ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.9

An Authenticated Trust and Reputation Calculation and Management System for Cloud and Sensor Network Integration

Harshakumar.H.S[1], H.R.Divakar[2]
Student[1], Assistant Proffesor[2]
Department of MCA
PES College of Engineering, Mandya, Karnataka, India

Abstract:
Inveigle by incorporating the data storage and data processing abilities of cloud computing as well as omnipresent data gathering capability of wireless sensor networks (WSNs), CC-WSN integration received a lot of attention from both academia and industry. However, validates as well as trust and reputation calculation and management of cloud service providers (CSPs) and sensor network providers (SNPs) are two very critical and hardly issues for this new model. To full fill the gap, this paper proposes a new validates belief, reputation calculation and management (ATRCM) system for CC-WSN integration. Considering the authenticity of CSP and SNP, the attribute requirement of cloud service user (CSU) and CSP, the cost, trust, and reputation of the service of CSP and SNP, the proposed ATRCM system achieves the following three functions: Authenticating CSP and SNP to avoid malevolent impersonation attacks. Calculating and managing trust and reputation regarding the service of CSP and SNP. Helping CSU choose desirable CSP and assisting CSP in selecting appropriate SNP. Detailed analysis, design and further functionality evaluation results are projected to demonstrate the effectiveness of ATRCM, followed with system security analysis.

Keywords: Wireless Censor Network Providers, Cloud Service Providers.

I. INTRODUCTION

Trust management is one of the most challenging issues for the adoption and growth of cloud computing. The highly dynamic, distributed, and non-transparent nature of cloud services introduces several challenging issues such as privacy, security, and availability. Preserving consumers' privacy is not an easy task due to the sensitive information involved in the interactions between consumers and the trust management service. Protecting cloud services against their malicious users (e.g., such users might give misleading feedback to disadvantage a particular cloud service) is a difficult problem. Guaranteeing the availability of the trust management service is another significant challenge because of the dynamic nature of cloud environments. We describe the design and implementation of Cloud Armor, a reputation-based trust management framework that provides a set of functionalities to deliver Trust as a Service (TaaS), which includes i) a novel protocol to prove the credibility of trust feedbacks and preserve users' privacy, ii) an adaptive and robust credibility model for measuring the credibility of trust feedbacks to protect cloud services from malicious users and to compare the trustworthiness of cloud services, and iii) an availability model to manage the availability of the decentralized implementation of the trust management service. The feasibility and benefits of our approach have been validated by a prototype and experimental studies using a collection of real-world trust feedbacks on cloud services.

II. RELATED WORK

According to researchers at Berkeley, trust and security is ranked one of the top 10 obstacles for the adoption of cloud computing. Indeed, Service-Level Agreements (SLAs). Consumers' feedback is a good source to assess the overall trustworthiness of cloud services. Several researchers have recognized the significance of trust management and proposed solutions to assess and manage trust based on feedbacks collected from participants.

III. LITERATURE SURVEY

A Survey of Trust and Reputation Management Systems in Wireless Communications: By Han Yu, Zhiqi Shen, Chunyan Miao, Cyril Leung, and Dusit Niyato Trust is an important concept in human interactions which facilitates the formation and continued existence of functional human societies. In the first decade of the 21st century, computational trust models have been applied to solve many problems in wireless communication systems. This cross disciplinary research has yielded many innovative solutions. In this paper, we examine the latest methods which have been proposed by researchers to manage trust and reputation in wireless communication systems. Specifically, we survey the state of the art in the application of trust models in the fields of mobile ad hoc networks (MANETs), wireless sensor networks (WSNs), and cognitive radio networks (CRNs). We classify the mainstream methods into natural categories and illustrate how they complement each other in achieving design goals. Major research directions are also outlined.

A survey on communication and data management issues in mobile sensor networks: C Zhu1, Lei Shu, Takahiro Hara, LeiWang, Shojiro Nishio and Laurence T. Yang1 Wireless sensor networks (WSNs) which is proposed in the late 1990s have received unprecedented attention, because of their exciting potential applications in military, industrial, and civilian areas (e.g., environmental and habitat monitoring). Although WSNs have become more and more prospective in human life with the development of hardware and communication technologies, there are some natural limitations of WSNs (e.g., network connectivity, network lifetime) due to the static network style in WSNs. Moreover, more and more application scenarios require the sensors in WSNs to be mobile rather than static so as to make traditional applications in WSNs become smarter and enable some new applications. All this induce the mobile wireless sensor networks (MWSNs) which can greatly promote the development and application of WSNs. However, to the best of our knowledge, there is not a comprehensive survey about the communication and data management issues in MWSNs. In this paper, focusing on researching the communication issues and data management issues in MWSNs, we discuss different research methods regarding communication and data management in MWSNs and propose some further open research areas in MWSNs.

IV. PROPOSED SYSTEM

According to researchers at Berkeley, trust and security is ranked one of the top 10 obstacles for the adoption of cloud computing. Indeed, Service-Level Agreements (SLAs). Consumers' feedback is a good source to assess the overall trustworthiness of cloud services. Many researchers have identified the importance of trust management and suggest solutions to determine and manage trust based on feedbacks gathered from participants.

V. SYSTEM ARCHITECTURE

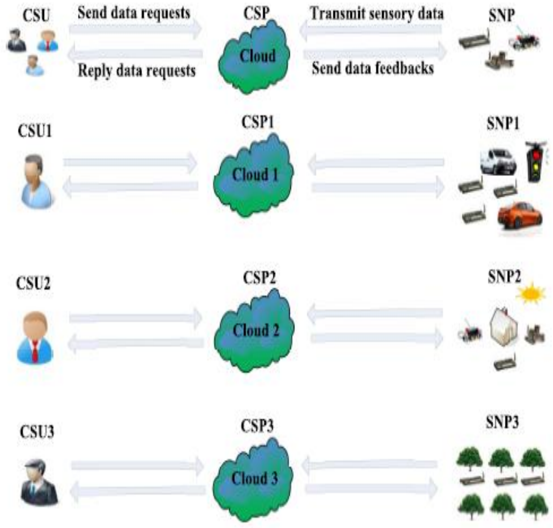

Figure.1. System Architecture

1. System Model:

There are multiple CSUs, CSPs and SNPs. Each CSU, CSP and SNP has several attributes. Particularly, the data service requested and required by the CSU owns the following attributes: data service pay (DSP); data type (DT); data size (DS); data request speed (DRS); data service time (DST). The cloud service provided and managed by each CSP has the following characteristics: cloud service charge (CSC); cloud operation cost (COC); sensor network service pay (SNSP); cloud service type (CST); cloud server number (CSN); cloud storage size (CSS); cloud processing speed (CPS); cloud operation time (COT).

2. Authentication of CSP and SNP:

In this module, we first develop the authentication of CSP and SNP. With that, we give some preliminaries about service level agreement (SLA) and privacy level agreement (PLA), followed with the preliminaries of trust and reputation and the preliminaries of trusted center entity (TCE). In this paper, as the key of our work is to enable CSU to choose the authentic and desirable CSP as well as assist CSP in selecting genuine and appropriate SNP, we focus on the authentication of CSP and SNP rather than the authentication of CSU. Specifically, the CSP needs to prove its authenticity to CSU and SNP has to show its authenticity to CSP. Generally, to evaluate trust from an entity (e.g., A or trustor) to another entity (e.g., B or trustee), A needs to gather evidence (e.g., honest, selfish, malicious behaviors), representing the satisfaction, about B either through direct interaction or information provided by third-parties.

3. Trust and Reputation of Service of CSP and SNP

In this module, we can obtain that the fulfillment of service of CSP needs to receive and store the raw sensory data from SNP first. Then CSP processes the raw sensory data and stores the processed sensory data. Finally, CSP transmits the processed sensory data to CSU on demand. In this process, there are various types of trust (e.g., cloud data storage trust, cloud data processing trust, cloud data privacy trust, cloud data transmission trust) which might concern the CSU to choose the service of CSP.

4. ATRCM system

In this module, we implement the proposed authenticated trust and reputation calculation and management (ATRCM) system with Authentication flowchart of CSP and SNP; Trust and reputation calculation and management flowchart between CSU and CSPs; Trust and reputation calculation and management flowchart between CSP and SNPs.

VI. CONCLUSION

Given the highly dynamic, distributed, and non-transparent nature of cloud services, managing and establishing trust between cloud service users and cloud services remains a significant challenge. Cloud service users' feedback is a good source to assess the overall trustworthiness of cloud services. However, malicious users may collaborate together to i) disadvantage a cloud service by giving multiple misleading trust feedbacks (i.e., collusion attacks) or ii) trick users into trusting cloud services that are not trustworthy by creating several accounts and giving misleading trust feedbacks (i.e., Sybil attacks). In this paper, we have presented novel techniques that help in detecting reputation based attacks and allowing users to effectively identify trustworthy cloud services. In particular, we introduce a credibility model that not only identifies misleading trust feedbacks from collusion attacks but also detects Sybil attacks no matter these attacks take place in a long or short period of time (i.e., strategic or occasional attacks respectively). We also develop an availability model that maintains the trust management service at a desired level. We have collected a large number of consumer's trust feedbacks given on real world cloud services.

VII. FUTURE ENHANCEMENT

There are a few directions for our future work. We plan to combine different trust management techniques such as reputation and recommendation to increase the trust results accuracy. Performance optimization of the trust management service is another focus of our future research work.

VIII. REFERNCES

[1]. S. M. Khan and K. W.Hamlen, “Hatman: Intra-Cloud Trust Management for Hadoop,” in Proc. CLOUD’12, 2012.

[2]. S. Pearson, “Privacy, Security and Trust in Cloud Computing,”in Privacy and Security for Cloud Computing, ser. Computer Communications and Networks, 2013, pp. 3–42.

[3]. J. Huang and D. M. Nicol, “Trust Mechanisms for Cloud Computing,”Journal of Cloud Computing, vol. 2, no. 1, pp. 1–14, 2013.

[4]. K. Hwang and D. Li, “Trusted Cloud Computing with Secure Resources and Data Coloring,” IEEE Internet Computing, vol. 14, no. 5, pp. 14–22, 2010.

[5]. M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “A View of Cloud Computing,” Communications of the ACM, vol. 53,no. 4, pp. 50–58, 2010.

[6]. S. Habib, S. Ries, and M. Muhlhauser, “Towards a Trust Management System for Cloud Computing,” in Proc. of TrustCom’11, 2011.

[7]. I. Brandic, S. Dustdar, T. Anstett, D. Schumm, F. Leymann, and R. Konrad, “Compliant Cloud Computing (C3): Architecture and Language Support for User Driven Compliance Management in Clouds,” in Proc. of CLOUD’10, 2010.