International Journal of Scientific Research in Computer Science and Engineering
Vol.4, Issue.4, pp.11-15, August (2016)

Research Paper

E-ISSN:2320-7639

Reputation Calculation and Trust Management System in Cloud Integrated Wireless Sensor Networks

V.S. Kumar[1*], G.K. Chakravarthi[2]

[1]Dept. of CSE, Sanketika Vidya Parishad Engineering College, Visakhapatnam – India
[2]Dept. of CSE, Sanketika Vidya Parishad Engineering College, Visakhapatnam - India

Corresponding Author: sampath.tinku@gmail.com

Available online at www.isroset.org

Received: Jun/22/2016, Revised: Jul/02/2016, Accepted: Aug/17/2016, Published: Aug/30/2016

Abstract—The integration in Cloud computing with Wireless sensor network has been attracting several researchers in the industry as it provides many opportunities for organizations by contributing a range of computing services. So, data gathering capability of wireless sensor networks (WSNs) become easy. For cloud computing to become widely adopted by both the enterprises and individuals, several issues have to be solved. However, authentication as well as trust and reputation calculation and management of cloud service providers (CSPs) and sensor network providers (SNPs) are two very critical and barely explored issues for this new paradigm. Trust management is one of the most challenging issues in the emerging cloud computing area. During the past few years, many studies have suggested different techniques to address trust management issues. Yet, despite these past efforts, several trust management issues such as identification, privacy, personalization, integration, security, and scalability have been usually neglected and need to be addressed. In this article, we present an overview of the cloud service models and we survey the main techniques and research prototypes that adequately support trust management of services in cloud environments. We present a generic analytical framework that assesses existing trust management research prototypes in cloud computing and relevant areas using a set of assessment criteria. Open research issues for trust management in cloud environments are also discussed.

Keywords- Cloud; sensor networks; integration; authentication; trust; reputation

I. INTRODUCTION

Distributed systems like peer-to-peer systems, grid, clusters and cloud computing have become very popular among users in the recent years. User's access distributed systems for different reasons such as downloading files, searching for information, obtaining goods and services or executing applications hosted remotely. With the popularity and growth of distributed systems, the service providers make modern services available on the system. All these services and service providers will have differing levels of quality and also, due to the anonymous nature of the systems, some untrustworthy suppliers may tend to cheat unsuspicious clients. Therefore it becomes necessary to identify the quality of services and service providers who would meet the requirements of the customers.

Cloud computing has been called the 5th advantage in line of electricity, water, telephony and gas. The reason why cloud has been classified with such a name is that cloud computing has been changing the way computer resources have been used up to now. Till the development of cloud computing, computing resources were invested completely or leased in the form of committed hardware and software resources. Cloud computing has brought an ideal change in how computing resources have been purchased. With the arrival of cloud computing, users can use the services that have been hosted on the internet without concerning about whether they have been hosted or handled in such a manner that the customers have to pay only for the services they utilize as in the case of making use of other services. Cloud providers host their resources through internet on virtual computers and make them available to multiple clients. Multiple virtual computers can run on one physical computer sharing the resources such as storage, memory, the CPU and interfaces giving the feeling to the client that each client has his own committed hardware to work on. Virtualization therefore gives the ability to the providers to sell the same hardware resources among multiple clients. This sharing of the hardware resources by multiple clients help minimizes the cost of hardware for clients while developing profits of providers.

Accessing or selling the hardware in the form of virtual computers is known as Infrastructure as Service (IaaS) in the cloud computing terminology. Once a client has bought up the infrastructure from a service provider, he is free to install and run any type of operating system platform and application on it. Other kinds of services that are made obtainable via the cloud computing model are Platform as a Service (PaaS) and

Software as a Service. Under PaaS, the development platform in the form of an operating system has been made available where customers can present the environment to suit their requirements and install their development tools. PaaS helps developers to develop and deploy applications without the cost of buying and managing the underlying hardware and software. PaaS provides all the required ease for the complete life cycle of building and delivering web applications. So PaaS usually offers facilities for application design, application development, testing, deployment and hosting as well as application services such as the team collaboration, web service integration and marshalling, database integration, security, scalability, storage, persistence, state management, application versioning, application instrumentation and developer community ease. SaaS is the cloud model where an application hosted by a service provider on the internet is made available to users in a ready to use state. SaaS removes the requirement of installation and maintenance of the application in the user‘s local computer or server in his premises. SaaS has the benefit of being accessible from any place at any time, no installation or maintenance, no in advance cost, no licensing cost, scalability, reliability and flexible payment schemes to suit the customer‘s requirements.

In this paper the authors take a look at the trust and trust management systems along with the trust models developed for the distributed systems. Then a critical look at the trust development and management systems for cloud computing systems reported in literature in the recent times has been taken with special reference to the pros and cons of each suggestion.

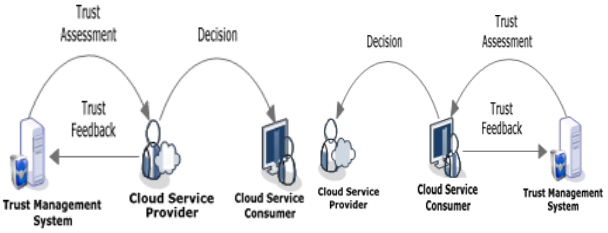
II. RELATED WORK

Trust management is one of the most important problems in the area of information security and several surveys have been conducted. One of the first few observations that tackles trust problems is done by Grandison and Sloman [1]. This observation outlines trust definitions from computer science, economic, and social psychology perspectives. It also outlines the trust relationship properties and trust classes that represent different types of trust. Suryanarayana and Taylor categorize trust management into three types, namely policy-based, reputation-based, and social network-based [2]. The authors compare nine trust management systems based on eleven different criteria parameters. Ruohomaa and Kutvonen outline several trust models [3]. They define trust actors and classify trust management into three tasks, including i) initialization of trust relationships, ii) behavior observation and iii) actions after a new experience. Artz and Gil compare several trust definitions for different research areas in the field of computer science [4]. Specifically, the authors discuss the relevance of trust and the semantic Web and point out some unique trust management challenges for the area. Finally, Fernandez-Gago et al. perform a trust management survey concentrating on wireless sensor networks. The observation overviews existing trust management solutions for ad-hoc and the peer-to-peer (P2P) wireless sensor networks [5]. A few surveys focus on the reputation-based trust management systems. For example, Marti and Garcia-Molina exploit a taxonomy technique to categorize different reputation-based trust management systems [6]. Sabater and Sierra overview the reputation-based trust management and scrutinize, the relationship between existing solutions and agent based perspective [7]. Agent-based or multi-agent trust and reputation systems use an artificial intelligence way where autonomous and intelligent software agents are used to notice and search for dependable entities in order to make better decisions. Josang et al. discuss general ideas of trust (e.g., trust classes and trust purpose) and explain the overlapping notions between trust and reputation terms. A few trust models are compared in the survey [8]. Silaghi et al. investigate whether existing trust management outlines can be applied to Grid environments [9]. A few instructions are given in the survey that may be useful to later research and the development of trust management systems in Grids. Wang and Vassileva present a systematic review of several trust and reputation systems. They categorize these systems into three categories including centralized versus decentralized, persons/agents versus resources, and global versus personalized [10]. A few potential research directions are given in the surveys that help develop reliable Web services. In [Hoffman et al. 2009], Hoffman et al. survey several attacks and defense mechanisms of reputation systems, particularly in P2P environments [11]. They specify the reputation system’s components and classify attacks against each component. Various defense mechanisms are also suggested. Most of the recent observations lack an integrated view on trust management techniques (e.g., policy, reputation, recommendation, and prediction) [12]. In particular, trust management issues such as distrusted feedbacks, poor identification of trust feedbacks, privacy of trust participants, and the lack of trust feedbacks integration have not been fully discussed. Additionally, our observation compares thirty representative trust management research prototypes based on fourteen different dimensions (i.e., assessment parameters) [13]. Our work specifically focuses on trust management issues in cloud environments, which makes original contributions by presenting trust management perspectives, a categorization of various trust management systems and an analytical framework for trust management prototypes assessment [14].

III. OVERVIEW OF TRUST MANAGEMENT

Trust management is initially developed by Blaze et. al [Blaze et al. 1996] to overcome the problem of centralized security systems, such as centralized control of trust relationships (i.e., global certifying authorities), inflexibility to support complex trust relationships in large-scale networks, and the heterogeneity of policy languages. Policy languages in trust management are responsible for setting

permission roles and implementing security policies. Permission roles are satisfied through a set of security policies, which themselves are satisfied through a set of credentials. Some early efforts to implementing the trust management are PolicyMaker and KeyNote [Blaze et al. 1998; Blaze et al. 1998; Blaze et al. 1999; Blaze et al. 2000]. These approaches are reckoned as policy-based trust management because they depend on policy roles to provide automated authorizations. Later, trust management inspired many researchers to specify the same concept in different environments such as e-commerce, P2P systems, Web services, wireless sensor networks, grid computing, and most recently cloud computing.



(a) Service Provider's Perspective (SPP) (b) Service Requester's Perspective (SRP)

Figure 1. Trust Management Perspectives

Trust management is an effective approach to assess and establish trusted relationships. Several approaches have been proposed for managing and assessing trust based on different perspectives. We classify trust management using two different perspectives, namely: Service Provider Perspective (SPP) and Service Requester Perspective (SRP). In SPP, the service provider is the main driver of the trust management system where service requesters' trustworthiness is assessed (Figure 1(a)). On the other hand, in SRP, the service requester is the one who assesses the trustworthiness of the service provider (Figure 1(b)).

IV. PROPOSED SYSTEM

In this section, we propose a generic analytical framework for trust management in cloud environments (see Figure 2). In the framework, interactions in cloud applications occur at three layers. For each layer, a set of dimensions is identified that will be used as a benchmark to evaluate and analyze existing trust management research prototypes.

A. Layer of the Trust Management Framework

The three layers of the trust management framework include: the trust feedback sharing layer, the trust assessment layer, and the trust result distribution layer (Figure 2). —Trust Feedback Sharing Layer (TFSL). TFSL consists of different parties including cloud service consumers and providers, which give trust feedbacks to each other. These feedbacks are maintained via a module called the Trust Feedback Collector. The feedbacks storage relies on the trust management systems, in the form of centralized, decentralized or even in the cloud environment through a trusted cloud service provider. —Trust Assessment Layer (TAL). This layer represents the core of any trust management system: trust assessment. The assessment might contain more than one metrics. TAL handles a huge amount of trust assessment queries from several parties through a module called the Trust Result Distributor. This typically involves checking the trust results database and performing the assessment based on different trust management techniques (more details on trust management techniques can be found in Section 4.1). TAL delivers the trust results to a database in the trust results distribution layer through the module of the trust result distributor. This procedure is taken to avoid redundancy issues in trust assessment. —Trust Result Distribution Layer (TRDL). Similar to TFSL, this layer consists of different parties including cloud service consumers and providers, which issue trust assessment inquiries about other parties (e.g., a cloud service consumer inquires about a specific cloud service).

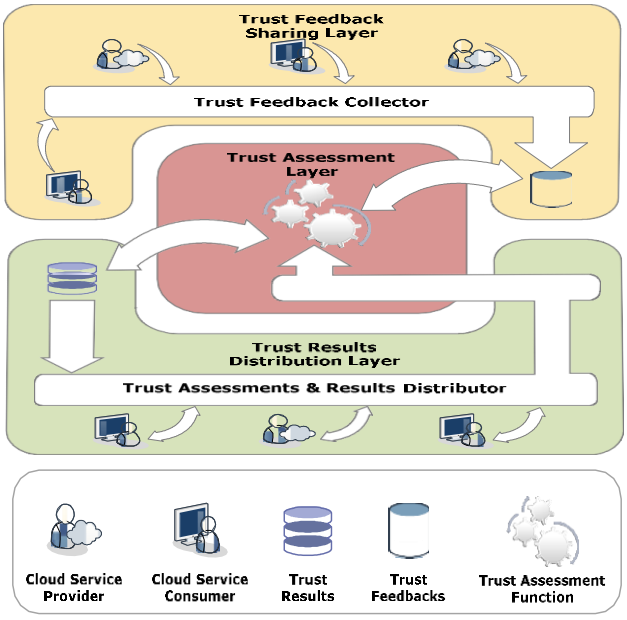


Figure.2. Architecture of the Trust Management Analytical Framework

All trust assessment inquiries are transmitted to the trust assessment function through the module of trust assessment and results distributor. The final results are maintained in a database where cloud service consumers and providers can retrieve.

B. Dimensions for Evaluating Trust Management Frameworks

We identify a set of dimensions to study trust management issues where each layer of the framework has several dimensions. These dimensions are identified by considering

the highly dynamic, distributed, and non-transparent nature of cloud environments.

The Trust Feedbacks Sharing Layer. There are four dimensions in this layer: —Credibility. Credibility refers to the quality of the information or service that makes cloud service consumers or providers to trust the information or service. The credibility evaluation appears in several forms including the entity's credibility (e.g., a cloud service credibility) and the feedback credibility (more details are explained in Section 4.1.1). Since there is a strong relation between credibility and identification as emphasized in [David and Jaquet 2009], the parallel data (i.e., feedback) processing require a proper identity scheme [Wei et al. 2009] for cloud service consumers and providers. For example, if no proper identity scheme is deployed, the trust management system can easily suffer from attacks such as Sybil attacks [Friedman et al. 2007], which leads to low accuracy in trust results. —Privacy. This dimension refers to the degree of sensitive information disclosure that the cloud service consumers might face during the interactions with the trust management system. There are several cases of privacy breaches that may occur such as leaks of the cloud service consumers' sensitive information (e.g., user names, passwords, date of birth, address) or behavioural information (e.g., with whom the cloud service consumer interacted, the kind of cloud services the consumer showed interest, etc.). Indeed, cryptographic encryption techniques will decrease the data utilization [Ren et al. 2012] and traditional anonymization techniques (e.g., de-identification by removing personal identification information[Fung et al. 2010]) are inadequate in cloud environments [Roy et al. 2010] due to its highly dynamic and distributed nature. —Personalization. Personalization refers to the degree of autonomy that the cloud service consumers and providers adhere to the trust management rules. Both can have proper personalization in their feedback designs and executions. This means that cloud service consumers and providers can select the feedback process (e.g., automated or manually driven) and the techniques they prefer. Personalization is applicable if the trust management system has fully autonomous collaboration, where each participant needs to interact via well-defined interfaces that allow participants to have control over their feedback and the flexibility to change their feedback processes without affecting each other. It is difficult to have a fully autonomous collaboration because of the complex translation features it requires integration. Integration refers to the ability to integrate different trust management perspectives and techniques. Participants can give their feedback from different perspectives (i.e., the cloud service provider and the cloud service consumer) through different trust management techniques (i.e., reputation, policy, etc.). Combining several trust management techniques can generally increase the accuracy of the trust results.

The Trust Assessment Layer. There are six dimensions in this layer:

—Perspective. Some trust management approaches focus on the cloud service provider's perspective while others focus on the cloud service consumer's perspective. It is therefore crucial to determine the perspective supported by a trust assessment function. The more perspectives the trust management system support, the more comprehensive the trust management system becomes. —Technique. This dimension refers to the degree a technique can be adopted by the trust management system to manage and assess trust feedbacks. It is important to differentiate between the trust assessment functions that adopt a certain technique for trust management from the ones that adopt several trust management techniques together. Adopting several trust management techniques together can increase the accuracy of the trust results

—Adaptability. Adaptability refers to how quickly the trust assessment function can adapt to changes of the inquisitive parties (i.e., cloud service providers or cloud service consumers). Some trust assessment inquiries can follow certain customized criteria from the inquisitive parties (e.g., weighing the feedback based on the size of the transaction), while others may follow the general trust assessment metric. In addition, updating feedbacks and trust results may be used as another indicator of adaptability because of the highly dynamic nature of cloud environments where new cloud service providers and consumers can join while others might leave at any time. —Security. This dimension refers to the degree of robustness of the trust assessment function against malicious behaviours and attacks. There are two different security levels where attacks can occur: the assessment function security level and the communication security level. In the assessment function security level, there are several potential attacks against the trust assessment function including whitewashing [Lai et al. 2003], self-promoting [Douceur 2002], and slandering [Ba and Pavlou 2002]. Self-promoting and slandering attacks can either occur in a Non-collusive Malicious Behavior (e.g., an attacker gives numerous misleading feedbacks in a short period of time to increase or decrease the trust results of a cloud service) or Collusive Malicious Behavior (e.g., several attackers collaborate to give numerous misleading feedbacks). At the communication security level, there are several attacks such as Man-in-the-Middle (MITM) attack [Aziz and Hamilton 2009] and Denial-of-Service (DoS) attack or distributed Denial-of Service (DDoS) attack [Hussain et al. 2003]. —Scalability. Given the highly dynamic and distributed nature of cloud environments, it is important that the trust management system be scalable. The scalability dimension refers to the ability of the trust management system to grow in one or more aspects (e.g., the volume of accessible trust results, the number of trust assessment inquiries that can be handled in a given period of time, and the number of trust relationships that can be supported). Trust models that follow a centralized architecture are more prone to several problems including scalability, availability and security (e.g., Denial-of-Service (DoS) attack) [Hoffman et al. 2009]. —Applicability. This dimension refers to the degree that the trust assessment function can be adopted to support trust management systems deployed for cloud services. It is important to differentiate the type of cloud services where the trust assessment functions

are suitable. The more types of cloud services the trust assessment function can support, the more comprehensive the trust assessment function is.

V. CONCLUSION

Trust is widely regarded as one of the top obstacles for the adoption and the growth of cloud computing. In this article, we have presented a comprehensive survey that is, to the best of our knowledge, the first to focus on the trust management of services in cloud environments. We distinguish the trust management perspectives and classify trust management techniques into four different categories. We further propose a generic analytical framework that can be used to compare different trust management research prototypes based on a set of assessment criteria. We overview and compare 30 representative research prototypes on trust management in cloud computing and the relevant research areas. Along with the current research efforts, we encourage more insight and development of innovative solutions to address the various open research issues that we have identified in this work.

REFERENCES

[1]. C. Zhu, V.C.M. Leung, "*An Authenticated Trust and Reputation Calculatio n and Management System for Cloud and Sensor Networks Integration*" IEEE Transactions on Information Forensics And Security, Vol. 10, No. 1, pp.118.131, 2015.

[2]. R. Piplode, P. Sharma, U.K. Singh, "*Study of Threats, Risk and Challenges in Cloud Computing*", International Journal of Scientific Research in Computer Science and Engineering, Vol.1, Issue.1, pp.26-30, 2013.

[3]. R. Buyya, C.S. Yeo, S. Venugopal, J. Broberg, I. Brandic, "*Cloud computing and emerging IT platforms : Vis ion, hype, and reality for delivering computing as the 5th utility*", Future Generation Computer System, Vol.25, No.6, pp.599–616, 2009.

[4]. C. Santhiya, KA. Vanishree, M.K. Chandrasekaran, "*Secured Group Data Bestow with Key-Agglomerative Searchable Encryption via Cloud Storage*", International Journal of Computer Sciences and Engineering, Vol.3, Issue.9, pp.242-247, 2015.

[5]. K.M. Sim, "*Agent-based cloud computing*", IEEE Transaction Services Computer, Vol.5, No.4, pp. 564–577, 2012.

[6]. Aditya Singh Mandloi and Vineeta Choudhary, "*Study of Various Techniques for Data Gathering in WSN"*, International Journal of Scientific Research in Network Security and Communication, Vol..1, Issue.3, pp.12-15, 2013.

[7]. C. Zhu, L. Shu, T. Hara, L. Wang, S. Nishio, L.T. Yang, "*A survey on communication and data management issues in mobile sensor networks*", Wireless Communication Mobile Computer, Vol.14, No. 1, pp. 19–36, 2014.

[8]. M. Li and Y. Liu, "Underground coal mine monitoring with wireless sensor networks," ACM Transaction Sensor Network., Vol.5, No.2, pp.1-29, 2009.

[9]. Q. Zhang, L. Cheng, R. Boutaba, "*Cloud computing: State-of-theart and research challenges*", Journal of Internet Services Applications, Vol. 1, No. 1, pp.7–18, 2010.

[10]. R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, I. Brandic, "*Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility*", Future Generation Computer System, Vol.25, No.6, pp.599–616, 2009.

[11]. J. Baliga, R. W. A. Ayre, K. Hinton, R. S. Tucker, "*Green cloud computing: Balancing energy in processing, storage, and transpor*t", Proceeding of IEEE, Vol. 99, No.1, pp.149–167, 2011.

[12]. P. Kaur, S. Majithia, "*Implementation and Analysis of Replicated Agent Based Load Balancing In Cloud Computing*", International Journal of Computer Sciences and Engineering, Vol.2, Issue.8, pp.21-27, 2014.

[13]. F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "Wireless sensor networks: A survey," Comput. Netw., Int. J. Comput. Telecommun. Netw., vol. 38, no. 4, pp. 393–422, Mar. 2002.

[14]. Mohd.A. Salam, A.C. Pandey, "*Mobile Cloud Computing: Taking Web-Based Mobile Applications to the Cloud*", International Journal of Computer Sciences and Engineering, Vol.2, Issue.1, pp.35-42, 2014.

