Original Research Paper

Volume-9 | Issue-10 | October - 2019 | PRINT ISSN No. 2249 - 555X | DOI : 10.36106/ijar

Information Technology

# TRUST EVALUATION & ENHANCEMENT: AN APPARATUS TO GET COMPETITIVE ADVANTAGE

**Archana B Saxena** Associate Professor, Department of Information Technology Jagan Institute of Management Studies (JIMS)

**Dr. Meenu Dave*** Dean, HOD, Department of Computer Science jaganNath University, chaksu, Jaipur, Rajasthan *Corresponding Author

**ABSTRACT** The reparations offered by cloud computing, make it admired & accepted among enterprises and individuals. This IT paradigm has seen a sharp rise in the last one and half decade. At its infancy stage, this technology has changed every body's perception of storage, infrastructure, software installation, software support, and development. The credit goes to the architecture of the technology which makes it possible to offer premium resources at economical prices, scalability of resources depending upon requirements and the most important financials are based on usage. In this success & acceptance ride, technology also had its share of breakers Like security, Trust, Privacy. These hurdles are making current and future consumers hesitant about adopting the technology.

Along with technology growth, last few years have witnessed a sharp rise in security lapse cases. These incidences are raising questions about security & privacy of data and information and finally leaving marks on the "Trust" relation between service consumer and service provider. In order to strengthen the relationship with service consumer, it is the responsibility of the provider to endow consumers with secure enclosures to keep their data and information protected. Standards and certifications are considered as best practices for providing security assurances in Information Technology. The objective of the paper is to design a framework that can help the provider to overcome this un-trusty situation, by converting one of the hesitant factors "Trust" into competitive advantage component by attaining suggested certifications or adopting recommended standards.

**KEYWORDS :** Trust, Cloud Services, Competitive Advantage, Security, Trust Framework

## INTRODUCTION

Cloud Computing, a new way to practice Information Technology requirements, has received much attention from all over the globe for both personal use and business perspectives. The rapid expansion of the technology is the upshot of enormous advantages like Low cost, energy efficient, resource management, on-demand availability and many more that are associated with it[1]. It is the architecture of the technology which makes it feasible to achieve the above-mentioned advantages and give it a distinct position among various peer technologies. Cloud computing a relatively new technology is based on a few old technologies like Virtualization, SOA, Distributed Storage System, and internet[2]. Technology offers a service for every need, IAAS gratify provisioning of Infrastructure resources like Storage, Networking [Providers: Amazon EC2, GoGrid]. PAAS deals with platform related requirements like OS support, Development framework support. [Providers: Microsoft Azure, Google App Engine]. SAAS: offers on-demand applications over the internet. [Providers: Salesforce.com, SAP]. The services are offered, processed and delivered from data centers administered, maintained and executed by the providers. Nowadays this well groomed and beneficial technology is facing a major threat: Security. Security is a broader term that encompasses: data security, privacy policy, Authentication and authorization issues, hardware and software security and many more. All these lead to data leakage or disclosure of confidential information. These incidences have a direct impact on providers goodwill, trust, and competitive advantage. The consumer that has suffered monitory or information loss will try to shift the provider to avoid any further loss. The legal system and private bodies that work for the betterment of technology also works as a safeguard for both consumers and providers. Keeping the current theft cases in mind and as per the need of security, these bodies issues certifications, standards, and guidelines that the provider must adopt and attain to ensure the security of data and information. By following these instructions and guidelines, some trust can be generated or retained to get a competitive advantage over fellow providers.

### Research Problems and Gaps:

Cloud Computing being a successful technology even at its infancy stage, is an area of interest for current researchers. A lot has been written and discussed about Cloud **[2] [1]** : Its utility in government schemes [3][4], its services **[5][6]**, its architecture[7] , challenges faced by the technology [8] **[9]** and many more aspects of the cloud can be easily found in the literature. A discussion on trust models[10] like QOS based trust[11], SLA based trust[12], trust models to enhance security are an integral part of cloud computing literature. "Cloud Security" is loosely related with "Cloud Trust". The notion has been drawn by the authors during the literature review while reading the papers that co-relate security or trust or use security as a tool to enhance trust[13][14][15][16]**.** Despite such a good work related to security and trust, the following gaps can be found in the concerned literature :

- Security components leave an impact on Trust. What is the percentage (%)contribution of these components on trust is still a question that needs to address?
- Cloud consumers perception about the relevance of these components.
- The exhaustive list of recommended (By legal system and private bodies working for the betterment of Cloud Computing) standards or certifications related to these components.
- IT industry is regulated through standards and certifications, no trust framework computes, trustworthiness based on attainment of recommended standards and certifications.
- No trust framework that can give recommendations to the provider for improving their trust value.

## OBJECTIVE

Despite a 1.1% increase in federal IT budget for Financial Year 2018 ($95.7 billion) as compared to $94.0 billion for 2017[17]. A sharp rise can be seen in the number of data breach cases. The major breach can be seen in health and financial industry. The other sectors have also seen an increased rise in data theft cases. The number of records that were breached was considerably up by 14 million and in future also the trend will be upwards, as per predictions[18]. while working towards solutions and reasons behind breaches, it has been found that one of the prominent reason behind breaches is unauthorized access. Insiders, including employees or partners, are the main source of unauthorized access. This unauthorized access is due to sheer negligence or an intentional means. A survey also reports the same "**Employees are the biggest threat to data breaches**". [18][19]**.** In this scenario, it is quite obvious for the consumers to drop trust among the providers.

To get a competitive advantage of this un-trusted situation, it is advisable for the provider to do the things that can gain consumers trust in their services. The Providers that abide the government norms and follow guidelines are always welcome and appreciated among the consumers. Besides government, there are private bodies like CSIG (Cloud Security Industry Group), CSCC (Cloud Security Customers Council), CASB(Cloud Access Security Broker) that works for the betterment of cloud services. These bodies and legal systems issue

Submitted : 17th May,2019 | Accepted : 29th July,2019 | Publication : 01st October, 2019

guidelines for the safety of data and privacy policy and try to safeguard consumers. They also issue a list of standards and certifications that consumers must check before enrolling for the service.

The prime objective of this paper is to propose a framework that can evaluate the trustworthiness of the cloud provider depending upon standards and certifications attained by the provider. This tool will provide a double fold utility: one for the Cloud Service Consumer (CSC)and another for the Cloud Service Provider(CSP).

**Cloud Service Consumer**: The tool will display the trustworthiness of registered providers that can offer the services, consumers are interested in. The trustworthiness is calculated on the basis of standards and certifications recommended by the private bodies or legal systems to ensure security, governance, SLA and other factors that can impact the trust of a consumer.

**Cloud Service Provider**: This tool will also act as guiding note for the provider by displaying its OTF (Overall Trust Factor) and also recommending the list of standards and certifications they must attain to improve their trust value and get a competitive advantage among fellow providers.

The guiding list is drawn from data saved in the tool by comparing the recommended list and certifications attained by the provider.

## RESEARCH METHODOLOGIES

A structured approach is followed during the development of a trust framework that will calculate trustworthiness OTF (Overall Trust Factor) and give suggestions to both the stakeholders (CSC & CSP )of cloud Provider:

**Component Selection (Step1)**: The first pace is to collect the components that can have an impact on trust. the following sources have been practiced to gather components:

- Security puncture that can lead to data leakage.
- Guidelines (By legal system and private bodies) that directs consumers to ensure the security of data before availing cloud services.
- Authors own previous work related to loss of Trust[20].

**Components Contribution in Trust (Step2):** The subsequent step if to analyze the contribution of these components in terms of % on trust. This is completed through an online survey among cloud consumers. An online is distributed among free and paid cloud consumers. Collected responses are filtered and analyzed in the excel and SPSS to obtain results[21]. a brief of analyzed results are mentioned in the table below:

**Table1: Components and their impact percentage on trust.**

| Component | Percentage (%) Contribution in Trust |
|---|---|
| Security | 32% |
| Governance | 20% |
| SLA | 19% |
| Audit | 15% |
| Diverse | 14% |

**Recommended Certifications and Standards Related to Components (Step3):** Step3 comprises the listing of recommended standards and certifications related to these components. The list is prepared on the basis of guidelines issued by the private bodies and legal system **[22], [23]**. the data collected in both step2 and step3 is submitted to compute engine for the calculation of OTF (Overall Trust Factor).

**Recommendations (step4)**: OTF is compared with customers QoS (Quality of Service Requirements) through comparison engine. On the basis of this comparison, a recommendation list of trustworthy providers is generated for the consumer (By comparing Threshold with the OTF) and list of suggested certification or standards is generated for cloud service Provider to improve its trust value. This list can be very helpful for the provider to gain an extra point over its fellow providers.

**Figure 1: Execution of Trust Framework**

## IMPLICATIONS OF THE WORK

The results generated by the proposed framework will be beneficial for the both(Cloud Service Consumer & Cloud Service Provider ) the stakeholders.

**Cloud Consumer**: The tool will display the OTF value of the cloud providers that can offer the services, the consumer is interested in keeping a note of QoS requested by the consumer at the time of registration.

**Cloud Provider:** The cloud provider will register with a tool by filling the required details at the time of registration. Depending upon the details, the tool will generate a trust value for the provider. The recommendation section of the framework will be a great help for the provider if he/she wants to improve its trustworthiness. The tool will act as a guidance note for the provider and list the standards and certifications provider can incorporate to improve trust value among consumer.

## CONCLUSIONS AND FUTURE WORK

This framework will calculate trustworthiness for the provider depending upon availability of recommended standards and certifications related to components that can lead to loss of trust. In the future to improve the current work authors can use the fuzzy logic or deep learning algorithms in the prediction and threshold values.

## REFERENCES


[1] L. Qian, Z. Luo, Y. Du and L. Guo, "Cloud Computing: An Overview," in Conference on Cloud Computing, Beijing, China, 2009.

[2] A. Lee-Post and R. Pakath, "Cloud Computing: A Comprehensive Introduction," in Security, Trust and Regulatory Aspects of Cloud Computing in business Environment, Texas, USA, IGI Global, 2014, pp. 1-23.

[3] D. Vats and B. Kumar, "DIGITAL INDIA: AN INITIATIVE to TRANSFORM INDIA INTO A DIGITALLY EMPOWERED SOCIETY," International Journal of Science Technology and Management, pp. 543-547, 2017.

[4] "Cloud computing crucial to Digital India, need safe practices', say, experts," [Online]. Available: https://indianexpress.com/article/technology/tech-news-technology/cloud-computing-crucial-to-digital-india-need-safe-practices-4463667/. [Accessed 11th September 2018].

[5] D. Marinescu, Cloud Computing Theory and Practice, NewYork, USA: Elsevier, 2017.

[6] L. Wang, G. v. Laszewski, M. Kunze and J. Tao, "Cloud Computing: A Prospective Study," in Cloud Computing: Benefits, Risks, and Recommendations for Information Security, Berlin, Heidelberg, Springer, 2010, pp. 1-12.

[7] Y. Jadeja and K. Modi, "Cloud Computing - Concepts, Architecture and Challenges," in ICCEET- International Conference on Computing, Electronics and Electrical Technologies, Kumaracoil, India, 2012.

[8] K. Hashizume, D. G. Rosado, E. Fernández-Medina and E. B. Fernandez, "An analysis of security issues for cloud computing," Journal of Internet Services and Applications, pp. 4-7, 2013.

[9] M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in Cloud Computing: Opportunities and Challenges," Information Sciences, pp. 357-383, 2015.

[10] A. Jagtap, A. Kamanache, Y. Sharma and S. Rathi, "Trust model for Cloud Computing," VJER- Vishwakarma Journal of Engineering Research, pp. 251-254, 2017.

[11] P. Manuel, "A Trust Model of Cloud Computing Based on Quality of Services," Annals of Operation Research, pp. 1-12, 2013.

[12] M. Alhamad, T. Dillon and E. Chang, "SLA-Based Trust Model for Cloud Computing," in International Conference on Network-Based Information System, Takayama, 2010.

[13] W. Li and L. Ping, "Trust Model to Enhance Security and Interoperability of Cloud Environment," in First Internation Conference Cloud Com-2009, China, Beijing, 2009.

[14] P. S. Hada, R. Singh, and M. M. Meghwal, "Security Agents: A mobile Agent-Based Trust Model for Cloud Computing," International Journal of Computer Applications, pp. 12-15, 2011.

[15] H. Takabi, J. B. D. Joshi and G. J. Ahn, "Secure Cloud: Towards a Comprehensive Security Framework for Cloud Computing Environments," in 34th Annual IEEE Computer Software and Applications Conference Workshops, Seoul, South Korea, 2010.

[16] G. Yimin, G. Yajun, P. Fei and G. Huidan, "The Intrinsic Relationship between Security Mechanisms and Trust Mechanisms," in International Conference on Applied Informatics and Communication, Heidelberg, 2011.

[17] N. Lewis, "Federal-IT-budget-Look-for-security-cloud-spending-in-2018," 27 November 2018. [Online]. Available: https://searchitchannel.techtarget.com/feature/Federal-IT-budget-Look-for-security-cloud-spending-in-2018. [Accessed 27 November 2018].

[18] "Data Breach In The Cloud – 2018 Trends That IT Pros Must Think," [Online]. Available: https://www.cloudcodes.com/blog/data-breach-in-the-cloud.html. [Accessed 27 November 2018].

[19] "6 Top Cloud Security Threats in 2018," 13 Feburary 2018. [Online]. Available: https://www.tripwire.com/state-of-security/security-data-protection/cloud/top-cloud-security-threats/. [Accessed 27 November 2018].

[20] D. M. Dawe and B. A. Saxena, "Loss of Trust at IAAS: Causing Factor and Mitigation Techniques," in International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN 2017), Gurgaon, Haryana, 2017.

[21] B. S. Archana and D. Meenu, "IAAS service in Public Domain: Impact of Various Security Components on Trust," in International Conference on Information and Communication Technology for Sustainable Development ICT4SD 2018, GOA, INDIA, 2018.

[22] C. Baudoin and R. Devlin, "Cloud Security Standards: What to Expect and what to Negotiate Version 2.0," Cloud Standards Customers Council, 2016.

[23] "Cloud Service Level Agreement Standardisation Guidelines," CSIG Memebers, Brussels, 2014.

[24] N. Robinson, L. Valeri, J. Cave, T. Starkey, H. Graux, S. Creese and P. Hopkins, "The Cloud: Understanding the Security, Privacy and Trust Challenges," Cambridge, United Kingdom, 2010.

[25] S. Almulla and C.. Y. Yeun, "Cloud Computing Security Management," in 2nd Engineering Systems Management and Its Applications (ICESMA), Sharjah, United Arab Emirates, 2010.