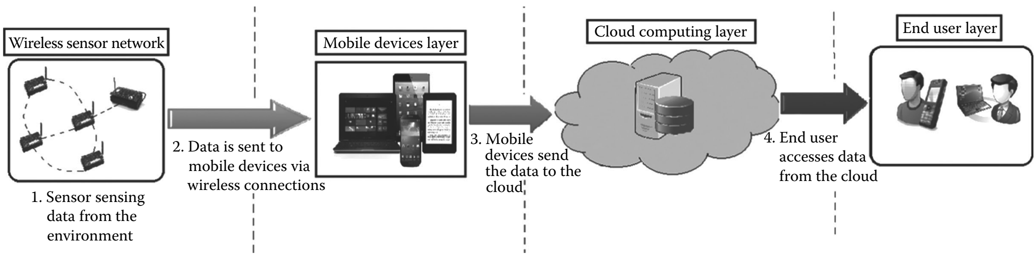
LECTURE NOTES

Mobile Technology and Cloud Computing

Session 09
Sensor Mobile Cloud Computing

7

Sensor Mobile Cloud Computing



ABSTRACT Sensor mobile cloud computing (SMCC) is an emerging research area today. It is an integration of wireless sensor network with mobile cloud computing (MCC). In this chapter, we study the architecture and applications of SMCC. A life cycle model of this architecture is developed. Different challenges of SMCC are also discussed.

KEY WORDS: *wireless sensor network, mobile cloud computing, sensor cloud, urban sensing.*

7.1 Introduction

Wireless sensor networks (WSNs) have been gaining much attention, from both commercial and technical points of view, because of their potential for providing attractive solutions in areas such as health care, industrial automation, asset management, environmental monitoring, transportation business, and so on. Limited processing power, battery life, and communication speed are the main problems of WSN [1]. Cloud computing provides new opportunities in aggregating sensor data and exploiting the aggregates for greater coverage and relevancy and provides scalable processing power. Cloud computing is becoming increasingly pervasive in our daily lives. Its increasing popularity in distributed computing environment is influencing the trend of using cloud environment for storage and data processing. The rapid growth of sensor network and cloud computing technology has led to the emergence of a new platform called sensor clouds. It integrates WSN with the data center model of cloud computing [2]. The primary goal of a sensor cloud is to facilitate connecting sensors and software objects to build community-centric sensing applications. To explore this sensor, data of all types will drive the need for an increasing capability to do analysis and mining on the cloud [3]. One of the applications of sensor cloud computing is doctors' virtual community, where various sensors and cloud computing technologies are used for monitoring health of patients.

Cloud computing is a real paradigm that provides applications and services that are executed on distributed networks using virtualized resources accessed by the Internet protocol. Cloud provides software as a service (SaaS), where software is deployed in the cloud in such a way that users can access the software through the Internet. This eliminates the need to install the software. Cloud services is a layer of the cloud computing stack, which includes software components running in a distributed fashion across the commercial Internet [4].

To extend the services of a sensor cloud, mobile devices can be integrated with it and this infrastructure is known as sensor mobile cloud computing (SMCC) [5]. In this scheme, the sensor data are sent to the cloud through the mobile devices. Because of the incorporation of mobile devices, communication becomes more real time and pervasive than the basic sensor–cloud communication. One of such SMCC applications is mobile health monitoring, which is used for monitoring patient health remotely.

7.2 Wireless Sensor Network

A sensor network is composed of a large number of sensor nodes that are densely deployed over a geographical area. Sensor network protocols and algorithms must possess self-organizing capabilities. WSN nodes are comprised of four basic components: a low-power sensing device, an embedded processor, a wireless communication subsystem, and a power module. The embedded processor is generally used for collecting and processing the signal taken from the sensors. The wireless communication subsystem is used for data transmission. For this purpose, different communication technologies such as IEEE 802.15.4, Zigbee, and radio frequency identification (RFID) are used. The power source consists of a battery with a limited energy level.

Sensor networks consist of many different types of sensors, such as thermal, radar, seismic, acoustic, magnetic, and visual, that are able to monitor a wide variety of conditions, which include temperature, humidity, vehicular movement, pressure, soil makeup, noise levels, the presence of certain objects, and so on. Sensor nodes can be used for continuous sensing, event detection, event ID, location sensing, and local control of actuators.

7.2.1 Different Deployment Technologies of WSN

In regular deployment, data are routed through a predefined path. This deployment is generally used in home networks, the industrial sector, and so on. Random deployment is where sensor nodes are scattered over a finite area. When the deployment of nodes is not predefined, optimal positioning of the cluster head becomes a critical issue. Random deployment is generally used in rescue operations. The mobility of sensor nodes compensates the deployment shortcomings and can be passively moved around by some external force such as wind, water, vehicles, and so on. This type of sensors is generally used in battle field surveillances and emergency situations such as fire, volcanic eruption, and tsunami [6].

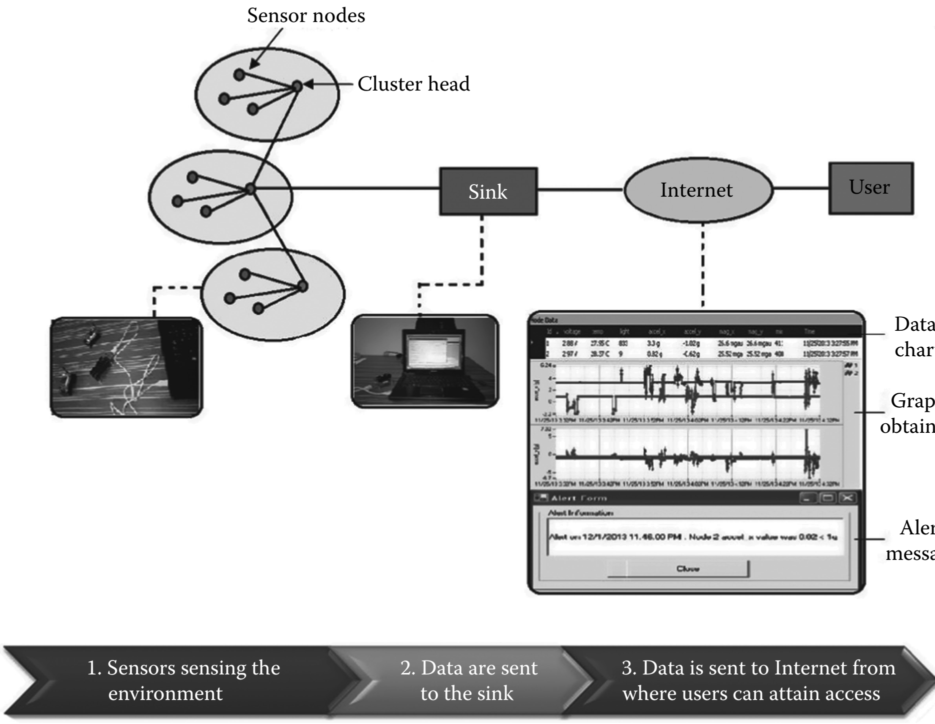


FIGURE 7.1
Basic architecture of sensor network.

7.2.2 Architecture of WSN

In WSN, one of the important methods is clustering to prolong the network lifetime. This method groups the sensor nodes into clusters and elects cluster heads (CHs), which acts as coordinators of the clusters. CHs gather data from sensor nodes and send the aggregated data to the sink or base station. The cluster heads can be selected randomly or based on one or more criteria. Sensor nodes are scattered all over the network. Sensors send data to the cluster head, and finally the cluster head sends the aggregated data to the sink. Then, through the Internet, users or the controllers can access those data from a remote place (Figure 7.1).

7.3 Sensor Cloud

Sensor cloud infrastructure is a broader form of cloud computing. Cloud computing elastically stores and processes data sensed by the sensors, which are scattered through the network. Sensor cloud service architecture integrates cloud computing with WSN to overcome the obstacles faced by WSN and provides new and better facilities [3]. A sensor cloud accumulates and processes information sensed by several sensor networks, facilitates information sharing, and collaborates with the applications on the cloud among users.

Cloud infrastructure manages a set or chain of filters that perform online analysis on sensor data. Physical sensor nodes are used to sense different applications such as transport monitoring, health monitoring, military uses, weather forecasting, and so on. Sensor nodes are programmed with the desired application. On each sensor node, application is sensed by the application program and is sent back to the gateway in the cloud directly through the base station or through multiple hops through other nodes.

Cloud provides on-demand services and storage resources to the clients. It provides access to these resources through the Internet and comes in handy when there is a sudden requirement of resources [2].

7.3.1 Architecture of Sensor Cloud

The main components of the sensor cloud are the client module, the portal module, the provisioning module, resource management, the monitoring module, the virtual sensor group module, and the physical sensor module.

Client module: Client layer is where end users can employ sensor cloud infrastructure by accessing the user interface through web browsers.

Portal module: This module offers interfaces to the client to access the sensor cloud infrastructure.

Provisioning module: This provides automatic provisioning of virtual sensor groups, in accordance with the user's specific need [3].

Resource management: Server, storage, and so on, are the IT resources used for the virtual sensor and the templates for the provisioning module used in sensor cloud architecture.

Monitoring module: This layer monitors the virtual sensor layer and the cloud infrastructure.

Virtual sensor group module: This layer is provided to help the user employ the physical sensor layer dynamically.

Physical sensor module: The sensors are used to sense the environment or a patient's body, as the application requires.

The main components of the layered architecture of sensor cloud are described in the following section.

1. *Login*: The portal is logged into by the end user through a web browser.
2. *Select the templates of virtual sensor group*: The portal wants the list of the templates of virtual sensors groups and virtual sensors from the database. The required template is selected by the end user from the list.
3. *Request the virtual sensor group*: By selecting the templates on the portal, the end user requests the virtual sensor groups. The portal calls the provisioning server providing the input parameters (e.g., the template IDs, user ID, and the virtual group names).
4. *Reserve IT resource*: The IT resources are first reserved by the provisioning server for the virtual sensor group and then, if there is no resource left on the existing virtual servers, a new virtual server is automatically provided with a monitoring agent, and the IT resource is reserved.

5. *Fetch the templates and provision*: The templates of the virtual sensors and the virtual sensor group are obtained by the provisioning server from the database. The virtual sensor groups are provisioned on the virtual server being selected.
6. *Notify the completion*: The end user is notified by the provisioning server of obtaining the virtual sensor group requested by e-mail. It also incorporates the latest records to describe virtual sensor groups (Figure 7.2).

The layered architecture of sensor cloud is described as follows:

Layer 1—Portal server: The portal server provides the web pages to the client browser for provisioning, for requesting or demolishing virtual sensor groups, for controlling those created templates of virtual sensors, for monitoring their virtual sensors, for checking their usage-related charges, and for logging in and logging out [6].

Layer 2—Provisioning server: The provisioning server takes initiatives to arrange the virtual sensor groups in response to requests from the portal server. Workflows are predefined and are controlled by a workflow engine. In a proper order, the workflows are executed. When the provisioning server receives a request from the client, the IT resource pool is checked first and reserved for further processing. The client uses virtual sensor groups through the templates. The server retrieves those templates and then provisions the virtual sensor groups. The job or definition of the virtual sensor groups is updated after provisioning, and agents are provisioned to monitor virtual servers [3].

Monitoring server: The status of virtual sensors is watched by the monitoring server through the agents of the servers and the virtual servers. The received data relating to the status report are stored in a database. Through the web browsers, monitoring information about the virtual sensors is available to the client. The status of the servers is also monitored by the sensor cloud administrators.

7.3.2 Benefits of Sensor Cloud

There are several advantages of merging WSN with cloud computing, thus forming the sensor cloud. The disadvantages of WSN are overcome by adding it to cloud computing [7]. The advantages of sensor cloud are shown in Figure 7.3.

7.3.3 Extension of Sensor Cloud with Mobile

The main reason for the extension of sensor cloud to SMCC is the features it provides [8]:

1. *Mobility*: To handle computing and to establish connection with the Internet to send the data.
2. *Low power consumption*: The mobile device consumes lower battery power than other devices, for example, limited energy availability on portable devices.
3. *Communication capabilities* (*Pervasive*): The mobile devices help establish wireless connection to access data from anywhere, anytime, or user profiles from host, and communication between users. Communication through voice, video calls, and massages is possible.

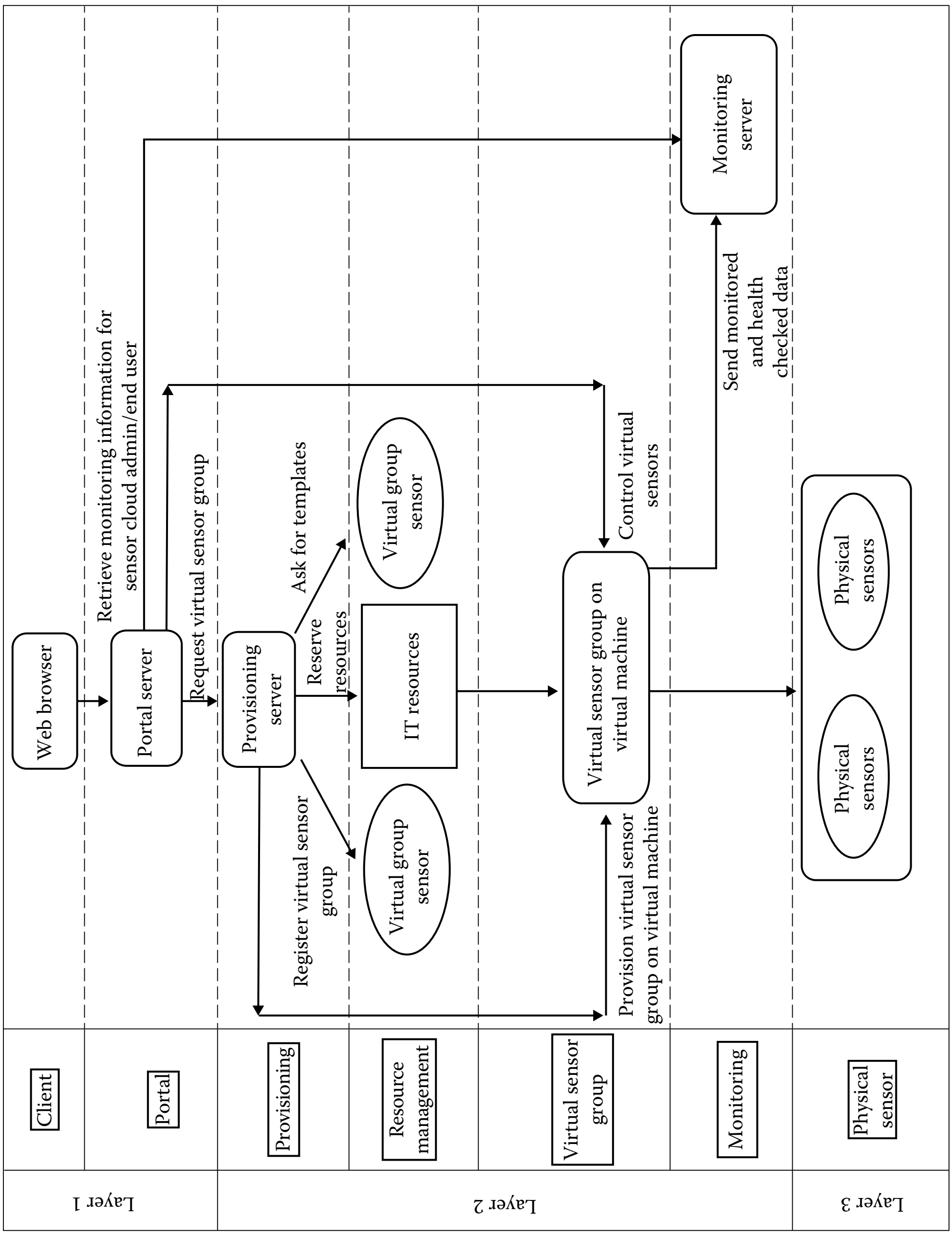


FIGURE 7.2
System architecture of sensor cloud computing.

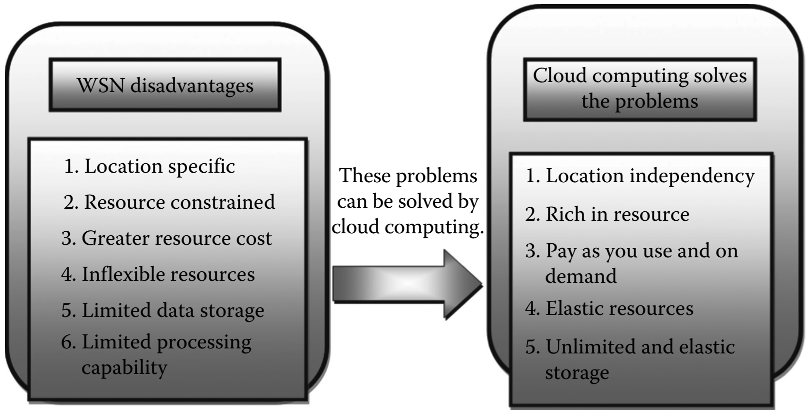


FIGURE 7.3
Incorporation of cloud computing with WSN.

7.4 Sensor Mobile Cloud Computing

SMCC is a new field of mobile cloud computing (MCC). It is used in some applications such as rescue services, healthcare, and so on. Mobile devices are being equipped with various sensors to sense data from the environment or the human body and send the aggregated data to the cloud through the Internet. By introducing a mobile phone between a sensor and the cloud server, data communication overhead can be reduced with the help of intelligent data filtering and fusing techniques. It has been shown that data transmission in a sensor mobile cloud requires less energy than that in a sensor cloud. Therefore, MCC plays an important role in wireless sensor networks.

7.4.1 Architecture of Sensor Mobile Cloud Computing

The sensor mobile cloud architecture is developed to improve the capability of a sensor mobile network. Here, capability means data processing, memory management, data communication, and energy efficiency. Since the capability increases from the sensor to the mobile and from the mobile to the cloud, integration of the sensor, the mobile, and cloud, which is SMCC, increases the capability tremendously [9]. The main components of the architecture are described in the following section, and their diagram is shown in Figure 7.4.

1. *Physical sensors*: Sensors are placed arbitrarily in various locations (e.g., on the human body) for monitoring. Different sensors are used in different applications. A portable electrocardiography (ECG) system uses smart phones attached to the heart and transmits heart rhythm data to the health provider. An asthma sensor has been developed to track the environmental conditions that can cause possible problems to asthma patients.
2. *Mobile phone*: From Figure 7.4, it is clear that the sensor's data are sent to the mobile phone via Bluetooth or Zigbee networks. A mobile phone collects the sensor data, processes the data, and transfers it to the cloud for further processing [9]. Low computational devices such as mobile phones can be used to filter the sensor data.

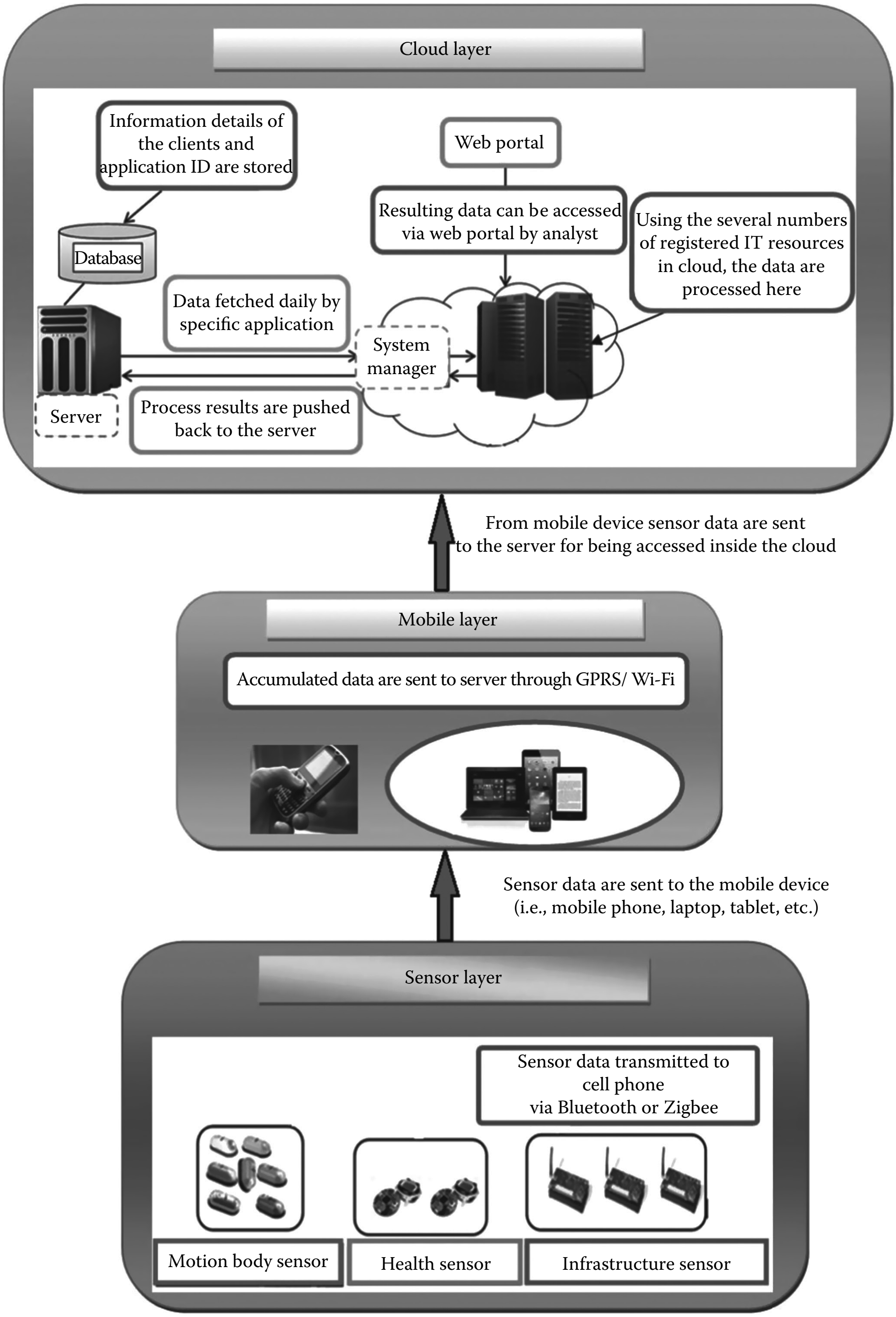


FIGURE 7.4
Block diagram of sensor mobile cloud.

Generally, Wi-Fi is used to establish communication between a mobile and the cloud. If Wi-Fi is not available, 3G and 4G technologies allow sending the collected sensor data to the cloud.

3. *Mobile network*: Mobile phones send sensor data to the WAP (wireless application protocol) server placed in the mobile network. A mobile network that contains a WAP server and a backend database is shown in Figure 7.4.

   Mobile devices are connected to the mobile networks via a base station, that is, base transceiver stations (BTSs) or access points that establish connection to the existing mobile network and provide functional interfaces between the networks and mobile devices [10]. HLR is an important database in mobile network, storing the mobile device's identification number (IMEI number) and user details with the corresponding SIM. This way, the particular user can be traced via the WAP server. Authentication, authorization, and accounting are controlled by mobile network operators based on home agent and the subscriber's information stored in databases. The subscriber's requests are delivered to the cloud through the Internet. The cloud provider processes the requests and sends them to the corresponding cloud services, which are developed with the concepts of utility computing, virtualization, and service-oriented architecture.
4. *System Manager*: The system manager manages the cloud, which is connected to the WAP server through the Internet. System manager fetches data from the WAP server to process it in the cloud server, which allots IT resources before starting data processing. The cloud server runs the user application and computes the data collected from sensor nodes. There exist web portals through which the analyst can access results and provide appropriate decisions to the client for particular application.

In SMCC, events are generated from the client side by mobile phones having certain event IDs and subscriber IDs and are sent to the cloud for processing. One of the main components of this architecture is the system manager which can retrieve data for the particular client from the HLR database placed in the mobile network. After identification of the client, the event is sent to the cloud server. Experts are logged in through web portal, and suitable decisions are sent to the client.

7.4.2 Service Life Cycle Model of Sensor Mobile Cloud Computing

In this section, the service life cycle of SMCC is described. The operation is triggered from the client side. A sensor collects data from the client or the environment, and this signal is passed to the cloud via the client's handheld mobile device. Finally, the experts monitor the information and send the response to the client. The work flow of this service model is described in detail in the following:

Physical sensor: The sensor senses data depending on the application.

Client side: An event is triggered by the end user, and the application sensor data are collected and sent to the cloud server through mobile devices.

Reserve IT resources: The cloud server is used to dynamically store the sensor data. Data management and computation are also handled by the cloud.

Expert monitoring: Experts such as doctors or rescue teams monitor the data received from the mobile phones and take action if there is any abnormality.

Response: Expert teams transmit their advice to the subscriber by sending messages to his or her mobile and taking quick actions to help him or her [6].

7.4.3 System Architecture for a Rescue Service Model

In this section, the specific system architecture for rescue service is demonstrated. This architecture is separated into four layers:

1. Multiple-sensed mobile device
2. Emergency cloud
3. Nearby people
4. Rescuer

The architecture is depicted in Figure 7.5.

1. *Multiple-sensed mobile device*: Multiple-sensed mobile devices can collect a wide range of sensing data from the environment or from the behavior of the people. The sensors, which collect important data for the rescue authority to make decisions when an emergency occurs, are mostly visual, audio, motion, location, ambient, and physiological. To detect any emergency event, the sensed signals should be processed automatically. To extract meaningful information, these sensing data are filtered into the mobile. Information is considered to be meaningful if it contains a predefined pattern. According to user-defined criteria, events are categorized and sent to the emergency cloud [6].

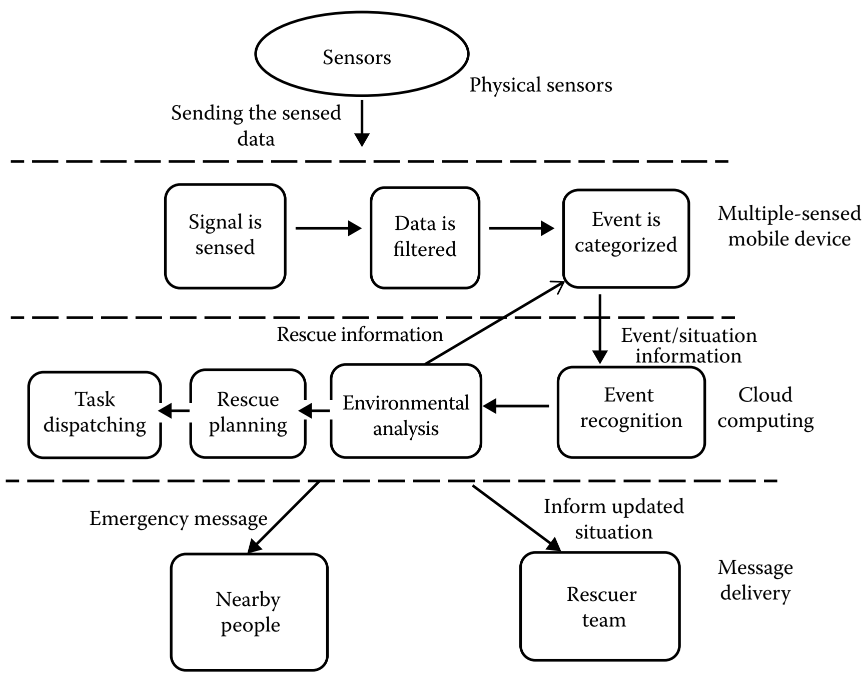


FIGURE 7.5
System architecture of sensor mobile cloud computing for rescue service. (From Chen, Y.J. et al., Sensors-assisted rescue service architecture in mobile cloud computing, *Wireless Communications and Networking Conference*, 2013, pp. 4457–4462.)

2. *Emergency cloud*: Since the information regarding an event from mobile devices is generated from a local perspective and may be incomplete as the sensing is done in an emergency situation, emergency cloud has to further recognize the complete event from a universal perspective. Then the environment within the range of the emergency event is analyzed with the collected data to support rescue planning. For example, emergency events in an urban district and a mountain area may require different rescue methods and policies. In addition, rescue information, such as the shortest path to the shelter that can provide guidance to the people in emergency, is sent to mobile devices. Finally, emergency cloud distributes the rescue tasks to appropriate rescue units according to their work load and locations.
3. *Nearby people*: It is possible that somebody near the victims can provide instant help compared to distant rescue units in an emergency. Thus, the emergency message can also be broadcast to nearby people. Sometimes, prediction of an evacuation process from the disaster area can be broadcast as the emergency message to people in the locality.
4. *Rescuer*: Mobile devices will keep updating information about the situation of people in the disaster area and send such information to the cloud in emergency service. The information about the situation is also analyzed and updated to provide urgent information to the rescue units.

7.4.3.1 Performance Analysis of Rescue Service Model

Performance analysis of the earlier rescue model is described in this section. Power consumption for transmitting a continuous signal is one of the main constraints in SMCC. Figure 7.6 shows the remaining battery life of the mobile device with respect to time. Figure 7.7 shows the delay time between the local server operation and the cloud server operation.

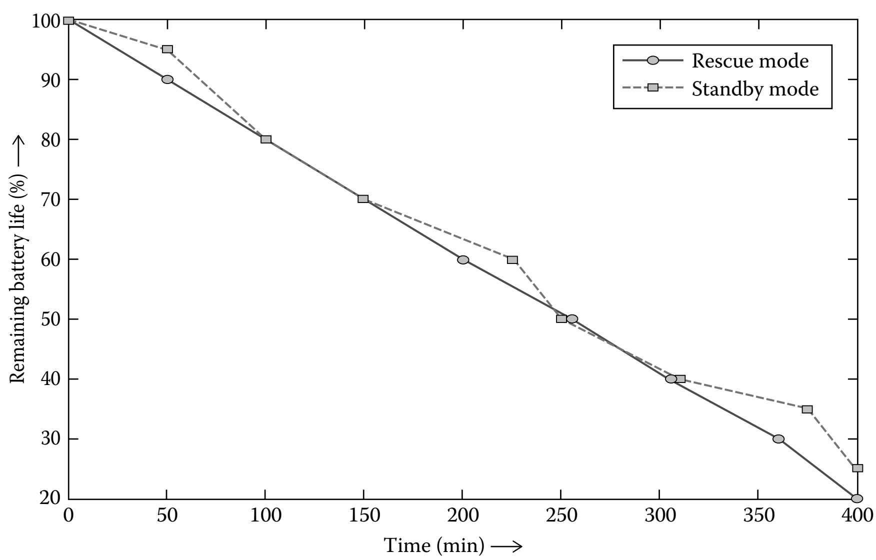


FIGURE 7.6
Time versus remaining battery life.

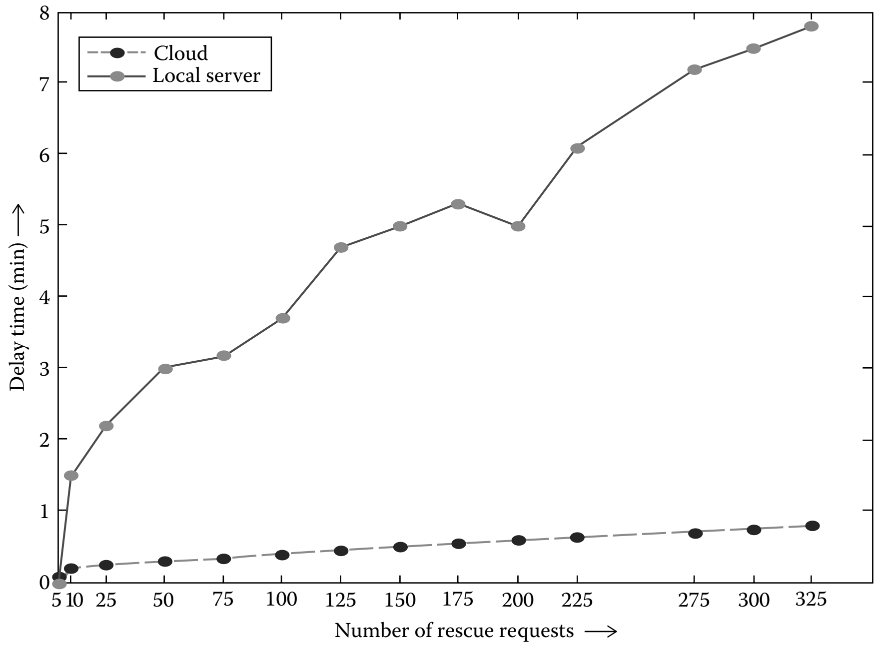


FIGURE 7.7
Number of rescue requests versus cloud and local server delay.

Power consumption: The rescue system works at the background, triggered by the users' smartphones during an unexpected emergency incident. It is necessary to calculate the power consumption by the mobile device. Figure 7.6 shows the power consumption in the rescue mode and in the standby mode. In the rescue mode, after a particular time period, data is sent from the mobile device to the cloud, and the GPS system helps identify the exact position of the person. During this time, the battery keeps losing power with time [6]. When a person needs help, he triggers an event. Data collected from sensors are sent from his mobile device. Rescue program is initiated by the cloud, starting the rescue mode. When the user does not require the application, it defaults to standby mode.

Delay analysis: Figure 7.7 shows the comparison of delays regarding the capacity of local server and the cloud server. Generally, the server placed in a mobile network is denoted "local server," which is equipped with an Intel Core i5 processor running at 2.4 GHz, and 8 GB of RAM. A cloud server can be built with up to 16 CPUs, 128 GB RAM, and 2.5 TB of storage. In the cloud server, the rescue route planning runs a dynamic programming algorithm to compute the fastest route to the disaster spot according to the real-time road status information [6]. But in the local server, the specification is not sufficient to run a dynamic programming algorithm. As a result, the delay in the local server is much higher than that in the cloud server. Here, the delay time is measured from the time of calculation of rescue route planning.

7.5 Internet of Things

Internet of things (IoT) is an upcoming technology that permits interaction between real-world physical elements such as sensors, actuators, personal electronic devices, and so on, over the Internet to facilitate various applications in the fields of e-health, intelligent transportation, and others. IoT is the convergence of different visions—things-oriented, Internet-oriented, and semantic-oriented [11]. Radio frequency identification (RFID) and sensing components are associated with everything used in daily lives, and information is uploaded into the computer, which monitors everything. RFID is the thing that connects the real world to the digital world. The basic idea of IoT is the pervasive utilization of things or objects—such as RFID tags, sensors, actuators, mobile phones, and so on—which, through unique addressing schemes, are able to interact with each other and cooperate with their neighbors to reach common goals. Wireless sensor network, RFID system, and RFID sensor network are used to collect data opportunistically [11]. Many challenges face this upcoming technology, in which technology and social network must be united for unique addressing, storing, and exchange of collected information. A remarkable point of contact for both sensing environments and cloud is IoT, where the underlying physical items can be further abstracted according to thing-like semantics [12]. With emerging technology IoT, a new framework is introduced to converge the utility-driven, cloud-based computing [13]. IoT provides several advantages. They are as follows:

1. It helps people to control household devices to save energy and in turn save money.
2. It can also be used to monitor the health of a person who needs immediate attention.
3. People can control their security systems at home through their mobile phone for their personal safety.
4. IoT can also be used in asset tracking and inventory control, shipping and location, security, individual tracking, and energy conservation.
5. It helps track consumer-based information given by the devices.

7.6 Urban Sensing

A wide range of technical, but also sociopolitical, challenges involve pervasive environmental monitoring, which applies especially to the sensitive context of a city. Urban sensing is an extended form of the existing sensor network. Urban areas comprise many different elements such as buildings, vehicles, citizens, and so on. People-centric urban sensing involves collecting data associated with people, such as their immediate surroundings, their characteristics, and the way they interact with their surroundings [14]. Here, people are involved not only as consumers of collected data but also as collectors of data from natural phenomena or ecological processes. The set of producers and consumers of data overlap in the urban sensing environment. People participate in both roles like a loop sensing and distributing the collected data. Interactions among the elements of the urban sensing scenario, as well as applications achieved through these interactions, are discussed in the following section. Issues that arise and applications that are enabled as a result of these interactions are also discussed. The traditional wireless sensor network is focused on application-specific deployment. Sensors are mobility-driven and data from the sensors are periodically updated into the cloud. Urban sensing uses mobile phone network data, such as the types of activities in different parts of the city, residential and working areas, population distribution, and commuting patterns. Since mobile phone technology is increasingly adopted by the population, every possible micro and macro behavior is available freely. The electronic communication sector is also concerned that the privacy of personal data is only partially addressed.

7.6.1 Opportunistic Sensing

In pervasive or ubiquitous computing, WSN is one of the important elements. The sensor network consists of multimodal sensors that provide opportunistic sensing (OS), which is used to produce more robust event recognition [15]. OS accomplishes automatic target recognition (ATR) and supports large-scale applications. It is adaptive in nature; there is no predefined circumstance for OS. Over the past decade, the focus of wireless sensor networking research has evolved from static networks of specialized devices deployed to sense the environment to networks making use of robotic or other controlled mobility to adapt to the sensing conditions and to a people-centric approach relying on the mobility of people. Hazards (any kind of hazards) are unpredictable, and they can happen at any place at any time, so a rescue team has to continuously monitor a large area in order to identify potential danger and take action. A single type of sensor is not efficient to find victims or to integrate different related information of a situation. A heterogeneous sensor network-based [16], multimodal information integration is required to collect different types of information. This kind of network is not specific or planned for a particular job. OS or networking is often associated with human-centric ubiquitous systems, such as in crowd sourcing and participatory sensing applications, focusing on human activity recognition [17].

The steps of OS are shown in Figure 7.8. In OS, the custodian may not be aware of active applications. Instead, a custodian's device (e.g., cell phone) is utilized whenever its state matches the requirements of an application [18]. OS prefers a standard for information and signal processing in which a network of sensing systems can automatically discover and select sensor platforms based on an operational scenario. In OS, data collection is automatic without user participation [5]. This approach helps the user get rid of the burden to

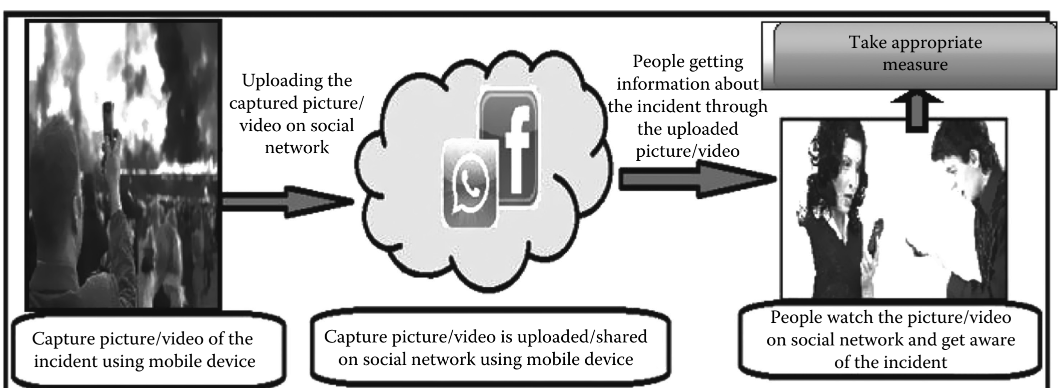


FIGURE 7.8
Steps of opportunistic sensing.

support the system and increases the range of applications and sensing field. The users need not be preoccupied with sensing the data, but system designers should carefully make a system that is only activated if predefined conditions have been satisfied. In the opportunistic approach, data quality is low and suffers from high data-miss rates because the exposure time for sensors may not be sufficient. In the opportunistic approach, missing sensing data is unavoidable in terms of time and space. WSN nodes are homogenous and fixed, whereas users monitor different target areas by moving dynamically during each sensing period in mobile phone sensing.

7.6.2 Participatory Sensing

Participatory sensing (PS) is an improvement on static WSN. Its deployment cost is very low in participatory sensing because it enhances existing sensing and communication infrastructure. Because of the mobility of the cell phone, it can cover different areas [19], and because sensors are already embedded into cell phones, it affords economies of scale. Because of the availability of app stores, it became easy to develop and deploy application in the mobile phone. In PS, people take part directly in the sensing loop, and the applications dramatically improve their daily lives. The sensing tasks by mobile sensors are triggered manually. In PS, the custodian has the opportunity to serve an application request without considering personal interest. People interfere in the sensing system to make decisions about data sharing, and privacy mechanisms should be allowed to impact data fidelity. PS is based on a preplanned system. A person interested in particular applications can install them into his or her mobile, and the sensing operation is triggered by him or her dependent on the condition. In PS, to meet the requests made by applications, people continuously coordinate with the sensing system, and critical decisions are made on sensing the target, location, and data [3]. The system is simplified, as complex operations are solved by the intelligence of the person, and high data quality is assured through users who are actively engaged in data collection. In PS, the burden is on the user and needs a support mechanism to encourage user activity.

For large-scale sensing, these features make it difficult to achieve using PS. PS is also a part of urban sensing and is used to organize less complex trustworthy ad hoc observatory applications that can be implemented in a metropolitan area. The applications are specific in nature, such as a GIS-based noise detection application, transport system, and so on. The steps of PS are shown in Figure 7.9. A public transport operator creates timetables, which contain other statistic information that does not reflect actual traffic conditions [20]. Mobile participatory sensing enhances the basic application with real-time updates that allow the crowd to collect the required data.

7.7 Application

Appropriate and real-time health monitoring of patient is very challenging and important issue nowadays. In a conventional healthcare system, nurses monitor the patient's health, record the data, and forward the data to doctors and other medical staff. All processes are manual. So, the delay or latency is the main drawback of this approach. In case the patient's health deteriorates rapidly, an emergency may occur, which may need real-time health monitoring without delay. To make this possible, an SMCC can be introduced in a conventional healthcare system. As SMCC is a combination of WSN and and CC with

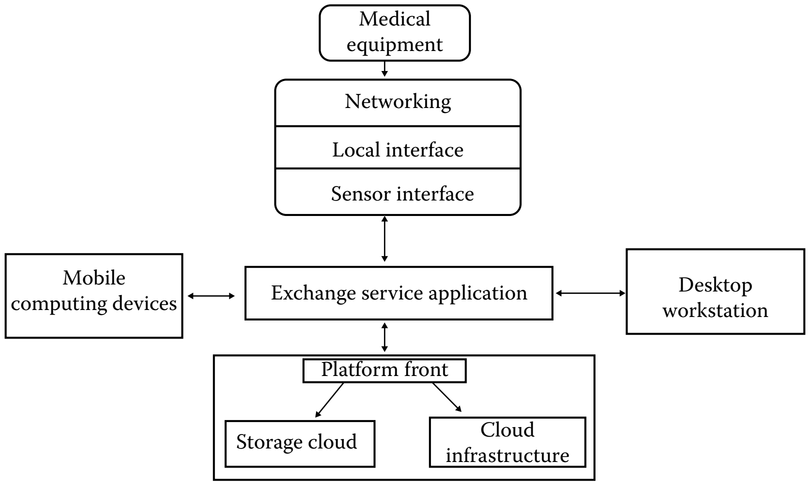


FIGURE 7.9
Steps of participatory sensing.

mobile, we can attach sensors to the patient's body or with various kind medical devices such as x-ray, ECG, or MRI. The sensor node will collect the data and send them immediately to the cloud through mobile devices. Then, doctor and other medical staff can access those data in no time from the Internet through their terminals without any latency. The benefits of the new approach over the existing approach are the system architecture and security issues. Examples are Microsoft's Health Vault and IBM's Smart Health. They provide a cloud solution to health monitoring on a very large scale throughout the world.
The traditional scenario of health care is as follows:

1. A nurse or other medical staff collects patient's data and writes the information down on paper.
2. Notes are submitted to a terminal for data entry.
3. The collected data are stored in a database server where they are organized, indexed, and able to be accessed through an interface.
4. Doctors and medical staff are able to access this information through an interface of any application.

The main drawback is the latency between data gathering (1) and information access (4). Real-time monitoring of a patient is not possible here. Besides, this scheme is inaccurate, as there is possibility of wrong input.

7.7.1 A Complete Architecture of Health Service Model

In Figure 7.10, a health service model is described. The main components of this model are the following:

1. *Sensor module*: Physical health sensors are used to measure the blood pressure, ECG, temperature, and other parameters. These data are extracted, transformed, and loaded from the sensor to the attached medical equipment. Software is loaded into the equipment to collect and process data locally. Then, the data are transmitted over the wireless network to "cloud services" [21].

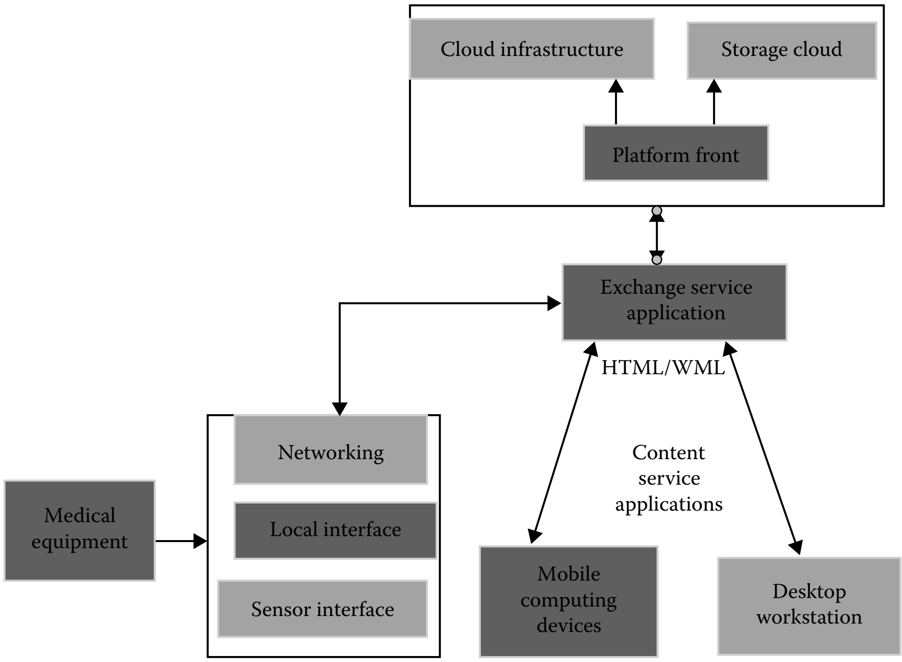


FIGURE 7.10
Detailed architecture of a healthcare system using sensor mobile cloud.

2. *Exchange service application*: This module organizes the patient's overall data related to the disease. It acts as a broker [22] between the local medical equipment and the remote cloud services. There are two main functions of this module:
   a. It is employed as an access point.
   b. It allows medical equipment to preprocess and store sensed data locally (e.g., the data is aggregated, filtered, and analyzed before the transmission to the cloud).
3. *Content service application*: These are the common interfaces used to provide information to doctors and other medical staff.
4. *Utility computing provider*: This module is responsible for providing physical infrastructure to store data, processing, and content delivery services.

Advantage of the scenario:

- This model facilitates continuous real-time data collection.
- Human interruption is eliminated and there is no possibility of erroneous data collection and data transmission to the database.
- Wireless sensors are easily deployed, as there is no fixed architecture of sensor network. Sensors attached to medical devices obviate the necessity of manual data gathering and data entry on the medical system.
- Computer resources available in the cloud are responsible for organizing, indexing, making the data accessible, and distributing the data to doctors and medical staff.

7.8 Challenges of Sensor Mobile Cloud Computing

1. *Wireless communication*: Though in wireless communication, the signals interact with personal digital assistants, the signal paths get blocked, and noise and echoes are introduced, causing more obstacles in wireless communication than in wired communication. As a result, wireless communication is characterized by lower bandwidths, higher error rates, and more frequent spurious disconnections. Hence for retransmissions, communication latency increases [1].
2. *Software development*: Designing software for a networked system for different applications in the mobile phone platform is a challenging process [22] without having the knowledge of the underlying hardware.
3. *Poor resources in mobile devices*: Mobile devices are resource-poor compared with static elements [2]. Computational resources such as disk capacity, processor speed, and memory size are limited due to fixed power consumption and weight limitations.
4. *Finite energy resources*: Battery life of every mobile device is fixed according to the hardware specification. Power consumption should be taken into consideration when developing hardware and software for mobile devices.
5. *Costing and charging issues of cloud computing*: Cloud consumers must be aware of the tradeoffs between integration, computation, and communication [3]. Migration of different applications to the cloud can significantly increase the cost of data communication. Since resources used for computation are likely to be high, the cost per unit of computing drastically increases. An elastic resource pool for intensive customization, performance, and security enhancement is necessary for simultaneous user access, and dealing with complexities increases charges to the customer.
6. *Security issues*: There is no doubt that putting data, running software on a remote machine's hard disk, and using its CPU appear daunting to many. Well-known security issues such as data loss, phishing, botnet [3] (running remotely on a collection of machines) pose serious threats to organization's data and software.
7. *Data availability*: Failure of Internet connectivity is a major risk to running an application in the cloud computing environment [23], especially in unnatural circumstances such as disasters. As applications are accessed by the mobile phones, they are dependent on Internet access for communication. In addition, if vulnerability is identified in a particular service provided by the cloud service provider, the application may have to stop all access to the cloud service provider until they could be secured, so that the vulnerability is resolved.
8. *Low bandwidth*: The main concern for mobile computing is the low bandwidth; wireless networks have much lower bandwidth than wired networks [20].
9. *Bandwidth variation is high*: Mobile devices have problems of greater variation in network bandwidth. Applications can assume high bandwidth and operate when plugged in or can assume low bandwidth or adjust with resources that are available.

10. *Various networks*: The problem with mobile devices in comparison with stationary devices is that the former change networks as they move beyond the range of the network in use. Also, some mobile devices use several networks at the same time.
11. *User interface is small*: It is difficult to open many windows simultaneously on its small screen.
12. *Low power*: The battery is the main reason for the weight of mobile devices. By reducing the size of battery, the need to recharge more frequently increases.

7.9 Conclusion

In this survey, the architecture of sensor mobile cloud was illustrated. The architecture facilitates the sensor data to be processed, categorized, and stored in such a way that it becomes easily accessible anytime, anywhere, and cost effective. Integrating sensors with MCC provides an open, extensible, scalable, interoperable, reconfigurable, and easy-to-use network of sensors for numerous applications. SMCC plays an important role in patient health monitoring by providing remote health data to analysts to handle emergency situations. In SMCC, if the mobile device is far away from the BTS, such as in urban area, the connection is not available properly. Transmitting sensor data from mobile to BTS consumes a lot of energy. So, power management is also a big issue in SMCC. Generally, a macro cell is used for data transmission between the mobile and cloud. The large distance between the mobile phone and the macro cell causes path loss. Femtocell can be used to reduce the path loss from the mobile to the BTS. Using SMCC, the situation of every person in a city can be traced, and gradually the city becomes a smart city.

Questions

1. What are the components of SMCC?
2. What is participatory sensing?
3. What is opportunistic sensing?
4. What are the basic differences between participatory sensing and urban sensing?
5. What is urban sensing?
6. What is a sensor cloud?
7. What is IoT? What are the components of IoT?
8. What are the applications areas of SMCC?
9. What are the open research problems in SMCC?
10. Draw the system architecture for a rescue service model.
11. What is service life cycle model of SMCC?

References

1. J. Yick, B. Mukherjee, and D. Ghosal, Wireless sensor network survey, *Computer Networks*, 52(12), 2292–2330, 2008.
2. W. S. Ansari, A. M. Alamri, M. M. Hassan, and M. Shoaib, A survey on sensor-cloud: Architecture, applications and approaches, *International Journal of Distributed Sensor Networks*, 2013, Article ID 917923, 1–18.
3. M. Yuriyama and T. Kushida, Sensor-cloud infrastructure—Physical sensor management with virtualized sensors on cloud computing, in *13th International Conference on Network-Based Information Systems*, Takayama, Japan, pp. 1–8, 2010.
4. B. P. Rimal, E. Choi, and I. Lumb, A taxonomy and survey of cloud computing systems, in *Fifth International Joint Conference*, Seoul, South Korea, pp. 44–51, 2009.
5. Y. J. Chen, C. Y. Lin, and L. C. Wang, Sensors-assisted rescue service architecture in mobile cloud computing, in *Wireless Communications and Networking Conference*, Shanghai, China, pp. 4457–4462, 2013.
6. S. K. Dash, S. Mohapatra, and P. K. Pattnaik, A survey on application of wireless sensor network using cloud computing, *International Journal of Computer Science and Engineering Technologies*, 1(4), 50–55, 2010.
7. K. Lee, Extending sensor networks into the cloud using Amazon web services, in *IEEE International Conference on Networked Embedded Systems for Enterprise Applications*, Suzhou, China, 2010.
8. R. A. Dhote and S. B. Belsare, The role of cloud computing in mobile, *International Journal of Computer Science and Applications*, 6(2), 262–266, 2013.
9. C. Perera, P. P. Jayaraman, A. Zaslavsky, P. Christen, and D. Georgakopoulos, MOSDEN: An internet of things middleware for resource constrained mobile devices, in *Proceedings of the 47th Hawaii International Conference on System Sciences (HICSS)*, Kona, Hawaii, January 2014.
10. 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*, 13(18), 1587–1611, 2011.
11. L. Atzori, A. Iera, and G. Morabito, The internet of things: A survey, *Computer Networks*, 54(15), 2787–2805, 2010.
12. N. Mitton, S. Papavassiliou, A. Puliafito, and K. S. Trivedi, Combining cloud and sensors in a smart city environment, *EURASIP Journal on Wireless Communications and Networking*, 2012(1), 1–10, 2012.
13. J. Soldatos, M. Serrano, and M. Hauswirth, Convergence of utility computing with the internet-of-things, in *Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, Palermo, Italy, IEEE, pp. 874–879, 2012.
14. A. T. Campbell, S. B. Eisenman, N. D. Lane, E. Miluzzo, and R. A. Peterson, People-centric urban sensing, in *Proceedings of the Second Annual International Workshop on Wireless Internet*, Kuala Lumpur, Malaysia, ACM, p. 18, 2006.
15. Q. Liang, X. Cheng, and D. Chen, Opportunistic sensing in wireless sensor networks: Theory and application, in *Global Telecommunications Conference*, *IEEE Transactions on Computers*, 63(8), 2002–2010, 2013.
16. H. Scholten and P. Bakker, *Opportunistic Sensing in Wireless Sensor Networks*, Toronto, Canada, 224–229, 2011.
17. R. Tavenard, O. Ambekar, E. J. Pauwels, and M. Waaijers, Opportunistic sensing and learning in sensor networks, in *International Workshop on Content-Based Multimedia Indexing*, Bordeaux, France, IEEE, pp. 46–52, 2007.
18. N. D. Lane, S. B. Eisenman, M. Musolesi, E. Miluzzo, and A. T. Campbell, Urban sensing systems: Opportunistic or participatory? in *Proceedings of the Ninth Workshop on Mobile Computing Systems and Applications*, New York, ACM, pp. 11–16, 2008.

19. S. S. Kanhere, Participatory sensing: Crowd sourcing data from mobile smartphones in urban spaces, in *12th IEEE International Conference on Mobile Data Management*, Lulea, Sweden, IEEE, vol. 2, pp. 3–6, 2011.
20. R. Szabo, K. Farkas, and B. Wiandt, Measurements of a real-time transit feed service architecture for mobile participatory sensing, in *Wireless Days, IFIP*, Valencia, Spain, IEEE, pp. 1–4, 2013.
21. C. O. Rolim, F. L. Koch, C. B. Westphall, J. Werner, A. Fracalossi, and G. S. Salvador, A cloud computing solution for patient's data collection in health-care institutions, in *Second International Conference on eHealth, Telemedicine, and Social Medicine*, St. Maarten, The Netherlands, pp. 95–99, 2010.
22. M. M. Hassan, B. Song, and E. Huh, A framework of sensor-cloud integration opportunities and challenges, in *Proceedings of the Third International Conference on Ubiquitous Information Management and Communication*, Danang, Vietnam, pp. 618–626, 2009.
23. W. Kurschl and W. Beer, Combining cloud computing and wireless sensor networks, in *Proceedings of the 11th International Conference on Information Integration and Web-Based Applications and Services*, New York, ACM, pp. 512–518, 2009.