IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727
PP 01-04
www.iosrjournals.org

A Review Paper On An Authenticated Trust and Reputation Calculation and Management System for Cloud and Sensor Networks Integration

Arati Phadtare
(*RSCOE, University of Pune, Pune, Maharashtra India*)

Abstract: *The integration Cloud computing – Wireless sensor network has been attracting the attention of several researchers both in the academia and the industry as it provides many opportunities for organizations by offering 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. In any case, authentication as well as trust and reputation calculation and management of cloud service providers (CSPs) and sensor network suppliers (SNPs) are two exceptionally critical and barely explored issues for this new paradigm. To fill the gap, our paper proposes a novel authenticated trust and reputation calculation and management (ATRCM) framework for CC-WSN combination or integration. Considering the authenticity of CSP and SNP, the attribute necessity of cloud service user (CSU) and CSP, the expense, trust, and reputation of the service of CSP and SNP, the proposed ATRCM framework accomplishes the three functions: 1) verifying CSP and SNP to stay away from malicious impersonation attacks; 2) computing and managing trust and reputation with respect to the service of CSP and SNP; and 3) helping CSU choose desirable CSP and assisting CSP in selecting suitable SNP. Detailed analysis and design as well as further functionality evaluation result are presented to exhibit the effectiveness of ATRCM, followed with system security analysis.*

Keywords: *Cloud, sensor networks, integration, authentication, trust, reputation.*

I. Introduction

Computing is being transformed to a model consisting of services that are commoditized and delivered in a manner similar to traditional utilities such as water, electricity, gas, and telephony. In such a model, users access services based on their requirements without regard to where the services are hosted or how they are delivered. Cloud computing (CC) is a model to enable convenient, on-demand network access for a shared pool of configurable computing resources (e.g., servers, networks, storage, applications, and services) that could be rapidly provisioned and released with minimal management effort or service provider interaction. Wireless sensor networks (WSNs) are networks consisting of spatially distributed autonomous sensors, which are capable of sensing the physical or environmental conditions.

Objectives:

1) Authenticating CSP and SNP to avoid malicious impersonation attacks.
2) Calculating and managing trust and reputation regarding the service of CSP and SNP.
3) Helping CSU choose desirable CSP and assisting CSP in selecting appropriate SNP.

II. Literature Survey

1) 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.

2) 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.

3) A Cloud Design for User-controlled Storage and Processing of Sensor Data

Ren´e Hummen, Martin Henze, Daniel Catreiny, Klaus Wehrle.

Ubiquitous sensing environments such as sensor networks collect large amounts of data. This data volume is destined to grow even further with the vision of the Internet of Things. Cloud computing promises to elastically store and process such sensor data. As an additional benefit, storage and processing in the Cloud enables the efficient aggregation and analysis of information from different data sources. However, sensor data often contains privacy-relevant or otherwise sensitive information. For current Cloud platforms, the data owner looses control over her data once it enters the Cloud. This imposes adoption barriers due to legal or privacy concerns. Hence, a Cloud design is required that the data owner can trust to handle her sensitive data securely. In this paper, we analyze and define properties that a trusted Cloud design has to fulfill. Based on this analysis, we present the security architecture of SensorCloud. Our proposed security architecture enforces end-to-end data access control by the data owner reaching from the sensor network to the Cloud storage and processing subsystems as well as strict isolation up to the service-level. We evaluate the validity and feasibility of our Cloud design with an analysis of our early prototype. Our results show that our proposed security architecture is a promising extension of today's Cloud offers.

4) SecuredTrust: A Dynamic Trust Computation Model for Secured Communication in Multi-Agent Systems

Authors: Anupam Das and M. Mahfuzul Islam, *Member, IEEE.*

Security and privacy issues have become critically important with the fast expansion of multi-agent systems. Most network applications such as pervasive computing, grid computing and P2P networks can be viewed as multi-agent systems which are open, anonymous and dynamic in nature. Such characteristics of multi-agent systems introduce vulnerabilities and threats to providing secured communication. One feasible way to minimize the threats is to evaluate the trust and reputation of the interacting agents. Many trust/reputation models have done so, but they fail to properly evaluate trust when malicious agents start to behave in an unpredictable way. Moreover, these models are ineffective in providing quick response to a malicious agent's oscillating behavior. Another aspect of multi-agent systems which is becoming critical for sustaining good service quality, is the even distribution of workload among service providing agents. Most trust/reputation models have not yet addressed this issue. So, to cope with the strategically altering behavior of malicious agents and to distribute workload as evenly as possible among service providers; we present in this paper a dynamic trust computation model called 'SecuredTrust'. In this paper we first analyze the different factors related to evaluating the trust of an agent in a and then propose a comprehensive quantitative model for measuring such trust. We also propose a novel load balancing algorithm based on the different factors defined in our model. Simulation results indicate that our model compared to other existing models can effectively cope with strategic behavioral change of malicious agents and at the same time efficiently distribute workload among the service providing agents under stable condition.

5) A Survey of Attack and Defense Techniques for Reputation Systems
Authors: Kevin Hoffman, David Zage, and Cristina Nita-Rotaru.

Reputation systems provide mechanisms to produce a metric encapsulating reputation for a given domain for each identity within the system. These systems seek to generate an accurate assessment in the face of various factors including but not limited to unprecedented community size and potentially adversarial environments. We focus on attacks and defense mechanisms in reputation systems. We present an analysis framework that allows for general decomposition of existing reputation systems. We classify attacks against reputation systems by identifying which system components and design choices are the target of attacks. We survey defense mechanisms employed by existing reputation systems. Finally, we analyze several landmark systems in the peer-to-peer domain, characterizing their individual strengths and weaknesses. Our work contributes to understanding 1) which design components of reputation systems are most vulnerable, 2) what are the most appropriate defense mechanisms and 3) how these defense mechanisms can be integrated into existing or future reputation systems to make them resilient to attacks.

III. Existing System:

WSNs are widely focused because of their great potential in areas of civilian, industry and military (e.g., forest fire detection, industrial process monitoring, traffic monitoring, battlefield surveillance, etc.), which could change the traditional way for people to interact with the physical world. For instance, regarding forest fire detection, since sensor nodes can be strategically, randomly, and densely deployed in a forest, the exact origin of a forest fire can be relayed to the end users before the forest fire turns uncontrollable without the vision of physical fire.

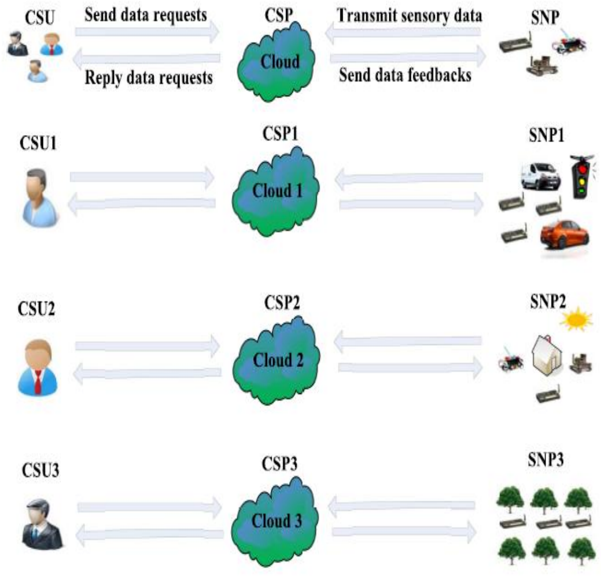
Disadvantageous of Existing System:

1. Security while authentication is less.
2. No trust.
3. Delay in accessing information.

IV. System Arcitecture:

This paper proposes a novel authenticated trust and reputation calculation and management (ATRCM) system for CC-WSN integration. Considering:

1. The authenticity of CSP and SNP.
2. The attribute requirement of cloud service user (CSU) and CSP.
3. The cost, trust and reputation of the service of CSP.



The system model is shown in Fig. 4.1

In the proposed ATRCM system, the SNP achieves the following goals:

1. Authenticating CSP and SNP to avoid malicious impersonation attacks;
2. Calculating and managing trust and reputation regarding the service of CSP and SNP;
3. Helping CSU choose desirable CSP and assisting CSP inselecting appropriate SNP.

Advantageous Of Proposed System:

1. There are different security policies for different domains.
2. The model considers the transaction context, the historical data of entity influences and the measurement of trust value dynamically.
3. The trust model is compatible with the firewall and does not break the firewall‘s local control policies.

V. Conclusion

We proposed a novel ATRCM system for CC-WSN integration. We explored the authentication as well as trust and reputation calculation and management of CSPs and SNPs, which are two very critical and barely explored issues with respect to CC and WSNs integration.

References

[1]. Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: State-of-theart and research challenges," J. Internet Services Appl., vol. 1, no. 1, pp. 7–18, 2010.

[2]. R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," Future Generat. Comput. Syst., vol. 25, no. 6, pp. 599–616, Jun. 2009.

[3]. J. Baliga, R. W. A. Ayre, K. Hinton, and R. S. Tucker, "Green cloud computing: Balancing energy in processing, storage, and transport," Proc. IEEE, vol. 99, no. 1, pp. 149–167, Jan. 2011.

[4]. K. M. Sim, "Agent-based cloud computing," IEEE Trans. Services Comput., vol. 5, no. 4, pp. 564–577, Fourth Quarter 2012.

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

[6]. C. Zhu, L. Shu, T. Hara, L. Wang, S. Nishio, and L. T. Yang, "A survey on communication and data management issues in mobile sensor networks," Wireless Commun. Mobile Comput., vol. 14, no. 1, pp. 19–36, Jan. 2014.

ABOUT AUTHOR

Arati Phadtare received B.E degree in Information Technology from Pune University, India in 2012 and pursuing ME degree in Computer Science and Engineering from Rajarshi Shahu College of Engineering, Pune, India.