2010 13th International Conference on Network-Based Information Systems

SLA-Based Trust Model for Cloud Computing

Mohammed Alhamad, Tharam Dillon, Elizabeth Chang
Digital Ecosystems and Business Intelligence Institute (DEBII)
Curtin University of Technology
Perth, Australia
Mohammed.Alhamad@postgrad.curtin.edu.au,
Tharam.Dillon@cbs.curtin.edu.au, Elizabeth.Chang@cbs.curtin.edu.au

Abstract. **Cloud computing is a new form of technology, which infrastructure, developing platform, software, and storage can be delivered as a service in a pay as you use cost model. However, for critical business application and more sensitive information, cloud providers must be selected based on high level of trustworthiness. In this paper, we present a trust model to evaluate cloud services in order to help cloud users select the most reliable resources. We integrate our previous work "conceptual SLA framework for cloud computing" with the proposed trust management model to present a new solution of defining the reliable criteria for the selection process of cloud providers.**

I. Introduction

Cloud computing has emerged as an effective technology, where the computing infrastructure, networking routers, software, and developing platform are delivered as a service available for users at any time and through which they can access the Internet[1]. With the increase of public cloud providers, cloud consumers face various challenges such as the security, privacy, and discovery of reliable resource providers. One of the major challenges that prevent many businesses from transferring their technology to external cloud providers is whether cloud users can trust cloud providers to deliver what they promise. Different trust and reputation models have been proposed in the literature of information technology. But none of these models are discussed in relation to cloud computing. In this paper, we propose a trust model using the SLA metrics presented in our previous work [2] with firsthand experience of trust values in order to determine a reliable method for selecting the most secure providers of cloud resources.

II. Background and Related Works

This section presents the definitions and main concepts of terms used in this paper. Also, the related works and the state-of-the-art approaches to trust and reputation in different areas are presented.

A. Background

Trust concepts have been used in many areas such as economics, law, commerce, and information technology. Many researchers have investigated the various challenges to trust management. The amount of literature relating to this topic is increasing as researchers continue to discuss different issues and propose innovative models to solve the problems that arise when two parties need to establish a business connection between them. A variety of meanings has been attached to the term 'trust' in multiple dimensions. So, some of the literature in this area is confusing when the use of the trust concept is used in projects, but with different definitions [3].

When the notion of trust appears in the literature, it is often without a formal definition. For instance, Deutch and Gambetta discuss the theoretical background and provide a basic definition of the trust concept for use in the real world [4]. An overview of trust and reputation definitions from the existing literatures presented by Hussain et al. [3] shows that the current notions of trust and reputation need to be formally defined. Many researchers use the definition presented by Dasgupta [5] who defines trust as: "the expectation of one person about the actions of others that affects the first person's choice, when an action must be taken before the actions of others are known". Deutsch [6] states that: "trusting behavior occurs when a person encounters a situation where she perceives an ambiguous path. The result of following the path can be good or bad and the occurrence of the good or bad result is contingent on the action of another person" [3]. Another definition often cited in the literature is that given by Gambetta [7]: "trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both before he can monitor such action (or independently of his capacity ever to be able to monitor it) and in a context in which it affects his own action".

978-0-7695-4167-9/10 $26.00 © 2010 IEEE
DOI 10.1109/NBiS.2010.67

Reputation mechanisms are used for large-scale open systems. In general, reputation is defined as the public's opinion about the object, character, or standing of an entity such as reliability, capability, and usability. Users can provide ratings about a person, a product, an agent, or a service. Mui et al [8] state that reputation is "a perception that an agent creates through past actions about its intentions and norms". Another definition presented by Abdul-Rahman et al. [9] is: "a reputation is an expectation about an agent's behavior based on information about or observations of its past behavior".

The SLA is a legal format documenting the way that services will be delivered as well as providing a framework for service charges. Service providers use this foundation to optimize their use of infrastructure to meet signed terms of services. Service consumers use the SLA to ensure the level of quality of service they need and to maintain acceptable business models for the long-term provision of services. The following are the main requirements of the SLA format which should:

- clearly describe a service so that the service consumer can easily understand the operation of the services
- present the level of performance of service
- define ways by which the service parameters can be monitored and the format of monitoring reports
- impose penalties when service requirements are not met
- present the business metrics such as billing and stipulate when this service can be terminated without any penalties being incurred.

B. Related Works

Reputation mechanisms are used in e-market systems (e.g. Amazon, E-bay) to secure the transactions of all users in a centralized architecture. Novel models of reputation and trust have been developed in e-market places to provide reliable services of security since traditional solutions to security issues do not adequately protect providers and services consumers [10]. The most important aspect of these models is the information relating to past behaviours of users. This information is used to present the reputation of those users in terms of availability, reliability, and security. As a centralized architecture of online reputation model, E-bay and Amazon exemplify this approach. Their systems are implemented based on a centralized rating model so that customers and sellers can rate each other using numerical ratings or feedback comments. Users can obtain a reputation profile for a given user to decide whether or not to proceed with a transaction with this user. For example, E-bay uses 1, 0, -1 scales which means positive, neutral, and negative respectively. Users use these scales to rate business partners based on past behaviours. The feedback from users is stored in a central system and the reputation score is computed regularly as cumulative results of user ratings [11]. The problem with this mechanism is that users with high scores for reputation can cheat other users in a few transactions even though they receive negative feedback, because these users still gain positive ratings from other customers. Also, this model cannot guarantee the consistent performance of all services from one user. This model employs a centralized architecture, therefore all services and reputation information has a single point of failure.

Unlike the centralized architecture of service discovery, the peer-to-peer model does not use a single point to manage and store descriptions of services and reputation information. Vu et al. [12] propose peer-to-peer web service discovery that uses QoS and users' feedback to rank and select services. QoS data of services and reputation rates from consumers are stored in multi-peers in peer-to-peer systems. Monitoring agents are used to prevent cheating by users and providers. Trusted agents monitor and provide reports of services to a UDDI peer and based on this information, services are evaluated and ranked. However, monitoring reports differ from peer to peer, because each peer uses different criteria to provide feedback about services.

Dellarocas [13] proposed a model which detects and excludes any highly unfair ratings. In this approach, two important classes of reputation system fraud are addressed: (1) the users who are providing unfairly high ratings or unfairly low ratings for sellers, (2) sellers who hide behind their good reputation in order to provide a service with low quality to different users. To avoid the unfairly low ratings, Dellarocas uses controlled anonymity and cluster filtering methods. A collaborative filtering scheme is used to calculate an unbiased personalized reputation score. Using this method, groups of buyers who give similar ratings are divided into two classes (upper and lower classes). The final reputation score is calculated using the lower classes only.

Yu and Sing [14] proposed a reputation system based on the Dempster-Shafer theory of evidence [15]. The proposed approach focused on detecting and protecting users against spurious ratings. Their method involves the use of a Weighted Majority Algorithm in order to distinguish the local belief and the total belief. Local belief is from direct interaction and can be transferred to other users. Total belief is a combination of local belief and external recommendations received from any user.

Much literature exists on trust and reputation systems. However, due to limitations of space, we are unable to present all the existing body of literature. However, from the above discussion, it is evident that the proposed works in trust and reputation management systems are designed mainly to enhance the security of the traditional web services. In cloud computing, the execution of services has changed to be completely independent of the consumer's infrastructure. Additionally, the price model for using cloud provider data centres is not the same as the price of the traditional web services model. So, cloud computing lacks new approaches to integrate it with the new technology and dynamic model of price. Our proposed architecture will present a novel architecture of trust for cloud computing. This architecture will use SLA and a business activities monitoring method to guarantee the quality of cloud services.

In the existing body of literature on cloud computing, there is no framework by which a cloud service consumer can make an intelligent trust-based decision regarding service selection from a service provider. Given the potential growth of cloud computing and the business implications, it is very important to have such architecture in place. In this we propose an architecture which is primarily SLA-based for selecting a given cloud service providers.

III. SLA-Based Trust Model for Cloud Computing

Our proposed solution recommends the most related and trusted resources from various cloud providers. The most related services mean the services which match all the main functional requirements of the desired service. Examples of the functional requirements are finding the average of millions of specific dataset or applying other types of statistical analysis of data. On other hand, the time needed for processing these tasks or the level of privacy to keep the data in secure places, are considered as non-functional requirements. The proposed model uses the SLA management and trust techniques to provide a reliable model to select the best available provider among various cloud providers to fulfil both types of requirements.

A. Architecture

In this section, we present the proposed architecture for a cloud computing environment. Figure 1 shows the basic components of the proposed architecture including SLA agent, cloud services directory, cloud providers, and cloud consumer entities.

1) SLA Agent: The new architecture of outsourcing of services forces the business decision makers to seek experts in

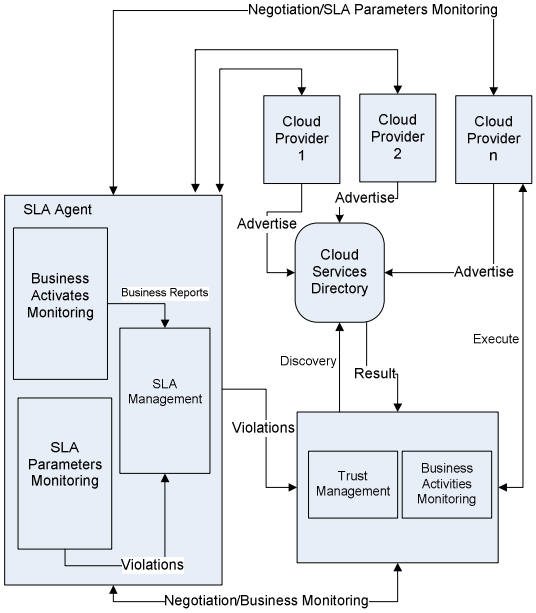

Fig 1. SLA-Based Trust Model for Cloud Computing.

the domains of IT, policy and legislation. These professionals can provide services such as designing IT metrics for SLA agreements, setting the value for SLA parameters and examining the policy and legislations for partners. In cloud computing, SLA agents are very important as an intermediary agent between consumers and cloud providers. In the proposed model, we use an SLA agent to perform the following major tasks:

A) Grouping cloud consumers according to different classes based on business needs

B) Designing SLA metrics based on the consumers' needs

C) Negotiating with cloud providers

D) Selecting cloud providers based on non-functional requirements. The discovery and selection processes to obtain the cloud services based on the functional requirements are made by the consumers in the early stage of communication with cloud providers.

E) Monitoring business activities for consumers

F) Monitoring SLA parameters

2) Cloud Consumer Model: Cloud consumer is the entity who requests the external execution of one or more services. A cloud consumer is required to pay the bill upon completed execution of services based on a well-defined model of prices. The design and discussion of price models for cloud computing are not considered in our study. The SLA agent has the authority to choose the optimal price model for services. The consumer model consists of two main parts:

A) Trust management model: this model manages the trust relationships between cloud providers and also the other users of cloud services. Three sources of information are used in the trust management model. The first source is the local experiences with cloud providers and users. The second source is the opinions of external cloud services. The last one is the reports which are provided by the SLA agent. To obtain reliable results from the trust management model, we will use credibility metrics associated with these three sources of information. Cloud consumers are able to assign various weights ($0 \leq$ summation of all weights ≤ 1).

The output of the trust management system will be used to rank the list of cloud providers obtained from the cloud services directory. Then, the ranked list will be sent to the SLA agent to select the final cloud provider based on non-functional requirements.

B) Business activities management: The key feature of our model that distinguishes it from the solution proposed by others who design online services is the use of an indicator of business activities. We propose to use this indicator as one of the main SLA parameters to determine who is responsible for the violation of the revenue or profit parameters. More details about these parameters are presented later in this paper.

3) Cloud Services Directory: Consumers of cloud services will not know about the existing cloud providers if there is no agent or registry to advertise and describe their services. At the present time, there is no public directory for storing the descriptions about cloud services and details about the cloud providers. In our proposed architecture, we use a common directory in order to help cloud consumers to find the services they require. We envisage that the directory will store at least the Ids of cloud providers and the functional advertisements of

their services. We are not considering the processes of discovery and service selection in detail here. So, the research scope is limited to the designing of SLA agreements and trust management only.

4) Cloud Providers: Cloud providers are the entities who own the cloud infrastructure and provide cloud services for consumers. Also, the design and implementation of cloud provider infrastructure and price models are outside the scope of this paper. We will investigate such issues in our future work.

B. Protocol

In this section, we present the proposed protocol for our model. We show the activities which this model involves without the implementation. Further details about the implementation processes will be considered in our future work.

A) Advertise Cloud Services

The first step of the proposed protocol is that cloud services must present their services in the cloud services directory. So, any consumer can easily find a suitable provider using the functional requirements discovery process.

B) Discovery of Cloud providers

Cloud consumers use the discovery operation to find the related providers who are able to fulfil the consumers' requirements. In this operation, consumers use the functional requirements of services to obtain the list of all matched providers.

C) The list of providers which are obtained in (B) must be submitted to the trust management system to filter out non-trusted providers using credibility values and the reports of the SLA agent.

D) A trusted list of cloud providers should be sent to the SLA agent together with more details about business objectives.

E) When cloud consumers submit the request for cloud services, they will wait to get the Id of cloud provider with all details of SLA agreements. If the consumers agree to continue the contract, they will be asked to sign the SLA with the SLA agent and start to communicate with the selected provider.

The SLA agent is involved in three main tasks in the proposed architecture. The first task is SLA management which should effectively divide the consumer classes into different groups. The business objectives of consumers are used to select related types of SLA agreements from among existing templates of SLA. The management unit of the SLA then starts the negotiation with the cloud consumer and finally, the contract must be signed. The second task for the SLA agent is business activities monitoring. The monitoring and auditing of business rules and business activities are essential to assign responsibility in the case of violations. We propose using this task because SLA metrics templates are designed to use business parameters such as consumers' profit. So, cloud providers should agree to pay some fees when the consumers' profit which is associated with a selected service decreases.

IV. Conclusion and Future Work

This paper presents a novel trust model that uses the service level agreements criteria and the first hand experiences of users as the main inputs to determine the level of trustworthiness for cloud resources. This model can be used for different domains of cloud services and based on that, domain users can obtain a more specific trust value of the same concept of services. As a future work, design requirements and the evaluation of the proposed work will be conducted with effective scenarios of simulation and experiment processes.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, and I. Stoica, "Above the clouds: A berkeley view of cloud computing" , EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2009-28, 2009.

[2] M. Alhamad, "Conceptual SLA Framework for Cloud Computing", Accepted for IEEE DEST 2010 on 15 March 2010 2010.

[3] F. K. Hussain and E. Chang, "An overview of the interpretations of trust and reputation", 2007, pp. 30-30.

[4] A. C. Squicciarini, E. Bertino, E. Ferrari, I. Ray, and D. I. e Comunicazione, "Achieving privacy in trust negotiations with an ontology-based approach", IEEE Transactions on Dependable and Secure Computing, vol. 3, pp. 13-30, 2006.

[5] A. Dasgupta and A. Prat, "Reputation and asset prices: A theory of information cascades and systematic mispricing", Manuscript, London School of Economics, 2005.

[6] M. Deutsch, Distributive justice: A social-psychological perspective: Yale University Press New Haven, CT, 1985.

[7] D. Gambetta, Trust: Making and breaking cooperative relations: Basil Blackwell New York, 1990.

[8] L. Mui, M. Mohtashemi, and A. Halberstadt, "A computational model of trust and reputation. System Sciences", 2002, pp. 7-10.

[9] A. Abdul-Rahman and S. Hailes, "Supporting trust in virtual communities,|| System Sciences, 2000", 2000, p. 9.

[10] T. Grandison and M. Sloman, "A survey of trust in internet applications", IEEE Communications Surveys and Tutorials, vol. 3, pp. 2-16, 2000.

[11] P. Resnick and R. Zeckhauser, "Trust among strangers in Internet transactions: Empirical analysis of eBay's reputation system", Advances in Applied Microeconomics: A Research Annual, vol. 11, pp. 127-157, 2002.

[12] L. H. Vu, M. Hauswirth, and K. Aberer, "Towards p2p-based semantic web service discovery with qos support", 2005, pp. 18-31.

[13] C. Dellarocas, "Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior", 2000, pp. 150-157.

[14] B. Yu, M. P. Singh, and K. Sycara, "Developing trust in large-scale peer-to-peer systems", 2004, pp. 1-10.

[15] J. Gordon and E. H. Shortliffe, "The Dempster-Shafer theory of evidence", Rule-Based Expert Systems: The MYCIN Experiments of the Stanford Heuristic Programming Project, pp. 272-292, 1984.