# Building Trust in Cloud: Service Certification Challenges and Approaches

Fahad Polash
Computer Science Department
The University of Memphis
Memphis, USA
mipolash@memphis.edu

Sajjan Shiva
Computer Science Department
The University of Memphis
Memphis, USA
sshiva@memphis.edu

***Abstract*— Cloud computing is a promising technology and its adoption is increasing rapidly. Still, many potential cloud customers are concerned about the security, privacy, and availability of their data in the cloud as they have less control over it. Cloud certification authorities can perform rigorous and thorough testing based on the well-known security standards procedures and make the audit reports public. Cloud customers can gain confidence by viewing those reports. However, the certification process for cloud services is more difficult than that of traditional IT services. In this paper, we have addressed the importance and challenges of the cloud service certification process and made a comparison among the cloud certification authorities which will enable potential cloud customers to evaluate the certification authorities.**

***Keywords—cloud; certification challenges; service provider; trust; certification approaches;***

## I. INTRODUCTION

Cloud computing has become a prominent paradigm in recent years. It has gained popularity among the IT world due to its ability to transfer the capital expenditure to operational expenditure [7]. A company can get access to high-end computing infrastructure of clouds by only paying for the duration of usage. It has other advantages as well: On-demand self-service, Broad network access, Resource pooling, and Rapid elasticity [1]. However, the cloud computing has also brought some vulnerabilities in addition to the existing security risks in traditional IT technology. According to Cloud Security Alliance (CSA) report [2], the number of cloud vulnerability incidents has increased from 33 in 2009 to 71 in 2011. A total of 172 unique cloud computing outage incidents were uncovered, of which 129 (75%) disclosed their cause(s) while 43 (25%) did not. This lack of transparency creates mistrust among the potential and existing cloud customers regarding their cloud service providers.

A survey to understand why people are not willing to adopt cloud services shows that the main reason that preventing them from the adoption of cloud computing is security [3]. People feel that whenever their data is on the cloud, it is more vulnerable to security risks. Their concerns come from the suspicion of the cloud provider's ability and honesty. In cloud computing technology, the customer's data, resources, application reside under the supreme control of the cloud provider. The customer needs to depend on the ability and honesty of the cloud service provider for the privacy, security, availability, and integrity of his data, resources and application. So, trust is an important factor for a customer to take the decision of migrating to cloud.

Since the cloud service providers handle personal information of customer, they have to prove the trustworthiness of their services. They should have convincible answers of some of the frequently arisen questions in customers' minds: Is data safe across all the cloud? Is the data handled by meeting the expectations of the customers? Is there enough redundancy and backup policy in the cloud to make the probability of data loss minimal? Does the customer have full control over his data throughout the lifecycle of data? Does the provider follow standard practices and rules to follow the privacy and security of data? The satisfying answers to those questions will build the trust of customers. So, here comes the need for the certification process. In cloud certification process, accredited authorities audit and verify the security properties of cloud services, and examine the standards and practices followed by the service providers. The customer can then choose the appropriate cloud service provider that meets his expectations.

The cloud computing market is growing rapidly as new service providers are entering into the market with new service offerings. Many of them are providing similar kinds of services. Service providers are competing among themselves to attract more customers by claiming the superiority of their services. However, it is pretty difficult for the customers to judge the quality level of those services. So, the cloud service certification organization can certify the cloud service providers to ensure customers that the providers are keeping up with standard and best practices. Many certification organizations are contributing in cloud service adoption by issuing certificates for the cloud service providers. In this paper, we present a comparative analysis of the existing cloud service certification organization. The rest of the paper is organized as follows: Section II presents the importance of cloud service certification, section III describes the challenges of cloud service certification, section IV provides the

comparative analysis of the cloud service certification organizations and finally section V concludes.

## II. IMPORTANCE OF CLOUD SERVICE CERTIFICATION

Certification is the process of confirming the quality or standard of a person, object or organization. The cloud service certification refers to the confirmation of the standards and best practices that are followed by the providers. Customers always have concerns about the privacy and security of their data in the cloud. A survey [4] conducted by Fujitsu Research Institute found that most of the potential customers have concerns about the accessibility of their data as depicted in Fig 1. Customers want more transparency about the incidents that are taken place behind the screen in the cloud. As there is lack of control and lack of visibility of customer's data in the cloud, it leads to suspicion and mistrust. To overcome this problem, there must be a mechanism by which the customer can be assured of proper handling of his data in a secured way. Cloud service certification is such a technique which can bring confidence among the customers. Cloud certification can help increase the cloud adoption in the following ways:

- **Customer Confidence:** Will the cloud service providers that hold the certificates of certification authorities be able to gain customer confidence? In fact, the customer should have more trust in the certification authorities than cloud service providers, only then the certification will be meaningful in gaining trust [5].
- **Selection of Cloud Service Provider:** With the increase of popularity of cloud computing, many players are entering into the market. So, it is somewhat difficult for the customers to choose the best cloud service provider. As the certification infers the level of standard and quality of cloud service providers, the customer can choose the suitable cloud service provider.
- **Improvement of Service Delivery:** In order to survive in the competitive market, the cloud service provider will try to be certified by a well-accepted cloud service certification authority. To achieve this, the cloud provider has to maintain the standard and quality of his service. Ultimately, this will raise the overall cloud service delivery standard of cloud computing market.
- **Development of Common Standard and Language:** Cloud computing technology is still young and common standards and languages to describe the service offerings and their properties have yet to be built [6]. As a result, service providers are deploying their own standard and using their own language to describe their service offerings. This confuses the customer while comparing different service providers. When all the cloud service providers go for certification, the certification authority can force them to follow a common standard and vocabulary to advertise their services. In this way, it would be easy to build a common standard and technological vocabulary for cloud computing paradigm.

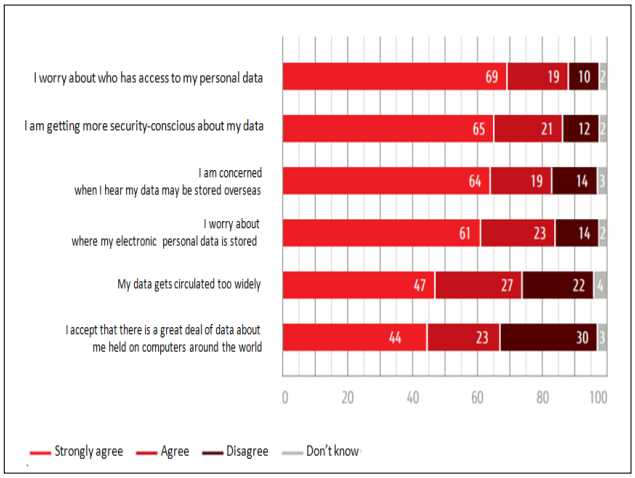


Fig 1. Current fears and concerns about access in data in cloud [4]

- **Less time in Cloud Service Adoption:** Some customers are very knowledgeable about cloud computing and they are very much conscious about their data security. So, in order to procure any cloud service, it is natural that they will try to verify themselves about the claims of the service offerings made by the cloud service providers. However, it is a time consuming process. If certification or audit report is available in the market for that cloud service provider, then the customers can rely on the report. And thus, the customer can adopt cloud computing technology quicker.
- **Elimination of repetitive verification of Cloud offering claims:** Potential cloud service customers will go for the verification of the provider's claims before service adoption. If each of every customer does the verification individually, then it will just be repetition of the same work. Instead of it, if any expert certification authority certifies the cloud service providers and put the audit report in a public repository, then it will save time and effort both for the cloud service providers and potential cloud service customers.

## III. CHALLENGES IN CLOUD SERVICE CERTIFICATION

The cloud service certification will definitely bring confidence among the customers and thus help remove the barrier in going forward with cloud computing technology. However, the certification process of cloud service providers is more difficult than that of ordinary IT service providers. It is because of the dynamic nature of cloud computing. The characteristics that made cloud computing promising also brought some potential risks with them. Those characteristics also made the cloud service certification difficult. In the following we present some of the challenges:

- **Minimal human intervention:** In cloud computing technology, it is desirable that almost all the activities are performed in automated fashion. As a result, there will be less control over data and application in the

cloud. This makes the evaluation of cloud system more difficult. And so the certification process is difficult.

- **Location Independence:** The cloud computing infrastructure of a cloud service provider might be scattered all over the world. So, if the auditors/certifying authorities need to visit the site, it requires some legal procedures, travel time, and extra expenses. This will eventually make the certification more challenging in cloud computing. Moreover, laws are different in different countries. So, it might be the case that one data center that is compliant to the laws in one country might not be compliant to the laws in another country although it follows the same standard practices.
- **Cost for small and medium sized cloud service providers:** If the certification becomes comprehensive, rigorous, and requires on-site auditing, then the cost of certification becomes higher. As a result, it sometimes becomes expensive for potential small and medium scaled cloud service providers. And thus it demotivates small and medium scaled cloud service providers to enter into the market. Ultimately it hinders the rapid growth of cloud computing technology. On the other hand, we need a reliable certification scheme to gain the confidence of cloud service customers. So, two opposing interests are working here and making the certification process more challenging.
- **Increased cost for the cloud service consumers:** As the certification process in cloud computing is more complex, it is time consuming and expensive. So, in order to be profitable, the cloud service providers need to increase the cost of cloud service consumption. It will affect the overall cost for cloud service customers.
- **Reliability of the certification authority:** Already a good number of cloud service certification authorities are providing the cloud service provider certification services. It sometimes creates confusion among the customers, which certification authority is better, which certification authority is more reliable. Sometimes, the auditors might be dishonest and take bribe from cloud service providers and present false certification. So, proper audit mechanism should be followed in the certification procedure.
- **Certification validity period:** Most of the exiting certification schemes have a validity period. That means, the certificate will be effective for a limited period. The cloud service providers have to renew it whenever it expires. There are two factors to be considered: 1) if the validity period is too short, then the cloud service providers have to spend money to re-certify again. 2) If the validity period is too long, by this time many changes will take place in the service offerings of the providers as cloud computing is a rapidly evolving technology [7] and the certification of the provider might no longer confirm the standard of the services. So, finding suitable validity duration is a challenging task in cloud certification process.
- **Change of Environment:** Cloud computing environment changes dynamically. To certify accurately, the certification authorities need to simulate all possible checking in all environments. But it might not be possible to get all available variations of the environment in the cloud service provider's site. For example, customer data need to be transferred from the cloud service provider to a third party subcontractor. This requirement might come into the cloud dynamically. The third party subcontractor might not have any certification. So, there might be an issue of data leakage which ultimately destroys the faith of customer.
- **Shared Responsibility:** In cloud computing paradigm different types of actors (e.g. cloud service provider, customer, auditor, and broker) have important roles to play. If any of the actors is unable to perform his job rightly, the cloud service might malfunction. For example, if the customer does not pay attention in recruiting honest employee as his system administrator or the system administrator does not perform his maintenance job properly, the cloud service for that specific customer might collapse though the service provider is certified. So, customer also should be knowledgeable.

## IV. APPROACHES IN CLOUD SERVICE CERTIFICATION

### A. *Dynamic vs Static Approach*

Traditional certification schemes audit the cloud services and issue certificate after the completion of the auditing job. The certificate remains valid for a certain period. Within this period, normally the cloud service is not being monitored by the certification authorities continuously. But, due to the rapid evolving nature of cloud computing, it is desirable to monitor the certified cloud service continuously so that any violation of the expected value of a property can cause the revocation of the certificate. Windhorst et al. [8] proposed a dynamic certification approach for cloud services. The dynamic certificate should have the following properties:

*1) The certificate should be machine-readable.*

*2) The certification scheme should monitor the certified cloud service continuously.*

*3) The composition of services from its service components should be performed by checking the certificate of the component services.*

*4) The certification process should be automated.*

A current research project [9] CUMULUS (Certification infrastrUcture for MUlti-Layer cloUd Services) is aiming at developing a certification infrastructure for the certification of IaaS, PaaS and SaaS services. Their framework consists of three models: 1) Test based certification – evidence of service property is collected after the execution of the test procedures, 2) Monitoring based certification – evidence is collected by

monitoring the service during its execution, 3) TPM (Trusted Platform Module) based certification – evidence is collected based on the lower layers of the cloud and on the function set of a TPM.

### B. *Security Measures Standards*

Certification authorities usually devise their auditing methodologies based on existing popular and wide-accepted audit frameworks. The most popular audit framework in the field of information technology is ISO27001. Most of the countries of the world get the recommendation of security controls from ISO27001. ISO 27001 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System (ISMS) within the context of the organization's overall business risks [10]. Some of other audit frameworks are: COBIT, Federal Information Security Management Act (FISMA), NERC Reliability Standards, ISPS Code, HIPAA, Sarbanes-Oxley (SOX), Trust Services, PCI-DSS, BASEL II, BSI-IT Grundschutz, and CESG. Along with one or more of these audit frameworks, each of the certification authorities has their own policies and methodology to assess cloud service providers.

### C. *Comparison among the Cloud Certification Schemes*

Many certification authorities are issuing certificates for cloud service providers. To gain the confidence of customers, sometimes many cloud service providers obtain more than one certificate though it is expensive. We have surveyed existing certification authorities and given an analytical comparison among them in Table I [11]. Some of the certification organizations are popular in Europe (e.g. EuroCloud), some are popular globally (e.g. CSA). Some of the organizations are nominated by the government and all the service providers must be certified through that organization to get a contract from the government. For example, any cloud service provider willing to get a contract from the federal government of USA, must be certified by FedRAMP [12]. In order to compare among the certification schemes, we have focused on some of the attributes: governing organization – the organization that devises the policy and rules-regulations for the certification, certified services – the types of services that are certified by the certification, static or dynamic – this property specifies if the certification evaluation scheme is automated and monitor the certified service always, standards – the audit frameworks that are followed by the certification authority, expiration – the validity period of the certificate, continuous monitoring – it specifies whether the certified service is being monitored on regular basis, and current adoption – it specifies how many organizations have been certified by the certification authorities. From this comparison, the potential customers will understand the differences among the certification schemes. This will help the customers to choose cloud service providers. From the comparison table we have the following observations:

*1) The number of adopted organizations for PCI certificate is higher, but the PCI certificate scheme only certifies Payment Card Service Providers, it is not generic and not dynamic.*

*2) CSA Start certification is the generic one and it is most popular worldwide but not dynamic.*

## V. CONCLUSION

The cloud service certification plays an important role in wide adoption of cloud computing technology. The more reliable and authentic process will be taken by the certification authority to certify cloud service providers, the more confidence customers will have to adopt cloud services. The cloud service certification will increase the trust among the cloud service customers. In this paper, we have outlined the importance and challenges that are faced in the cloud service certification process. We have also given comparison among the existing cloud service certification authorities which will help customers to judge the acceptability of a cloud service certification scheme. We can conclude that a dynamic cloud certification process is desirable to meet the challenges of cloud certification process.

## REFERENCES


[1] Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.

[2] Ko, S. R., & Lee, S. (2013). Cloud computing vulnerability incidents: A statistical overview.

[3] IDC (2009) Enterprise Panel, September. http://www.slideshare.net/JorFigOr/cloud-computing-2010-an-idcupdate

[4] Fujitsu Research Institute (2010) Personal data in the cloud: A global survey of consumer attitudes. http://www.fujitsu.com/downloads/SOL/fai/reports/fujitsu_personaldata-in-the-cloud.pdf

[5] Cimato, S., Damiani, E., Zavatarelli, F., & Menicocci, R. (2013, June). Towards the certification of cloud services. In Services (SERVICES), 203 IEEE Ninth World Congress on (pp. 92-97). IEEE.

[6] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: State-ofthe- art and research challenges," *J. Internet Serv. Appl.*, vol. 1, no. 1, May 2010, pp. 7–18.

[7] Srinivasan, S. Building Trust in Cloud Computing: Challenges in the Midst of Outages.

[8] Windhorst, I., & Sunyaev, A. (2013, September). Dynamic Certification of Cloud Services. In Availability, Reliability and Security (ARES), 2013 Eighth International Conference on (pp. 412-417). IEEE.

[9] Cimato, S., Damiani, E., Zavatarelli, F., & Menicocci, R. (2013, June). Towards the certification of cloud services. In *Services (SERVICES), 203 IEEE Ninth World Congress on* (pp. 92-97). IEEE.

[10] Fenz, S., Goluch, G., Ekelhart, A., Riedl, B., & Weippl, E. (2007, December). Information security fortification by ontological mapping of the ISO/IEC 27001 standard. In Dependable Computing, 2007. PRDC 2007. 13th Pacific Rim International Symposium on (pp. 381-388). IEEE.

[11] Cloud Computing Certification - CCSL and CCSM. https://resilience.enisa.europa.eu/cloud-computing-certification

[12] Council, I. A. (2012). Federal Risk and Authorization Management Program (FedRAMP).

TABLE I: COMPARISON AMONG CLOUD SERVICE CERTIFICATION SCHEMES

| Certification Name | Governing Organisation | Certified Services | Static or Dynamic | Standards | Expiration | Continuous Monitoring | Current Adoption |
|---|---|---|---|---|---|---|---|
| Certified Cloud Service - TÜV Rheinland | TUEV Rheinland | SaaS, PaaS, IaaS | Static | Requirement catalogue for Certified Cloud Service of TÜV Rheinland (based on *ISO 27001, NIST recommendation*) | Every 3 years | Yes | 8 (Mainly in Germany and Europe) |
| EuroCrloud Star | EuroCloud Europe | SaaS, PaaS, IaaS | Static | EuroCloud Guideline Law, Data Privacy and Compliance, EuroCloud Data Privacy Guide (based on ISO 20000,ISO 27001, ISO 27018, ITIL V3, Data Center Star Audit) | Every 2 years | Will be integrated from 2015 | 4(Mainly in Europe) |
| CSA Star | Cloud Security Alliance (CSA) | SaaS, PaaS, IaaS | Static | Cloud Controls Matrix and ISO/IEC 27001:2013 | Every 3 years | Yes | 92(Globally) |
| PCI Certificate | Payment Card Industry Security Standards Council (PCI SSC) | SaaS, PaaS, IaaS | Static | Payment Card Industry (PCI) Data Security Standard, v3.0 | Every 1 year | Yes | More than 130 (Globally) |
| AICPA Certificate | American Institute of Certified Public Accountants (AICPA) | SaaS, PaaS, IaaS | Static | Assurance Services Executive Committee (ASEC) Guidance. | Yes(Issued either at a moment or covering for a period) | No | Data Not Available |
| Truste Certificate | TRUSTs | SaaS, Paas, IaaS | Static | Privacy Program Requirements | Every 1 year | Yes | Data Not Available |
| FEDRamp | US Government | Iaas, PaaS, SaaS | Static | NIST SP 800-53 security control baseline | Every 1 year | Yes | 15 |
| Security Rating Guide | Leet Security | SaaS, PaaS, IaaS | Static | Leet Security Guide (based on OWASP,ANSI942,CERT Res Mgmnt,95/46/EC,DataCenter Tier Std,ISO27k,NIST SP800-*53,PCI-DSS,SSECMM*) | Every 1 year | Yes | 3 |