ISSN No.: 2455-6130
Volume 1, Issue 3, 2016, pp. 12-18

website: www.ijoetr.com

International Journal of Emerging Trends in Research

Integration of Cloud with Sensor Networks

R. Rajalakshmi[1,*], V. Ramya[2], S. Anusha[3]
[1, 2, 3] *Department of Computer Science and Engineering, Dhanalakshmi College of Engineering, Chennai (TN), India*

* Corresponding author. E-mail: rajirajendern2012@gmail.com (R. Rajalakshmi)

Abstract

Induced by including the powerful data storage and data processing capability of cloud computing as well as everywhere data gathering ability of wireless sensor networks, this integration received a lot of attention from both industry and academia. However, verification as well as trust and reputation calculation and organization of cloud service providers and sensor network providers are two very serious and hardly explored issues for this new paradigm. To fill the gap, this paper suggests an authenticated trust and reputation calculation and organization system for this integration. In view of the validity of SNP and CSP, the attribute requirement of cloud service user and CSP, the trust, cost, and reputation of the service of SNP and CSP, the suggested ATRCM system achieves the three functions as: calculating and managing trust and reputation regarding the service of CSP and SNP; authenticating CSP and SNP to avoid malicious impersonation attacks; helping CSU choose desirable CSP and assisting CSP in selecting appropriate SNP.

Keywords: Wireless sensor networks; CC-WSN integration; ATRCM system.

1. Introduction

The mobile computing is human–computer interface by which a computer is likely to be transported during usual usage. Mobile computing rivet mobile communication, mobile hardware, and mobile software. The communication issues comprise ad hoc and infrastructure networks and communication properties, protocols, data formats and concrete technologies. Hardware contains mobile devices or device components. Mobile software contracts with the characteristics and necessities of mobile application. Mobile Computing is a skill that allows transmission of data, voice and video via a computer or any other wireless enabled tool without having to be connected to a fixed physical link [1-3]. This paper will give an impression of mobile computing and then it will take through how it evolved and where is the skill headed to in potential along with the classifications and safety issues involved.

The wireless sensor networks (WSN) is a key skill extensively applied in a lot of fields, such as transportation, health-care and environment monitoring. Despite rapid development, the exponentially rising data emanating from WSN is not professionally stored and used. Besides, the

data from manifold different types and locations of WSN wants to be well analyzed, fused and supplied to a variety of types of clients, such as PC, workstation and smart phone. The rising cloud computing technology offers scalable data process and storage power and a few types of connectable services, which can helpfully use sensor data from WSN. In this paper, we suggest an integration framework of cloud computing with WSN, in which sensor data is transmit from WSN to cloud and procedure and stored in cloud, then mined and analyzed so as to be supplied to a variety of clients. By applying virtualization and cloud storage skill, and Infrastructure as a Service and Software as a Service of cloud service model, the frameworks can fully process and store mass sensor data from manifold types of WSN. In addition, it efficiently mines and analyses sensor data, based on which the data purpose are well supplied to various types of clients in form of services.

According to the national institute of standards and technology (NIST), *Cloud Computing (CC) is an innovative technological paradigm that provides convenient, on-demand network access to a shared pool of configurable computing resources (for example, sensors) that can be rapidly provisioned and released with minimal management effort or service provider interaction.* This means that Cloud Computing offers several benefits such as on-demand self-service, resource pooling (location independence), broad network access, rapid elasticity, measured service, massive scale, homogeneity, virtualization, resilient computing, low cost software, geographic distribution, service orientation and advanced security [4-7]. The idea of integrating a Wireless Sensor Network (WSN) nodes which consists of a huge number of low-cost, low-power, multifunctional and resource-constrained sensor nodes with cloud computing is a thing of interest in this paper; bearing in mind WSN are designed with the flexibility to resist harsh environmental situation in some cases while other cases it is difficult. In the proceedings of the Information Integration and Web-based use & Services conference; iiWAS2009, some research papers offered a concept and implementation of combining Wireless Sensor Networks with Cloud computing.

2. Related work

The trust is significant concept in human interactions which facilitates the pattern and continued existence of functional human societies. In the first decade of the 21st century, computational trust models were implemented to solve many problems in wireless communication systems. This cross disciplinary research has yielded a lot of innovative solutions. In this paper, we inspect the latest methods which have been projected by researchers to manage trust and reputation in wireless communication systems. Purposely, we review the state of the art in the application of trust models in the fields of mobile ad hoc networks (MANETs), cognitive radio networks (CRNs) and wireless sensor networks (WSNs). We classify the mainstream techniques into natural categories and illustrate how they complement each other in attaining design goals.

Wireless sensor networks (WSNs) which are planned in the late 1990s have received unprecedented attention, as of their exciting potential use in military, industrial, and civilian areas. Although WSNs have become more and more potential in human life with the development of hardware and communication skill, there are some natural limits of WSNs (e.g., network connectivity, network lifetime) due to the static network style in WSNs [8-11]. Furthermore, more application scenarios require the sensors in WSNs to be mobile rather than static so as to make traditional use in WSNs become smarter and enable some new applications. All this bring

the mobile wireless sensor networks (MWSNs) which can greatly promote the development and use of WSNs. on the other hand, to the best of our knowledge, there is not a comprehensive review 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 argue different research methods regarding communication and data management in MWSNs and suggest some further open research areas in MWSNs.

Everywhere sensing environments such as sensor networks meet large amounts of data. This data quantity is destined to grow even further with the dream of the Internet of Things. Cloud computing assure to elastically store and process such sensor data. As an extra benefit, storage and processing in the Cloud allow the efficient aggregation and study of information from diverse data sources. On the other hand, sensor data often hold privacy-relevant or otherwise sensitive information. For current Cloud platforms, the data owner loses control over the data once it enters the Cloud. This imposes adoption fence due to legal or privacy anxiety. Hence, a Cloud design is necessary that the data owner can trust to handle her sensitive data securely. In this manuscript, we analyze and define assets that a trusted Cloud design has to fulfill. Based on this study, we proposed the security architecture of Sensor Cloud. Our planned security architecture enforces end-to-end data access control by the data owner reaching from the sensor network to the Cloud storage and dispensation subsystems as well as strict isolation up to the service-level. We assess the validity and feasibility of our Cloud design with psychoanalysis of our early prototype. Our results show that our proposed security architecture is a promising extension of today's Cloud offers.

Security and privacy matter have become critically significant with the fast expansion of multi-agent systems. Most network use such as pervasive computing, grid computing and P2P networks can be viewed as multi-agent scheme which are open, anonymous and dynamic in nature. Such uniqueness of multivalent systems brings in vulnerabilities and threats to providing secured message. One feasible way to reduce the threats is to assess the trust and reputation of the interacting agents [11-13]. Many trust/reputation models have done so far, but they fail to correctly evaluate trust when malicious agents start to behave in a random way. Furthermore, these models are unproductive in providing quick response to a malicious agent's oscillating actions. Another aspect of multi-agent systems which is fetching critical for sustaining good service excellence, is the even distribution of workload among service providing manager. 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 Secured Trust‟. In this paper we first analyze the different factors related to evaluating the trust of an agent in 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 professionally distribute workload among the service providing agents under stable condition.

Reputation systems give mechanisms to create a metric encapsulating reputation for a given domain for every identity within the system. These systems look for to generate an accurate assessment in the face of a variety of factors including but not limited to unprecedented group of people size and potentially adversarial surroundings. We center on attacks and defense

mechanisms in reputation systems. We propose an analysis framework that allows for universal decomposition of existing reputation systems. We categorize attacks against reputation systems by identifying which system components and design choice is the target of attacks. We review 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; a) which design components of reputation scheme are most vulnerable, b) what are the majority appropriate protection mechanisms and c) how these defense mechanisms can be integrated into obtainable or future reputation systems to make them resilient to attacks.

3. Existing system

There are considerable works concerning verification in cloud. For example, a user confirmation framework for CC is proposed in existing, aiming at offering user friendliness, identity organization, mutual validation and meeting key agreement between the users and the cloud server. About authentication in CC-WSN incorporation, an extensible and secure cloud planning model for sensor information system is planned in one of the accessible system. It first describes the work and mechanism of the projected architecture form. Then it puts forward sanctuary mechanism for authenticating legal users to admittance sensor data and information services inside the design, based on a certificate authority based Kerberos etiquette. Finally the model deployment and imitation experiment of the projected architecture model are introduced.

The existing structure comes with the following limitations: Malicious attackers may imitate authentic CSPs to converse with CSUs, or fake to be reliable SNPs to commune with CSPs. Then CSUs and CSPs cannot ultimately achieve any examine from the counterfeit CSPs and SNPs respectively. In the intervening time, the trust and status of the genuine CSPs and SNPs are also impaired by these fake CSPs and SNPs.

Without belief and reputation computation and administration of CSPs and SNPs, it is simple for CSU to prefer a CSP with low conviction and reputation. Then the overhaul from CSP to CSU fails to be fruitfully delivered rather often. Moreover, CSP may without difficulty select an undependable SNP that delivers the repair that the CSP requests with an intolerable large latency. Moreover, the disloyal SNP probably may only be able to give the requested examine for a very short time period unpredictably.

4. Proposed system

To the finest of our acquaintance, there is no investigation discussing and analyzing the verification as well as conviction and status of CSPs and SNPs for CC-WSN combination. Filling this gap, this paper analyzes the verification of CSPs and SNPs as well as the conviction and repute about the services of CSPs and SNPs.

Additional, this paper recommends a narrative legitimate trust and status computation and management system for CC-WSN incorporation. Mainly, considering (i) the legitimacy of CSP and SNP; (ii) the characteristic 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.

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.

Furthermore, we provide this authenticator can be efficiently generated by the data owner simultaneously with the encoding procedure. Extensive analysis shows that our scheme is provable secure, and the performance evaluation shows that our scheme is highly efficient and can be feasibly integrated into An Authenticated Trust and Reputation Calculation and Management System for Cloud and Sensor Networks Integration system.

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. Here, ISO/IEC 27001 certification is applied to authenticate CSP and SNP, as it is an internationally recognized information security management system (ISMS) standard by the International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC). It requires that the information management of an organization (e.g., CSP or SNP) meets;

- The organization's information security risks are systematically examined;
- A coherent and comprehensive suite of information security controls is designed and implemented to solve those risks that are deemed unacceptable;
- An overarching management process is adopted to ensure that the information security controls continue to satisfy the organization's information security needs on an ongoing basis. Particularly, it provides confidence and assurance to trading clients of the organization, as the security status of the organization is audited to be qualified, by issuing a certificate with the ISO/IEC 27001 certification. After CSP and SNP are certificated with ISO/IEC 27001, they obtain the certificates respectively.

An SLA is a negotiated agreement between two or more parties, in which one is the customer and the others are service providers. In short, it is a part of a service contract, in which a service is formally defined. SLA specifies the levels of availability, serviceability, performance, operation and other attributes of the service. Usually, an SLA addresses the following segments about a service: definition, performance measurement, problem management, duties, warranties, termination. The subject of SLA is the result of the service received by the customer. An PLA is an agreement to describe the level of privacy protection that the CSP will maintain. Thus it is an appendix to the SLA between CSU and CSP. The SLA between CSU and CSP provides specific parameters and minimum levels on other performance (e.g., cloud processing speed, cloud operation time) of the cloud service, while PLA addresses information privacy and personal data protection issues about the cloud service.

Defined by Merriam Webster's Dictionary, trust is "assured reliance on the character, ability, strength or truth of someone or something" and reputation is "overall quality or character as seen or judged by people in general". However, trust and reputation are multidisciplinary concepts with different definitions and evaluations in various fields (e.g., psychology, sociology,

economics, philosophy, wireless networks. For example, in the scenario of wireless communications, "Trust of a node A in a node B is the subjective expectation of node A receiving positive outcomes from the interaction with node B in a specific context". Also, "Reputation is the global perception of a node's trustworthiness in a network". 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 with that, trustor;

(A) Maps the gathered information from the evidence space to the trust space through a predefined mapping function and an aggregation function to obtain the trustworthiness value of trustee

(B) Specifically, the trustworthiness obtained by mapping evidences from direct interaction is known as direct trust, while the trustworthiness achieved through mapping evidences from third-parties is indirect trust. Furthermore, a trustor can bring into account recent trust, which reflects only the recent behaviors, as well as historical trust, which is built from the past experiences and it reflects long-term behavioral pattern. For instance, using indirect trust and historical trust helps trustor to protect trust evaluation (and trust system in general) from attacks such as good mouthing and bad mouthing, or sudden selfishness of a trustee. More discussion about these terms and definitions can be found in our references, for instance in. In addition, to evaluate reputation about a trustee (e.g., B), the aggregated trust opinion of a group of entities are usually taken to represent the reputation value.

In this paper, based on the five main roles (e.g., cloud customer, cloud provider, cloud broker, cloud auditor and cloud carrier) in CC, we assume that the role of the cloud auditor is assigned to TCE. Furthermore, we assume that TCE consists of multiple entities in various locations with a shared and secured database, e.g., in a data center.

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. Furthermore, for various CSUs, the types of trust that they concern are different. In this paper, we assume that the following three types of trust about CSP concern the CSU to choose the service of CSP and we further show how they are calculated.

5. Conclusions

In this paper, we have 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

- the authenticity of CSP and SNP;
- the attribute requirement of CSU and CSP;
- 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.
[7] M. Li and Y. Liu, "Underground coal mine monitoring with wireless sensor networks," ACM Trans. Sensor Netw., vol. 5, no. 2, Mar. 2009, Art. ID 10.
[8] Singh, R. P. & Singhal, S. (2016) Rotary ultrasonic machining: a review. *Materials and Manufacturing Processes*, doi: 10.1080/10426914.2016.1140188.
[9] Sharma, P., Singhal, S., & Prasad, B. (2016). Selection of layout alternative using factor evaluation. *International Journal of Emerging Trends in Research*, 1(1), 01-04.
[10] Singh, R. P., Kumar, J., Kataria, R., & Singhal, S. (2015) Investigation of the machinability of commercially pure titanium in ultrasonic machining using graph theory and matrix method. *Journal of Engineering Research*, 3(4): 75-94.
[11] 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.
[12] 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.
[13] 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.