An Authenticated Trust and Reputation Calculation and Management System for Cloud and Sensor Networks Integration

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.

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.

PROPOSED SYSTEM:

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

ADVANTAGES OF PROPOSED SYSTEM:

1. 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.
2. 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 SPECIFICATION

Hardware Requirements:

- System : Pentium IV 3.5 GHz or Latest Version.
- Hard Disk : 40 GB.
- Monitor : 14’ Colour Monitor.
- Mouse : Optical Mouse.
- Ram : 1 GB.

Software Requirements:

- Operating system : Windows XP or Windows 7, Windows 8.
- Coding Language : Java – AWT,Swings,Networking

- Data Base : My Sql
- Documentation : MS Office
- IDE : Eclipse Galileo
- Development Kit : JDK 1.6