Internet of Things

Contents

11 SENSOR CLOUD

11.1. Introduction

The advancement and application of Wireless Sensor Networks become an invincible trend into the various industrial, environmental and commercial fields. A typical sensor network may consist of a number of sensor nodes acting upon together to monitor a region and fetch data about the surroundings. A WSN contains spatially distributed self-regulated sensors that can cooperatively monitor the environmental conditions like sound, temperature, pressure, motion, vibration, pollution and so forth. Each node in a sensor network is loaded with a radio transceiver or some other wireless communication device, a small microcontroller and an energy source most often cells or battery. The nodes of sensor network have cooperative capabilities, which are usually deployed in a random manner. These sensor nodes basically

consist of three parts: sensing, processing and communication. Some of the most common sensor devices deployed in sensor network as sensor nodes are camera sensor, accelerometer sensor, thermal sensor, microphone sensor and so forth.

Currently, WSNs are being utilized in several areas like healthcare, defense such as military target tracking and surveillance, government and environmental services like natural disaster relief, hazardous environment exploration, seismic sensing and so forth. These sensors may provide various useful data when they are closely attached to each of their respective applications and services directly. However, sensor networks have to face many issues and challenges regarding their communications like short communication range, security and privacy, reliability, mobility, etc. and resources like power considerations, storage capacity, processing capabilities, bandwidth availability, etc. Besides, WSN has its own resource and design constraints. Design constraints are application specific and dependent on monitored environment. Based on the monitored environment, network size in WSN varies. For monitoring a small area, fewer nodes are required to form a network whereas the coverage of a very large area requires a huge number of sensor nodes. For monitoring large environment, there is limited communication between nodes due to obstructions into the environment, which in turn affects the overall network topology or connectivity. All these limitations on sensor networks would probably impede the service performance and quality. In the midst of these issues, the emergence of cloud computing is seen as a remedy.

In a sensor network, the sensors are utilized by their specific application for a special purpose, and this application handles both the sensor data and the sensor itself such that other applications cannot use this. This makes wastage of valuable sensor resources that may be effectively utilized when integrating with other application's infrastructure. To realize this scenario, Sensor-Cloud infrastructure is used that enables the sensors to be utilized on an IT infrastructure by virtualizing the physical sensor on a cloud computing platform. These virtualized sensors on a cloud computing platform are dynamic in nature and hence facilitate automatic provisioning of its services as and when required by users. Furthermore, users need not worry about the physical locations of multiple physical sensors and the gapping between physical sensors. Instead, they can supervise these virtual sensors using some standard functions.

Within the Sensor-Cloud infrastructure, to obtain QoS, the virtual sensors are monitored regularly so users can destroy their virtual sensors when they become meaningless. A user interface is provisioned by this Sensor-Cloud infrastructure for administering, that is, for controlling or monitoring the virtual sensors, provisioning and destroying virtual sensors, registering and deleting of physical sensors and for admitting the deleting users. For example, in a health monitoring environment, a patient may use a wearable computing system that may include wearable accelerometer sensors, proximity sensors, temperature sensors, etc. like Life Shirt and Smart Shirt or may use a handheld device loaded with sensors and consequently the data captured by the sensors may be made accessible to the doctors. But out of these computing systems, active continuous monitoring is most demanding, and it involves the patient wearing monitoring devices to obtain pervasive coverage without being inputted or intervened.

Sensor modeling language (SML) can be used to represent any physical sensor's metadata like their type, accuracy, physical location and so forth. It also uses Extensible Markup Language (XML) encoding for the measurement and description processes of physical sensors. This XML encoding for physical sensors enabled these to be implemented across several different hardware, platforms (OS), applications and so forth with relatively less human intervention. To transliterate the commands coming from users to virtual sensors and in turn to the commands for their pertinent physical sensors, a mapping is done between the physical and virtual sensors.

11.2. Comparison with WSN

In a traditional WSN, there is only one single user. Data is aggregated and sent to the WSN user. At the device level, the device is dedicated to a single user. But in a sensor cloud, the benefits can be reaped by multiple users or applications. Data aggregation in sensor cloud is taken care by the sensor-cloud infrastructure. Nodes in sensor cloud can serve multiple applications. Figure 11.1 shows the comparison of WSN with sensor cloud.

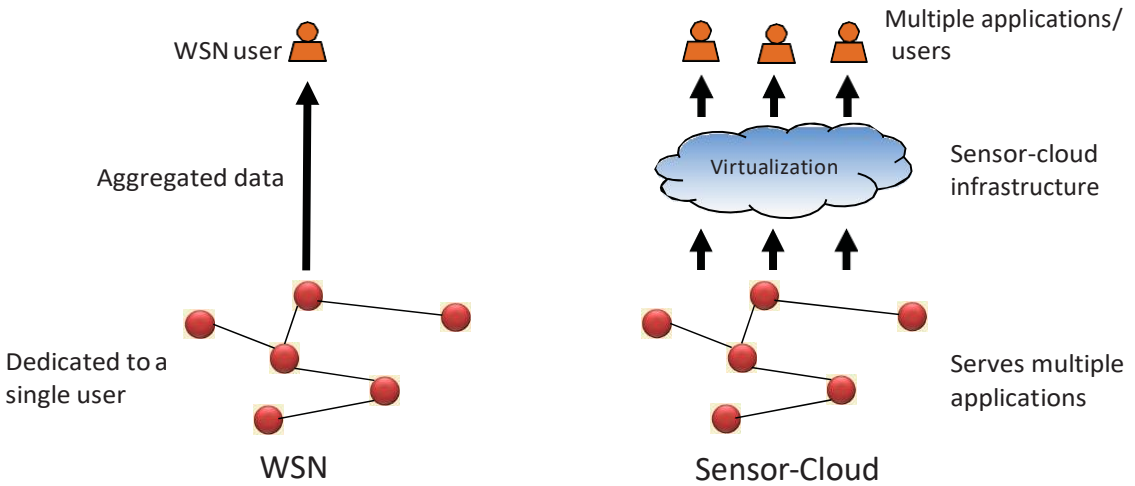

Fig.11.1: Comparison of WSN with Sensor Cloud

In a sensor cloud there is more than one actor and multiple roles. Various actors in Sensor Cloud are end users, sensor owner and Sensor Cloud Service Provider (SCSP). End users enjoy Sensor-as-a-Service (Se-aaS) through applications as per the requirements. The end users are unknown about what and which physical sensor is allocated to serve the application. Sensor owner plays a role from business perspective. They purchase physical sensor devices deployed over different geographical locations and lend these devices to the sensor cloud. Sensor Cloud Sensor Provider (SCSP) is a business actor. SCSP charges from the end users as per their usage of Se-aaS.

In traditional WSN, all attributes like ownership, deployment, redeployment, maintenances, overhead and usage are managed by the WSN users. In Sensor Cloud, the redeployment, maintenances and overhead are managed by SCSP while ownership and deployment are managed by sensor owner and usage by end users. Figure 11.2 shows a comparison of attributes in WSN with Sensor Cloud.

Actors and Roles		
Attributes	**WSN**	**Sensor Cloud**
Ownership	WSN-user	Sensor-owner
Deployment	WSN-user	Sensor-owner
Redeployment	WSN-user	SCSP
Maintenances	WSN-user	SCSP
Overhead	WSN-user	SCSP
Usage	WSN-user	End-user

Fig.11.2: Comparison of WSN and Sensor Cloud

11.3. Sensor Cloud Architecture

Cloud computing service framework delivers the services of shared network through which the users are benefited by the services and they are not concerned with the implementation details of the services provided to them. When a user requests, the service instances (e.g., virtual sensors) generated by cloud computing services are automatically provisioned to them.

Users, other than their relevant sensor services, cannot use these physical sensors directly when needed. Therefore, these physical sensors should be supervised by some special sensor-management schemes. The Sensor Cloud infrastructure would subsidize the sensor system management, which ensures that the data-management usability of sensor resources would be fairly improved.

There exists no application that can make use of every kind of physical sensors at all times. Instead, each application required pertinent physical sensors for its fulfillment. To realize this concept, publish/subscription mechanism is being employed for choosing the appropriate physical sensor. In multiple sensor networks, every sensor network publishes its sensor data and metadata. The metadata comprises of the types, locations and so forth for the physical sensors. Application either subscribes to one or maybe to more sensor networks to retrieve real-time data from the physical sensors by allowing each application to opt for the appropriate physical sensors' type. The Sensor Cloud infrastructure procreates virtual sensors from multiple physical sensors, which can then be utilized by users. However, prior to availing the virtual sensor facility, users should probe first for the physical sensor's availability and might also inspect the physical sensor's faults to maintain the data quality emerging from these physical sensors. Also on every sensor node, application program senses the application and sends the sensor data back to the gateway in the cloud directly through the base station or in multihop manner through other nodes.

Sensor Cloud infrastructure provides service instances (virtual sensors) automatically to the end users as and when requested, in such a way that these virtual sensors are part of their IT resources (like disk storage, CPU, memory, etc.). These service instances and their associated appropriate sensor data can be used by the end users via a user interface through the web crawlers. Figure 11.3 shows the architecture of Sensor Cloud.

For the service instance generation, the IT resources (like CPU, storage devices, etc.), sensor capable devices and service templates (which is used to create virtual sensors) should be prepared first in Sensor Cloud infrastructure. Users make the request for service instances according to their needs by selecting an appropriate service template of Sensor Cloud, which will then provide the needed service instances freely and automatically because of cloud computing services integration. Once service instances become useless, they can then be deleted quickly by users to avoid the utilization charges for these resources. Sensor service provider will manage the service templates (ST) and it can add or delete the new service template when the required template is no longer needed by applications and services. Automation of services plays a vital role in provisioning of cloud computing services and automation can cause the delivery time of services to be better. Before the emergence of cloud computing, services were

provided by human influence and the performance metrics like efficiency, flexibility, delivery times and so forth would have experienced an adverse effect on the system. However, the cloud computing service model has reduced the cost expenses and delivery time and has also improved the efficiency and flexibility.

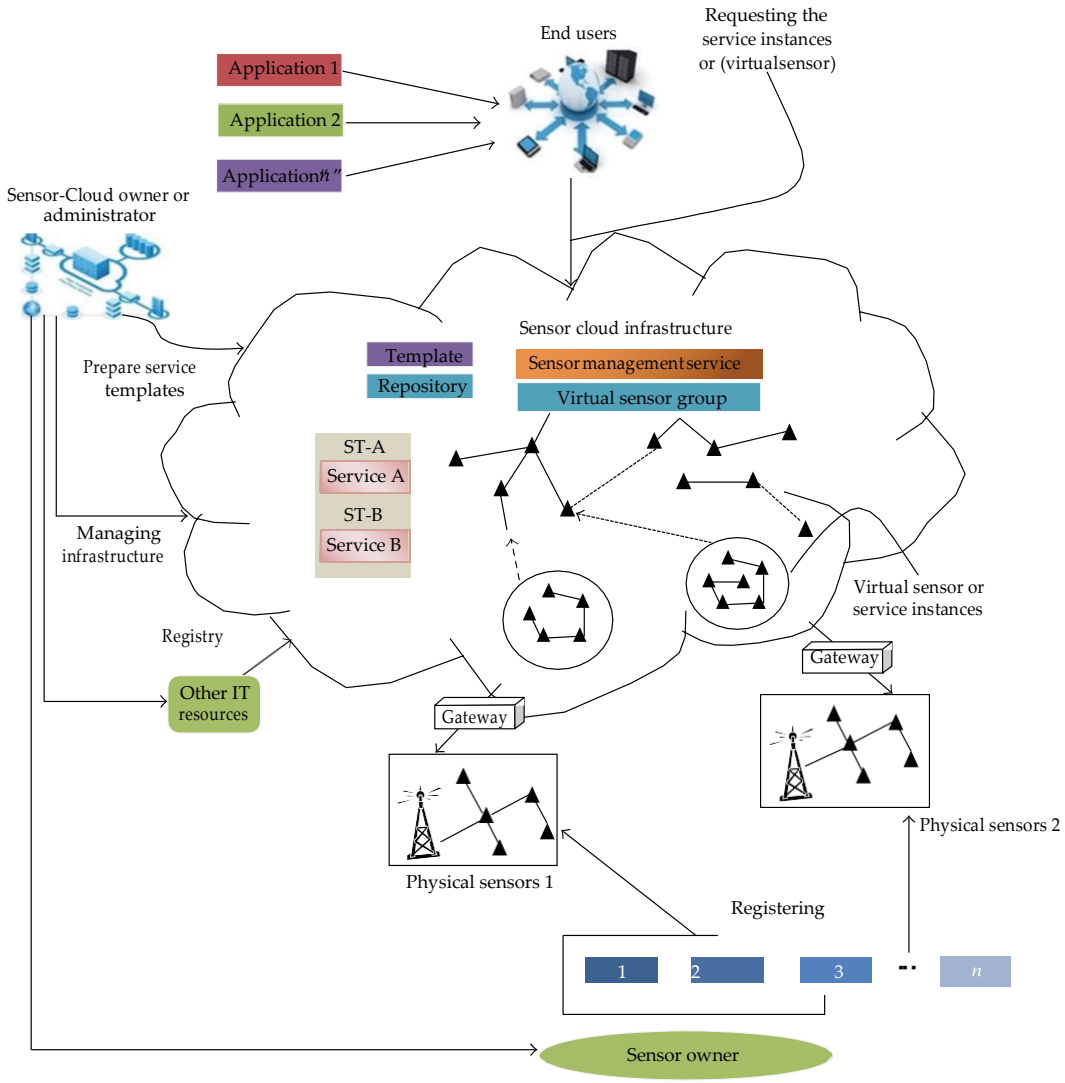

Fig.11.3: Architecture of Sensor Cloud

The physical sensors are ranked on a basis of their sensor readings as well as on their actual distance from an event. Since the cloud computing enables the physical sensors to be virtualized, the users of the Sensor Cloud infrastructure need not worry about the status of their connected physical sensors (i.e., whether a fault free or not). However, they should concern only with the status of their virtual sensors provided only when the users are not

concerned with the accurate results. To achieve accurate results, users must be concerned about the status of physical sensors too. In a Sensor Cloud infrastructure, sensor owners are free to register or unregister their physical sensors and can join this infrastructure. These IT resources (physical sensors, database servers, processors, etc.) and sensor devices are then prepared to become operational. After that, templates are created for generating the service instances (virtual sensors) and its groups (virtual sensors). Once templates are prepared, the virtual sensors are able to share the related and contiguous physical sensors to receive quality sensor data. Users then request these virtual sensors by choosing the appropriate service templates, use their service instances (virtual sensors) after being provisioned and discharge them when became useless.

11.4. Advantages of Sensor Cloud

Cloud computing is very encouraging solution for Sensor Cloud infrastructure due to several reasons like the agility, reliability, portability, real-time, flexibility etc. Structural health and environment-based monitoring contains highly sensitive data and applications of these types cannot be handled by normal data tools available in terms of data scalability, performance, programmability or accessibility. So a better infrastructure is needed that may contain tools to cope with these highly sensitive applications in real time. Following are the several advantages and benefits of Sensor Cloud infrastructure.

1. **Analysis** – The integration of huge accumulated sensor data from several sensor networks and the cloud computing model make it attractive for various kinds of analysis required by users through provisioning of the scalable processing power.
2. **Scalability** – Sensor Cloud enables the earlier sensor networks to scale on very large size because of the large routing architecture of cloud. It means that as the need for resources increases, organizations can scale or add the extra services from cloud computing vendors without having to invest heavily for these additional hardware resources.
3. **Collaboration** – Sensor Cloud enables the huge sensor data to be shared by different groups of consumers through collaboration of various physical sensor networks. It eases the collaboration among several users and applications for huge data sharing on the cloud.
4. **Visualization** – Sensor Cloud platform provide a visualization API to be used for representing the diagrams with the stored and retrieved sensor data from several device assets. Through the visualization tools, users can predict the possible future trends that have to be incurred.
5. **Free Provisioning of Increased Data storage and Processing Power** - It provides free data storage and organizations may put their data rather than putting onto private computer systems without hassle. It provides enormous processing facility and storage resources to handle data of large-scale applications.

6. **Dynamic Provisioning of Services** – Users of Sensor Cloud can access their relevant information from wherever they want and whenever they need rather than being stick to their desks.
7. **Multitenancy** – The number of services from several service providers can be integrated easily through cloud and Internet for numerous service innovations to meet user's demand. Sensor Cloud allows the accessibility to several numbers of data centers placed anywhere on the network world.
8. **Automation** – Automation played a vital role in provisioning of Sensor Cloud computing services. Automation of services improved the delivery time to a great extent.
9. **Flexibility** – Sensor Cloud provides more flexibility to its users than the past computing methods. It provides flexibility to use random applications in any number of times and allows sharing of sensor resources under flexible usage environment.
10. **Agility of Services** – Sensor Cloud provides agile services and the users can provision the expensive technological infrastructure resources with less cost. The integration of Wireless Sensor Networks with cloud allows the high-speed processing of data using immense processing capability of cloud.
11. **Resource Optimization** – Sensor Cloud infrastructure enables the resource optimization by allowing the sharing of resources for several number of applications. The integration of sensors with cloud enables gradual reduction of resource cost and achieves higher gains of services. With Sensor-Cloud, both the small and midsized organizations can benefit from an enormous resource infrastructure without having to involve and administer it directly.
12. **Quick Response Time** – The integration of WSN with cloud provides a very quick response to the user, that is, in real-time due to the large routing architecture of cloud. The quick response time of data feeds from several sensor networks or devices allows users to make critical decisions in near real time.

11.5. Sensor Cloud Service Life Cycle Model

The Sensor Cloud service life-cycle model is illustrated in this section. Figure 11.4 depicts the Sensor-Cloud service life cycle. The users of the sensors can select the appropriate service template and request the required service instances. These service instances are provided automatically and freely to the users, which can then be deleted quickly when they become useless. From a single service template, multiple numbers of service instances can be created. Service provider regulates the service templates and can add new service templates as and when required by a different number of users.

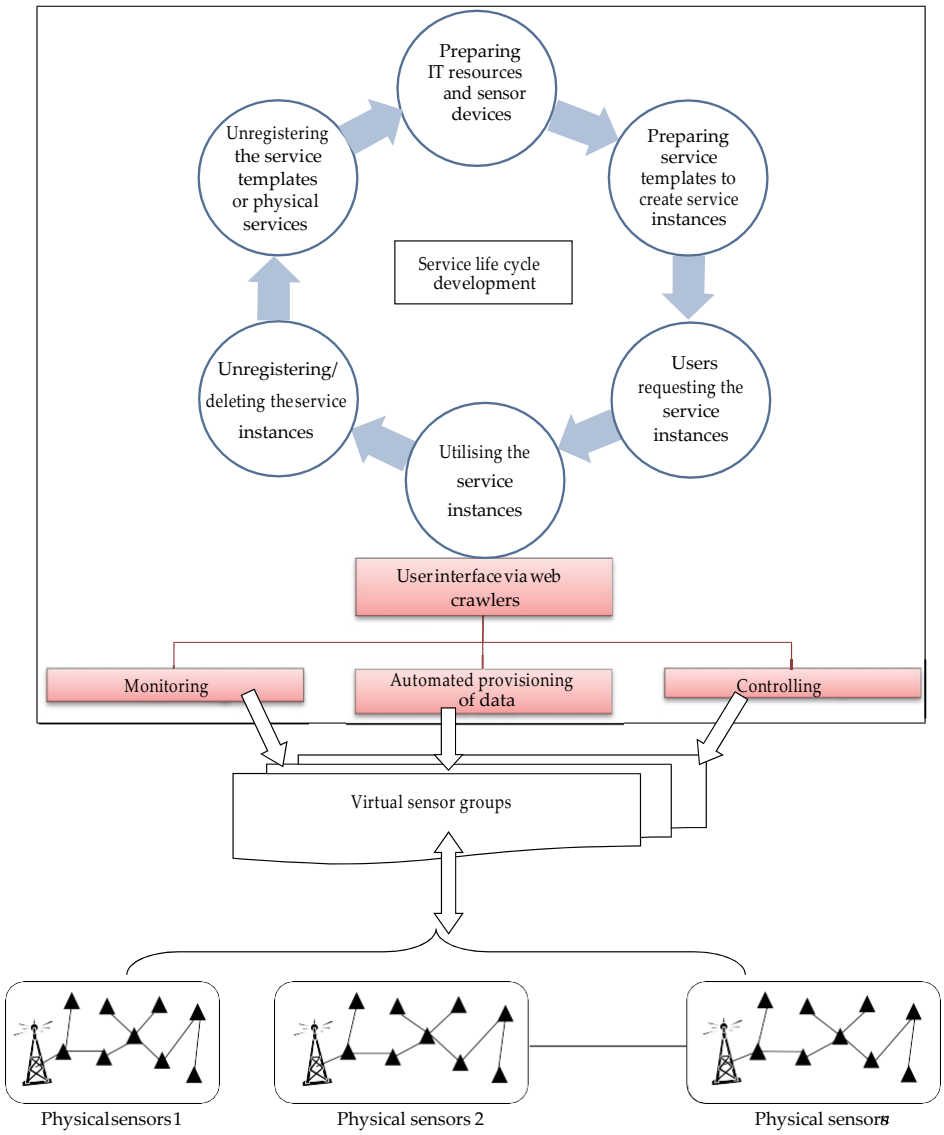

Fig.11.4: Sensor Cloud Service Life Cycle

Before creating the service instances within Sensor Cloud infrastructure, preparation phase is needed which includes (1) Preparing the IT resources (processors, storage, disk, memory etc.) (2) Preparing the physical sensor devices (3) Preparing the service templates.

11.6. Sensor Cloud Layered Structure

Figure 11.5 depicts the layered architecture of the Sensor Cloud platform, which is divided mainly into three layers: (1) User and application layers (2) Sensor Cloud and virtualization layers (3) Template creation and tangible sensor layers.

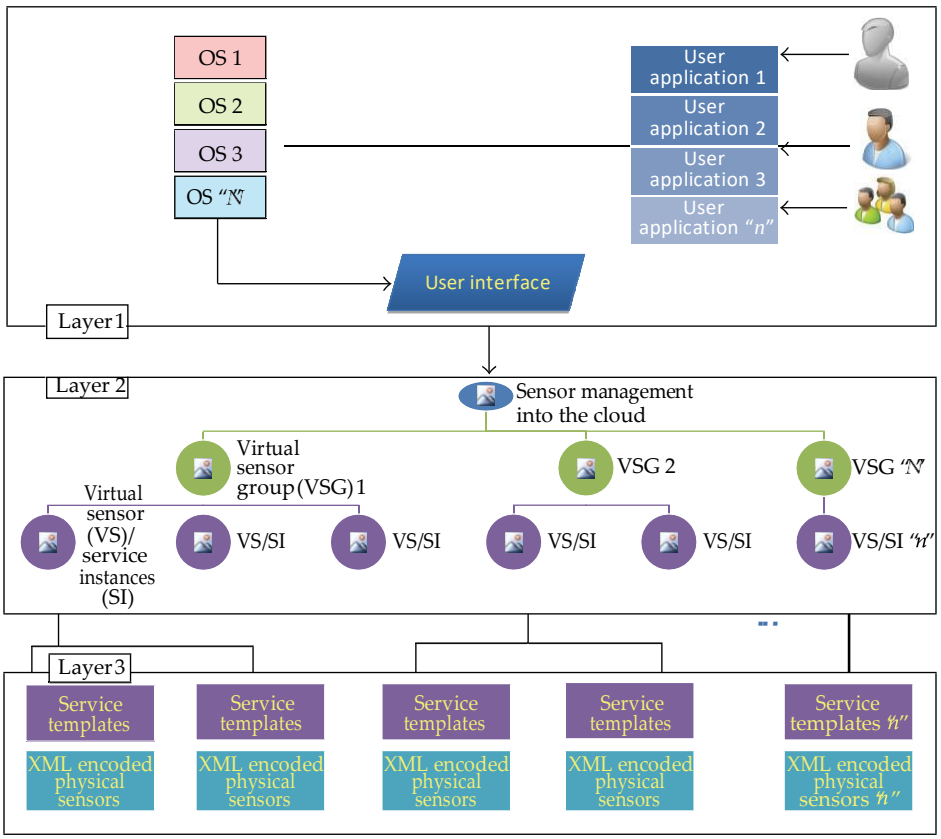

Fig.11.5: Layered Architecture of Sensor Cloud Platform

Layer 1 - This layer deals with the users and their relevant applications. Several users want to access the valuable sensor data from different OS platforms, such as mobile phones OS, Windows OS, or Mac OS for a variety of applications. This structure allows users of different platforms to access and utilize the sensor data without facing any problem because of the high availability of cloud infrastructure and storage.

Layer 2 - This layer deals with virtualization of the physical sensors and resources in the cloud. The virtualization enables the provisioning of cloud-based sensor services and other IT resources remotely to the end-user without being worried about the sensor's exact locations. The virtualized sensors are created by using the service templates automatically. Service templates are prepared by the service providers as service catalog and this catalog enables the creation of service instances automatically that are accessed by multiple users.

Layer 3 - This is the last layer which deals with the service template creation and service catalog definition layers in forming catalog menu. Physical sensors are located and retrieved from this layer. Since each physical sensor has its own control and data collection mechanism, standard mechanisms are defined and used to access sensors without concerning the differences among various physical sensors. Standard functions are defined to access the virtual sensors

by the users. In Layer 2, Sensor Cloud infrastructure translates standard functions of virtual sensors into some specific functions for diverse physical sensors in Layer 3. Physical sensors are XML encoded that enable the services provided through these sensors to be utilized on various platforms without being worried to convert them onto several platforms.

Sensor Cloud provides a web-based aggregation platform for sensor data that is flexible enough to help in developing user-based applications. It allows users quick development and deployment of data processing applications and gives programming language flexibility in accordance to their needs.

11.7. Sensor Cloud Applications

Sensors are very limited and specific to their applications or services when they are linked to a typical sensor network. Therefore, the number of organizations that can provide the sensor services are very limited. However, when the services of sensors move onto the cloud, it is possible to include them to realize a variety of applications. A number of services can be provided to the users for different applications such as health applications, environmental monitoring, industrial tasks (e.g., refining), surveillance, senior residents monitoring or even the applications that monitor the vibration in buildings during an earthquake.

In the Sensor Cloud infrastructure, the sensors and service templates are constructed as catalog menu service on the cloud and the requesters can create new sensor services with the existing sensors in these service instances. For example, service requester can create a sensor service to analyze the impact of earthquake to each floor or room of the rehabilitation center or hospital, and at the same time it can also create sensor services to support older residents with the same set of sensors (virtualized sensors). This service will then help the caregiver to shift the older adults one by one into a safe place. Using the identical sensor services for healthcare, another service requester can create dissimilar sensor service to track the patient's medicine intake and then to analyze the effectiveness of pills through the use of some selected healthcare sensors. Thus, the service requesters can be provided with new services using the same set of sensors on cloud service platforms. This will reduce the cost for resource usage and could have numerous elastic merits to it. Various Sensor Cloud applications that exist are given below.

1. **Nimbits** - Nimbits is a free and social service that is used to record and share sensor data on cloud. It is a cloud-based data processing service and is an open-source platform for the IoT (Internet of Things). We can feed the versatile numeric, text-based, JSON, GPS, or XML values by creating a data point in the cloud. The data points can be connected to Scalable Vector Graphic (SVG) process control, spreadsheets, diagrams, websites and more. Data points can also be configured to generate alerts data-relay to social networks and to perform calculations. Nimbits also provide an alert management mechanism, data compression mechanism and data calculation on received sensor data by employing some simple mathematical formulas.

2. **Pachube Platform** - Pachube is one of the first online database service providers, which allows us to connect sensor data to the web. It is a real-time cloud-based platform for IoT with a scalable infrastructure that enables us to configure IoT products and services, store, share and discover real-time energy, environment and healthcare sensor data from devices and buildings around us. Pachube has a very interactive website for managing the sensor data and an open easily-accessible API. Pachube system provides free usage and has several number of interfaces for producing a sensor or mobile-based application for managing the sensor data within a cloud framework anytime.
3. **IDigi** - IDigi is a machine-to-machine (M2M) Platform as a Service (PaaS) that minimizes the barriers to build scalable, secure and cost-effective solutions, which can bind the enterprise applications and device assets together. IDigi eases the connectivity of remote assets devices and provides all the tools to manage, store, connect and move the information across the enterprise irrespective of its reach. To simplify the remote device connectivity and integration, it uses connector software called IDigi Dia. Regardless of the network location, IDigi platform manages communication between remote device assets and enterprise applications.
4. **ThingSpeak** - ThingSpeak is another open source IoT application and has an open API to store and retrieve data from device assets or things via LAN or using HTTP over the Internet. With this platform, location tracking applications, sensor logging applications and social network of device assets with proper update of its status can be created. ThingSpeak allows numeric data processing like averaging, time-scaling, rounding, median, summing and so forth to store and retrieve the numeric and alphanumeric data. ThingSpeak application features a JavaScript-based chart, read/write API key management and a time-zone management.

Although the above services are able to visualize the sensor data and sensor-driven information, they are lacking secure access to data and interface availability for linking the external or mobile applications for further processing. It means that most of these aforementioned projects do not address the issues of data management and interoperability issues caused by heterogeneous data resources found in the present modern environmental tracking or electronic healthcare systems. But introducing these aforementioned works with Cloud computing infrastructure may overcome the issues related to heterogeneous data access and data management functionality. There are many other applications that are emerging based on the Sensor-Cloud infrastructure, which can be summarized as follows.

1. **Ubiquitous Healthcare Monitoring** - Sensor Clouds can be used for health monitoring by using a number of easily available and most often wearable sensors like accelerometer sensors, proximity, ambient light and temperature sensors and so forth to collect patient's health-related data for tracking sleep activity pattern, blood sugar, body temperature and other respiratory conditions. These wearable sensor devices must have support of BWI (Bluetooth's Wireless Interface), UWB (Ultra Wide Band)

and so forth interface for streaming of data and are connected wirelessly to any smart phone through this interface. These smart phone devices pretend to function like a gateway between the remote server and sensor through the Internet, maybe GPRS/ Wi-Fi or other sort of gateways.

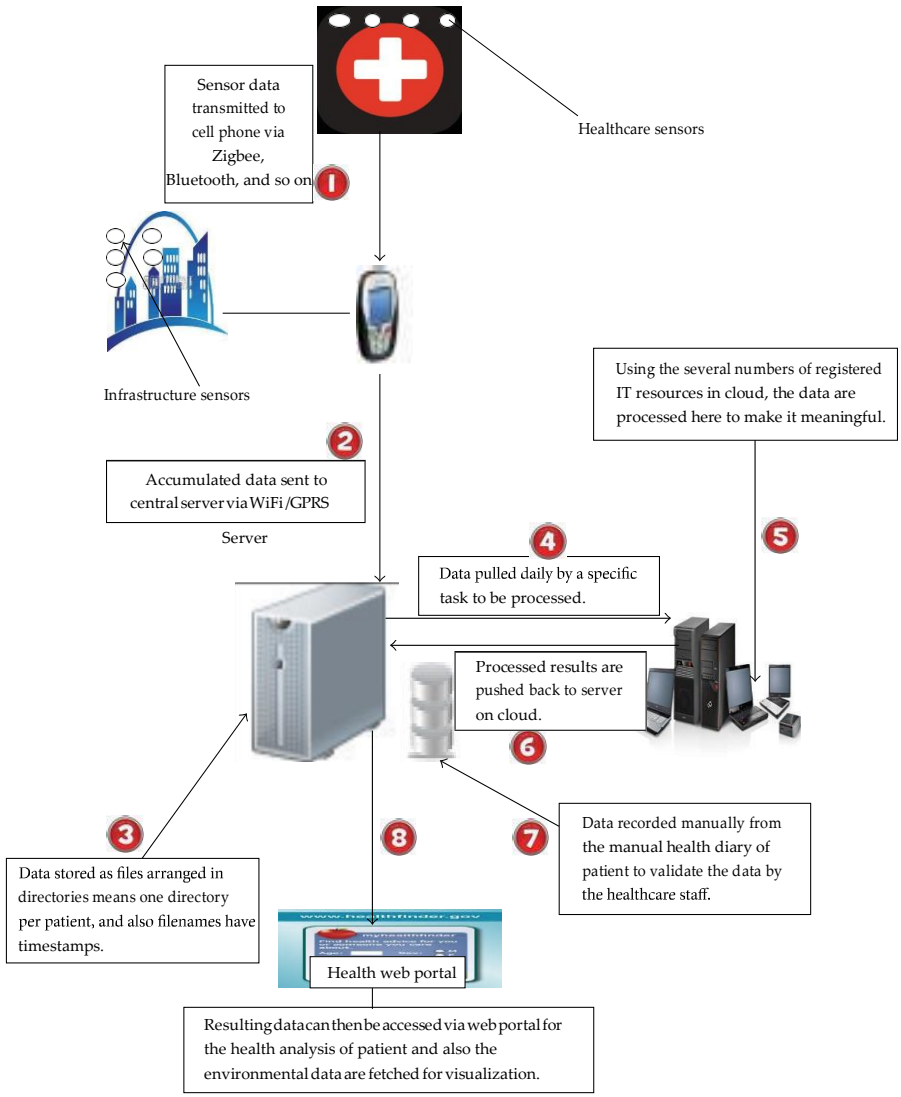

Fig.11.6: Sensor-Cloud Implementation in Healthcare

To transform this system into services-based structure, web-services-based interfaces are used by smart phone device to connect to the server. The system prototype should have made to be robust, mobile and scalable. Robust in the sense means that it should recover itself from circumstances which may lack connectivity issues due to power (i.e., battery), failure, or gateway cutoff to patient's wearable

devices. Mobile in the sense means that it should be capable of tracking signals into heterogeneous environments. It must catch the signals irrespective of whether the patient went outside or still resided into the hospital or building. It should be scalable so that it could be deployed easily for several users concurrently without affecting the performance metrics.

Finally, such prototype system should be re-targetable and extensible in nature. Re-targetable refers to the fact that it can handle various displays with distinct form factors and screen resolution. It means that the same health applications can be displayed to any smart phone display like PDA (Personal Digital Assistant) or to a bigger console device in a hospital where doctors, helpers or nurses may track the acquired data or processed information from distance. The extensibility aspect requires that if any newer sensing devices are introduced into the system for acquiring the patient's health-based information, the system should function efficiently and conveniently without affecting backend server of the services. In this platform, context awareness can be achieved that can direct us to derive a better level of emergency services to the patient. The information regarding recent operational laboratories, missing doses of pills, number of handicaps and other situations would be helpful in health monitoring. The system should not adhere to any changes made into the operating system or intermediate components of sensing devices and is designed in such a way that it would cause minimal disturbance to services provided to existing end users of the system. Sensor Cloud implementation is shown in Figure 11.6.

In this scenario, several numbers of sensors pick up the patient data and these accumulated data are uploaded to a server on cloud. If any noise data is found, they are filtered using some filtering mechanism on a server. The doctors or health employees, nurses and others can then access the patient's data on cloud through a web service portal after being authenticated or permitted by the patient.

2. **Environmental Monitoring for Emergency or Disaster Detection** - In environmental applications, it is possible to detect the earthquake and volcano explosion before its eruption by continuously monitoring them through the use of several numbers of different sensors like strain, temperature, light, image, sound, acceleration, barometer sensors and so forth through the use of Wireless Sensor Networks. Through the Sensor Cloud infrastructure, the sensor instances engaged in environmental monitoring can be used in parallel with several other sensor instances. For example the healthcare department can avoid any future casualty, or with crop harvesting application services they can avoid the damage caused by bad weather condition.
3. **Telematics** – Sensor Clouds can be used for telematics, meant to deploy the long distance transmission of our computerized or information to a system in continuum. It enables the smooth communication between system and devices without any intervention.

4. **Google Health** - It is a centralization service of Google that provides personal health information and serves as cloud health data storages. Google users are allowed to monitor their health records by logging into their accounts at collaborated cloud health service providers into the Google health system. However, in a recent declaration Google has announced the discontinuation of this health service.
5. **Microsoft HealthVault** - This cloud platform is developed by Microsoft to store and maintain health and fitness-related information. HealthVault helps users to store, gather and share their health relevant information and its data can be acquired from several pharmacies, cloud providers, health employees, health labs, equipment and from the users itself.
6. **Agriculture and Irrigation Control (Field Server Sensors)** – Sensor Cloud can be used in the field of agriculture to monitor the crop fields in order to upkeep it. For this, a field server is developed that comprises of a camera sensors, air sensor, temperature sensor, concentration sensor, soil moisture and temperature sensors and so forth. These sensors continuously upload the field data via Wi-Fi access point to the field owner to track the health of their crops. This can also be used for harvesting.
7. **Earth Observation** - A sensor grid is developed for data gathering from several GPS stations, to process, analyze, manage and visualize the GPS data. This GPS data would then be uploaded onto the cloud for efficient monitoring, early warning and decision-making capability for critical situations like the volcanic eruptions, earthquakes, tsunamis, cyclones and so forth to the users all around the world.
8. **Transportation and Vehicular Traffic Applications** – Sensor Cloud can be used to provide an efficient, stable, equilibrium and sustainable tracking system. Earlier existing technologies like GPS navigation can only track the status and current location of vehicle. On the other hand, when vehicle monitoring is implemented using cloud computing, it is possible to incorporate centralized web service, GPS and GSM enabled devices and embedded device with sensors which will provide the following benefits:
   i. To identify the current name of the location.
   ii. To predict the time of arrival.
   iii. To find status of driver via alcohol breath sensor.
   iv. To find the total distance covered.
   v. To track the level of fuel.

   All the data fetched are stored onto some centralized server that will be resided into the cloud. The vehicle owner can access this data on cloud via web portal and can retrieve all data on cloud in real time to visualize the vehicle information.
9. **Tunnel Monitoring** - WSN can be used to implement the distributed sensing of light levels inside the tunnel and under-bridges to provide necessary input information for adapting light functionality. This tunnel information can be put onto the cloud and is

used to monitor the light intensity in real time to avoid the automobile users (drivers) casualty and to save the energy spent unnecessarily for lightening throughout the day.

10. **Wildlife Monitoring** – Sensor Cloud can also be used for tracking the wildlife sanctuaries, forests and so forth to regularly monitor the endangered species in real time.

11.8. Multiservice Provisioning on Multiple Platforms

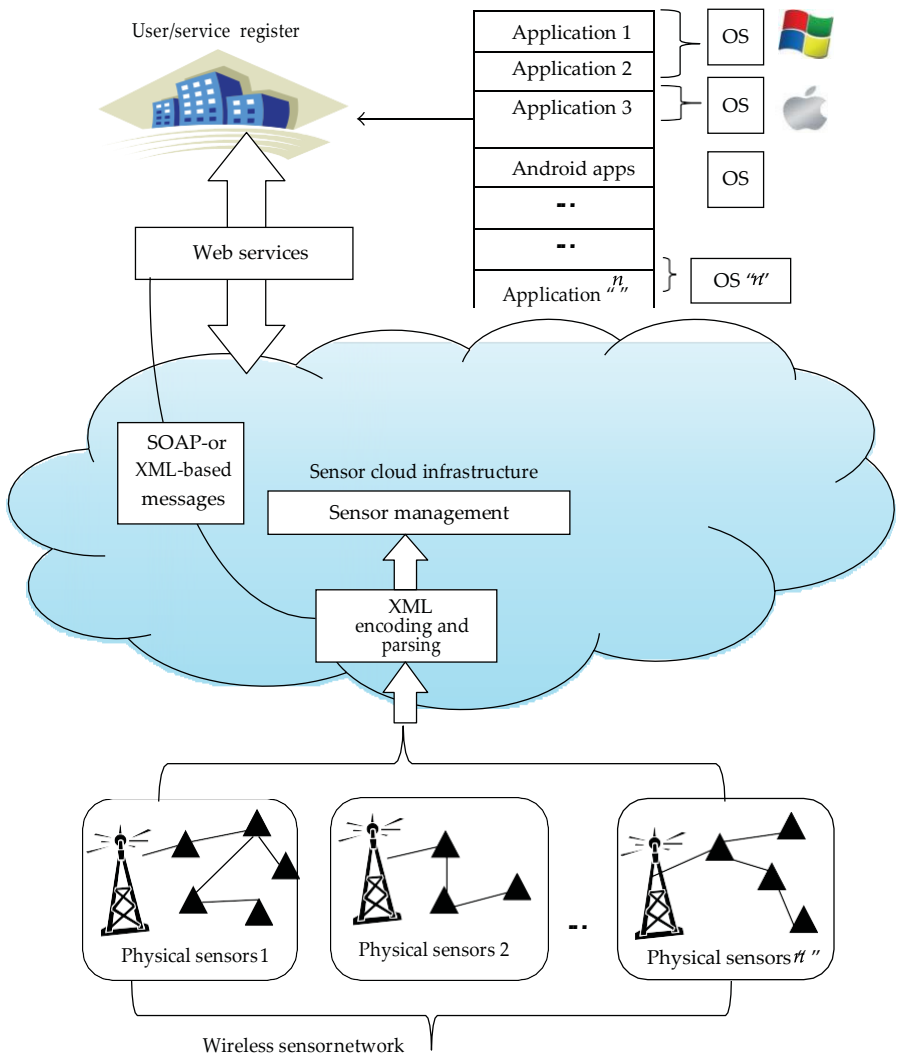

Fig.11.7: XML Encoded Physical Sensors into the Sensor Cloud

Integrating the WSN into heterogeneous networks is a complex task. The reason behind this is the absence of standardized data exchange functions, which may support the participating sub-networks of heterogeneous network. Using XML in sensor networks encourages the

interchangeability of different types of sensors and systems. Figure 11.7 shows XML encoded physical sensors into the Sensor Cloud.

The lower part of Figure 11.7 deals with the XML encoded physical sensors. The XML encoding defines some set of rules for these physical sensors such that it will be both human readable and machine readable with less intervention and will enable these to be implemented on several number of different platforms. XML enables documents to give physical sensor's metadata, that is, the type of the physical sensors, its specifications, the accuracy or intensity of these physical sensors, the exact location and so forth. But sensor nodes have limited storage and power constraints, and conflict may occur while using the XML encoding. For this reason, the XML support should be based on efficient data binding techniques to preserve the time, space and energy by minimizing the XML overhead.

To access the sensor information by using the Web Service Description Language (WSDL) and structure data, multiple applications may access sensor information. But the key issue in using the web services on sensor nodes is energy and bandwidth overhead of structured data formats used in the web services. In heterogeneous sensor networks, integration is a complex task because there is an absence of standardized data exchange format between the heterogeneous systems and networks. XML has evolved to overcome this insufficiency by providing a standard data exchange format between heterogeneous network and systems. Because of the limited hardware resources within sensor networks, XML usage was not fully introduced earlier. But now XML usage in sensor networks is made applicable by introducing the XML template objects in an optimized manner. XML is basically a key feature towards the service-oriented sensor networks and a proper medium to support complex data management and heterogeneous sensor networks.

To enable the applications to communicate with each other and to provide remote access to the services offered by Sensor Cloud platform, web services are introduced. Web services mainly refer to access the services over Internet connection. It has WSDL (Web Service Description Language) definitions, which describe what the web service can do, how a web service can be used by client applications and where the web service is located. Simple Object Access Protocol (SOAP) messages are used to communicate with web services, and these SOAP messages are XML based that are transported over the Internet protocols like Simple Mail Transfer Protocol (SMTP), File Transfer Protocol (FTP) and Hyper Text Transfer Protocol (HTTP).

11.9. Issues and Challenges in Sensor Cloud

There are several issues like designing, engineering, reliable connection, continuous data flow, power issues and so forth that need to be handled while proposing Sensor Cloud infrastructure for health care and other different applications. Some of the main issues are as follows.

11.10. Design Issues

There are several issues while designing the system in real scenario like nursing home, health

care, hospitals and so forth which require fault-tolerant and reliable continuous transfer of data from sensor devices to the server. For example, in a private health care, the patient may be out of coverage area from the smart phone gateway because of patients coming in and out frequently. This scenario would be more prone to connection failure between the server and smart phone (or any other display device, like PDA) and thus this scenario must be considered while designing such system in order to avoid accumulation of errors.

11.11. Storage Issues

Some engineering issues like storage of data at server side and transferring data from phone to server must have to be considered. To tackle this, timestamps are sent with each data packet to assist in reconstruction of data on the server side. Most of the data processing is done at server end so the system must be designed to avoid the bursty processing due to multiple users connected simultaneously to the system. The system must be designed to accommodate multiple users to connect at the same time.

Storage issues can be tackled with the introduction of predictive storage concept. This concept of storage keeps it easily fit to the correlated behavior of the physical environment and builds an architecture that focuses the sensor data archival at some remote sensors of Sensor Cloud infrastructure. It also uses predictive caching at proxies.

11.12. Authorization Issues

A web-based user interface is used for doctors, patients, helpers, care-givers and so forth to inspect and analyze the patient's health-related results remotely. Therefore, the system should offer different authorization roles for different types of users and authenticated via this web interface. This will enable the privacy to some extent by allowing the care givers to restrict them to the patients that he or she will take care of.

11.13. Power (Battery) Issues

While using smart phone as a gateway, power (battery) is the main issue that has to be taken care of because the continuous processing and wireless transmission would drain out the mobile battery within few hours or days. Thus, it is important to tackle power issues while connecting mobile phone gateway with the Sensor Cloud infrastructure.

11.14. Event Processing and Management

Sensor Cloud has to cope with very complex event processing and management issues such as the following.

i. How the events have to be synchronized that may come from different sources in different time because of delays in network?

ii. How the event processing rules have to be changed without affecting the system?

iii. How the messages and events of varying types are supported?

iv. How to support the enormous numbers of events and its conditions in an optimal way?

v. How can we recognize the context (*i.e.*, spatial, temporal, semantic) to its relevant situation detection?

11.15. Service Level Agreement (SLA) Violation

Consumer's dependency on cloud providers for their application's computing needs (i.e. their processing, storage, and analysis of enormous sensor data) on demand may require a specific Quality of Service (QoS) to be maintained. But if cloud providers are unable to provide QoS on user's demand even in the case of processing huge sensor data in critical environmental situations, it would result in SLA violation and cloud provider must be responsible for that. So, we need a reliable dynamic collaboration among cloud providers. But opting for the best combination of cloud providers in dynamic collaboration is a big challenge in terms of cost, time and discrepancy between providers and QoS.

11.16. Need for Efficient Information Dissemination

In Sensor Cloud, an efficient information dissemination mechanism is needed that can match the published events or sensor data to appropriate user's applications. But there are some issues like maintaining flexibility in providing a powerful subscription schema, which may capture information about events, guaranteeing the scalability with respect to a number of subscribers and published events or sensor data. Since the data sets and their relevant access services are distributed geographically, the allocation of data storage and dissemination becomes critical challenges.

11.17. Security and Privacy Support Issues

There are fewer standards available to ensure the integrity of the data in response to change due to authorized transactions. The consumers need to know whether his/her data at cloud center is well encrypted or who supervises the encryption/decryption keys (i.e., the cloud vendor or customer himself). Private health data may become public due to fallacy or inaccuracy. A consumer's privacy may be lost into cloud and sensor data or information uploaded into clouds may not be supervised correctly by user. The US WellPoint disclosed that 130,000 records of its consumers had leaked out and become available publicly over the Internet. So better privacy policies are demand of the time which can offer services themselves while maintaining the privacy.

11.18. Real-Time Multimedia Content Processing and Massive Scaling

Usage of large amount of multimedia data and information in real time and its mining is a big challenge in the integration of heterogeneous and massive data sources with cloud. To classify this real-time multimedia information and contents such that it may trigger the relevant services and assist the user in his current location is also a big challenge to be handled.

11.19. Collective Intelligence Harvesting

The heterogeneous real-time sensor data feed enhances the decision-making capability by using the appropriate data and decision level fusion mechanisms. But maximization of intelligence developed from the massively collected information in cloud is still a very big challenge.

11.20. Energy Efficiency Issues

The basic disadvantages of a WSN and cloud computing are almost the same and energy efficiency of sensor nodes is lost due to the limited storage and processing capacity of nodes. For example, a health monitoring using the textile sensors can work much better and give more accurate results. These textile sensors can be easily sewed and are even washable. Although the proposed system of textile sensors is performing well in the majority of aspects, the battery can last only 24 hours after continuous monitoring and data transmitting regarding user's heartbeat rate, movement, respiratory conditions and so forth. The gathered accumulated data can then be visualized in charts using some web applications and the results are received at user end through an alert message remotely on user's smart phone. But in order to extend system independency, energy efficiency of such systems (textile sensors and microcontroller based) is a primary issue that has to be handled.

Data caching mechanism can be used to reuse bygone sensor data for applications that are tolerant to time. For example, an application related to variant room temperature. If this bygone sensor data is used to satisfy the various requests for a common sensor data, the energy consumption will be reduced. Still more work is needed to overcome the energy consumption.

To improve the energy efficiency and memory usage in a Sensor Cloud infrastructure, there should be a middleware which can tackle the adverse situation in case of continuous and long duration monitoring of data. This can be done through the gateway that is acting as a middleware and collects the huge sensor data from sensor nodes. This middleware should be able to compress the sensor data to avoid the transmission load and then transmits it back to the gateway acting as a middleware on cloud side which in turn decompresses and stores it there. When the transmission overload reduces, the energy consumption of sensor nodes improves automatically due to less processing.

11.21. Bandwidth Limitation

Bandwidth limitation is one of the current big challenges that have to be handled in Sensor Cloud system when the number of sensor devices and their cloud users increases dramatically. However, there is a number of optimal and efficient bandwidth allocation methods proposed, but to manage the bandwidth allocation with such a gigantic infrastructure consisting of huge device assets and cloud users, the task of allocating bandwidth to every devices and users becomes very difficult.

11.22. Network Access Management

There are various numbers of networks to deal with in Sensor Cloud architecture applications.

So a proper and efficient access management scheme for these networks is needed because this will optimize the bandwidth usage and improve link performance.

11.23. Pricing Issues

Access to the services of Sensor Cloud involves both the Sensor Service Provider (SSP) and Cloud Service Provider (CSP). However, both SSPs and CSPs have different customer's management, services management and modes and methods of payments and pricing. So all this together will lead to a number of issues such as

i. How to set the price?

ii. How the payment is to be made?

iii. How the price is be distributed among different entities?

The growing demand for controlling and monitoring the environment and its applications results in the growth of a large number of devices while the cost of deployment and connecting them to heterogeneous network continues to drop. However, the interfaces, protocols, connections and so forth increase at exponential rate, thereby making it difficult and expensive for information technology (IT) people to integrate the devices (sensor devices) into the cloud world. To eradicate the complexity and cost associated with integrating the sensors into cloud or any highly distributed system, there exists emerging and existing standards from both domains. For example, embedded sensor and IT domains within a service-oriented sensor architecture (SOSA).

The service oriented paradigm can be extended to a sensor network and use the service oriented process parameter (like profiling sensors for web services), which helps in intelligence integration into the Internet. This solution when extended to Sensor Cloud would result in high availability and reliability. It was found that the energy consumption of sensor nodes reduced drastically when the data exchange is done among sensors into a heterogeneous network with gateway through the SPWS (Sensor Profiles for Web Services) as compared to traditional SOAP messages. It has been observed also that the cost of memory usage in sensor nodes remains constant with SPWS whereas it is increased with SOAP messages.

The entity which is most responsible for the cost of Sensor Cloud service model is the message exchanged among sensors into a heterogeneous network environment. Using SPWS, power consumption of sensor nodes as well as the memory usages in sensor nodes is reduced drastically. In the Sensor Cloud infrastructure, the cost of communication among sensors is more than the processing cost. Hence the reduction in power consumption and memory usage leads to less communication cost which also enables an energy efficient model of Sensor Cloud.

11.24. Interface Standardization Issues

Web interfaces currently provide the interface among Sensor Cloud users (may be smart phone users) and cloud. But web interface may cause overhead because the web interfaces are not

specifically designed for smart phones or mobile devices. Also, there would be compatibility issues for web interface among devices and in this case signaling, standard protocol, and interface for interacting between Sensor Cloud users and the cloud would require seamless services for implementation. Thus, interoperability would be a big issue when the Sensor Cloud users need to access the services with cloud.

11.25. Maintenance Issues

In order to keep the end user's loyalty, the cloud should cope with the service failure. For this a regular maintenance is needed and redundancy techniques should be implemented to ensure the smooth and continuous flow of services. This can be done by backing up the data regularly and by distributing their multiple data centers geographically across the world.

11.26. Resource and Hardware Compatibility Issues

Hardware compatibility as well as software compatibility both can be solved in cloud computing environment by allowing the sharing of hardware or software resources or services. But there may be the case when sensor or some other resources being used are lost due to some calamity or severe weather condition. To handle these issues, there is an architecture called PRESTO architecture that enables users or clients to view the data in a single logical view which is distributed across several sensor proxies and remote sensors. This enables the users to view variability at several lossy levels and unreliable remote sensor network resources. The PRESTO also supports archival queries on data resources that enable the historical data query to prevent any unusual events to better understand them for future application scenarios.

11.27. Conclusion

This Chapter gives a detailed explanation of the Sensor Cloud. The comparison with WSN, Sensor Cloud architecture, advantages of Sensor Cloud, Sensor Cloud service life cycle model and Sensor Cloud layered structure are well explained. Various Sensor Cloud applications and multiservice provisioning on multiple platforms are illustrated in detail. Finally issues and challenges in Sensor Cloud like design issues, storage issues, authorization issues, power (battery) issues, event processing and management, service level agreement (SLA) violation, need for efficient information dissemination, security and privacy support issues, real-time multimedia content processing and massive scaling, collective intelligence harvesting, energy efficiency issues, bandwidth limitation, network access management, pricing issues, interface standardization issues, maintenance issues and resource and hardware compatibility issues are lucidly explained.