EAI Endorsed Transactions
on Scalable Information Systems
Research Article ICST.ORG

A WSN based Environment and Parameter Monitoring System for Human Health Comfort: A Cloud Enabled Approach

Manohara Pai[1], Pooja B[2*] and Radhika M. Pai[3]

[1]Department of I&CT, Manipal Institute of Technology, Manipal University, Manipal, 576104, India
[2] Department of I&CT, Manipal Institute of Technology, Manipal University, Manipal, 576104, India
[3] Department of I&CT, Manipal Institute of Technology, Manipal University, Manipal, 576104, India

Abstract

The number and type of sensors measuring physical and physiological parameters have seen dramatic increase due to progress in the MEMS and Nano Technology. The Wireless Sensor Networks (WSNs) in turn is bringing new applications in environment monitoring and healthcare in order to improve the quality of service especially in hospitals. The adequacy of WSNs to gather critical information has provided solution but with limited storage, computation and scalability. This limitation is addressed by integrating WSN with cloud services. But, once the data enters the cloud the owner has no control over it. Hence confidentiality and integrity of the data being stored in the cloud are compromised. In this proposed work, secure sensor-cloud architecture for the applications in healthcare is implemented by integrating two different clouds. The sink node of WSN outsources data into the cloud after performing operations to secure the data. Since the SaaS and IaaS environments of Cloud Computing are provided by two different cloud service providers (CSPs), both the CSPs will not have complete information of the architecture. This provides inherent security as data storage and data processing are done on different clouds.

Keywords:, Cloud Computing, Confidentiality, Environmental Monitoring, Integration of Clouds, Integrity, Sensor Cloud Architecture, Wireless Body Ares Networks (WBANs), Wireless Sensor Networks (WSNs).

Received on 28 February 2014, accepted on 29 April 2014, published on 27 May 2014

doi: 10.4108/ sis.1.3.e2

1. Introduction

The health comfort of an individual depends on the right values associated with environmental parameters such as temperature, humidity, percentage of oxygen and carbon dioxide, exchange rate of air and many more. However measuring these physical parameters will not be sufficient to conclude the values for human comfort. It is also necessary to measure physiological parameters of human body and identify the relationship between environmental parameters and physiological parameters.

The Wireless Sensor networks (WSNs) and Wireless Body Area Networks (WBANs) play a major role in generating the values for physiological and physical parameters**.** The raw data obtained from these WSNs need to be processed and analyzed in order to provide better information services to the users. But due to the limitation of WSNs in terms of memory, energy, computation and scalability, management of WSNs data to provide efficient observation services to the users is an important issue to deal with. To address this problem a scalable storage infrastructure and a powerful high-performance computing environment is essential for real-time processing, storing and analysis of WSN data. Cloud computing is one among the new generation technologies to provide these features and thus a remedy to this issue.

Cloud computing is a pioneer technology to provide a flexible stack of massive computing, storage and software services in a scalable and virtualized manner at low cost [1]. As defined by the NIST standard “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” [2]. This paradigm renders services in three elementary levels; Software as a Service (SaaS - for example, application level programs), Platform as a Service (PaaS - for example, operating platforms) and Infrastructure as a Service (IaaS - for example, storage and server). These three levels provide

*Corresponding author. poojab2789@gmail.com

the users with dynamically scalable and virtualized resources through the Internet on "pay per usage" basis. [1]. Thus in order to overcome the shortfall of WSNs in terms of storage and computation it is integrated with the cloud computing environment, leading to the introduction of sensor-cloud infrastructure [1].

A Sensor-Cloud "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 through a simple API" [3]. The sensor-cloud collects and process data from several sensor networks and enables the users to access, monitor, visualize, analyze, store and share the data among different users. Though the resources provided by the sensor-cloud can be used to provide better observation services, the owner becomes totally dependent on availability of these services and has no control over the data that enters the cloud. This creates a hindrance on the confidentiality and integrity factor of the data stored in the cloud. Thus in this paper we propose a secure sensor-cloud architecture.

The paper is organized as follows. Section 2 gives an overview of the existing literature. Section 3 introduces the proposed scheme. Section 4 provides experimental setup details and section 5 concludes the paper.

2. Related Work

This section gives an overview of the works related to relationship between physical and physiological parameters and integration of WSNs with the cloud computing paradigm.

Ivanov et al [9] has proposed a co-operative WBAN environment that supports multi hop transmission through cooperative WSNs and WBAN nodes. The essentiality of considering the values of both environmental parameters and WBAN nodes for deciding the comfort of a person is discussed.

In reference with integration of WSN with Cloud services, Figure1. shows the conventional sensor-cloud architecture. The conventional sensor cloud is shown comprising one or more end user devices, cloud service provider, gateway and one or more sensors.

An end user may initiate a service request through the end user device. The end user device which may be any communication device with internet facility, is configured to send request for a data. The end user device communicates with the cloud service provider (CSP) to obtain the information services.The cloud service provider is a shared computing infrastructure comprising storages, processors, operating systems etc. The cloud infrastructure is designed to provide easy, scalable access to software applications, storage resources and other related data management services. The CSP process the end user request by fetching the data stored in the database and providing the required services.

The sensor network consists of a group of (wireless) sensors which may communicate with each other using the standard communication protocols for example, ZigBee, Bluetooth etc. The sensors are used to measure and collect periodic data of known parameters. The parameters include temperature, pressure, percentage of different gases in the environment etc. The data measured (or collected) by sensor (referred to as raw data) is forwarded to the database through the gateway. As may be seen in the conventional system, the raw data is stored in the database of the cloud service provider who provides information service to the user. Since, the storage and information services are managed and administrated by the same cloud service provider, the raw data is vulnerable and confidentiality and integrity of data may be compromised.

Apart from this Yuriyama et al. [6] has suggested an infrastructure where the WSNs can be configured as virtual sensors. Although the user can request and release the resources on demand, it is not very much user friendly as the end user needs to do most of the processing and provisioning. M.M Hassan et al. [7] proposed a framework for sensor-cloud integration based on the pub-sub broker model. This model is used for channelization of sensor data to the SaaS application. A.Deshwal et al [8] has also provided an end to end solution to access data generated from remotely located WSN by using a smart device. The IaaS paradigm of cloud computing was utilized to provide virtualization of sensor. Also, R. Hummen et al [5], introduced a sensor-cloud architecture that is suitable for different kinds of sensor. Though the works of [7], [8] and [5] have proposed different architectures to integrate WSNs into cloud neither of these architectures provides security features to the outsourced WSN data.

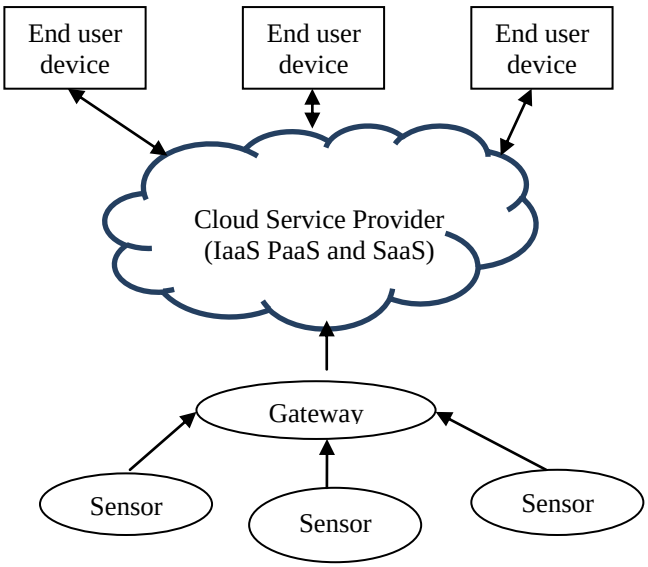

Figure 1. Conventional Sensor Cloud Architecture

Apart from the above works, there also exists many services that provide sensor-cloud infrastructure to store and process the sensor based information. Few of them are Nimbits [10], Pachube Platform [11], IDigi [12] and

ThingSpeak[13]. Although the above sensor-cloud provides observation services, they lack secure access to the data.

The NIST has identified certain high level security objectives in order to address the threats that are specific to outsourcing of data to the cloud [4]. These objectives are confidentiality, integrity, availability, assurance and accountability. R. Hummen [5] has discussed the essentiality of these five objectives with respect to sensor-cloud scenario.

Thus considering the confidentiality and integrity factor of the outsourced data we propose secure sensor-cloud architecture.

In this research since we are dealing with human being as a subject, it is essential to consider the relationship between the physiological and physical parameters in order to develop a fool proof parameter measurement system on one hand and secure the stored data in cloud on the other hand.

3. The Proposed System Architecture

This section discusses the proposed sensor-cloud architecture with security features and the parameter measurement and acquisition system. The system architecture is shown in Figure 2. The architecture is designed by taking the following assumptions into consideration. Within the boundaries of the sensor network, we assume that data is transferred securely to the gateway. Considering the gateway, we assume that its configuration is secure and access control mechanisms are implemented properly. With respect to assurance, we assume that the IaaS and PaaS provider ensure compliance to the security standards. Most importantly, the cloud service provider does not handover the data to an unauthorized third party.

As shown in the Figure 2 the overall system comprises of WSNs henceforth represented as Sensor networks, Gateway, Virtual Sensor Cloud, Service cloud and the Client device. Each subsystem is discussed below.

1) Client Device

Client devices are the devices that the end user interacts with, in order to access the applications. Any device that has internet and web-browser facility can be used as a client device. These devices can either be a smart phone, tablet, laptop or a desktop. The end user can request for the different services using the client device.

2) Sensor Networks

The sensor network is composed of WSN and Wireless Body Area Network (WBAN). WBAN has different sensors embedded on human body which are used for measuring the physiological parameters. The WSN consists of a group of wireless sensors that can communicate with each other using the standard communication protocols like ZigBee. These sensors can be used to measure different physical parameters (like temperature, pressure, amount of different gases in the environment etc) periodically. This raw data is forwarded to the sink node or the gateway directly or through multiple hops.

3) Gateway

The gateway acts as an interface between the sensor network and the cloud network. The gateway or the sink node receives raw data from various sensor nodes. The received data consists of various parameters like sensor identity, observation values, geo-location, manufacture information and many more. The gateway extracts the sensor observation values to perform the integrity and encryption operations and accesses the services of cloud computing to store data into the cloud.

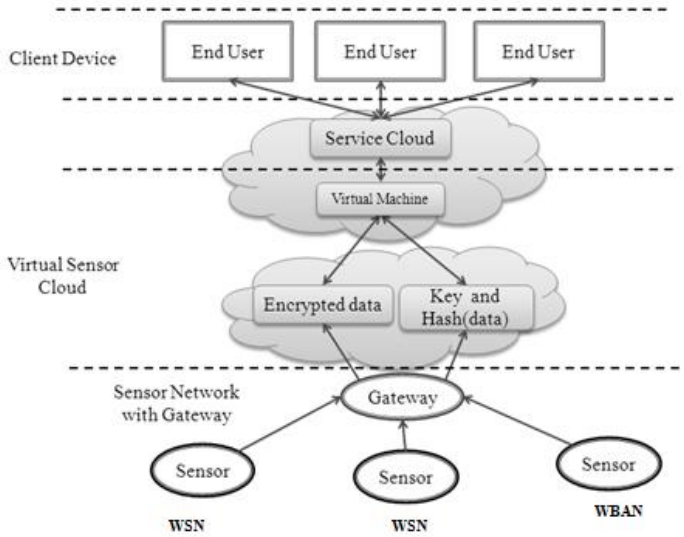

Figure 2. Proposed Sensor Cloud Architecture

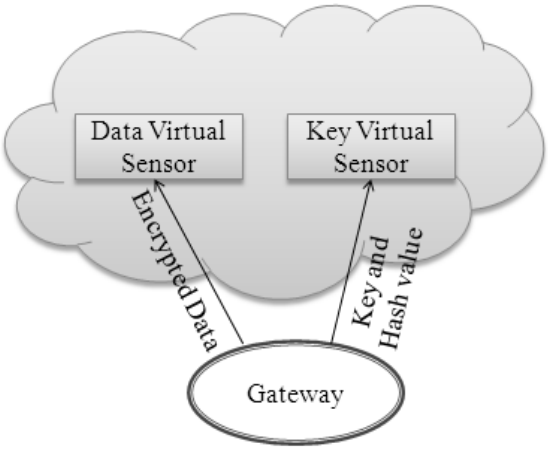

Figure 3. Interface between the gateway and the Virtual sensors (database).

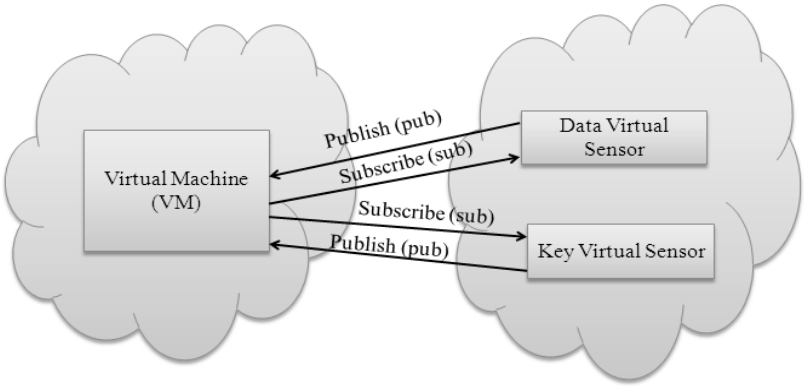

Figure 4. Interconnection between Virtual machine and Virtual Sensors (database) using pub/sub mechanism

4) Virtual Sensor Cloud

The virtual sensor cloud refers to the interface between the storage services provided by the IaaS architecture of a CSP and data processing services provided by another CSP. This subsystem is responsible for sensor data management and sharing operations. The sensor data may be requested for different applications by the service cloud. Based on the requirements the sensor data needs to be represented accordingly. To support these operations a virtualization layer is essential. The virtualization layer consists of two different levels. These levels are:

a) *Virtual Sensors:* The virtual sensor consists of databases to store the data. The infrastructure services for storage are provided by the CSP, say CSP_A. We consider that each gateway has a one to one connection with two virtual sensors. This is shown in Figure 3. The data virtual sensor is used to store the encrypted data and key virtual sensor is used to store the computed hash value and the key that was used for performing the encryption operation. In order to identify the key used for encrypting the data, the timestamp at which the operation is performed is also stored in the corresponding databases.

b) *Virtual Machines*: The Virtual machine is spawned on the request of the service cloud. Based on the request of the service cloud the virtual machines (VMs) extract the information from the virtual sensors and process it. These processing services are provided by the second CSP say CSP_B. The connection between the VMs and the virtual sensors follow a publish/subscribe mechanism which is as shown in the Figure 4. Once the encrypted data, key and the hash values are obtained the corresponding integrity and decryption operations are performed. The decrypted data is sent to the service cloud. There are many advantages of using the above IaaS based architecture when compared to ad-hoc based solutions and thread based solutions as explained in [8]. Thus deployment of IaaS based architecture with virtualization makes the proposed architecture suitable to any working environments.

5) Service Cloud

This subsystem provides SaaS environment to the end users. The data obtained from the virtual sensor cloud is processed and represented for visualization based on the request of the end user.

4. Operation of the Proposed Architecture

The entire operation can be divided into two phases. The first phase involves outsourcing of the data into the cloud by the gateway. This is represented as a flowchart in Figure 5. The sensors measure the parameters periodically and send the data to the gateway either directly or by multiple hops. The gateway continuously monitors if it has received any data from the sensors. On receiving the data the gateway performs the corresponding integrity and the confidentiality operations. To maintain the confidentiality of the data, encryption is performed and for integrity the encrypted data is hashed. The hash value that is stored in the cloud is computed as:

$$H_i(m) = Hash(E_i(m) \| Key_i) \quad (1)$$

Where $H_i(m)$ is the hash value of the i^{th} data, E_i is the encrypted value of i^{th} data and Key_i is the key used for encrypting the i^{th} data. Thus $H_i(m)$ maintains the integrity of the encrypted data and also the key used for performing the encryption.

The gateway then connects to the virtual sensor cloud and puts the encrypted data into the first virtual sensor, the key and the corresponding hash value into the second virtual sensor as illustrated in Figure 5.

The second phase involves providing observation services to the end user. This is shown in Figure 6. When the user access the application using the client device, the service cloud invokes a virtual machine in the virtual sensor cloud in order to provide services as requested by the client. Based on the request of the service cloud the VMs obtain the corresponding data from the virtual sensors using publish/subscribe (Pub/Sub) mechanism. On obtaining the data from the virtual sensors the VM checks for the integrity constraint. If satisfied, the decryption operation is performed using the corresponding key. This decrypted information is forwarded to the service cloud. The service cloud displays the results in the required format to the end user.

In the proposed architecture we observe that the encryption and the hash operations are performed at the gateway before outsourcing the data to the cloud. As the encrypted data and the key required for performing the encryption are stored in different virtual sensors (databases), the attacker must obtain the database in which the key is stored to decrypt the data. Since the cloud architecture provides IaaS paradigm to several users, finding the exact pair of databases is challenge.

Hence, the path for an attacker to obtain the sensitive information from the cloud is obstructed to a major extent. Therefore, the proposed architecture maintains the confidentiality and integrity of the data stored in the cloud. Thus the sensor-cloud architecture helps in providing better observation services to the end user, in-turn helping the customers to perform better analysis. Also this architecture provides dynamic provision of services to the customers; as a result the users can access relevant information from anywhere and at anytime.

Apart from this as the storage services are provided by the CSP_A and processing services are provided by CSP_B. Thus, either of the two service providers have complete information of the overall architecture. CSP_A neither knows the contents of the database nor the application for which this data needs to be processed and CSP_B does not have the stored data. As a result this architecture provides inherent security as the data storage and data processing are performed by two different clouds.

5. Experimental Setup

The experimental setup consists of WBAN nodes to monitor the physiological parameters of a human being and WSN nodes to monitor environmental parameters such as percentage of oxygen, carbon dioxide, temperature, humidity etc. The experimental setup is as shown in Figure 7. As discussed in section 3, the system architecture consists of 4 subsystems, namely client device, service cloud, Virtual sensor cloud and the wireless sensor networks. For each of these subsystems the following tools are used for implementation.

We consider the Client device to be a laptop or a desktop. SQL service of CSP_A is used for the implementation of Virtual sensor. Java Virtual machines provided by CSP_B is used for virtualization and service cloud. Thus the storages services are provided by CSP_A and processing services are provided by CSP_B. For demonstration purpose we have measured the levels of oxygen and carbon-dioxide in an air-conditioned room. To measure these values oxygen sensor (SK-25) [16] and carbon-dioxide (TGS-4116) [16] of Libelium Company [14] were used. These sensors were embedded on the Waspmote board [15] provided by Libelium Company.

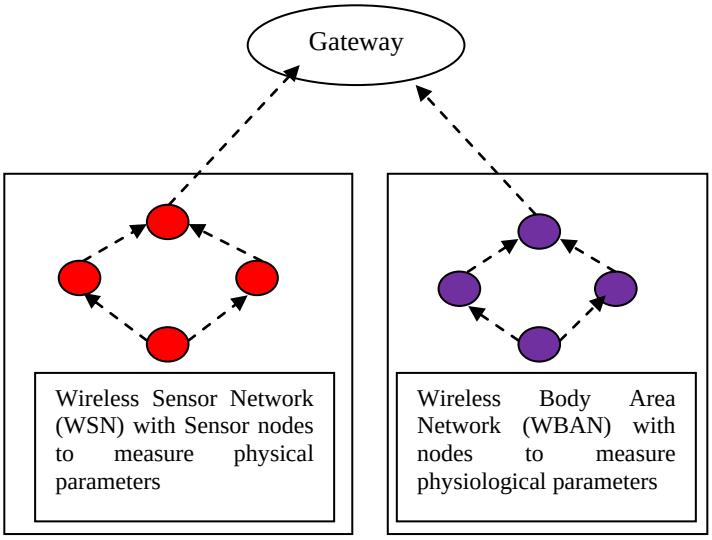

Figure 7. Experimental setup

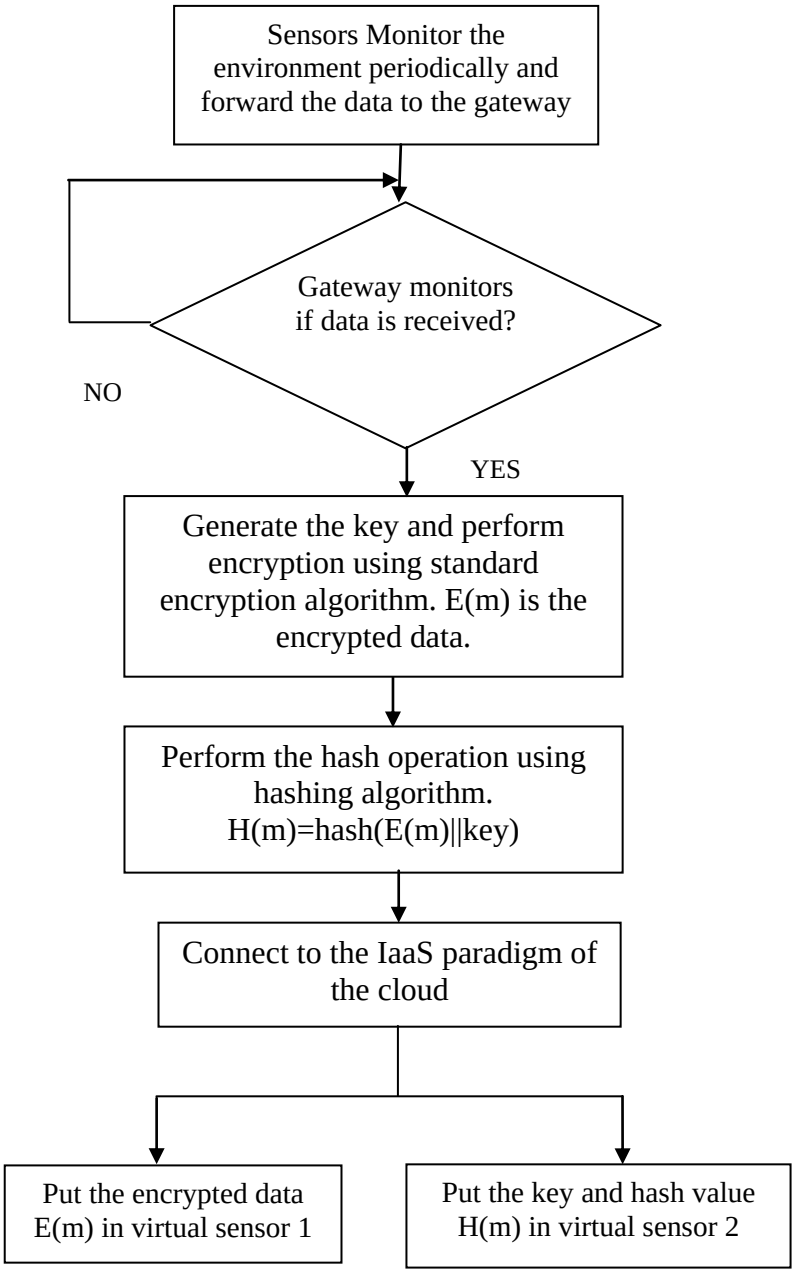

Figure 5. Phase –I Gateway outsourcing the data into the cloud after performing encryption and hashing operations

Java platform is used for programming with the help of NetBeans-7.3 IDE [17]. Any of the standard encryption/decryption algorithm and hashing algorithm (which provides both pre-image resistance and second pre-image resistance) can be used. In this work, DES algorithm is used to perform the encryption and decryption operations and SHA-256 is used to perform hash operations. Thus if an attacker tries to access the data stored in cloud, the task of finding the pair of databases in order to decrypt the data is a challenge. Thus the path for a third party attacker to manipulate the data is obstructed, thereby making the overall system more secure.

Figure 8 and Figure 9 shows a pictorial representation of information services provided to the user. The figure 8 demonstrates the percentage of oxygen and carbon dioxide for the current instance. Figure 9 demonstrates the percentage of carbon dioxide and oxygen for a period of duration.

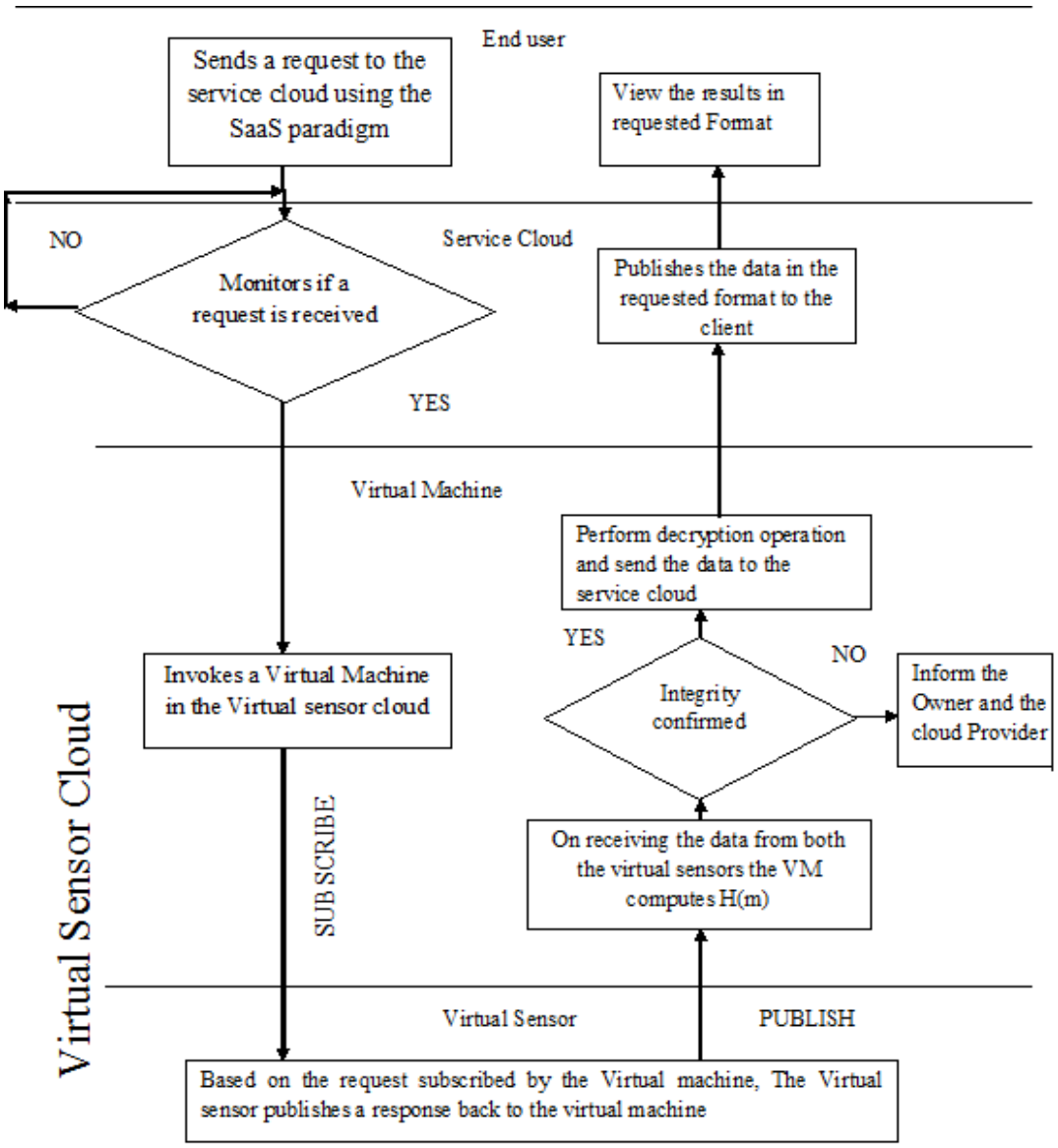

Figure 6. Phase –II Flowchart showing the steps involved in providing observation Services to the end user

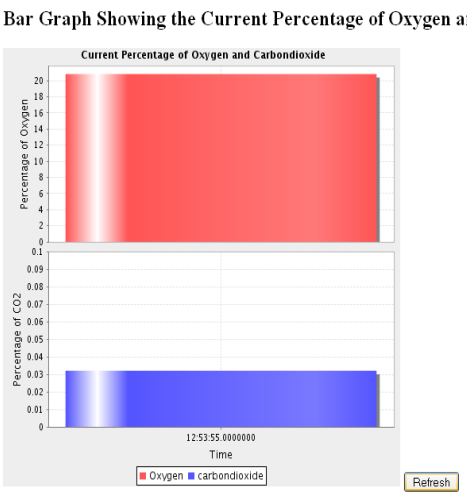

Figure 8. Visualization of percentage of oxygen and carbon-dioxide for the current instance of time

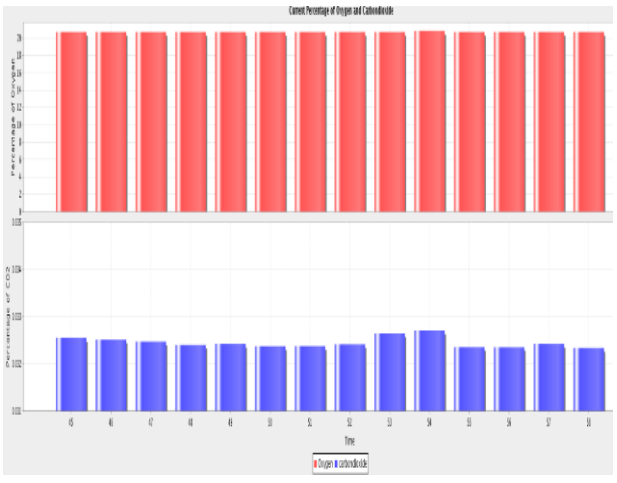

Figure 9. Visualization of percentage of oxygen and carbon-dioxide for a period of time (past values)

6. Conclusion

The measurement of physiological parameters aided in depicting the requirement for health comfort level. On the other hand, measurement of environmental/physical parameter has specified the current environmental suitability for comfort. These two values have helped in deciding and analyzing the relationship and hence suggest the corrective measures for a comfortable living.

The sensor-cloud architecture has provided better provision for storing, processing and analyzing the data, and also ubiquitous computing. The security features such as confidentiality and integrity parameters are implemented as a part of this architecture to provide better information services to the end user anywhere and anytime.

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", International journal of Distributed Sensor Networks, Hindawi publishing corporation, volume 2013.

[2] S. K. Dash, J. P. Sahoo, S. Mohapatra, and S. P. Pati, "Sensorcloud: 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.

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

[4] G. Stoneburner, "Underlying Technical Models for Information Technology Security," NIST Special Publication 800-33, National Institute of Standards and Technology, 2001.

[5] Ren´e Hummen, Martin Henze, Daniel Catrein, Klaus Wehrle " A Cloud Design for user- controlled storage and processing of sensor data", 4th International Conference on Cloud Computing Technology and Science, IEEE Computer Society, 2012

[6] Yuriyama, M.; Kushida, T.; "Sensor-Cloud Infrastructure - Physical Sensor Management with Virtualized Sensors on Cloud Computing," 13th International Conference on Network-Based Information Systems (NBiS),, vol., no., pp.1-8, 14-16 Sept. 2010

[7] Mohammad Mehedi Hassan, Biao Song, Eui-Nam Huh; "A framework of sensor-cloud integration opportunities and challenges",, Proceedings of the 3rd International Conference on Ubiquitous Information

[8] Deshwal, A.; Kohli, S.; Chethan, K.P., "Information as a service based architectural solution for WSN," 1st IEEE International Conference on Communications in China (ICCC), vol., no., pp.68,73, 15-17 Aug. 2012

[9] S. Ivanov and D. Botvich, "Cooperative Wireless Sensor Environments Supporting Body Area Networks", in IEEE Transactions on Consumer Electronics, vol. 58, issue 2, pp. 284-292,2012

[10] "Nimbits Data Logging Cloud Sever", http://www.nimbits.com.

[11] "Pachube Feed Cloud Service", http://www.pachube.com.

[12] "iDigi—Device Cloud", http://www.idigi.com.

[13] "IoT—ThingSpeak", http://www.thingspeak.com.

[14] "Libelium - Connecting sensors to the Cloud", http://www.libelium.com

[15] "Waspmote Sensors Overview", www.libelium.com/products/waspmote/sensors

[16] *"Gases 2.0 Libelium"*, www.libelium.com/uploads/2013/02/gases-sensor-board_2.0

[17] *"NetBeans IDE 7.3", netbeans.org/community/releases/73/*