Controlling System for Cloud and Sensor Networks by Authenticated Trust and Reputation Calculation Integration

Ms.Vedambika M
M.Tech Scholar, Dept. of Computer Science and Engineering,
New Horizon College of Engineering,
Bangalore, India
E-mail: veda299@gmail.com

Ms. Soja Rani S
Assistant professor,
Dept. of Computer Science and Engineering,
New Horizon college of Engineering
Bangalore, India
***E-mail:* soja.naveen@gmail.com**

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 computing, Wireless sensor network, cloud service providers, sensor network suppliers, authenticated trust and reputation calculation and management (ATRCM) and cloud service user (CSU).

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. 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. In addition, with respect to battlefield surveillance, as sensors are able to be deployed to continuously monitor the condition of critical terrains, approach routes, paths and straits in a battlefield, the activities of the opposing forces can be closely watched by surveillance center without the involvement of physical scouts.

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.

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).

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.

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

III. System Architecture

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.

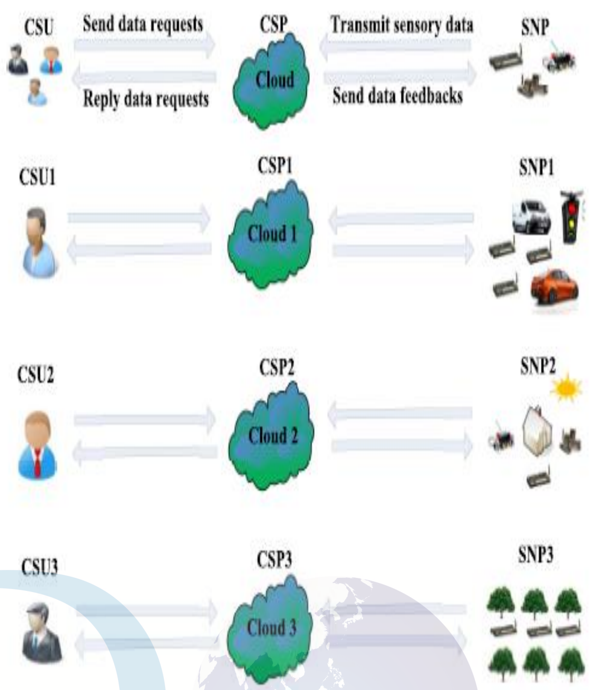


***Figure:* Example of application scenarios of CC-WSN integration.**

- ❖ To the best of our knowledge, there is no research discussing and analyzing the authentication as well as trust and reputation of CSPs and SNPs for CC-WSN integration. Filling this gap, this paper analyzes the authentication of CSPs and SNPs as well as the trust and reputation about the services of CSPs and SNPs.
- ❖ Further, this paper proposes a novel authenticated trust and reputation calculation and management (ATRCM) system for CC-WSN integration. Particularly,

considering (i) the authenticity of CSP and SNP; (ii) the attribute requirement of CSU and CSP; (iii) 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 malicious 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.

ADVANTAGES OF PROPOSED SYSTEM:

- ❖ This paper is the first research work exploring the trust and reputation calculation and management system with authentication for the CC-WSN integration, which clearly distinguishes the novelty of our work and its scientific impact on current schemes integrating CC and WSNs.
- ❖ This paper further proposes an ATRCM system for the CC-WSN integration. It incorporates authenticating CSP and SNP, and then considers the attribute requirement of CSU and CSP as well as cost, trust and reputation of the service of CSP and SNP, to enable CSU to choose authentic and desirable CSP and assists CSP in selecting genuine and appropriate SNP.

IV. PROPOSED AUTHENTICATED TRUST AND REPUTATION CALCULATION AND MANAGEMENT (ATRCM) SYSTEM

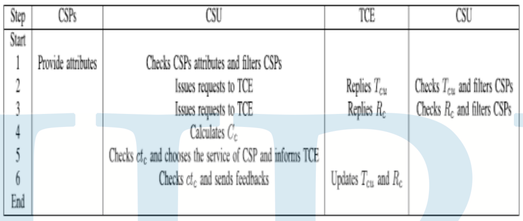
A. System Overview

The proposed authenticated trust and reputation calculation and management (ATRCM) system is introduced from the following three parts: Part 1) Authentication flowchart of CSP and SNP; Part 2) Trust and reputation calculation and management flowchart between CSU and CSPs; Part 3) Trust and reputation calculation and management flowchart between CSP and SNPs. Specifically, Part 1) shown in Table II aims at identity authentication of CSP and SNP to avoid malicious impersonation attacks, based on the certificate of ISO/IEC 27001 certification illustrated in Section IV. In addition, Part 2) and Part 3) are presented in Table III and

Table IV focus on (i) calculation and management of trust and reputation with respect to the service of CSP and SNP as well as (ii) helping the CSU choose desirable CSP and assisting the CSP in selecting appropriate SNP, considering the attribute requirement of CSU and CSP as well as cost, trust and reputation of the service of CSP and SNP.

TABLE III

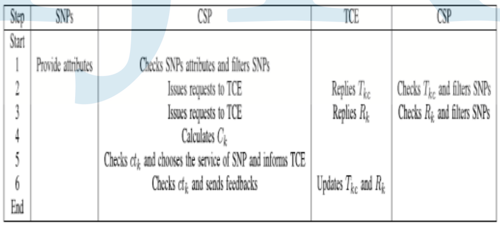
TRUST AND REPUTATION CALCULATION AND MANAGEMENT FLOWCHART BETWEEN CSU AND CSPS



Step	CSPs	CSU	TCE	CSU
Start				
1	Provide attributes	Checks CSPs attributes and filters CSPs		
2		Issues requests to TCE	Replies T_{cu}	Checks T_{cu} and filters CSPs
3		Issues requests to TCE	Replies R_c	Checks R_c and filters CSPs
4		Calculates C_c		
5		Checks ct_c and chooses the service of CSP and informs TCE		
6		Checks ct_c and sends feedbacks	Updates T_{cu} and R_c	
End				

TABLE IV

TRUST AND REPUTATION CALCULATION AND MANAGEMENT FLOWCHART BETWEEN CSP AND SNPS



Step	SNPs	CSP	TCE	CSP
Start				
1	Provide attributes	Checks SNPs attributes and filters SNPs		
2		Issues requests to TCE	Replies T_{kc}	Checks T_{kc} and filters SNPs
3		Issues requests to TCE	Replies R_k	Checks R_k and filters SNPs
4		Calculates C_k		
5		Checks ct_k and chooses the service of SNP and informs TCE		
6		Checks ct_k and sends feedbacks	Updates T_{kc} and R_k	
End				

V. EVALUATION OF SYSTEM FUNCTIONALITY

In this section, we evaluate whether our proposed ATRCM system can fulfill the predetermined functions: 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, based on (i) the authenticity of CSP and SNP; (ii) the attribute requirement of CSU and CSP as well as (iii) the cost, trust and reputation of the service of CSP and SNP.

A. Evaluation Setup

To perform the evaluation, all the three aimed functions are analyzed based on the flowcharts and processes of the corresponding functions. Particularly, the third function is evaluated utilizing two representative case studies to demonstrate the effectiveness of ATRCM. Case study 1 involves small quantities of CSUs, CSPs and SNPs, while case study 2 involves a large number of CSUs, CSPs and SNPs. The evaluation processes of the third function shown in these two case studies are universal for CSUs, CSPs and SNPs with other attributes and parameters.

Evaluation Results

Authenticating CSP and SNP: With respect to the authentication of CSP and SNP, Part 1) authentication flowchart of CSP and SNP shown in Section V presents the detailed steps. Based on the flowchart, we can observe that if a malicious attacker impersonates the authentic CSP or authentic SNP, then it needs to own the *ctc* certificate or the *ctk* certificate first. If it cannot provide a certificate, then it is not a genuine organization. In addition, even if the malicious attacker further a) offers a fake certificate (e.g., *f ctc* or *f ctk*) or b) provides a real but revoked certificate (e.g., *rctc* or *rctk*), it still cannot launch the impersonation attacks, since CSU and CSP check whether the signature of the certificate is valid and whether the certificate is revoked.

1) *Calculating and Managing Trust and Reputation of Service of CSP and SNP:* For the calculation and management of trust and reputation with respect to the service of the CSP and SNP.

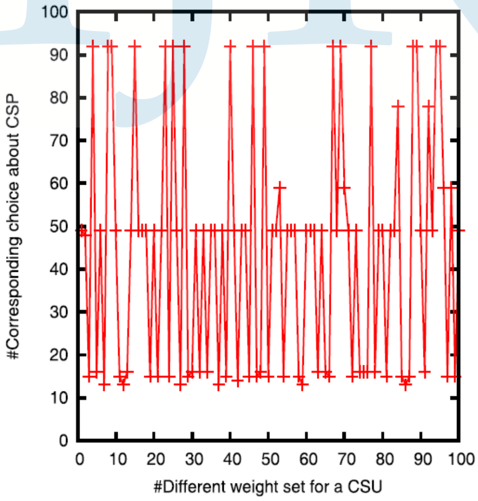


Fig. 2. Different weight set for a CSU and Corresponding Choice About CSP.

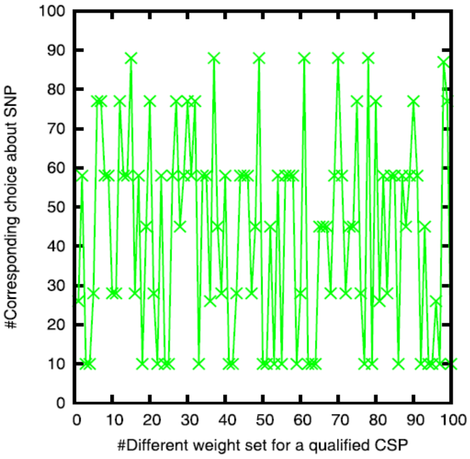


Fig. 3. Different weight set for a qualified CSP and corresponding choice about SNP.

VI. CONCLUSION

In this paper, we advancing 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. Further, we proposed a novel ATRCM system for CC-WSN integration. Discussion and analysis about the authentication of CSP and SNP as well as the trust and reputation with respect to the service provided by CSP and SNP have been presented, followed with detailed design and functionality evaluation about the proposed ATRCM system. All these demonstrated that the proposed ATRCM system achieves the following three functions for CC-WSN integration: 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, based on (i) the authenticity of CSP and SNP; (ii) the attribute requirement of CSU and CSP; (iii) the cost, trust and reputation of the service of CSP and SNP. In addition, our system security analysis powered by three adversary models showed that our proposed system is secure versus main attacks on a trust and reputation management system, such as good mouthing, bad mouthing, collusion and white-washing attacks, which are the most important attacks in our case.

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.

[8] M. Yuriyama and T. Kushida, "Sensor-cloud infrastructure—Physical sensor management with virtualized sensors on cloud computing," in *Proc. 13th Int. Conf. Netw.-Based Inf. Syst.*, Sep. 2010, pp. 1–8.

[9] G. Fortino, M. Pathan, and G. Di Fatta, "BodyCloud: Integration of cloud computing and body sensor networks," in *Proc. IEEE 4th Int. Conf. Cloud Comput. Technol. Sci.*, Dec. 2012, pp. 851–856.

[10] Y. Takabe, K. Matsumoto, M. Yamagiwa, and M. Uehara, "Proposed sensor network for living environments using cloud computing," in *Proc. 15th Int. Conf. Netw.-Based Inf. Syst.*, Sep. 2012, pp. 838–843.

[11] R. Hummen, M. Henze, D. Catrein, and K. Wehrle, “A cloud design for user-controlled storage and processing of sensor data,” in *Proc. IEEE 4th Int. Conf. Cloud Comput. Technol. Sci.*, Dec. 2012, pp. 232–240.

[12] C. Zhu, V. C. M. Leung, L. T. Yang, X. Hu, and L. Shu, “Collaborative location-based sleep scheduling to integrate wireless sensor networks with mobile cloud computing,” in *Proc. IEEE Globecom Workshops*, Dec. 2013, pp. 452–457.

[13] C. Zhu, V. C. M. Leung, H. Wang, W. Chen, and X. Liu, “Providing desirable data to users when integrating wireless sensor networks with mobile cloud,” in *Proc. IEEE 5th Int. Conf. Cloud Comput. Technol. Sci.*, Dec. 2013, pp. 607–614.

[14] A. Alamri, W. S. Ansari, M. M. Hassan, M. S. Hossain, A. Alelaiwi, and M. A. Hossain, “A survey on sensor-cloud: Architecture, applications, and 2016.