ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A Novel Technique for Calculation of Authentication and Trust Management System for Cloud and Sensor Networks Integration

Thummuluri Mounika
M.Tech- Computer Science,
Department of CSE,
SRTIST Nalgonda, Telangana.

CD.Amulya
Assistant Professor,
SRTIST Nalgonda, Telangana.

T.Madhu
HOD,
SRTIST Nalgonda, Telangana.

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.

INTRODUCTION

A. Cloud Computing (CC)

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 [1]–[4]. CC is featured by that users can elastically utilize the infrastructure (e.g., networks, servers, and storages), platforms (e.g., operating systems and middleware services), and software's (e.g., application programs) offered by cloud providers in an on-demand manner. Not only the operating cost and business risks as well as maintenance expenses of service providers can be substantially lowered with CC, but also the service scale can be expanded on demand and web-based easy access for clients could be provided benefiting from CC.

B. Wireless Sensor Networks (WSNs)

Furthermore, wireless sensor networks (WSNs) are networks consisting of spatially distributed autonomous sensors, which are capable of sensing the physical or environmental conditions (e.g., temperature, sound, vibration, pressure, motion, etc.) [5]–[7]. 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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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.

C. CC-WSN Integration

Induced by incorporating the powerful data storage and data processing abilities of CC as well as the ubiquitous data gathering capability of WSNs, CC-WSN integration received much attention from both academic and industrial communities (e.g., [8]–[14]). This integration paradigm is driven by the potential application scenarios shown in Fig. 1. Specifically, sensor network providers (SNPs) provide the sensory data (e.g., traffic, video, weather, humidity, temperature) collected by the deployed WSNs to the cloud service providers (CSPs). CSPs utilize the powerful cloud to store and process the sensory data and then further on demand offer the processed sensory data to the cloud service users (CSUs). Thus CSUs can have access to their required sensory data with just a simple client to access the cloud. In this new paradigm, SNPs are the data sources for CSPs, and CSUs act as the data requesters for CSPs.

D. Research Motivation

However, during the CC-WSN integration, the following two very critical and barely explored issues should be taken into consideration. These two issues not only seriously impede the CSU from obtaining the desirable service they want from the authentic CSP, but also prevent the CSP from obtaining the satisfied service from the genuine SNP.

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.

DISADVANTAGES OF EXISTING SYSTEM:

- Malicious attackers may impersonate authentic CSPs to communicate with CSUs, or fake to be authentic SNPs to communicate with CSPs. Then CSUs and CSPs cannot eventually achieve any service from the fake CSPs and SNPs respectively. In the meantime, the trust and reputation of the genuine CSPs and SNPs are also impaired by these fake CSPs and SNPs.
- Without trust and reputation calculation and management of CSPs and SNPs, it is easy for CSU to choose a CSP with low trust and reputation. Then the service from CSP to CSU fails to be successfully delivered quite often. Moreover, CSP may easily select an untrustworthy SNP that delivers the service that the CSP requests with an unacceptable large latency. Moreover, the untrustworthy SNP probably may only be able to provide the requested service for a very short time period unexpectedly.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

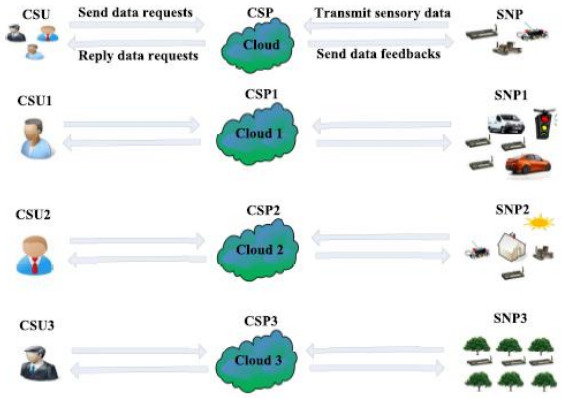
PROPOSED SYSTEM:

- 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;
- 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.

SYSTEM ARCHITECTURE:



IMPLEMENTATION

MODULES:

1 Data Owner

- Owner Registration
- Upload file
- Verify and Delete file
- View cloud details

2 Cloud Servers

- View all data owners
- View End users
- View all files
- View all attackers
- All data owner and End User feedback
- Data Owner and User reviews
- All transaction

3 Third Party Arbitrator

- Receive Metadata
- View all Attackers

4 End User

- Register
- Login
- Select the cloud
- Search file
- Request file

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

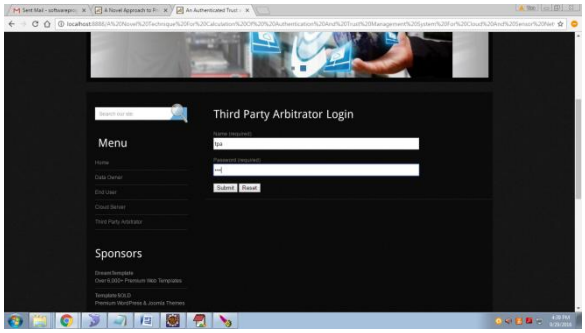
5 Attacker

- Modify user uploaded files

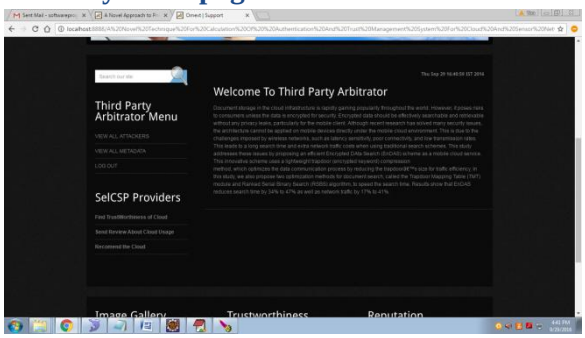
SCREEN SHOTS

Home Page:

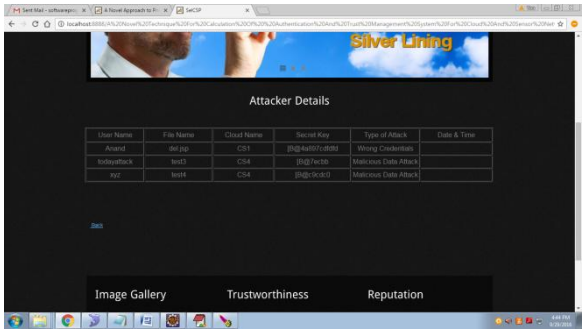
Third Party Arbitrator Login



Third Party Homepage:



Attacker Details:



Cloud Files:

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 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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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.

[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 approaches," Int. J. Distrib. Sensor Netw., vol. 2013, 2013, Art. ID 917923.

[15]S. Grzonkowski and P. Corcoran, "Sharing cloud services: User authentication for social enhancement of home networking," IEEE Trans. Consum. Electron., vol. 57, no. 3, pp. 1424–1432, Aug. 2011.

Author's Details:

Tummuluri Mounika

B.Tech college : KRISHNA MURTHY INSTITUTE OF TECHNOLOGY AND ENGINEERING

Specialisation : M.Tech CSE I hereby declare that the project work entitled "**A NOVEL TECHNIQUE FOR CALCULATION OF AUTHENTICATION AND TRUST MANAGEMENT SYSTEM FOR CLOUD AND SENSOR NETWORKS INTEGRATION"** submitted to the JNTU Hyderabad, is a record of an original work done by me under the guidance of **CD.AMULYA**, Department of Computer

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Science & Engineering, **SWAMI RAMANANDA THIRTHA INSTITUTE OF SCIENCE & TECHNOLOGY,** and this project work is submitted in the partial fulfillment of the Requirements for the award of the degree of Master of Technology in Computer Science& Engineering. The results embodied in this thesis have not been submitted to any other University or Institute for the award of any degree.

Mrs. Ch.Amulya

Received the B.Tech degree in Computer Science and Engineering and M.Tech degree in Computer Science and Engineering from J N T U Hyd-University. She is working as a Assistant Professor in Swami Ramananda Tirtha Institute of Science and technology, Nalgonda,Telangana, India. She has having 8 years of teaching Experience.

T. Madhu

(HOD) Associate professor and head of the department in CSE Swami Ramananda Tirtha Institute of Science and technology, Nalgonda,Telangana.