Selection of Cloud Service Providers

Sitaram Adarkar[1] Siddhesh Abnave[2] Dayanand Sanap[3]
[1,2,3]Student
[1,2,3]Department of Information Technology
[1,2,3]Padmabhushan Vasantdada Patil Pratishthans College of Engineering, Mumbai, India

Abstract— With rapid technological advancements, cloud marketplace witnessed frequent emergence of new service providers with similar offerings. However, service level agreements (SLAs), which document guaranteed quality of service levels, have not been found to be consistent among providers, even though they offer services with similar functionality. In service outsourcing environments, like cloud, the quality of service levels are of prime importance to customers, as they use third-party cloud services to store and process their clients' data. If loss of data occurs due to an outage, the customer's business gets affected. Therefore, the major challenge for a customer is to select an appropriate service provider to ensure guaranteed service quality. To support customers in reliably identifying ideal service provider, this work proposes a framework, SelCSP, which combines trustworthiness and competence to estimate risk of interaction. Trustworthiness is computed from personal experiences gained through direct interactions or from feedbacks related to reputations of vendors. Competence is assessed based on transparency in provider's SLA guarantees. A case study has been presented to demonstrate the application of our approach. Experimental results validate the practicability of the proposed estimating mechanisms.

Keywords: Cloud, Service provider, Trust, Reputation, Relational risk, Performance risk, Competence, Service Level Agreement, Control, Transparency

I. INTRODUCTION

CLOUD computing facilitates better resource utilization by multiplexing the same physical resource among several tenants. Customer does not have to manage and maintain servers, and in turn, uses the resources of cloud provider as services, and is charged according to pay-as-you-use model. Similar to other on-line distributed systems, like e-commerce, p2p networks, product reviews, and discussion forums, a cloud provides its services over the Internet. Among several issues that prevented companies from moving their business onto public clouds, security is a major one. Some of the security concerns, specific to cloud environment are: multi-tenancy, lack of customer's control over their data and application, lack of assurances and violations for SLA guarantees, non-transparency with respect to security profiles of remote datacenter locations, and so on. Recent advancements in computation, storage, service oriented architecture, and network access have facilitated rapid growth in cloud marketplace.

Support for customer-driven service management based on customer profiles and QoS requirements;

For any service, a cloud customer may have multiple service providers to choose from. Major challenge lies in selecting an "ideal" service provider among them. By the term ideal, we imply that a service provider is trustworthy as well as competent. Selection of an ideal service provider is non-trivial because a customer uses third-party cloud services to serve its clients in cost effective and efficient manner. In such a scenario, from the cloud customer's perspective, persisting to a guaranteed level of service, as negotiated through establishing service level agreement (SLA), is of prime importance. Data loss owing to provider's incompetence or malicious intent can never be replaced by service credits. In the present work, we focus on selection of a trustworthy and competent service provider for business outsourcing.

II. LITERATURE SURVEY

The authors JOSANG and S. L. PRESTI Analyzing the relationship between risk and trust stated that among the various human factors impinging upon making a decision in an uncertain environment, risk and trust are surely crucial ones. Several models for trust have been proposed in the literature but few explicitly take risk into account. This paper analyses the relationship between the two concepts by first looking at how a decision is made to enter into a transaction based on the risk information. They then drew a model of the invested fraction of the capital function of a decision surface. They finally defined a model of trust composed of a reliability trust as the probability of transaction success and a decision trust derived from the decision surface.

The authors R.ISMAIL, and C. BOYD stated that Trust and reputation systems represent a significant trend in decision support for Internet mediated service provision. The basic idea is to let parties rate each other, for example after the completion of a transaction, and use the aggregated ratings about a given party to derive a trust or reputation score, which can assist other parties in deciding whether or not to transact with that party in the future.

The authors stated that emerging digital environments and infrastructures, such as distributed security services and distributed computing services, have generated new options of communication, information sharing, and resource utilization in past years. However, when distributed services are used, the question arises of to what extent we can trust service providers to not violate security requirements, whether in isolation or jointly. Answering this question is crucial for designing trustworthy distributed systems and selecting trustworthy service providers. This paper presents a novel trust measurement method for distributed systems, and makes use of propositional logic and probability theory. The results of the qualitative part include the specification of a formal trust language and the representation of its terms by means of propositional logic formulas. Based on these formulas, the quantitative part returns trust metrics for the determination of trustworthiness with which given distributed systems are assumed to fulfill a particular security requirement.

The authors stated that Cloud services are becoming popular in terms of distributed technology because they allow cloud users to rent well-specified resources of computing, network, and storage infrastructure. Users pay for their use of services without needing to spend massive amounts for integration, maintenance, or management of the IT infrastructure. Before interaction occurs between cloud providers and users, trust in the cloud relationship is very important to minimize the security risk and malicious attacks. The notion of trust involves several dimensions. SLA-oriented Resource Allocation Through Virtualization Recently, virtualization has enabled the abstraction of computing resources such that a single physical machine is able to function as multiple logical VMs (Virtual Machines).

A key benefit of VMs is the ability to host multiple operating system environments which are completely isolated from one another on the same physical machine. Another benefit is the capability to configure VMs to utilize different partitions of resources on the same physical machine. Physical machine, one VM can be allocated 10% of the processing power, while another VM can be allocated 20% of the processing power. Hence, VMs can be started and stopped dynamically to meet the changing demand of resources by users as opposed to limited resources on a physical machine.

III. Limitations of Existing System

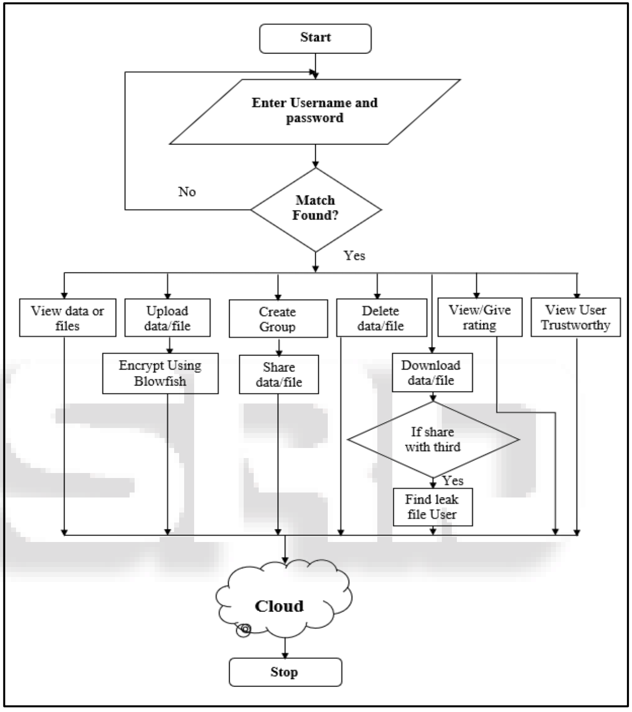
Reference	Limitations
[1]	Some results have been given to establish higher accuracy of the model, but lacks analysis.
[2]	Complex and lengthy process. Time consuming.
[3]	Time consuming. Complex process as compared to Blowfish algorithm.
[4]	Lack of assurances and violations for SLA guarantees.
[5]	By sharing storage and networks with many other users/customers it is possible for other customers to access your data.
[6]	Complex structure. Time consuming.
[7]	Multi-tenancy, lack of customer’s control over their data and application. Non-transparency with respect to security profiles of remote datacenter locations.

IV. Proposed System

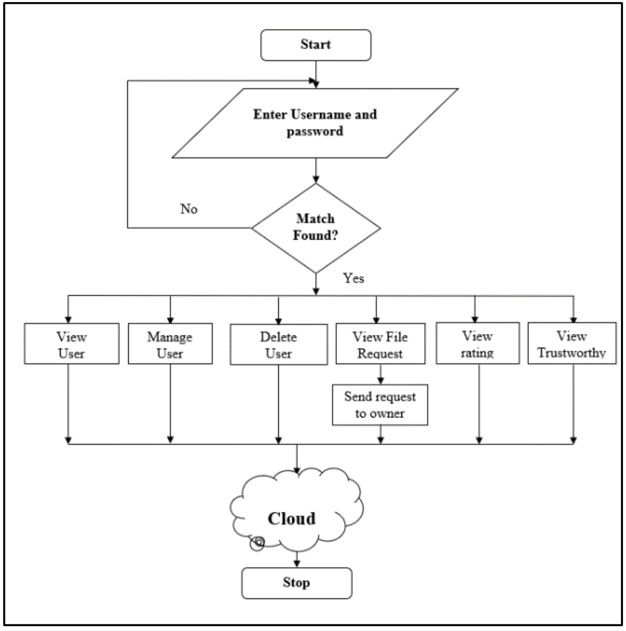
The current work is significant as it proposes a framework, Sel-CSP, which attempts to compute risk involved in interacting with a given cloud service provider (CSP). The framework estimates perceived level of interaction risk by combining trustworthiness and competence of cloud provider. Trustworthiness is computed from ratings obtained through either direct interaction or feedback. Competence is estimated from the transparency of SLA guarantees. A framework, termed as Sel-CSP, has been proposed to facilitate customers in selecting an ideal cloud service provider for business outsourcing which depicts different modules of the framework and how these modules are functionally related. Sel-CSP framework provides APIs through which both customers and providers can register themselves. After registering, customer can provide trust ratings based on interactions with provider. Cloud provider needs to submit its SLA to compute competence. At present, verifying the correctness of submitted ratings or sanitizing the erroneous data in the framework is beyond the scope. We assume that only registered customers can provide referrals/feedbacks and they do not have any malicious intents of submitting unfair ratings.

A. Flow chart of our proposed System

1) Flow chart for User/Owner:



2) Flow chart for Admin (CSP):



V. Conclusion

Moreover, as customers are outsourcing their businesses onto a third-party cloud, capability or competence of CSP determines if former's objectives are going to be accomplished. In this work, we propose a novel framework, SelCSP, which facilitates selection of trustworthy and competent service provider.

Acknowledgement

The physical support and the technical contribution of Prof. Pravin Shinde is highly appreciable without their moral support it was impossible to reach the goal.

References

[1] T. Noor and Q. Sheng, "Trust as a service: A framework for trust management in cloud environments", in Proc. 12th Int. Conf. Web Inf. Syst. Eng., pp. 314–321,2011.

[2] Schryen, M. Volkamer, S. Ries, and S. M. Habib, "A formal approach towards measuring trust in distributed systems," in Proc. ACM Symp. Appl. Comput., 2011, pp. 1739–1745.

[3] Y. Zhu, H. Hu, G.J. Ahn, and M. Yu, "Cooperative Provable Data Possession for Integrity Verification in Multicloud Storage", IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 12, pp. 2231-2244, Dec. 2012.

[4] S. K. Garg, S. Versteeg, and R. Buyya, "A framework for ranking of cloud computing services", Future Gener. Comput. Syst., vol. 29, no. 4, pp. 1012–1023, 2013.

[5] Nirnay Ghosh, Soumya K. Ghosh, and Sajal K. Das, "SelCSP: A Framework to Facilitate Selection of Cloud Service Providers" IEEE TRANSACTIONS ON CLOUD COMPUTING, VOL. 3, NO. 1, JANUARY-MARCH 2015.

[6] Huaqun Wang "Identity-Based Distributed Provable Data" IEEE TRANSACTIONS ON SERVICES COMPUTING, VOL. 8, NO. 2, MARCH-APRIL 2015.