International Journal of Natural Computing Research
Volume 9 • Issue 1 • January-March 2020

Certification Attainment - A Gizmo to Evaluate Provider's Trust:

Trust Evaluation is Grounded on Provider's Attainment Status Concerning Recommended Certifications

Archana B Saxena, Jagan Institute of Management Studies, JIMS, Delhi, India
Meenu Dave, JaganNath University, Chaksu, Jaipur, India

ABSTRACT

The relevance and recompense offered by cloud services make it obligatory for researchers to address the issues faced by this paradigm. The two major issues faced by this fast growing and most rising technology of the last one and a half decades is trust and security. Although the literature has witnessed and practiced a lot of models that can address these issues, despite the efforts, a sharp increase can be seen in data leakage incidences and its leads to hamper trust of the consumers in the cloud services and service providers. In order to remove the obstacles that are hampering the growth of the technology. The authors have tried to work on the areas which are not yet explored to solve the trust problem which is an indirect outcome of security lapse instances. The idea is to utilize the power of certifications or implications of the following standards or working according to the guidelines mentioned. The objective of this research article is to analyze the service provider on these aspects and generate its trustworthiness.

KEYWORDS

Certifications, Cloud Computing, Cloud Service Provider, Cloud Services, OTF, Overall Trust Factor, Standards, Trust, Trust Factor

INTRODUCTION

Cloud Computing: The hottest buzzword on the internet and fastest growing technology of the decade were coined somewhere two decades back. This Paradigm came in the picture when major giants like Google and Amazon wanted to describe a model where people will use more of internet and web for their IT related tasks. While backtrack from this period you can also trace coinage of this term in the mid-'90s when Netscape Navigators was in use. Cloud Computing has been searched around 50 million times on the internet and one of the most searched topics on Google scholar as well (Regalado, 2011). This new fancy term is actually based on some few old technologies. Precursors of this technology are Time-sharing, Peer to Peer and client-server technology, Grid Computing, Utility Computing, Virtualization, SOA, etc (Lee-Post & Pakath 2014). Cloud Computing gained popularity among masses because of its features like no upfront investments, low cost, scalable as per needs, easy to use and no maintenance. (Zhang, Cheng, & Boutaba May 2010). Not only features make it's better, in comparison with other technologies but it offers services for almost every IT requirement;

DOI: 10.4018/IJNCR.2020010101

like IAAS for infrastructure related requirements, SAAS offers software solution, PAAS can offer various platforms as per the need of applications (Takabi, Joshi, & Ahn 2010). Except for service, other comforts that technology offers are: various deployment models as per requirements of the customers. Like; for extremely sensitive data: Private Deployment model, for normal data: Public deployment model. Combination of both(Public & Private) can also be used in the hybrid deployment Model (Jadeja & Modi 2012). These positive impact of technology is being hampered due to data breach incidences. Despite an increase in the security budget for cloud services, a sharp rise can be seen in data breach cases in the last year and the same trend will be followed in next few years (Data Breach In The Cloud – 2018 Trends That IT Pros Must Think n.d.) (Lewis, 2018). This upward trend of data breach cases is now living a mark on Trust.

Trust is considered a very important aspect for cloud services because of the architecture of the technology. This technology delivered the services from some remote locations that are under the control of the cloud service provider and practically not event known to the cloud service consumer when confidential data is in the hands of some unknown administrators, the concern of TRUST automatically arises. How much trustworthy is the provider who is taking care of data? How consistent is there working methodology? How reliable are there employees? How secure are their network boundaries and their internal procedures? All these questions go round and round in the mind of the cloud consumers. A survey result has deduced that 88% of the potential cloud consumers are concern about whom all can have access to their data (Khan & Malluhi 2010)?

There comes the need of a legal system that can safeguard the concerns of consumers who want to use the technology and contribute to the digital growth of the country. Being the most popular technology not only legal system but there are many private bodies that work for the betterment of the technology like CSCC (Cloud Security Customer Council), CSIG (Cloud Select Industry), STAR (Security Trust and Assurance Registry) and many more. These private bodies in concern with regional legal system issue guidelines, standards or certifications to protect consumers concern. It's is the responsibility of the consumers to be updated about such guidelines and keep them on the check before availing services from any provider. The objective of the author explores this angle and develop a tool base on the above-mentioned phenomenon and try to evaluate the trustworthiness of the cloud provider.

In order to explain the strategy being used in order to achieve the objective of this paper, contents are organized in following sections: Literature Review will be discussed the work done in this area and concluded with gaps find by the authors. These gaps are the basics of objectives formation, that the author would like to conclude through this paper. The methodology will discuss the steps taken by the authors to attain the objective. Implications of the study will explain how this work can help various stakeholders linked with the cloud computing paradigm. Future Scope will explore what can be done in the same area to refine the current search.

LITERATURE REVIEW

A vast literature concerning cloud, its services, models and features can be understood from various perspectives that authors have mentioned in their work (Armbrust et al., 2010; Qian et al., 2009; Lee-Post & Pakath, 2014). To understand the technology in deep it required to get a deep knowledge about the architecture of the technology (Jadeja & Modi, 2012) and especially the architecture of IAAS services which is the concerned areas of the authors (Moreno-Vozmediano, S. Montero, & Llorente, 2012). Term "Trust" is used with differential fields: life Finance, Medical, Law, Accounts, Education. Now a new field added in this list is Cloud. It is termed as "Cloud Trust" (Huang & Nicol, 2013). The area has been explored by many researchers and everyone has discovered some new dimensions of the term. Trust has defined with these four keywords: Control, Ownership, prevention, and security. Relation of all these in the trust is well explained through an image processing example. what is in the relevance of these words in data that is saved in the cloud (Khan & Malluhi, 2010). Another