**INTRODUCTION**

1. **Cloud Computing (CC)**

**C**LOUD 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 softwares (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.

1. **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. 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.

1. **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.

**I. Authentication of CSPs and SNPs:**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.

**II. Trust and Reputation Calculation and Management of CSPs and SNPs:**Without trust and reputation calculationand management of CSPs and SNPs, it is easy for CSUto choose a CSP with low trust and reputation. Thenthe 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. 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:

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.

1. **Research Contribution and Organization**

The main contributions of this paper are summarized as follows.

• 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.