Survey on different issues of Sensor-Cloud

K.Lakshmanarao
AsstProfessor
IT-Dept,GMRIT

Ch.R. VinodKumar
AsstProfessor
IT-Dept,GMRIT

K.Kanakavardhini
Asstprofessor
IT-Dept,GMRIT

Abstract

In the advanced world, Wireless sensor network(WSN) applications have been used in several areas, such as Environment Monitoring(weather forecasting, disaster sensing),Healthcare, Education, Defence, Smart Home, Agriculture, critical infrastructure monitoring, surveillance and manufacturing. Still, the limitations of WSNs in terms of storage capacity, computation capabilities, communication flexibility, and scalability, effective management of the large-scale sensor data are important issues to deal with. There is a requirement of powerful and scalable high performance computing and massive storage infrastructure for real time processing and storing as well as analysis of sensor data. Therefore, in recent past, Sensor-Cloud infrastructure is becoming popular that can provide an open, flexible, and reconfigurable platform for several monitoring and controlling applications. In this paper we focus survey on comprehensive study of representative works on Sensor-cloud infrastructure, which will provide general readers an overview of the Wireless Sensor networks, the Cloud, The Integration of WSN in Cloud, The need of virtualization in Sensor-Cloud, Applications of WSN using cloud, Security aspects in Sensor-Cloud, The Serviceware: A Service Based Management Approach for Sensor-Cloud, Agent-Based System in Sensor-Cloud and self-management in Sensor-Cloud.

1. Introduction

The research advancement and various applications of wireless sensor networks become an invincible trend into the various industrial, environmental, manufacturing, traffic surveillance, health care, military sensing, air traffic control and distributed robotics and commercial fields[1,2].

One important research topic in sensor networks is how to utilize sensor data effectively so as to benefit the users [2]. Sensor network may consist group of sensor nodes working together to monitor a region and fetch data about the surroundings [1]. Wireless Sensor network comprises spatially distributed self-manage[4] sensors that can cooperatively monitor the environmental conditions, like natural disasters, sound pollution, atmospheric phenomenon, temperature in a certain reaction, and so on . Every sensor-node in a WSN is equipped with a radio transceiver or some other wireless communication device, a small microcontroller, and battery as energy source. In general each sensor-node consists three parts: sensing, processing, and communicating [1]. In traditional days the most commonly deployed sensors in sensor-network are camera sensors, accelerometer sensor, thermal sensor, microphone sensor, and so forth. As stated above the WSNs are being used in several areas like government, non-governmental and for disaster relief [1] and so on. These sensors provide useful sensed data when they are connected together for respective applications and services [1]. However, sensor nodes have numerous challenging issues to solve like communication and resources. Cloud computing is a future generation's computing paradigm. The US NIST (National Institute of Standards and Technology) defines the concept of Cloud computing as follows:

Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [5].

The benefits of cloud [1] are that the end users need not to worry about the exact location of data storage, servers and so forth. The users switch to their application by connecting to the server on cloud and start working without any trouble. Sensor-Cloud [1] can be used in many real-life applications like environmental monitoring, disaster monitoring, telemetric, agriculture, irrigation, healthcare, and so forth. As an illustration, we can use the Sensor-Cloud infrastructure implemented health-related applications such as monitoring patients and response to their disease, and so forth. In traditional approach, the diseases are reported everyday through some telemedicine interface [7]. This system suffers when the patient randomly moves from its current location thus, a more progressive, rapid, and mobile approach is needed where the recorded data from several sensor nodes of a WSN can be processed. To process this huge amount of

data integration of Sensor-Cloud can serve as a remedy in this direction.

The below Figure.1 [8, 13] consists of WSNs (i.e. WSN1, WSN-n) and cloud infrastructure. WSN consists of physical wireless sensor nodes to sense data for different applications like environmental monitoring, disaster monitoring, agriculture, healthcare, Military Application etc. Each sensor node is programmed with the required application. Sensor node also consists of operating system components and network management components. On each sensor node, application program senses the application and sends back to gateway in the cloud directly through base station or in multi-hop through other nodes. The client's access sensed data from cloud at any time at any place.

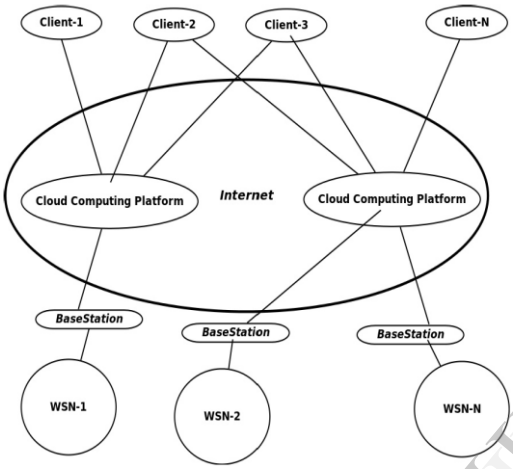
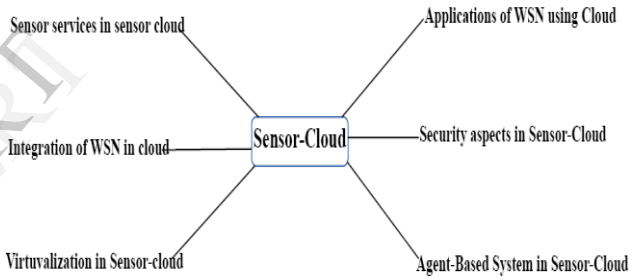


Figure 1. WSN-Cloud

This paper presents a comprehensive survey on usage of WSNs in Cloud (Sensor-Cloud). Section 2 of this paper concise overview of the concept, its definitions, services of Sensor-Cloud, its architecture, section 3 describes about different sensor services, section 4 gives overview on integration of sensors in cloud, section 5 draws attention on make use of virtualization in sensor-cloud, applications of sensor-cloud are described in section 6, the security issues discussed in section 7 and section 8 concentrates on sensor-agent-cloud.

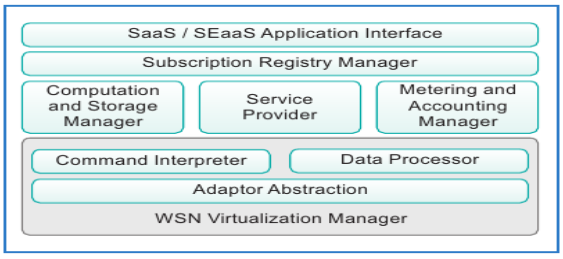
2. Overview and related work:

The Sensor-Cloud is a new model in cloud computing that uses the physical sensors to accumulate its data and transmit all sensor data into a cloud computing infrastructure. Sensor-Cloud handles sensor data efficiently, which is used for many monitoring applications. According to IntelliSys, Sensor- Cloud defined as follows: An infrastructure that allows truly pervasive computation using sensors as an interface between physical and cyber worlds, the data-compute clusters as the cyber backbone and the internet as the communication medium[9,10] .According to MicroStrains's Sensor-Cloud definition "it is a unique sensor data storage, visualization and remote management platform that leverage powerful cloud computing technologies to provide excellent data scalability, rapid visualization, and user programmable analysis. It is originally designed to support long-term deployments of MicroStrain wireless sensors, Sensor-Cloud now supports any web-connected third party device, sensor, or sensor network through a simple Open-data API" [11]. Sensor-Cloud infrastructure provides service to the end users as and when requested either through physical or virtual sensors. The virtual sensors are part of IT resources (like disk storage, CPU, memory, etc.) [12] Through these services appropriate sensor data can be used by the end users via a user interface through the web crawlers. This paper focus on the below taxonomy of the sensor-cloud and integration of each section in Sensor-Cloud in detail.



3. Sensor services in sensor cloud:

The sensor-cloud services are classified in two ways first services in cloud, second services of



sensor. The important services of sensor are Sensor Event as a Service (SEaaS)[13] , Sensing as a Service (SaaS)[13]. A WSN cloud computing platform[13] consists of WSN virtualization manager (WSNVM) , computation and storage manager (CSM), subscription registry manager (SRM), service provider (SP), metering and accounting provider (SP), metering and accounting interfaces are as shown on below Figure.2.

Figure 2: WSN Cloud Computing Platform.

4. Integration of WSN in cloud:

Hassan et al. [14] proposed a framework integrating sensor networks and cloud computing. Their proposed framework has a minor flaw in the implementation of the publish/subscribe broker. The paper does not provide a clear understanding of the components and steps that are involved in building the proposed framework. The objective of the integration framework[15] is to store the WSN sensed data to the Cloud Computing environment so that the sensed data may be fully utilised.

The below Figure. 3[14] shows the WSN and Cloud Computing integration framework.
The framework components include: Data Processing Unit (DPU), Pub/Sub Broker, Request Subscriber (RS), Identity and Access Management Unit (IAMU), and Data Repository (DR). Data collected from the WSN moves through a gateway to the DPU. The DPU will process the data into a storage format and then send the data to the DR.

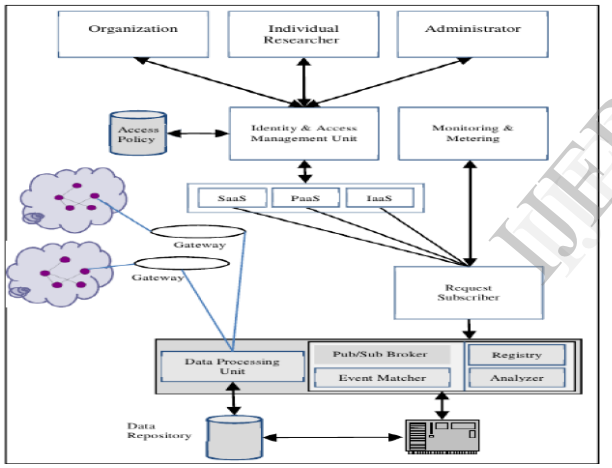


Figure 3: Sensor-Cloud Integration frame work.

5. Virtualization in Sensor-cloud:

A sensor network consists of a large number of sensor nodes that are densely deployed to monitor a region and fetch data about the surroundings[1,15]. The virtualization of WSN avoids idle time of physical sensor nodes. The rebirth of virtualization of WSN has been caused mainly from the recognition that most of the sensor nodes remains unused for most of the time. The WSN virtualization is used for effective utilization of physical sensor nodes by avoiding idle time of the physical sensor node[15]. Virtualization on sensor networks (VSN)[15] has two parts such as sensor infrastructure provider (SInP) that manages the physical sensor infrastructure, and sensor virtualization network service provider (SVNSP) that develops the VSN by aggregating resources from multiple SInPs and offer services to the application level users (ALU). The VSN model is as shown in Figure 4.

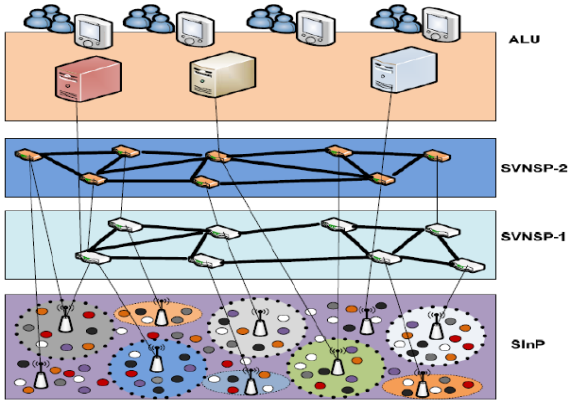


Figure 4: The VSN Model.

The VSN in sensor-cloud has three major roles[17] sensor-owner, cloud-administrator and end-user as shown in Figure 5. The sensor-owner is one who owns group of physical sensors. The sensor-owner registers the physical sensors with the cloud then others are allowed to use these physical sensors through cloud. The cloud administrator provides services like user interface to the sensors, virtual sensors and monitoring. The end user is one who uses one or more applications or services that use the sensor data. An end user requests the use of virtual sensor that satisfies the requirements from the templates.

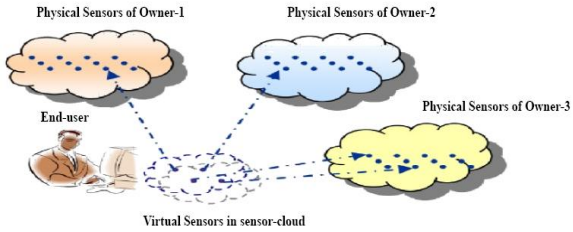


Figure 5: virtualization of Sensors in sensor-cloud.

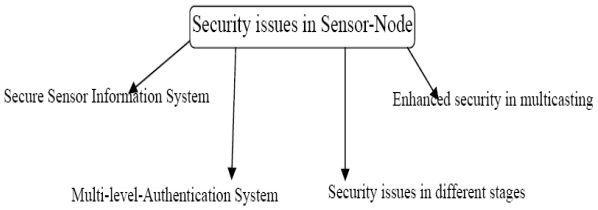
6. Applications of WSN using cloud:

Integration of WSN with cloud for ease of sharing and analysing real time sensor data on the fly. The sensor nodes inherent property of sensing as a service to sense data and sensing event as a service to trigger events over the internet adds advantages

to the sensor-cloud[8]. Some of the real time applications are[8] transport monitoring, weather forecasting, military use, health care and so forth.

7. Security aspects in sensor-cloud:

This paper describes security related issues which are based on below classification as shown below.



7.1 Secure Sensor Information System:

The secure cloud architecture [18] proposed for sensor information system is useful to strengthen the security issues in sensor-cloud while sensing data under Sensing as a service. The secure cloud architecture [18] has a dedicated layer to deal security issues which is named as security management layer. This layer objective is to avoid breaches in Identity based Authentication and encryption/decryption of data. A cloud based architecture model of sensor information system [18] proposes six layers in the architecture physical infrastructure layer, virtualization management layer, Service platform layer, Application layer, Security management layer and user interface layer. Among these layers the application layer provides security to the sensor data.

The security model [18] kept in security management layer, which has three main parts: identity authentication unit, resource access control unit, and data encryption unit. The identity authentication unit improves Kerberos protocol.

7.2 Enhanced security in multicasting:

Secure multicasting method is used for secure data transmission. It not only ensures secure data transmission but also enhance the resistance of the system. The existing multicast methods like LKH, ELK, and so forth are cost effective in updating Group-key to prevent the vulnerabilities. The users in general leave and join the system more frequently requires Group-Key update. The CoGKTK[19] combined Time-Key with Group-Key minimizes the number of Group-Key updates when user dynamically leaves and joins the system. The CoGKTK multicast key exchange method works based on the content-based publish/subscribe system for secure data transmission to the WSN users. This key exchange algorithm propagates data in a secure manner as well as do not require update key whenever user leaves the sensor-cloud.

7.3 Multi-level-Authentication System:

The Multi-Level Authentication[20] system authenticates cloud access in multiple levels while fetching sensor data from cloud. It generates a common password and adds this password at multiple levels. One should successful in processing passwords at all levels to access the cloud service. This method useful to check the authentication of the services as well as privileges of accessed user.

7.4 Security issues in different stages:

To control sensor data storage and process sensor data effectively there are different methods proposed in [21] they are as stated below:

OAuth-Protocol: This method is used to establish a secure connection in between the data owner/cloud-platform and Trust Point.

Object Security from Trust Point to Service: This technique provides security to the individual data fields (representing meta-data and raw data) and an integrity checksum (ICS) covering the complete data item. Each data field may be encoded using a key with a different ID and a different algorithm allowing for different confidentiality mechanisms to be used on individual data fields.

Service Assurance and Data Access Granting : In this method the data owner looks up a service and its service description in the Cloud Service Marketplace. She then instructs her Trust Point to encrypt her data for the selected service. The Trust Point stores the encryption keys for this service in the encryption key-store.

8. Agent based system in sensor-cloud:

Now a day's self-management [22] is an integral part of the most wireless sensors. The Self-configuring, Self-healing, Self-optimizing and Self-protecting are required properties for a system to be self-managing. The Sensor-Agent-cloud [22] virtualizes a physical sensor node as a virtual "sensor agent [22]". By using sensor agent concept without knowing whereabouts the users can access the sensor nodes. Each sensor agent operates on

behalf of its user. That is users can register, delete, control, monitor and destroy sensors agents base on their needs. The mandatory coordination of these sensor agents, which might belong to different users and try to access the same sensor node, is related to the system management. Therefore, Sensor Agent Cloud shall be self-managing.

9. Conclusion:

This paper surveyed the usage of Sensor-Cloud in the context of sensor services, Integration of WSN in cloud, virtualization, applications of WSN using cloud, Security issues, and agent based cloud. The integration frame work gives idea in integrating WSN in cloud, the security issues enables users in designing more secure approaches. Hence this overview gives complete idea to the researchers on Sensor-cloud.

References:

[1]Atif Alamri, Wasai Shadab Ansari, Mohammad Mehedi Hassan, M. Shamim Hossain, Abdulhameed Alelaiwi, and M. Anwar Hossain , "A Survey on Sensor-Cloud: Architecture, Applications, and Approaches ", Hindawi Publishing Corporation , International Journal of Distributed Sensor Networks Volume 2013, Article ID 917923, 18 pages , http://dx.doi.org/10.1155/2013/917923 .

[2]Pengfei You and Yuxing Peng An, "Architecture Model of Sensor Information System Based on Cloud Computing", National Key Laboratory for Parallel and Distributed Processing, School of Computer Science, National University of Defense Technology, China .

[3]M. Hassan, B. Song and E. Huh, "A Framework of Sensor-Cloud Integration Opportunities and Challenges," in Proc. of the 3rd International Conference on Ubiquitous Information Management and Communication, 2009, pp. 618-626 .

[4]Nithya Gopalakrishnan Nair , Philip J. Morrow and Gerard P. Parr , "Design Considerations for a Self-Managed Wireless Sensor Cloud for Emergency Response Scenario", PGNet 2011.

[5]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, Springer- Link, 2012 .

[6]H. T. Dinh, C. Lee, D. Niyato, and P. Wang, A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches, Wireless Communications and Mobile Computing-Wiley Online Library, 2011.

[7] M. O'Brien, Remote Telemonitoring—A Preliminary Review of Current Evidence, European Center for Connected Health, 2008.

[8] Sanjit Kumar Dash, Subasish Mohapatra and Prasant Kumar Pattnaik, " A Survey on Applications of Wireless Sensor Network Using Cloud Computing", International Journal of Computer Science & Emerging Technologies (E-ISSN: 2044-6004) Volume 1, Issue 4, December 2010 .

[9] http://www.ntu.edu.sg/intellisys.

[10] K. T. Lan, "What's Next? Sensor+Cloud?" in Proceeding of the 7th International Workshop on Data Management for Sensor Networks, pp. 978–971, ACM Digital Library, 2010.

[11]Sensor-Cloud, http://sensorcloud.com/system-overview.

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

[13] Adi Mallikarjuna Reddy V, Siva Prasad Katru and Kumar Padmanabh , "Can We Plug Wireless Sensor Network to Cloud? ", Infosys - Cloud Computing SETLabs Research briefings, vol.7, no.7, 2009.

[14]M. Hassan, B. Song and E. Huh, "A Framework of Sensor-Cloud Integration Opportunities and Challenges," in Proc. of the 3rd International Conference on Ubiquitous Information Management and Communication, 2009, pp. 618-626.

[15]Khandakar Entenam Unayes Ahmed and Mark A Gregory , " Integrating Wireless Sensor Networks with Cloud Computing ", ISSNIP Wireless Sensor Network with Cloud Computing, 2011.

[16] Md. Motaharul Islam, Mohammad Mehedi Hassan, Ga-Won Lee and Eui-Nam Huh , "A Survey on virtualization of Wireless Sensor Networks ", Sensors 2012 , www.mdpi.com/journal/sensors.

[17] Maki Matandiko Rutakemwa, "FROM PHYSICAL TO VIRTUAL WIRELESS SENSOR NETWORKS USING CLOUD COMPUTING", International Journal of Research in Computer Science(EISSN 2249-8265) Volume 3, Issue 1, 2013, pp. 19-25.

[18] Pengfei You and Zhen Huang , "Towards an Extensible and Secure Cloud Architecture Model for Sensor Information System ", International Journal of Distributed Sensor Networks , Hindawi Publishing Corporation, Volume 2013, Article ID 823418, 12 pages, http://dx.doi.org/10.1155/2013/823418 .

[19]Tien-Dung Nguyen and Eui-Nam Huh, "An efficient key management for secure multicast in Sensor-Cloud",http://ltis.icnslab.net/ALTIS/Files/20110524_Tien-ungNguyen_1365569677175.pdf.

[20]Dinesha H, A R Monica and V.K Agrawal , "Formal Modeling for Multi-Level Authentication in Sensor-Cloud Integration System ", International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868 ,Foundation of Computer Science FCS, New York, USA ,Volume 2– No.3, May 2012 – www.ijais.org .

[21] Ren´ Hummen, Martin Henze , Daniel Catrein, and Klaus Wehrle , "A Cloud Design for User-controlled Storage and Processing of Sensor Data", http://www.comsys.rwth-aachen.de/fileadmin/papers/2012/2012-hummen-cloud.pdf.

[22] Yu-Cheng Chou, Bo-Shiun Huang and Bo-Jia Peng , "An Agent-Based System for Sensor Cloud Management ", http://aims.me.cycu.edu.tw/articles/bookchapters/embed_system/EmbedSystem_Chou_2012.pdf.