International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 06
May 2017

An Authenticated Trust and Reputation Calculation

Y.SUDHIR KUMAR YADAV[1]&ISHAQ SHAREEF C [2]

[1]M-Tech, Dept. of CSE P.V.K.K INSTITUTE OF TECHNOLOGY
Sanapa Road, Rudrampeta, Anantpaur,AP

[2]Assistant Professor, Dept. of CSE P.V.K.K INSTITUTE OF TECHNOLOGY
Sanapa Road, Rudrampeta, Anantpaur,AP

Abstract

Induced by incorporating the powerful data storage and data processing abilities of cloud computing (CC) as well as ubiquitous data gathering capability of wireless sensor networks (WSNs), CC-WSN integration received a lot of attention from both academia and industry. 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. To fill the gap, this paper proposes a novel authenticated trust and 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: 1) authenticating CSP and SNP to avoid malicious impersonation attacks; 2) calculating and managing trust and reputation regarding the service of CSP and SNP; and 3) helping CSU choose desirable CSP and assisting CSP in selecting appropriate SNP. Detailed analysis and design as well as further functionality evaluation results are presented to demonstrate the effectiveness of ATRCM, followed with system security analysis.

Keywords: - CSP, CC-WNS, ATRCM, authenticating

1. INTRODUCTION

Computing is being transformed to a model consisting of services that are commoditized and conveyed in a way like traditional utilities, for example, water, electricity, gas, and telephony. In such a model, users access services in light of their prerequisites without respect to where the services are facilitated or how they are delivered. cloud computing (CC) is a model to enable convenient, on-demand network access for a shared pool of configurable processing resources (e.g., servers, networks, storage, applications, and services) that could be

quickly provisioned and released with minimal management effort or service supplier interaction. W ireless sensor networks (WSNs) are networked system comprising of spatially appropriated distributed autonomous sensors, which are capable of sensing the physical or environmental conditions.

Cloud network

Cloud networking is a new networking paradigm for building and managing secure private networks over the public Internet by utilizing global cloud computing infrastructure. In cloud networking, traditional network functions and services including connectivity, security, management and control, are pushed to the cloud and delivered as a service.

Sensors

Sensors are sophisticated devices that are frequently used to detect and respond to electrical or optical signals. A Sensor converts the physical parameter (for example: temperature, blood pressure, humidity, speed, etc.) into a signal which can be measured electrically. Let's explain the example of temperature. The mercury in the glass thermometer expands and contracts the liquid to convert the measured temperature which can be read by a viewer on the calibrated glass tube.

2. RELATED WORK

Existing system

There are substantial works regarding authentication in cloud. For instance, a user authentication framework for CC is proposed in existing, aiming at providing user friendliness, identity management, mutual authentication and session key agreement between the users and the cloud server. There are a number of research works with respect to trust or reputation of cloud. For example, focusing on the trustworthiness of the cloud resources in a existing work, a framework is proposed to evaluate the cloud resources trustworthiness, by utilizing an amor to constantly monitor and assess the cloud environment as well as checking the resources the armor protects. About authentication in CC-WSN integration, an extensible and secure cloud architecture model for sensor information system is proposed in one of the existing system. It first describes the composition and mechanism of the proposed architecture model. Then it puts forward security mechanism for authenticating legal users to access sensor data and information services inside the architecture, based on a certificate authority based Kerberos protocol. Finally the prototype deployment and simulation experiment of the proposed architecture model are introduced.

Proposed system

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.

3. IMPLEMENTATION

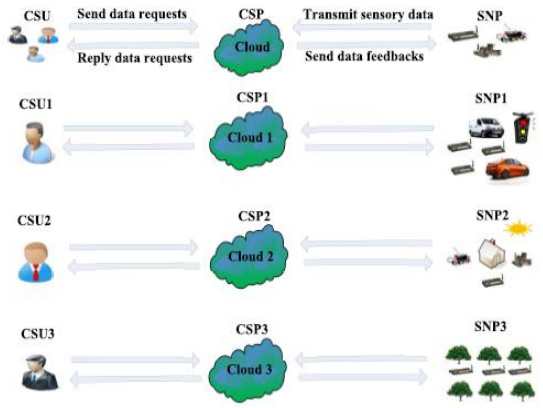

Fig 1 System architecture

Authentication

There are substantial works regarding authentication in cloud For instance, a utilizer authentication framework for CC is proposed in, aiming at providing utilizer cordiality, identity management, mutual authentication and session key acquiescent between the users and the cloud server. Paying particular attention to the lightweight of authentication since the cloud handles astronomically immense amounts of data in authentic-time, shows a lightweight multi-utilizer authentication scheme predicated on cellular automata in cloud environment. Certificate ascendancy predicated one-time password authentication is utilized to perform authentication. Fortifying innominate authentication, a decentralized access control scheme for secure data storage in clouds is presented in. The proposed scheme provides utilizer revocation, averts replay attacks as well as fortifies engenderment, modification and reading data stored in the cloud. Observing the demerits of losing opulent information facilely as well as the poor performances resulting from the intricate inputs of traditional dactyl gram apperception approaches during utilizer authentication by, it introduces an incipient dactyl gram apperception scheme predicated on a set of assembled geometric moment and Zernike moment features to authenticate users in cloud computing communications.

Trust and Reputation

There are a number of research works with deference to trust or reputation of cloud. For example, fixating on the trustworthiness of the cloud resources in, a framework is proposed to evaluate the cloud resources trustworthiness, by utilizing an amour to perpetually monitor and assess the cloud environment as well as checking the resources the armor bulwarks. For efficient reconfiguration and allocation of cloud computing resources to meet sundry utilizer requests, a trust model which amasses and analyzes the reliability of cloud resources predicated on the historical information of servers is proposed in, so that the best available cloud resources to consummate the utilizer requests can be yare in advance. To determine the credibility of trust feedbacks as well as managing trust feedbacks in cloud environments, presents a framework denominated trust as accommodation to amend current trust managements, by introducing an adaptive credibility model to distinguish the credible and maleficent feedbacks. Discussing the cloud accountability issue in, it first uses detective controls to analyze the key issues to establish a trusted cloud and then gives a trust cloud framework consisted of five abstraction layers, where technical and policy-predicated approaches are applied to address accountability.

Authentication of CSP and SNP

In this paper, as the key of our work is to enable CSU to cull the authentic and desirable CSP as well as avail CSP in culling genuine and congruous SNP, we fixate on the authentication of CSP and SNP rather than the authentication of CSU. Categorically, 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 apperceived 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 (i) the organization's information security risks are systematically examined; (ii) a coherent and comprehensive suite of information security controls is designed and implemented to solve those perils that are deemed unacceptable; (iii) an overarching management process is adopted to ascertain that the information security controls perpetuate to gratify the organization's information security needs on an perpetual substructure. Concretely, it provides confidence and assurance to trading clients of the organization, as the security status of

the organization is audited to be eligible, by issuing a certificate with the ISO/IEC 27001 certification. After CSP and SNP are certificated with ISO/IEC 27001, they obtain the certificates (i.e., ctc and ctk) respectively.

Preliminaries of SLA and PLA

An SLA is a negotiated acquiescent between two or more parties, in which one is the customer and the others are accommodation providers. In short, it is a component of an accommodation contract, in which an accommodation is formally defined. SLA designates the calibers of availability, serviceability, performance, operation and other attributes of the accommodation. Customarily, an SLA addresses the following segments about an accommodation: definition, performance quantification, quandary management, obligations, warranties, termination. The subject of SLA is the result of the accommodation received by the customer. An PLA is an acquiescent to describe the caliber of privacy bulwark that the CSP will maintain. Thus it is an appendix to the SLA between CSU and CSP. The SLA between CSU and CSP provides concrete parameters and minimum levels on other performance (e.g., cloud processing haste, cloud operation time) of the cloud accommodation, while PLA addresses information privacy and personal data bulwark issues about the cloud accommodation.

4. EXPERIMENTAL RESULTS

Fig:-2 Cloud Server Login

Fig:-3 Data Transaction Table

Fig:-4 Data Upload

Fig:-5 Files In Cloud

5. CONCLUSION

In this paper, we advancingly explored the authentication as well as trust and reputation calculation and management of CSPs and SNPs, which are two very critical and remotely explored issues with deference 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 veneration to the accommodation 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 eschew malevolent impersonation attacks; 2) calculating and managing trust and reputation regarding the accommodation of CSP and SNP; 3) availing CSU optate desirable CSP and availing CSP in culling opportune SNP, predicated on (i) the authenticity of CSP and SNP; (ii) the attribute requisite of CSU and CSP; (iii) the cost, trust and reputation of the accommodation of CSP and SNP. In integration, 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, lamentable mouthing, collusion and white-washing attacks, which are the most paramount attacks in our case.

6. 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. 130 IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 1, JANUARY 2015

[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] 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.