Advances in Computational Sciences and Technology
ISSN 0973-6107 Volume 10, Number 8 (2017) pp. 2519-2525
© Research India Publications
http://www.ripublication.com

Trust Based Cloud Framework for Service Provider Selection

Neeraj Mangla[1], Sanjeev Rana[2] and Manpreet Singh[3]

[1.2]Department of Computer Science & Engineering, M. M. University, Mullana, Ambala, Haryana, India.

[3]Department of Computer Science & Engineering, M. M. University, Sadopur, Ambala, Haryana, India.

Abstract

The Cloud computing paradigm offers numerous benefits to both Cloud users and service providers. However, a lack of trust between these two stakeholders has delayed the worldwide acceptance of Cloud for outsourced facilities. In this research work, a trust management framework has been proposed for effective selection of Cloud providers to fulfil numerous Cloud users' requirements in a reliable manner.

Keywords- Cloud computing, Service Level Agreement, Trust and Reputation.

1. INTRODUCTION

Cloud computing gives cost-proficient chances for organizations by offering an assortment of dynamic, versatile, and shared services. An extremely dispersed and opaque nature of Cloud computing signifies a major hurdle for the acceptance of Cloud facilities. Probable clients of such Cloud facilities normally feel that they lost the control over their data, and they aren't assured whether they can trust the Cloud providers. A current study [1], accompanied among more than 3000 Cloud customers from 6 countries, shows that 84% of the customers are worried about their data storage place and 82% of the customers concern about who has access to their data.

Customer worries can be relieved by utilizing anticipatory actions for privacy and security. Currently, Cloud providers give affirmations by indicating specialized and practical descriptions in Service Level Agreements (SLAs) for the offered services. The descriptions in SLAs are not predictable among the Cloud providers despite the fact that they offer same type of services. In this way, clients are not certain whether they can distinguish a reliable Cloud provider just taking into account its SLA.

As the market is developing quickly with new providers arriving in the market, Cloud providers will progressively strive for clients by giving comparative functionality. Conversely, there can be vast alterations concerning the level of quality provided for such facilities. Such type of economical market desires the means to reliably survey the quality level of the service providers. Trust and Reputation (TR) frameworks [2] are effectively utilized as a part of various application situations to support clients in recognizing the reliable and trustworthy providers, e.g., eBay, Amazon, and mobile app markets. Existing TR frameworks depend on client advice without considering different sources and roots of information. Besides, there are extra constraints [3] that are compulsory to support the clients in selecting providers in a Cloud commercial environment. Consequently, TR frameworks need to develop into Trust Management (TM) frameworks as characterized in [4] to support the clients in creating transparent appraisals before picking reliable trustworthy Cloud providers [5].

2. LITERATURE SURVEY

Various models have been proposed in literature to resolve the trust-related issues. However, there is still scope of improvements regarding effective dynamic trust establishment in Cloud environment. Inferable from the dynamic nature of the Cloud, persistent checking on trust characteristics is important to authorize SLA.

The author [6] presents Cloud-Trust, a scalable trust service model for proficiently assessing the fitness of a Cloud service in view of its various trust properties. In this model for mining of trust related, data rough set and Induced Ordered Weighted Averaging (IOWA) tools are used. Utilizing rough set to find information from trust qualities makes the model outshine the weaknesses of conventional models, where weights are allocated subjectively. Also, Cloud-Trust utilizes the IOWA administrator to generate the global trust value using time series, in this manner empowering better real-time execution. The results demonstrate that Cloud-Trust merges more quickly and precisely than do existing methodologies, subsequently confirming that it can adequately tackle trust estimation tasks in Cloud computing.

The author [7] portray the configuration and execution of CloudArmor, a trust management architecture that provides Trust as a Service (TaaS) and incorporates i) a novel protocol to demonstrate the validity of trust feedback and safeguard clients' security, ii) a robust credibility model for measuring the credibility of trust inputs to

shield Cloud services from malignant clients and to make a comparison between the reliability of Cloud services, and iii) an accessibility model to deal with the accessibility of the decentralized usage of the trust administration. The plausibility and advantages of proposed methodology have been validated by a model and results generated using real trust inputs on Cloud services.

The susceptibility of Cloud Computing Systems (CCSs) to Advanced Persistent Threats (APTs) is a critical worry to government and industry. The author [8] presents a Cloud security evaluation model to determine the level of secrecy and integrity offered by a CCS or Cloud Service Provider (CSP). The model is utilized to survey the security level of four multi-tenant Infrastructure as a Service (IaaS) Cloud structures furnished with option Cloud security controls and to demonstrate the likelihood of CCS infiltration is high if a negligible arrangement of security controls are actualized. The invasion into CCS drops considerably if a strong security architecture is adopted to safeguard Virtual Machine (VM) images, reinforces CSP and Cloud tenant framework overseer access controls, and which also utilizes other system security controls to minimize Cloud system surveillance.

In recent times, workflow innovation has been utilized to develop composite services at more pace. Efficient and dependable Work Flow Scheduling (WFS) is essential for incorporating enterprise system. While WFS has been generally contemplated, WFS-related techniques are essentially centred on execution time or cost. In Cloud computing environment, WFS is up against the dangers of the intrinsic vulnerability and lack of quality to the applications. In order to manage this, the author [9] offered a trust service-oriented workflow scheduling algorithm. The scheduling algorithm embraces a trust metric that combines direct trust and recommendation trust. Along with it, the author provides balance approaches to empower clients to adjust diverse necessities, including time, cost, and trust.

3. PROPOSED TRUST MANAGEMENT FRAMEWORK

Trust evaluation module is used to calculate the trust value of a service provider based on the user's feedback (direct trust, recommended trust) and service provider credentials. Trust manager maintains the comprehensive trust value generated by trust evaluation module corresponding to each registered service provider in the trust repository as shown in Fig.1.

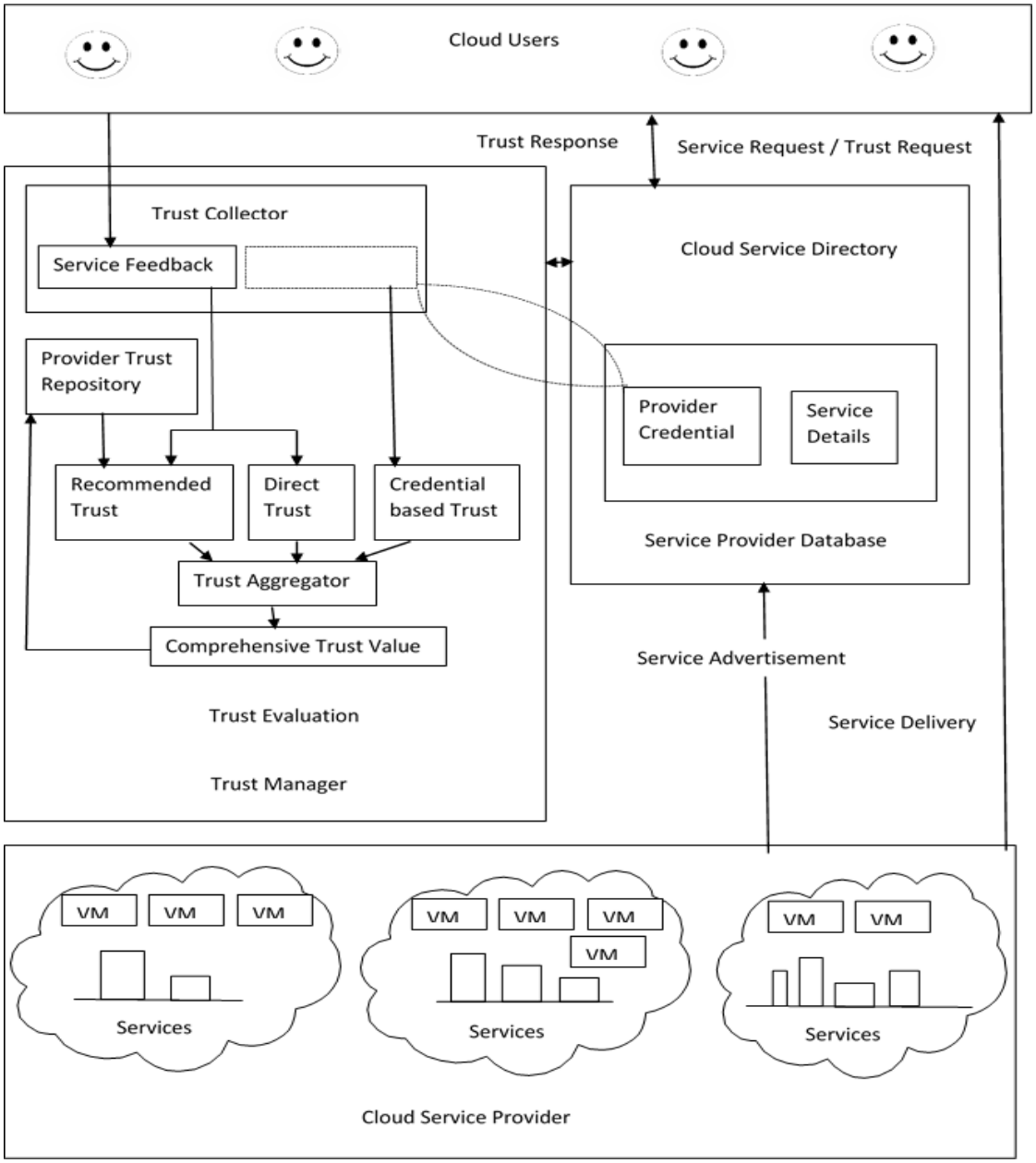

Fig. 1. Proposed trust based Cloud model for service provider selection

Cloud users refer to the trust repository through Cloud service directory in making decision regarding suitable Cloud service provider. Initially, Cloud service provider register themselves to the Cloud service directory providing details pertaining to all types of services offered along with their credential attributes.

4. TRUST EVALUATION

The comprehensive trust value of a service provider comprises of direct trust, recommended trust and trust based on service provider credential attributes.

4.1 Direct Trust: Direct trust (D_u^p) between Cloud user (C_u) and Cloud Service provider (S_p) is computed on the basis of direct interactions.

$$D_u^p = \begin{cases} \dfrac{\alpha_{up}}{\alpha_{up} + \delta\beta_{up}} \times T_u(t) & \text{where } \alpha_{up} \geq \beta_{up} \\ 0 & \text{otherwise} \end{cases}$$

α_{up} represents the number of successful service delivery cases by the service provider and β_{up} corresponds to failure due to wrong credentials of provider or non-attainability of specified Quality of Service (QoS) parameters. $\delta \geq 1$ is the punishment factor forcing the service provider to advertise authentic information.

The weightage of user feedback is related to time, the longer the time is the lesser is the reliable information available. Let $T_u(t)$ is a time delay function representing the weightage of u[th] Cloud user at time 't' then:

$$T_u(t) = \frac{1}{1 + \theta(t - t_i)} ;\ \theta \succ 0$$

Where θ is the time delay speed factor and t_i represents the time when i[th] feedback for same provider was given.

4.2 *Recommended Trust:* Recommended trust (R^p) for a service provider refers to the trust information obtained from other Cloud users which have interacted with the same service provider. It can be obtained by taking average of all Cloud users having experience with the services of service provider S_p .

$$R^p = \frac{\sum_{i=1}^{n} D_u^p}{n}$$

4.3 *Credential based Attribute Trust Information:* The important credential attributes of a service provider are availability, reliability, data integrity, and turnaround efficiency as given below:

- *Availability:* Availability (AV) is the degree to which the required services are accessible. Let α^p and β^p represents the number of service requests submitted to and accepted by S_p over a period of time T. So, the availability of S_p can be determined as:

$$AV^p = \frac{\beta^p}{\alpha^p}$$

- *Reliability:* Reliability (RE) of a service provider is measured in terms of successful completion of completed service requests. Let γ^p denotes the number of successful service delivery by S_p over a period of time T then reliability of S_p can be determined as:

$$RE^p = \frac{\gamma^p}{\beta^p}$$

- *Data Integrity:* Data Integrity (DI) refers to the security and privacy of data. Let ψ^p denotes the requests successfully served with desired data security by S_p over a period of time T, then data integrity of S_p can be determined as:

$$DI^p = \frac{\Psi^p}{\gamma^p}$$

- *Turnaround Efficiency:* Turnaround time is the time elapsed between submissions of service request to the successful service delivery. It is an important parameter incorporated in the SLA between service provider and Cloud user. Turnaround Efficiency (TE) of S_p can be evaluated as:

TE^p = (Promised turnaround time for a service in SLA) / (Actual turnaround time for the service)

Let w_1, w_2, w_3, and w_4 are the weights associated with AV, RE, DI, and TE respectively on the basis of priority of these attributes. The Credentials Attribute (CA) based trust of S_p can be evaluated as:

$$CA^p = w1 \times AV^p + w2 \times RE^p + w3 \times DI^p + w4 \times TE^p$$

Where $w_1 + w_2 + w_3 + w_4 = 1$

The Comprehensive Trust Value (CTV) of service provider S_p can be evaluated as:

$$CTV^p = \mu 1 \times D^p + \mu 2 \times R^p + \mu 3 \times C^p$$

Where $\mu_1 + \mu_2 + \mu_3 = 1$ and these weights are assigned on the basis of the priority.

5. CONCLUSION

The commercial sector of Cloud computing is growing quickly. New Cloud providers are entering into the business sector with vast investments and the well-known providers are putting millions into new data centres around the world. In vibrant and failure-prone enormous distributed systems, an absence of trust amongst big business and Cloud service providers frequently keep organizations away from completely receiving the Cloud services. In this research work, a TM framework for effective matching of Cloud facilities to fulfil numerous Cloud users' requirements is presented. Also an outline is made to compute the trust worth of any service provider based on the individual perception, collaborative decision and on the credential characteristics of provider itself.

REFERENCES

[1] Sato M., "Personal data in the cloud: A global survey of consumer attitudes", Minato-u, To yo., pp. 105-7123, 2010.

[2] A. Josang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," Decision Support Systems, vol. 43(2), pp. 618–644, 2007.

[3] S. M. Habib, S. Ries, and M. Muhlhauser, "Cloud computing landscape and research challenges regarding trust and reputation," Symposia and Workshops on ATC/UIC, vol. 0, pp. 410–415, 2010.

[4] A. Josang, C. Keser, and T. Dimitrakos, "Can we manage trust?" in iTrust. Springer, pp. 93–107, 2005.

[5] Li X, Ma H, Zhou F, Yao W., "T-Broker: A Trust-Aware Service Brokering Scheme for Multiple Cloud Collaborative Services. Information Forensics and Security", IEEE Transactions pp. 1402-15, July 2015, IEEE.

[6] Li X, Du J., "Adaptive and attribute-based trust model for service level agreement guarantee in cloud computing", Information Security, IET, pp. 39-50, Mar 2013, IEEE.

[7] Noor T, Sheng Q, Yao L, Dustdar S, Ngu A., "CloudArmor: Supporting reputation-based trust management for cloud services", 2015, IEEE.

[8] Gonzales D, Kaplan J, Saltzman E, Winkelman Z, Woods D., "Cloud-trust-a security assessment model for infrastructure as a service (IaaS) clouds", 2015, IEEE.

[9] Tan W, Sun Y, Li LX, Lu G, Wang T., "A trust service-oriented scheduling model for workflow applications in cloud computing", IEEE Systems Journal, pp. 868-78, Sep 2014, IEEE.