Computers in Human Behavior 60 (2016) 280–292

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

Full length article

A new method for trust and reputation evaluation in the cloud environments using the recommendations of opinion leaders' entities and removing the effect of troll entities

Matin Chiregi, Nima Jafari Navimipour*

Department of Computer Engineering, Tabriz Branch, Islamic Azad University, Tabriz, Iran

ARTICLE INFO

Article history:
Received 9 July 2015
Received in revised form
29 December 2015
Accepted 9 February 2016
Available online xxx

Keywords:
Trust
Cloud computing
Opinion leaders
Troll
Reputation

ABSTRACT

Trust in the cloud environment is not written into an agreement and is something earned. In any trust evaluation mechanism, opinion leaders are the entities influencing the behaviors or attitudes of others, this makes them to be trustworthy, valid among other characteristics. On the other hand, trolls are the entities posting incorrect and unreal comments; therefore, their effect must be removed. This paper evaluates the trust by considering the influence of opinion leaders on other entities and removing the troll entities' effect in the cloud environment. Trust value is evaluated using five parameters; availability, reliability, data integrity, identity and capability. Also, we propose a method for opinion leaders and troll entity identification using three topological metrics, including input-degree, output-degree and reputation measures. The method being evaluated in various situation where shows the results of accuracy by removing the effect of troll entities and the advice of opinion leaders.

1. Introduction

Nowadays, Internet and web services facilitate the information and data sharing (Navimipour & Zareie, 2015; Souri & Jafari Navimipour, 2014). Cloud computing as new web-based service is increasingly regarded as a method to reduce infrastructure costs and is being used by a wide range of organizations (Kumar, Quamar, Deshpande, & Khuller, 2014). It is an open standard model, which can enable pervasive computing and offer on-demand network access to a shared pool of resources (Younis, Kifayat, & Merabti, 2014). The cloud computing services offered by large-scale data centers of companies like Amazon, Google, or Microsoft attract every day many new clients (Bouabana-Tebibel & Kaci, 2015). Its services enable organizations and individuals to outsource the management of their data to a service provider in order to save on hardware investments and reduce maintenance costs (Yiu, Ghinita, Jensen, & Kalnis, 2010). Cloud computing as an economic and computational model has made its statement, achieving a lot of recognition in the past few years (Pitropakis, Pikrakis, & Lambrinoudakis, 2014). Cloud is a back to the future proposition that was foreseen in the 1950s and is as old as computing itself (Ryan & Falvey, 2012). The cloud computing as a paradigm that shares computing and storage infrastructure over a scalable network of resources (Manuel, 2013) is rapidly becoming an important platform for scientific applications (Wang, Zeng, Tang, & Yao, 2012). It is a new pattern of business computing and it can dynamically provide computing services supported by state-of-the-art data centers that usually employs Virtual Machine (VM) technologies (Armbrust, Fox et al. 2010; Buyya, Yeo, Venugopal, Broberg, & Brandic, 2009; Wu, Zhang, Zeng, & Zhou, 2013). Cloud infrastructure supports four types of service delivery models including Software as a Service (SaaS) (Espadas et al., 2013; Gani et al., 2014), Platform as a Service (PaaS) (Anselmi, Ardagna, & Passacantando, 2014), Infrastructure as a Service (IaaS) (Manuel, 2013) and Expert as a Service (EaaS) (Navimipour, 2015; Navimipour, Navin, Rahmani, & Hosseinzadeh, 2015; Navimipour, Rahmani, Navin, & Hosseinzadeh, 2014, 2015; Navin et al., 2014), Storage as a Service (STaaS) (Whaiduzzaman, Sookhak, Gani, & Buyya, 2014), Security as a Service (SECaaS), Data as a Service (DaaS), Database as a Service (DBaaS), Test

Abbreviations: API, Application Programming Interface; APIaaS, API as a Service; Baas, Backend as a Service; B2C, Business to Customer; C2C, Customer to Customer; DaaS, Data as a Service; DBaaS, Database as a Service; EaaS, Expert as a Service; HD, Home Domain; IaaS, Infrastructure as a Service; OD, Outsourced Domain; PaaS, Platform as a Service; QoS, Quality of Service; SaaS, Software as a Service; SECaaS, Security as a Service; STaaS, Storage as a Service; TEaaS, Test environment as a Service; VM, Virtual Machine.

* Corresponding author.
E-mail address: jafari@iaut.ac.ir (N.J. Navimipour).

http://dx.doi.org/10.1016/j.chb.2016.02.029
0747-5632/

Environment as a Service (TEaaS), API as a Service (APIaaS) and Backend as a Service (BaaS) (Tameem & Cho, 2014). One of the key promises of cloud is the speed and ease with which organizations can temporarily access additional compute resources (Everett, 2009).

In the cloud computing, there are many issues, among them trust becomes a complex and important issue (Manuel, 2013). It is an important factor in the real world human society, and on the Internet environments (Quinn, Lewis, O'Sullivan, & Wade, 2009). Trust is a kind of abstract psychological cognition that is established on historical experience that two sides have owed and related information (Jie, Zhang, & Wen, 2010). It is one of the most important tools to improve safety and efficient alternative means to construct safety in cloud environments. It depends mainly on two factors, one is the operational trust which deals with the operations of cloud service provider and other is the mechanization of different mechanisms for service providers to provide trust (Hyder & Ismail, 2015). We can view trust in the cloud as the customers' level of confidence in using the cloud, and try to increase this by mitigating technical and psychological barriers for cloud services (Ko, Jagadpramana et al. 2011). Establishing trust in cloud computing will undoubtedly require identity and data privacy through encryption (Khan & Malluhi, 2010). Trust is always made only if sufficient services and expectations are attained (Jaiganesh, Aarthi, & Kumar, 2015). It has different meanings for different people in different contexts. Also, it is critical in the electronic markets as it can provide buyers with high expectations of satisfying exchange relationships; since then, many C2C marketplaces have introduced the trust evaluation model based on B2C to evaluate the credibility of each online store, like (Yang & Chen, 2009). Trust can be defined as some criteria that can be used to support the decision about with whom we should share and accept information, from whom we should trade in e-markets, and what consideration to give information to people when aggregating or filtering data. To effectively use trust in e-markets, it is important to understand what users mean when they say that they trust someone and how much they trust them (Pereira, Silva, Meira, & Almeida, 2009). Most of C2C e-commerce sites provide a set of authentication mechanism for sellers to avoid the Internet fraud brought by anonymous transaction (Li, 2014). Also, trust is the major concern of the consumers and provider of services that participates in the cloud environment as a popular C2C environment (Shen, Li, Yan, & Wu, 2010). Therefore, trust management is a vital part of commercial aspects of cloud technology (Noor & Sheng, 2011) where opinion leader selection and troll entity identification play the important roles on its effectiveness.

Opinion leaders in any distributed systems like the Internet are very important, which play an important role in promoting the formation of public opinions (Farley, Hanbury, & Thompson, 2014). They are an often-used method of influencing such behaviors in implementation studies, but reliability and cost effectively identify them is not straightforward (Farley et al., 2014). Their superior status, leadership, and social prestige enable them to influence followers, which is a key element of making a community interconnected to achieve the best group performance (Li, Ma, Zhang, & Huang, 2013). Opinion leader is a concept that has already been proposed in the social networks. In this paper, we adopt this term to cloud environments. Simply, in the cloud environments, they can be the entities with high trust and reputation. We have used this concept for increasing the accuracy of the trust evaluation mechanism in the cloud environments. On the other hand, a troll will make obvious and inflammatory statements that are meant to bait new entities into reacting, which is sometimes called trolling. Social networks as distributed systems usually have a special group of entities who have the ability and responsibility of banning those entities that they consider malicious or trolls (Ortega, Troyano, Cruz, Vallejo, & Enríquez, 2012). Also, they create a suspicious situation, such that an unplanned criticism can cause an inappropriate reaction.

In the cloud networks, users can use the services of the developer company until they are not scared of the destruction or disclosure of their information. Also, trust evaluation plays an important role in the cloud computing. Therefore, due to the importance of this problem, if there isn't any suitable trust evaluation mechanism, troll entities can easily enter the incorrect information in the network. On the other hand, opinion leaders are entities who may influence the behaviors or attitudes of others. Therefore, the leaders are needed in the cloud environments whose opinions can remarkably affect the customer trust. So, the main contribution of this paper is to improve the trust evaluation mechanism in the cloud environments using the opinion leaders' recommendations and removal of the troll entities. Our approach intends to build a degree of trust, according to availability, reliability, data integrity, identification and capability presented in the cloud environments. The approach also avoids the negative effects that the troll entities can cause in the network. Also, we applied three topological measures, including input-degree, output-degree and trust measure to identify the opinion leaders. Finally, the trust and reputation values are updated by removing the effect of troll entities and using the advice of opinion leaders.

The rest of the paper is organized as follows. Section 2 discusses the related works. Section 3 introduces our approach. The design and the results of the experiments performed to test our approaches are shown in sections 4 and the discussion is provided in section 5. Finally, in section 6 we point out the conclusions and future work in this field.

2. Related work

In this section, we review the relevant literature in term of trust, opinion leaders and troll entities in the cloud environments.

2.1. Trust in cloud computing

Yang and Chen (2009) have proposed a dynamic trust evaluation model on C2C marketplaces. A dynamic model for assessing the credibility of each store on C2C marketplaces so that it can help to solve the present problems in the current models and create the most applicable and effective trust evaluation systems for C2C marketplaces. The advantage of this dynamic model will help to establish a credible environment on C2C marketplaces. But its method has low confidentiality.

Jie et al. (2010) have proposed a trust evaluation model based on the cloud model for C2C electronic commerce. Aiming at solving the problem of the transaction security in C2C e-commerce, a valuation model is proposed based on cloud model theory. By the use of merging algorithm of the trust cloud and similar computing in the trust cloud, the sub-attribute evaluation and comprehensive evaluation will be achieved. The advantage of this method is that it provides a valuable method for trust valuation in opened network. In this method, if the same value is not obtained or computing, then it will be an unsuccessful transaction.

Abbadi and Alawneh (2012) have proposed a framework to consider the cloud properties based on practical understanding of how clouds work. They proposed a foundation framework, which can help in addressing the identified challenges. The focus is on IaaS cloud type and on organizations as cloud entities. The proposed framework delegates the management of OD and HD to their own organization rather than to the provider. Also, the organization and