INTEGRATION OF SENSOR NETWORKS IN CLOUD COMPUTING

George MANEA[1], Sorin POPA[2]

The paper proposes a framework for supporting cost-effective cloud computing for intensive sensor utilization using a dedicated Sensor-Cloud Infrastructure (SCI). SCI virtualizes a physical sensor as a virtual sensor on the cloud computing. Dynamic grouped virtual sensors on cloud computing can be automatic provisioned on users request. Several configurations of virtual sensor groups are discussed, as well as some particular security policies. Finally, the advantages, but also the drawbacks of the proposed solution are presented.

Keywords: Wireless Sensor Networks; Cloud Computing; Senor-Cloud Infrastructure, Virtualization; Software as a Service; Quality of Services

1. Introduction

Cloud computing is a model for enabling on demand network access to a shared pool of configurable computing resources (networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing offers two major benefits in IT market: efficiency,
which is achieved through the highly scalable hardware and software resources, and agility, which is achieved through parallel batch processing, using real-time mobile interactive applications, most of them based on intensive use of wireless sensor networks (WSN) [1].

Due to the increasing demand of sensor network applications and their support in cloud computing for a number of services, a new type of service architecture named Sensor Cloud (SC) was introduced as an integration of cloud computing into the WSN. A sensor cloud is composed of virtual sensors built on top of physical wireless sensors, which users automatically and dynamically can utilize on the basis of applications demands. The main advantages of this approach are: 1) it enables better sensor management capability; 2) data captured by WSNs can be shared among multiple users; 3) it reduces the overall cost of

[1] Faculty of Automatic and Control Computers, University POLITEHNICA of Bucharest, Romania
[2] Faculty of Automatic and Control Computers, University POLITEHNICA of Bucharest, Romania, e-mail: sorin.popa@upb.ro

data collection for both the system and user; 4) the system is transparent regarding the types of sensors used.

On the other hand, for enterprises to be convinced to migrate the services that they offer to the cloud, there are a number of strict requirements that any cloud system must fulfill. In this way, the cloud software services must be: highly reliable, scalable, autonomic to support ubiquitous access, dynamic discovery and composability. More of that, a SC must offer the required service level indicated by users through QoS (Quality of Service) parameters.

The main objective of this paper is to develop a framework for supporting cost-effective cloud computing for intensive sensor utilization in a SC that must have QoS guarantees related to efficient resource utilization and execution timeliness. The proposed framework will work on providing a cloud computing platform capable of providing real-time services for environmental sensing, monitoring, and process control systems. For this purpose, a QoS-aware cloud model is provided, able to satisfy different QoS levels regarding cost-effective resource management, timely service provisioning and high reliability.

2. Related work

The increasing complexity of process control systems require as primary goal of development to facilitate connecting sensor, people and software objects to build community-centric sensing applications where people can share and analyse real-time sensor data. The Cloud Computing comes as a possible answer to the problem. A WSNs-Cloud Computing integration can utilize the ever-expanding sensor data as SaaS (Software as a Service) on the Cloud. Integrating WSNs and Cloud Computing is a recent approach. In the following different proposals appeared in the last five years are analysed. We have classified them into three categories taking into account the main objectives of the approaches.

Interaction between WSNs and Cloud. Some discussed issues are: finding the shortest path between a sensor node (from the WSN) and a cloud server node (from the Cloud) [2], the ability to deploy large number of tiny nodes that assemble and configure themselves and to exploit the immense power of cloud in their management [3], the integration of industrial WSN, composed of low-power wireless field devices with cloud infrastructures, implementing RESTful services at a coordinator node level of the WSN [4], design of a “device-centric” architecture that can efficiently replace classical host-centric architectures to handle critical condition and its implementation of the Time Synchronized Channel Hopping as supported by commercial WirelessHART systems [5].

Interaction between WSNs and Cloud users. The proposals of this category are mainly focused on the way the data collected from the sensors can be obtained

by Cloud users. It implies solution for virtualization of the physical sensors. The Service Oriented Architecture (SOA) is considered in [6]. The architecture uses SOA and features of cloud like virtualization to deal with heterogeneity. Services are used to allow the interaction between WSNs, subscribers and other clouds. In [7[a model which combines the concept of wireless sensor networks with the cloud computing paradigm is presented. The authors show the benefit resulted from this combination, by moving sensor data access from loosely managed system to a well managed cloud. A new concept, the predictive storage, is introduced in [8]. This concept allows to correlate the storage process to the behavior of the physical environment. Its implementation needs to build an architecture that focuses the sensor data archival at some remote sensors of Sensor-Cloud infrastructure. In [9], trust and reputation management for Cloud and WSNs integration is explored, in order to prevent the cloud service users (CSUs) from choosing the desirable cloud service providers (CSPs) or hinder the CSP from selecting appropriate sensor network providers (SNPs). The proposed system allows to calculate and manage the trust and reputation regarding the service of CSP and SNP and helps CSU to choose CSP and to assist CSP in choosing SNP.

Interaction between Cloud and Physical world in application scenarios. There are multiple issues approached in this domain, which refers directly to the Sensor-Cloud Infrastructure and its capability to easily gather, process, visualize, store and analyze for a large number of sensor data from several types of applications. In [10] the authors analyze the characteristics of job scheduling with respect to CC-WSN integration, then study two classical job scheduling algorithms (Min-Min and Max-Min) and then propose two priority-based novel algorithms for CC integrated with WSN. The paper [11]focuses on secure processing of sensor data in the collaboration of WSN and cloud, and proposes a novel data processing framework for integrating WSN with cloud computing. In [12] the authors presents a model for integrating an advanced process control library in a cloud-based environment. The aim is to lower the development time, to reduce the maintenance effort and to decrease the complexity of process control applications by adopting a modular approach consisting of generic, reusable control strategies following an IEC 61499 representation. Last mentioned, a layered architecture of a sensor cloud which responds to the security challenges of such a system is provided in [13].

3. Sensor-Cloud architecture

Fig.1 shows the system architecture of SC, more precisely the SC infrastructure (SCI) and its relationship with Actors (Users at the top, Physical

Sensors at floor). The SCI has a structure similar which those described in [14]. It contains the following main parts:

1) Client: Users can access the user interface of SCI using their Web browsers.

2) Portal: Portal provides the user interface for SCI. A portal server gives sensor owners the menus for logging in, logging out, registering or deleting physical sensors. It also sends requests to other servers as required.

3) Provisioning: A provisioning server provide access of the virtual sensor groups for the requests from the portal server. After provisioning, the provisioning server updates the definitions of the virtual sensor groups.

4) Resource Management: SCI uses IT resources for the virtual sensors and the templates for provisioning. Special attention will be paid to the minimum set of generic characteristics for the middleware to offer support for integrating an intensive sensor-data and timely delivery. For the experiments, the distributed and reactive data storage is realized using the tinyDSM middleware [3]. Specific for Distributed Shared Memory (DSM) systems, the appropriate utilization of required services (e.g., location and discovery) is handled by the DSM run-time middleware that transparently intercepts user access attempts to remote memory addresses and translates them into the appropriate messages.

5) Monitoring: A monitoring server receives the data about virtual sensors from the agents. It stores the received data in a database. The monitoring information for the virtual sensors is available using a Web browser.

6) Virtual Sensor Group: SCI provisions virtual sensor groups for end users. A virtual sensor group is automatically provisioned on a virtual server by the provisioning server.

7) Physical Sensors: Real-time working sensors which are used in the application.

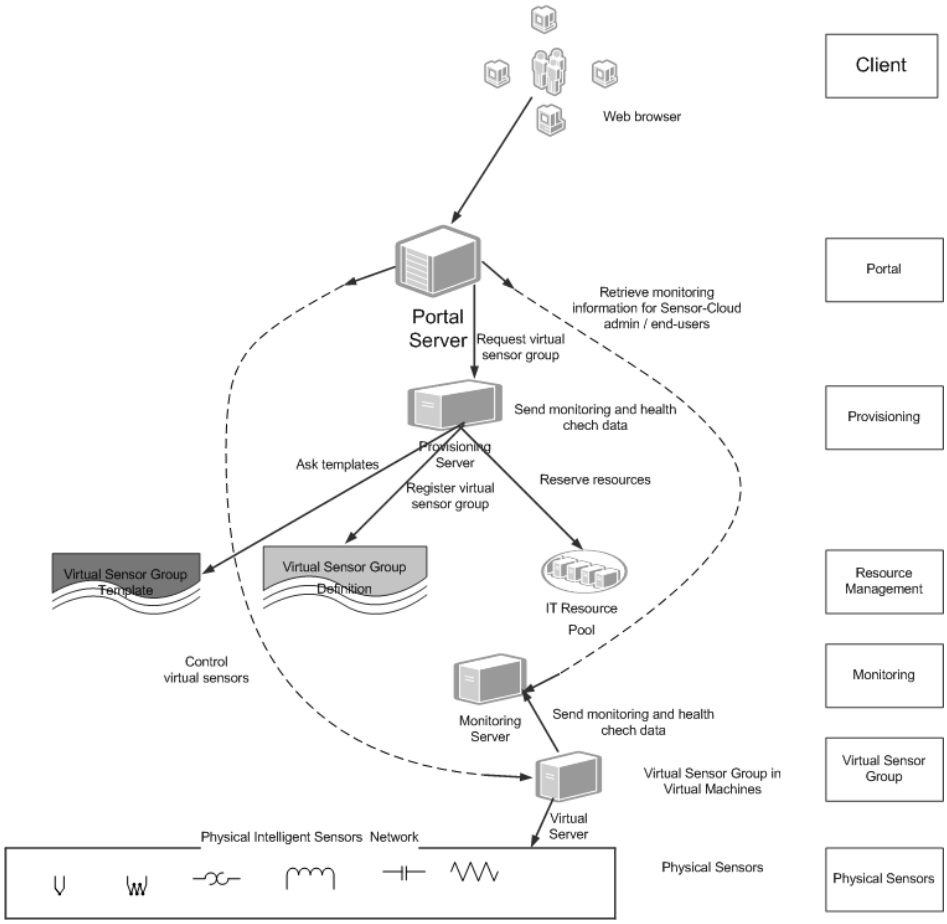

Fig.1. System architecture of SCI

In the following are listed several advantages and benefits of the proposed Sensor-Cloud infrastructure.

- Various Big Data analysis required by users can be developed on the basis of huge amount of sensor data accumulated in the cloud
- SC enables to scale the sensor networks on very large size because of the large routing architecture of cloud and to add the extra services from cloud computing vendors without having to invest heavily for these additional hardware resources.
- SC eases the collaboration among several users and applications for huge data sharing on the cloud
- SC provides free data storage and significant processing facility and storage resources to handle data of large-scale applications

- The number of services from several service providers can be integrated easily through cloud for numerous service innovations to meet user's demand.
- Through automation of provisioning of SC computing services one can improve the delivery time.
- SC provides flexibility to use random applications in any number of times and allows sharing of sensor resources under flexible usage environment.
- SC provides agile services and the users can provision the expensive technological infrastructure resources with less cost
- The integration of wireless sensor networks with cloud provides a very quick response to the user and so allows the high-speed processing of data using immense processing capability of cloud.
- SC infrastructure enables the resource optimization by allowing the sharing of resources for several number of applications and achieves higher gains of services.

4. Configuration of virtual sensor groups.

The novelty in this structure is the virtual sensor. A virtual sensor is an emulation of a physical sensor that obtains its data from underlying physical sensors. In our application we implemented virtual sensors as an image in the software of the corresponding physical sensors. The virtual sensors contain metadata about the physical sensors and the user currently holding that virtual sensor. Additionally the virtual sensor can have a data processing code, which can be used to process data in response to complex queries from the user.

For responding to the requirements of various industrial applications, we have considered four different configurations of virtual sensors, as shown in fig.2 : one-to-many, many-to-one, many-to-many, and derived configurations.

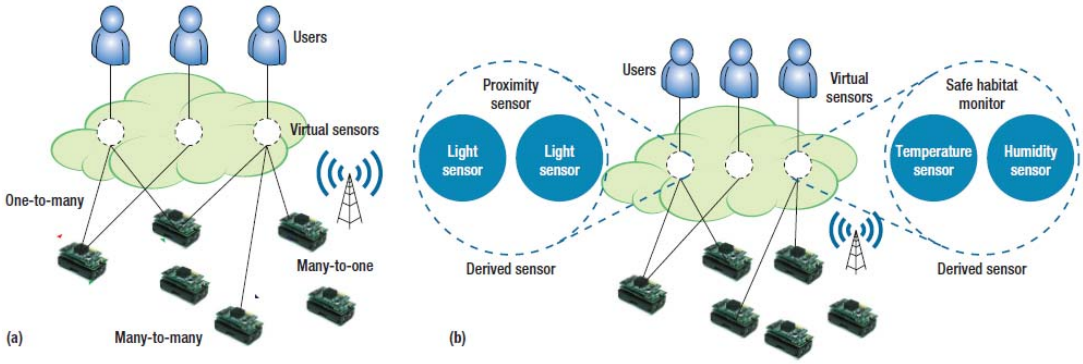

Fig.2. Typical configurations of virtual sensors (after [15])

One-to-Many Configuration. In this configuration (fig.2a), one physical sensor corresponds to many virtual sensors. Although individual users own the virtual image, the underlying physical sensor is shared among all the virtual sensors accessing it. The middleware computes the physical sensor sampling duration and frequency by taking into account all the users and dynamically reevaluates these two parameters when new users join or existing users leave the system.

Many-to-One Configuration. In this configuration (fig.2a), the controlled area is divided into zones and each zone can have one or more physical sensors and sensor networks. When a user requires aggregated data from a zone, all underlying WSNs switch on and the user has access to these data. The sampling time interval at which all underlying sensors sense is equal to the sampling time interval requested by the user. So, a virtual sensor communicates with a number of underlying physical sensors and it shows the aggregate view of the data to the user.

Many-to-Many Configurations. This configuration is a combination of the one-to-many and many-to-one configurations (fig.2a). A physical sensor can correspond to many virtual sensors, and it can also be a part of a network that provides aggregate data for a single virtual sensor.

Derived configuration. A derived configuration (fig.2b) refers to a combination of virtual sensors derived from a combination of multiple physical sensors and can be seen as a generalization of the other three configurations, where the difference lies in the possiblity of the virtual sensor to communicate with various types of physical sensors, while in the other three configurations, the virtual sensor communicates only with the same type of physical sensors. Derived sensors can be used either to virtually sense complex phenomenon or to substitute for sensors that are not physically deployed.

In the experiments, a virtual sensor can fall under any of the four configurations. A user might interact with one particular traffic flow sensor to assess traffic condition. Multiple users might also use the same sensor. A user might also configure derived virtual sensors to calculate parameters through indirect measurements.

5. Security policies in SC

There are several challenges to be solved by development of security preserving algorithms in such complex and heterogeneous system as wireless real-time, scarce resources and sometimes even systems under control of different authorities. We will investigate and implement suitable security mechanisms with respect to real-time, fault-tolerance and resource constrained heterogeneous networks. The main focus in implementation of suitable security mechanisms was

on secure cooperation between individual sensor nodes as well as between different systems eventually represented by a wireless sensor network.

The proposed solution for SC is to virtualize the wireless sensor network and by that create kind of a virtual sensor which then is becoming part of the cloud. Therefore all operations executed in the cloud are run with the data present in the virtual sensor. It allows also for splitting the security level into two parts, a high Security Layer between the cloud and the virtual sensors, and a low Virtual Sensor Network Layer between the virtual sensors and the real sensor nodes (as shown in fig.3). The first can be handled by standard security means as they are already in place. For the second only lightweight means are necessary, in order to ensure that security features are not contradicting other system properties.

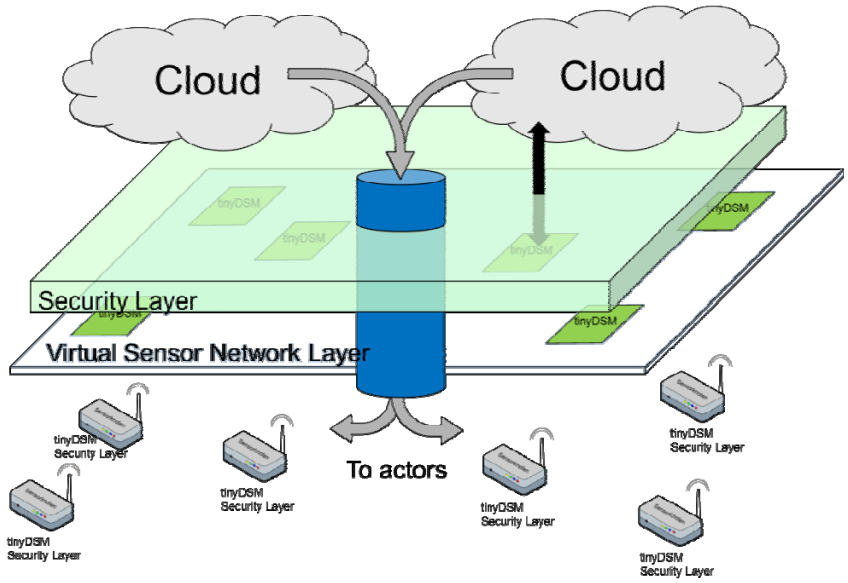

Fig.3. Security layers in sensor-cloud infrastructure

As mentioned before, in order to ensure a consistent and accurate view on the real world system in the virtual sensor layer the tinyDSM approach was used [16]. In order to ensure real time behaviour especially for emergency situations, the idea was not to compromise security for efficiency, but to allow direct communication from the application in the cloud to the real world sensor/actor. The system was enabled with a direct cloud to real word sensor communication through a “security wormhole”, if and only if there are predefined emergency conditions fulfilled and reflected in the virtual sensor network. In such a case the security configuration is subject of transient change, namely as soon as the emergency situation is solved the original security regime is re-established.

6. Conclusions

As a result of this approach, the paper proposes a framework that bridges the gap between the cloud computing environments and the domains that are traditionally reluctant to adopting this model due to their special needs for intensive sensor data dependency, real-time requirements, and criticality of the processes being monitored. The proposed Sendor-Cloud Infrastructure can introduce cloud-based sensor-intensive SCADA systems provided as SaaS (Software as a Service). In this way, instead of having the SCADA system software installed on local computers, the entire system and its data will be stored and maintained in the cloud. Therefore, customers will have off-site support for the information technologies used and a scalable server space in a private cloud space.

SCI virtualizes physical sensors in order for end users to share them with no concerns about the details of them (i.e. location and specification). It enables end users to create virtual sensor groups dynamically by selecting the templates of virtual sensors or virtual sensor groups with IT resources. Because the end user can create on request a new template of a virtual sensor, the user can create a virtual sensor group more flexibly. Users can use virtual sensors only during needed by the automatic provisioning mechanism. Automatic provisioning also improves the delivery time, reduces the cost and increases the usability of the users. The end users can check the status of their virtual sensors by the monitoring mechanism and can also control their virtual sensors freely. On the other hand, there are some drawbacks: for end users, because they cannot select the sensors dynamically and can use them only during the previous assigned sensory task and for Sensor-Cloud administrators, which have to prepare carefully the templates for virtual sensors.

Related to the methods and techniques uses in this architecture, was used fractal analysis for sensors and sensor network. Fractal analysis is assessing fractal characteristics of data. It consists of several methods to assign a fractal dimension and other fractal characteristics to a dataset which may be a theoretical dataset.

In terms of testing were used real data from RoEdunet.

R E F E R E N C E S

[1]. *A. Alamri, W. Ansari, M. Hassan, S. Hossain, A. Alelaiwi, A. Hossain*, A Survey on Sensor-Cloud: Architecture, Applications, and Approaches, International Journal of Distributed Sensor Networks, pp.1-18 , 2013

[2]. *S. K. Dash, J. P. Sahoo, S. Mohapatra, and S. P. Pati*, "Sensor cloud: assimilation of wireless sensor network and the cloud," in Advances in Computer Science and Information Technology, Networks and Communications, **vol. 84**, pp. 455–464, 2012.

[3]. *G. Sadhana, S. Devi, M. Trishant*, Virtual Wireless Sensor Networks using Cloud-computing, International Journal of Technological Exploration and Learning, **vol. 2**, Iss. 6, pp. 303-305, 2013

[4]. *O. Chenaru, G. Stamatescu, I. Stamatescu, D. Popescu*, Towards cloud integration for industrial wireless sensor network systems, Proceedings of the 9-th International Symposium on Advanced Topics in Electrical Engineering (ATEE), pp. 917-922, 2015

[5]. *L. Ascorti, S. Galimberti, S. Savazzi*, (2014) Cloud-based WirelessHART networking for critical industrial monitoring and control, Proceedings of the 12-th IEEE International Conference on Industrial Informatics, pp. 362-369, 2014

[6]. *K. Pandey, S.V. Patel*, Design of SOA based framework for collaborative cloud computing in wireless sensor networks, International Journal of Grid and High Performance Computing, **vol. 2**, Issue 3, pp. 60-73, 2010

[7]. *R.S. Ponmagal, R. Raja*, An extensible cloud architecture model for heterogeneous sensor services, International Journal of Computer Science and Information Security, **vol. 9**, no. 1, 2011

[8]. *M. M. Islam, M. M. Hassan, G.W. Lee, E.N. Huh*, A survey on virtualization of wireless sensor networks, Sensors Journal, **vol. 12**, no. 2, pp. 2175–2207, 2012

[9]. *L. Wenxiang, Z. Chunsheng, H. Nicanfar, V. Leung, L. Yang*, A trust and reputation management system for cloud and sensor networks integration, Proceedings of the IEEE International Conference on Communications, pp. 557-562, 2014

[10]. *Z. Chunsheng, H. Xiuhua, V. Leung*, et al. Job Scheduling for Cloud Computing Integrated with Wireless Sensor Network, Proceedings of the 6th IEEE International Conference on Cloud Computing Technology and Science, pp. 62-69. 2014

[11]. *F. Banaie, S. A. H. Seno*, A cloud-based architecture for secure and reliable service provisioning in wireless sensor network, Proceedings of the 4th International Conference on Computer and Knowledge Engineering, pp. 96-101, 2014

[12]. *O. Chenaru, A. Stanciu, D. Popescu, V. Sima, G. Florea, R. Dobrescu*, Open cloud solution for integrating advanced process control in plant operation, Proc. of 23th Mediterranean Conference on Control and Automation (MED), pp. 973-978, 2015

[13]. *N. Poolsappasit*, et al. Challenges in Secure Sensor-Cloud Computing, Secure Data Management, LNCS 6933, Springer, pp. 70–84. 2011

[14]. *M. Yuriyama, T. Kushida*, Sensor-Cloud Infrastructure - Physical Sensor Management with Virtualized Sensors on Cloud Computing, Proc. of the 13th Inte, Conference on Network-Based Information Systems, pp. 1-8. 2010

[15]. *S. Madria, V. Kumar, R. Dalvi*, Sensor Cloud: A Cloud of Virtual Sensors, IEEE Software, **vol. 31**, iss.2, pp. 70-77, 2014

[16]. *K. Piotrowski, P. Langendoerfer, S. Peter*, tinyDSM: A highly reliable cooperative data storage for Wireless Sensor Networks, International Symposium on Collaborative Technologies and Systems, pp. 225-232. 2009