Cloud Armor: A Platform for Credibility-Based Trust Management of Cloud Services

Talal H. Noor[1], Quan Z. Sheng[1], Anne H.H. Ngu[2], Abdullah Alfazi[1] and Jeriel Law[1]
[1]School of Computer Science, The University of Adelaide, SA 5005, Australia
{talal, qsheng, alfazi, jlaw}@cs.adelaide.edu.au
[2]Department of Computer Science, Texas State University, TX 78666-4616, USA
angu@txstate.edu

ABSTRACT

Trust management of cloud services is emerging as an important research issue in recent years, which poses significant challenges because of the highly dynamic, distributed, and non-transparent nature of cloud services. This paper describes Cloud Armor, a platform for credibility-based trust management of cloud services. The platform provides a crawler for automatic cloud services discovery, an adaptive and robust credibility model for measuring the credibility of feedbacks, and a trust-based recommender to recommend the most trustworthy cloud services to users. This paper presents the motivation, system design, implementation, and a demonstration of the Cloud Armor platform.

Categories and Subject Descriptors

H.3.5 [**Information Storage and Retrieval**]: On-line Information Services, Commercial services, Data sharing—*Web-based services*; K.6.3 [**Management of Computing and Information Systems**]: Software Management—*Software process*

General Terms

Information Systems, Management, Design, Measurement, Performance

Keywords

Trust management, cloud services discovery, recommendation, credibility, reputation

1. INTRODUCTION

Cloud services refer to flexible and on-demand infrastructures, platforms and software provided as services. With the highly dynamic, distributed, and non-transparent nature of cloud services, trust management is considered one of the top 10 obstacles for cloud computing [3]. Trust management of cloud services is not an easy task due to some unique characteristics of cloud services.

Firstly, cloud services are dynamic (e.g., new cloud services can be established to join other cloud services while old cloud services might discontinue around the clock (`http://raydepena.wordpress.com/2011/01/01/90-cloud-computing-companies-to-watch-in-2011/`)). The majority of publicly available could services are not based on description standards which make the cloud service discovery a challenging problem (e.g., some cloud services such as Dropbox do not use the word *cloud* in their description) [10, 4]. Secondly, determining the credibility of trust feedbacks is a significant challenge. It is difficult to know how experienced a cloud service consumer is and from whom malicious trust feedbacks are expected [7]. Last but not the least, trust-based cloud services recommendation is not an easy task because of the variety in cloud services' functionalities and features (i.e., some cloud services have similar functionalities and features while others do not [2, 9]). It is difficult to recommend trustworthy cloud services that suit all cloud service consumers (i.e., each user is looking for cloud services that support specific functionalities and features).

Motivated by these concerns, we have developed Cloud Armor, a platform for a credibility-based trust management of cloud services. The salient features of the platform are: i) the innovative use of a web crawling approach for automatic cloud services discovery; ii) an adaptive and robust credibility model for measuring the credibility of feedbacks; and iii) a trust-based recommender to recommend trustworthy cloud services that suit the users needs. In the following sections, we overview the design and implementation of the platform and sketch the proposed demonstration. Interested readers are referred to [8, 7, 6] for more technical details.

2. CLOUD ARMOR OVERVIEW

Cloud Armor provides an environment where consumers can give trust feedback and request trust assessment for a particular cloud service. The platform (Figure 1) exploits a web crawling approach for automatic cloud services discovery, which consists of the following main components:

The Trust Data Provisioning. This component is responsible for collecting cloud services and trust information. We developed the *Cloud Services Crawler* module based on the Open Source Web Crawler for Java (crawler4j - `http://code.google.com/p/crawler4j/`) and extend it to

CIKM'13, Oct. 27–Nov. 1, 2013, San Francisco, CA, USA.

http://dx.doi.org/10.1145/2505515.2508204.

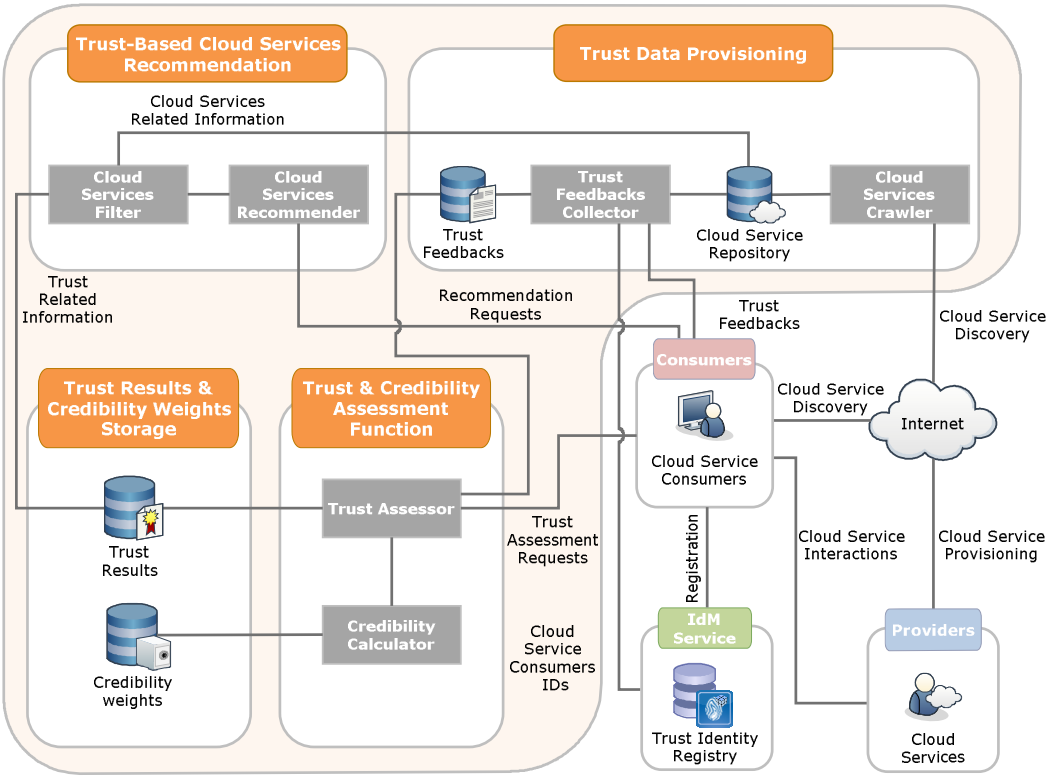

Figure 1: Cloud Armor's Architecture

allow the platform to automatically discover cloud services on the Internet and store cloud services' information (e.g., the cloud service ID, URL and description) in the *Cloud Services Repository*. We implemented a set of functionalities to simplify the crawling process and make the crawled data more comprehensive (e.g., `addSeeds()` and `selectCrawlingDomain()`). In addition, we developed the *Trust Feedbacks Collector* module to collect trust feedbacks directly from cloud service consumers in the form of history records and stores them in the *Trust Feedbacks Database*. Indeed, the cloud service consumers typically have to establish their identities for the first time they attempt to use the platform through registering their credentials at the *Identity Management Service* (IdM) which stores the credentials in the *Trust Identity Registry*.

The Trust and Credibility Assessment Function. This function is responsible for handling trust assessment requests from users where the trustworthinesses of cloud services are compared and the credibilities of trust feedbacks are calculated. We developed the *Credibility Calculator* to measure the credibility of trust feedbacks based on a set of credibility factors to aggregate the credibility weights. The credibility factors include the cloud service consumers' experience factor (i.e., which is calculated based on the cloud service consumer's capability and the majority consensus factors) and feedback density factor (more details on how the credibility factors are calculated can be found in [8, 7, 6]). Moreover, we developed the *Trust Assessor* to compare the trustworthiness of cloud services through requesting the aggregated credibility weights from the *Credibility Calculator* to weigh the trust feedbacks and then calculate the mean of all trust feedbacks given to each cloud service. The trust results for each cloud service and the credibility weights for trust feedbacks are stored in the databases (i.e., the *Trust Results and Credibility Weights Storage* in Figure 1).

Trust-Based Cloud Services Recommendation. This component is responsible for recommending trustworthy cloud services to users. We developed the *Cloud Services Recommender* to recommend trustworthy cloud services that suit the users' needs using the *Cloud Services Filter*. The *Cloud Services Filter* filters cloud services based on the cloud service's category (e.g., IaaS, PaaS, and SaaS based on keywords such as *storage* and *host*) and their corresponding trust results. Consequently, the *Cloud Services Recommender* uses the trust assessment requests from users to recommend trustworthy cloud services that suit requesters' need.

We crawled review websites such as `CloudHostingReviewer.com` and `cloud-computing.findthebest.com` where consumers usually give their feedback on cloud services that they used. The collected data represents consumers feedback based on several Quality of Service (QoS) parameters including availability, security, response time, etc. We managed to collect 10,076 feedbacks given by 6,982 consumers to 113 real-world cloud services. The collected dataset will be release to the research community in the project website (`http://cs.adelaide.edu.au/~cloudarmor`).

3. DEMONSTRATION SCENARIO

Cloud Armor provides an environment where cloud service consumers can give trust feedback and request trust

assessment for a particular cloud service. In this demonstration, we will focus on demonstrating: (i) how the cloud services are discovered and the trust feedbacks are collected, (ii) how the trust assessment requests are handled and the credibility aggregated weights are configured, and (iii) how the trustworthy cloud services are recommended.

Trust Data Provisioning. The cloud service crawler offers several functionalities that a system administrator can use for cloud service discovery and information collection. The system administrator can add specific keywords for the crawling process, select the domain, and specify the time that the crawler starts the crawling process and the crawling period. The cloud services' information is stored in the *Cloud Services Repository* to be displayed when users search for cloud services. Users can easily search for desirable cloud services and provide feedback to a particular cloud service.

Trust and Credibility Assessment. The Trust Assessor gives cloud service users the ability to search for the cloud service that they want to assess where the trust result for the searched cloud service is then displayed. In addition, a detailed analysis of the trust feedback for the cloud service is also displayed. Several analysis controllers are provided for users such as credibility factors in calculating the trust result and the ability to visualize the trust results for the cloud service based on different time period (e.g., in day, month, or year). The credibility calculator allows the administrator to tweak the credibility weights according to the trust assessment preferences.

Trust-Based Cloud Services Recommendation. The Cloud Service Recommender allows users to receive recommendations of trustworthy cloud services based on the query that they used to search for cloud services. Cloud services are ranked according to their corresponding trust results where the top 10 trustworthy cloud services for all cloud services regardless their category (i.e., IaaS, PaaS or SaaS) are displayed. The Cloud Services Filter also provides the administrator with several functionalities such as the ability to choose the filtering technique (e.g., to filter the recommended cloud services based on the cloud services' category) where the top 10 trustworthy cloud services that are in the same category are displayed. The cloud services are categorized using keywords chosen by the administrator (e.g., *Storage, Online Backup,* and *WebHosting* indicate IaaS).

4. DISCUSSIONS AND CONCLUSION

Over the past few years, trust management has been one of the hot topics especially in the area of cloud computing. Some of the research works use policy-based trust management techniques. For example, Ko et al. [5] proposed TrustCloud framework for accountability and trust in cloud computing which consists of five layers including workflow, data, system, policies and laws, and regulations layers to address accountability in the cloud from all aspects. Brandic et al. [1] proposed a novel approach for compliance management in cloud environments to establish trust. Unlike previous works that use policy-based techniques, we evaluate the trustworthiness of a cloud service using reputation-based trust management techniques.

Other research works use reputation-based trust management techniques. For instance, Habib et al. [2] proposed a multi-faceted Trust Management (TM) system architecture which models uncertainty of trust information collected from multiple sources using a set of Quality of Service (QoS) attributes such as security, latency, availability, and customer support. Hwang et al. [3] proposed a security-aware cloud architecture where trust negotiation and data coloring techniques are used to support cloud providers and the trust-overlay to support consumers. Unlike previous works, we present a platform that not only measures the credibility of trust feedbacks, but also has the ability to recommend trustworthy cloud services based on the users' preferences.

In this demo, we have presented Cloud Armor, a platform for credibility-based trust management of cloud services. The platform exploits a web crawling approach for automatic cloud services discovery and a credibility model for measuring the credibility of trust feedbacks that underpin a trust-based recommender to suggest trustworthy cloud services based on the users' preferences. We are currently extending and enhancing the cloud services crawler to have better cloud services discovery results. The performance optimization of the trust management service is another focus of our future research work. Interested readers are referred to the project website for more details.

Acknowledgments

Talal H. Noor and Abdullah Alfazi work has been supported by King Abdullah's Postgraduate Scholarships, the Ministry of Higher Education: Kingdom of Saudi Arabia.

5. REFERENCES

[1] I. Brandic and et al. Compliant Cloud Computing (C3): Architecture and Language Support for User-Driven Compliance Management in Clouds. In *Proc. of CLOUD'2010*, 2010.

[2] S. Habib and et al. Towards a Trust Management System for Cloud Computing. In *Proc. of TrustCom'2011*, 2011.

[3] K. Hwang and D. Li. Trusted Cloud Computing with Secure Resources and Data Coloring. *IEEE Internet Computing*, 14(5):14–22, 2010.

[4] J. Kang and K. M. Sim. Towards Agents and Ontology for Cloud Service Discovery. In *Proc. of CyberC'2011*, 2011.

[5] R. Ko and et al. TrustCloud: A Framework for Accountability and Trust in Cloud Computing. In *Proc. of SERVICES'2011*, 2011.

[6] T. H. Noor and et al. Reputation Attacks Detection for Effective Trust Assessment of Cloud Services. In *Proc. of TRUSTCOM'2013*, 2013.

[7] T. H. Noor and Q. Z. Sheng. Credibility-Based Trust Management for Services in Cloud Environments. In *Proc. of ICSOC'2011)*, 2011.

[8] T. H. Noor and Q. Z. Sheng. Trust as a Service: A Framework for Trust Management in Cloud Environments. In *Proc. of WISE'2011*, 2011.

[9] R. Ranjan and et al. *Cloud Computing: Principles, Systems and Applications*, chapter Peer-to-Peer Cloud Provisioning: Service Discovery and Load-Balancing, pages 195–217. Springer, 2010.

[10] Y. Wei and M. B. Blake. Service-oriented Computing and Cloud Computing: Challenges and Opportunities. *Internet Computing, IEEE*, 14(6):72–75, 2010.