al have developed a trust model that is easy to use (Wang, 2010). Another related work is the joint effort of Intel and Ubuntu to create trust in the cloud services. Their contribution is the creation of Trust Pools, which are launch platforms on which the launch process has been measured and verified to be trustworthy (Intel, 2013). Customers using such Trust Pools for launching their infrastructure needs on the cloud can feel confident that these devices have been tested and are trustworthy. IBM has contributed to the question of trust in the cloud through a Thought Leadership Whitepaper in which they emphasize eight questions that are important for consideration concerning security and trust (Coleman, 2010). These eight questions about the cloud service provider (CSP) are:

1. What types of controls are in place at the CSP?
2. Where is the cloud service located?

3. Where will the data be stored?
4. Who all have access to the cloud management layer?
5. How resilient is the cloud?
6. How does the CSP handle data backup on the cloud?
7. How is audit performed for security?
8. How is the CSP security team involved in security upkeep?

Cloud is well-known for supporting many mobile applications. It has become an essential part for all cloud service providers to have a mobile presence. With mobile devices the security becomes difficult as the devices do not have the high powered resources for validation and authentication such as a strong encryption scheme. However, since customers demand the convenience of mobile devices major companies such as Apple, PayPal and Google have developed alternatives to Point of Sale (POS) transaction with a card swipe. This new approach depends on the reliability of the phone and its communication provider. Thus, a new trust scenario is being developed for mobile payments (Thales, 2012). Cachin and Schunter analyzed the implications of using cloud and how the users could trust such service providers (Cachin, 2011). Thus, the topic of trust and security in the cloud has received plenty of attention in the published literature over the years.

Building Trust

In the above sections we have laid the foundation for considering the question of building trust for the cloud customer. We will examine in detail several factors that will contribute to such trust building for cloud services. Our hypothesis is as follows:

> *Cloud computing will grow in popularity and cloud service providers will benefit by enhancing trust in their services.*

We will establish the validity of this hypothesis through several best practices and secondary analysis of global business surveys. The most important aspect of trust in a cloud service comes from its reliability. This implies that the service provider is able to guarantee service availability through Service Level Agreement (SLA) and provide documentation to show that their service would be available when the customer needs it. Customers realize that when they manage their own computing services there are service disruptions. So a service outage in itself is not a trust breaker but it should follow the guarantees in the SLA. Typically cloud service providers offer SLAs at 99.9% availability, which translates to a total downtime of at most 9 hours per year. Certain cloud service providers may tout 100% or 99.99% availability of their service. These are unreasonable as the latter guarantee translates to a total downtime of only 52 minutes per year. Reality is that all major services have experienced significant outages over the past five years. An important trust builder is the communication with customers of the cause of the problem.

The second trust builder practice is to be transparent with the access control policies at the service provider level. By design the service provider manages the cloud infrastructure but does not own the customer data which resides in their servers. Customers need reassurance that at the service management level there are only a handful of privileged users who may have access to the customer data and that logs are available for anyone having access to customer data. The ability of the customer to have access to such a log on demand eases the concern that a rogue privileged user might have access to their data.

The third trust builder best practice would be for the service provider to have industry standard audit data. The prevailing such practice relates to SAS 70 Type II audit which validates the internal controls of the service provider along with validation of their claim for uptime. This standard has been strengthened to SSAE 16 Type II audit (SSAE, 2011). The fourth trust builder best practice would be for the service provider to have specific compliance certifications such as Health

Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), Federal Information Security Management Act (FISMA) and Payment Card Industry Data Security Standard (PCI-DSS). These certifications would enable the customer meet their compliance requirements. In this regard the service provider should make available several types of log data for customer to access on demand.

Service providers understand that customer trust is earned and that they should strive to maintain the trust once earned. One way to earn the trust initially would be to associate themselves with other trusted entities. For example, major multinational corporations such as Amazon Web Services, Microsoft, Google, Apple and Salesforce have earned customer trust over many years of reliable service. Even these services partner with other best-of-breed providers for specific aspects of their service such as associations with Cisco and RSA. The main trust builder is transfer of trust from several trusted entities in parts rather than as a whole. Thus, businesses could enhance their trust standing with customers by having some services such as security provided by trusted companies like McAfee. One of the best ways of building trust is by association with the customer. However, in cloud computing this is not possible in most instances prior to the initial service experience. But, customers place trust in organizations that have a good reputation. Thus, reputation of the organization is one aspect of trust.

Cloud Security Alliance (CSA) is an industry consortium that develops security standards and best practices. Its members include all the major cloud service providers – Amazon Web Services, Google, Microsoft, Rackspace, Salesforce, IBM and Cisco. In 2011, CSA developed a new Registry called Security, Trust and Assurance Registry (STAR). The main goal of STAR is to provide in one source the security policies and practices of cloud service providers. All the members have included their policies in this Registry so that the potential cloud customer could check this one single source and obtain the necessary information they need. Since CSA enjoys the reputation of being impartial in its security assessments and advisories, STAR would be a good source to build and maintain trust for a cloud service provider. Cloud Security Alliance has also developed Cloud Control Matrix in which one can find information about the business' compliance with industry-accepted security standards, control frameworks, audits and regulations.

Along these lines in which a neutral third party has developed measurement metrics that can be used to judge the potential cloud service provider. The first of this kind is the Service Measurement Index (SMI) from the Cloud Commons project which provides a set of business-relevant Key Performance Indicators (KPIs) (Cloud Commons, 2011). The second is the Consensus Assessment Initiative Questionnaire (CAIQ) from CSA. Responses found in this questionnaire enable the potential customer to assess the cloud service provider attributes such as compliance with standards like HIPAA, security and governance policies. Any cloud service organization that is not already well established has several of these avenues to establish trust with customers. Based on the things that are under the control of the cloud service provider and the specific data stored in the STAR registry as well as in the SMI with Cloud Commons, we can conclude the validity of the hypothesis.

Cloud Outages

As discussed in the previous section, cloud outages affect customer trust. When a cloud service such as Google's Gmail is unavailable for any brief period of time its impact is huge. All major cloud service providers offer services that are used globally and so the service spans all time zones. Furthermore, users have the ability to access the services on their mobile devices. Consequently service availability all the time becomes critical. The service providers will be able to maintain customer trust in their service if they communicate with the user base during outages and explain the cause of the outage and steps taken to remedy them. Only a few service providers have been forthcoming in this aspect.

In this section we will briefly discuss the major outages only and the known causes for several of the outages. Amazon Web Services (AWS) is the largest cloud service provider in the world. Its cloud service usage is five times larger than the total cloud usage of the 14 cloud service providers combined, listed in Gartner's Cloud Magic Quadrant (Gartner, 2013b). It has had several service outages during the last five years due to human error or power interruption due to natural causes such as hurricanes. Its 2011 outage lasted over three days and it clearly did not meet its uptime guarantee. It affected several other major businesses such as Pinterest and Flickr as well because they depend on AWS. Google had a 30-hour service outage in email in 2008 and several other smaller duration outages since then. The problems were traced to human error. Microsoft Windows Azure had multiple outages during the past five years. Some of the reasons offered by Microsoft shows that even large companies are vulnerable to simple mistakes. In the case of Microsoft one outage was due to a programming error that did not take into account the leap year in 2012. In another instance, Microsoft failed to renew its security certificate in time which caused the other systems to reject Microsoft connectivity.

Rackspace is a large global cloud service provider who prides in providing best customer service to its clients and named their service as Fanatical Support. Their SLA touts 100% availability of their systems. But, it had multiple outages during the last five years, some due to human error while others were due to power disruption for extended periods of time. Dropbox is a pioneer in cloud storage service for customers to share files over the cloud. Dropbox service is used by over 200 million customers worldwide. It stores over one billion files daily. With over 10,000 servers, Dropbox stores all file metadata in these servers and store the actual files in Amazon Web Services S3, a storage service offered by AWS. This arrangement of file storage shows that if either Dropbox servers or AWS S3 service has a problem then Dropbox becomes unavailable. Such a situation happened multiple times over the past three years for short durations. Unfortunately Dropbox did not reveal the cause of the problem thereby making it difficult for the customer to trust Dropbox. This has resulted in Dropbox losing several business customers to rival service providers such as Box. Other cloud service providers who experienced outages include Salesforce, Apple, VMware and EMC^2. This discussion shows the importance of keeping customers informed during outages so that trust is enhanced.

Conclusion

Cloud computing is a rapidly growing global technology. Amidst the growth cloud computing is also experiencing serious customer concerns about security. Major service providers such as Amazon Web Services continue to thrive in the cloud market. The analysis shows that trust is essential to attract more customers. We discussed the ways a cloud service provider could enhance the trust. In this context the role of third party providers such as the Cloud Security Alliance is proving to be important. We discussed some additional tools available for potential cloud customers to evaluate the cloud service providers based on their STAR registry information and their Service Management Index Cloud Commons information. As a service cloud computing will continue to attract customers but at the same time it has to earn customer trust. We pointed out the challenges in maintaining customer trust amidst the many cloud outages. In spite of the many challenges in managing the trust, the service provider has many ways to enhance and maintain customer trust. This analysis enabled us to validate our hypothesis that cloud service providers will benefit from trusted service offering.

References

Cachin, C., & Schunter, M. (2011). A cloud you can trust. *IEEE Spectrum, 48*(12), 28-51.

Cloud Commons. (2011). *Service Measurement Index*. Retrieved 1/15/14 from http://www.cloudcommons.com/about-smi

Cloud Security Alliance. (2011). *Cloud Controls Matrix*.

Coleman, N., & Borrett, M. (2010). *Cloud security – Who do you trust?* IBM Thought Leadership White Paper.

CSA STAR. (2011). *Security, Trust & Assurance Registry*.

Gartner. (2013a). *Cloud revenue forecast report*. Retrieved 1/15/14 from http://www.gartner.com/newsroom/id/2352816

Gartner. (2013b.) *Comparison matrix for cloud infrastructure as a service provider*.

Greenbook. (2011). *Private vs. public cloud: Which is the next big thing?* Retrieved 1/15/14 from http://www.greenbook.org/marketing-research/private-vs-public-cloud-40073 Retrieved 1/15/14

Habib, M., Hauke, S., Ries, S., & Muhlhauser, M. (2012). Trust as a facilitator in cloud computing: A survey. *Journal of Cloud Computing: Advances, Systems and Applications, 1*, 19-36.

Hollis, C. (2013). *When public cloud is not cheaper*. Retrieved 1/15/14 from http://chucksblog.emc.com

Intel. (2013). *Creating trust in the cloud*. Retrieved 1/15/14 from http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/creating-trust-in-cloud-ubuntu-intel-white-paper.pdf

Josang, A., Ismail, R., & Boyd, C. (2007). A survey of trust and reputation systems for online provision. *Decision Support Systems, 43*(2), 618-644.

O'Neill, S. (2011). Forrester: Public cloud growth to surge, especially SaaS. *CIO*, April 26. Retrieved 1/15/14 from http://www.cio.com/article/680673/Forrester_Public_Cloud_Growth_to_Surge_Especially_SaaS

Poenemon Institute. (2011). *Security of cloud computing providers study*. Retrieved 1/15/14 from http://www.ca.com/~/media/Files/IndustryResearch/security-of-cloud-computing-providers-final-april-2011.pdf

Ristenpart, T. et al. (2009). Hey, you, get off of my cloud! Exploring information leakage in third-party compute clouds. *Proceedings of the 16th ACM CCS*, 199-212.

Srinivasan, S. (2014a). Is security realistic in cloud computing? *Journal of International Technology and Information Management, 13* (1/2).

Srinivasan, S. (2014b). *Security, trust and regulatory aspects of cloud computing in business environments*. Hershey, USA: IGI Global.

SSAE. (2011). *SSAE 16 Type II Audit Standard*. Retrieved 1/15/14 from http://ssae16.com/SSAE16_overview.html

Thales. (2012). *Trust in the cloud or trust in the phone?* Thales e-Security White Paper.

Wang, S. X., Zhang, L., Wang, S., & Qui, X. (2010). A cloud-based trust model for evaluating quality of web services. *Journal of Computer Science Technology, 25*, 1130-1142.

Zhang, Y, Juels, A., Reiter, M., & Ristenpart, T. (2012). *Cross-VM side channels and their use to extract private keys.* ACM Digital Library.

Biography

S. Srinivasan (nickname Srini) joined TSU on August 1, 2013 as Associate Dean for Academic Affairs and Research as well as a Distinguished Professor of Business Administration. Prior to coming to TSU, I was the Chairman of the Division of International Business and Technology Studies at Texas A & M International University's A.R. Sanchez School of Business in Laredo, TX. I was there from 2010 to 2013. Before coming to Laredo, I spent 23 years at the University of Louisville (UofL) in Louisville, Kentucky. At UofL I held joint appointments in the Computer Information Systems Department in the College of Business and the Computer Science Department in the Speed School of Engineering. During my time there I started the Information Security Program as a collaborative effort of multiple colleges. I was Director of the InfoSec program until 2010 when I left for Laredo. The program was designated a National Center of Academic Excellence in Information Education by the National Security Agency (NSA) and the Department of Homeland Security (DHS). I successfully wrote several grant proposals in support of the InfoSec Program. My first book on Cloud Computing was published in March 2014. The second book on Cloud Computing is scheduled for publication in May 2014. My area of research is Information Security. I am now working on a new project on Big Data Analytics. I have taught the Management of Information Systems course at the MBA level in US as well as in our international programs in El Salvador and Greece. I have spent my sabbatical leaves from UofL in Siemens at their R & D facility in Munich, Germany; UPS Air Group in Louisville, KY; and GE Appliance Park in Louisville, KY. Besides these industry experiences, I have done consulting work with US Army, IBM and a major hospital company in Louisville, KY.