Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2021 SCPE. Volume 22, Issues 4, pp. 445–462, DOI 10.12694/scpe.v22i4.1878

ENABLING INTERNET OF THINGS THROUGH SENSOR CLOUD: A REVIEW

JYOTSNA VERMA [*]

Abstract. With the inception of the Internet of Things (IoT), wireless technology found a new outlook where the physical objects can interact with each other and can sense the environment. The IoT has found its way in the real world and has connected billions of devices throughout the world. However, its limitations, such as limited processing capability, storage capability, security and privacy issues, and energy constraints prevent the IoT system to be properly utilized by the real-world applications. Hence, the integration of IoT with various emerging technologies like big data, software defined networks, machine learning, fog computing, sensor cloud, etc., will make the IoT system a more powerful technology. The sensor cloud provides an open, secure, flexible, large storage and a computational capable infrastructure which makes the ensemble architecture of IoT and sensor cloud more efficient. An extensive review of the IoT system enabled sensor cloud is presented in the paper, and with this context, the paper attempts to summarize the sensor cloud infrastructure along with its challenges. In addition, the paper presents the possible integrated architecture of the IoT and the sensor cloud which enables the network to be properly utilized. Further, the importance of integrating these two promising technologies and research challenges associated with it is also identified. Finally, the paper analyses and discusses the motivation behind the ensemble system along with future research direction.

Key words: Sensor cloud architecture, Internet of Things, Cloud computing, WSN.

AMS subject classifications. 68M14

1. Introduction.

The world apparently has been focused on connectivity and convergence since the late 1980s; way back in the twentieth century, machines had no senses; they only had brains capable of understanding what we asked them to do. But this is not the case with the ”Internet of Things,” yet machines and other physical things must sense for themselves [1]. With the proliferation of the IoT we have reached an era where we envision the objects or physical things around us connected to the internet allowing them to send, receive, and exchange data. The advent of the term “Internet of Things” was coined by Kevin Atshon in 1999 and is considered as the world’s third wave of the information industry after the invention of computers and the internet [2]. According to IETF [3] definition “The Internet of Things is the network of physical objects or ”things” embedded with electronics, software, sensors, and connectivity to enable objects to exchange data with the manufacturer, operator, and/or other connected devices”. The physical objects in the Internet of Things embedded with sophisticated sensors for sensing the environment of the real-world scenarios, self-configuring nodes (things), actuators to communicate with other smart devices or nodes, and RFID (Radio Frequency Identification) chips for unique digital identification of the things with which they are connected and are integrated into the network. Each physical object is automatically identified by their unique digital identities which makes them share and exchange data with each other.

By the rapid and increasing growth of IoT, it has marked its place and has made ground in the world of wireless networking. IoT systems are supposed to provide connectivity and intelligence to billions of physical objects and are being widely deployed in different application domains like smart home applications, health care sectors, smart cities, agriculture, industrial automation, wearable, etc. Probably, in the coming years say by 2025 the cumulative installed base of linked Internet of Things (IoT) devices is expected to be 75.44 billion worldwide, a five-fold increase in ten years [4]. The IoT, allowed by the omnipresent internet technology, is the next important step in fulfilling the promise of the internet to make the world connected and hence opens the door for emerging technologies like Big Data, real-time analytics, Software Defined Networks (SDN), machine learning, sensor cloud and many more to come up and integrate with the IoT to maximize its potentials. IoT generally deals with various concerns like limited storage capacity, limited processing capabilities and energy

[*] Department of Computer Science, The ICFAI University, Jaipur, Rajasthan, India. (jyotsna.verma@iujaipur.edu.in).

constraints etc., which ultimately affects the security, reliability, efficiency, and privacy of the physical objects. By integrating with these emerging technologies, the IoT can reach a next level milestone in the near future.

Cloud computing, which is another network paradigm characterized to have virtualized storage, computation, and network resources which makes the cloud infrastructure simple, cheap, scalable, and manageable than physical devices. According to the definition provided by the NIST [5] "Cloud computing is a technological and operational model for ubiquitous, on-demand network access to a shared pool of configurable infrastructure, processing, storage and application services that can be provisioned and released for use with minimal system management effort or service provider interaction". The cloud computing provides three types of services: Software as a service (SaaS) which is the top layer of the cloud infrastructure and it offers applications like Google App Engine, HEROKU, IBM Bluemix, and Microsoft Azure running on the cloud environment, Platform as a service (PaaS) is the middle layer and offers platform layer resources, and the lowest layer of the cloud infrastructure is Infrastructure as a service (IaaS) which offers the computing, storage, and network resources. The economic and technical benefits of cloud computing like virtually unlimited storage, low cost computing capabilities, provision of providing leased virtualized resources on an on-demand basis have gained popularity and attention from the research community and the paradigm has been widely adopted by large companies like Google, IBM, Amazon, Oracle, Microsoft, Facebook etc. The convergence of IoT and cloud computing, the two relatively thriving networking paradigm helps in efficiently collecting and analyzing real-time data [6-9].

The integration of Cloud Computing and IoT solves various issues of IoT constrained devices such as data analysis, computation, data access, storage and is called as Cloud of Things [10] or as CloudIoT [11]. The CloudIoT offers various services such as Things as a service, SenaaS (Sensor as a Service) [12]. Merely integrating IoT with the cloud is not enough to solve the technical limitations of the IoT rather IoT should be integrated with various other technologies like big data, software defined networks, fog computing, sensor cloud, etc., to provide efficient real-world applications. IoT is highly dependent upon sensor based data acquisition and processing of the data. Hence, enabling IoT through cloud sensors helps in the efficient data acquisition, storage, and processing of data in real time. Cloud sensor or sensor cloud is another networking paradigm that gathers all the data or information from the physical sensors deployed in a particular application domain and transfers them to the cloud infrastructure. The ensembling of IoT with sensor cloud opens up new horizons for the data aggregation, data storage, real-time processing of data, and scalability of nodes.

1.1. Contributions. The contributions of this paper are as listed below:

1. Presents a comprehensive literature review of IoT and sensor cloud with their applications, challenges, and architectures.
2. Presents the possible ensemble architecture of the IoT and the sensor cloud.
3. Analysed and discussed the integration of IoT with the sensor cloud and presents the significance and research challenges of two integrated networking paradigms.
4. Finally, the effect of mobility models on network performance with respect to the mobility under Dynamic Source Routing (DSR) protocol is evaluated.
5. Presents the future research directions for the integrated system of IoT and sensor cloud.

1.2. Organization of the paper. The paper primarily focuses on the review of the integration of IoT with sensor cloud and research challenges associated with it. The rest of the paper is organized as follows: Section 2 discusses the sensor network and the cloud. Section 3 presents the architecture of the sensor cloud and Section 4 discusses the sensor virtualization. Section 5 summarizes the challenges and constraints associated with the sensor cloud infrastructure. Section 6 presents the integration of IoT with sensor cloud and Section 7 presents the possible ensemble architecture of the IoT and the sensor cloud. The research challenges associated with the integration of IoT and sensor cloud is presented in Section 8. Section 9 analyses and discusses the integrated architecture of IoT and sensor cloud. Further, future research directions for the integrated system are identified and are presented in Section 10. Finally, Section 11 concludes the paper.

2. Sensor network and the cloud. With the advancements in wireless networking, smart sensing becomes a reality. Sensor network is an infrastructure-less, distributed network of a set of large number of sensor nodes that are deployed in a particular domain. Sensor nodes are light weighted, low power multifunctional tiny devices that have the capability of data computation, communication over the network and sensing the physical parameters. It senses the physical parameters (temperature, humidity, speed etc.) and converts them to electrical or optical signals. This signal helped the sensor network to measure the physical parameters electrically to monitor and control sensors which eventually provides various services like weather forecasting, environment monitoring, healthcare services, agricultural services, military services, government services etc., by using various types of sensors like thermal sensor, body sensor, a seismic sensor, visual sensor and environmental sensors etc. The mobility of a sensor node in the sensor network is not a mandatory requirement and the network is much more scalable and fault tolerant than the ad hoc wireless network.

The activity of sensing a particular application domain in a sensor network can be periodic or sporadic [13]. A periodic sensing senses the application scenario periodically; for instance, environmental factors such as humidity, temperature, pollution, and nuclear radiation etc., can be measured periodically whereas sporadic sensing, senses the particular application domain sporadically, such as border intrusion detection, threshold detection of a furnace, pressure, motion, stress measurement of a building or machinery etc. [13]. The sensor network has two important functions: data dissemination and data aggregation. Data dissemination disseminates or propagate the data throughout the sensor network i.e., the collected information from the sensor nodes is communicated to the base station and the nodes which are interested in seeking that data or information, whereas the data aggregation function aggregates or gathers the sensed data from each sensor node to a sink node. The node from which the data or information is gathered is called as source node and the node that seeks data or information is called as sink node. The endless applications of the sensor network make the sensing reality and are a key component of the Internet of Things. They can coordinate with RFID system for monitoring the status of the physical objects or things, to get the information about the position, temperature, movement of the objects etc. However, there are various limitations pertaining to the wireless sensor network like security, privacy, limited energy and power constraints, mobility, short communication range, processing capabilities, storage capacity, bandwidth availability etc., that is needed to be addressed [14].

The research communities are trying to deal several limitations of sensor networks like energy efficiency, reliability, scalability, robustness etc., at different layers [15]. Moreover the research is more focused on the physical sensor localization [16, 17], sensor node programming [18-20], power consumption [21], sensor data processing [22] and the management and deployment of physical sensors; as the sensor resides in its local domain and it is hard to access them from external servers. The users of the sensor network should also need to know about the status of the sensor nodes, whether the node is faulty or the node disconnects the network, so that the alternative functioning nodes should be used for the proper functioning of the network [23]. These limitations along with the heterogeneity of the sensor nodes create complexity for the engineers. For establishing the communication between the network they have to examine the interface of the sensors and study their protocols; this eventually leads to the integration of sensor networks and the cloud as cloud sensors.

According to the IntelliSys Sensor Cloud is an “infrastructure that allows truly pervasive computation using sensors as an interface between physical and cyber worlds, the data-compute clusters, as the cyber backbone and the internet as the communication medium” [24, 25]. The sensor network and the cloud infrastructure are linked with their respective gateways i.e., sensor gateway and cloud gateway. The sensor gateway collects all the data from the sensor nodes in a compressed form and transfers the collected data to the cloud gateway. The cloud gateway then decompresses the data and stores the data into cloud storage which has sufficiently large storage. The integration of cloud and sensor network solves the problem of data processing and storage capacity of wireless sensor network as cloud infrastructure has huge data storage capacity and data processing capabilities. The cloud sensor also frees the engineer to bother about the heterogeneity of the sensors and offers them to fully focus on the applications and services provided to the users. Traditional sensor network deployed the sensors into the application domain and be able to provide the data for one purpose only and hence, does lots of wastage of resources; as the collected data from the sensor network can be used for a variety of applications. For example, if we consider the application where the sensors deployed for the traffic monitoring has data about the traffic flow in the specific area. Now, this collected data from the sensor can be used for the purpose of satellite navigation, possible route suggestions for the travellers to avoid the congested traffic area etc. The same sensor network can thus be utilized for various applications and be able to provide various services through cloud sensors. This is just one instance where we saw how sensor cloud help to reduce the resource wastages, there are a variety of other applications also where sensor cloud proves their applicability in an efficient manner. Some applications like environmental monitoring [26], health monitoring [27], telematics [25], transportation and vehicular applications [28] can be benefited with such infrastructure.

3. Architecture of Sensor cloud. The infrastructure of sensor cloud has been evolved in recent years. Sensor cloud allows user to easily collect, process, archive, access, share and visualize the sensor data collected from various application domains by using the computational and storage resources of the cloud computing [29]. The infrastructure of cloud computing has been extended, to support and manage the sensors deployed in various application domains. It basically integrates several networks with sensing applications and cloud infrastructure to provide cross disciplinary application support which can scale up to multiple organizations [25]. The framework of cloud computing services does not support the implementation details of the services provided to the user. They make use of services provided to them when they make a request for the corresponding services. The user cannot make use physical sensors when needed as the physical sensors are bound to provide services pertaining to specific applications. Hence there is a need and the requirement to manage these sensors so that the resources are properly and efficiently utilized by the users. Literature showcases the studies on physical sensors focused only on power management [30], localization [31], data processing [32], routing [33], and clock synchronization [34].

There is a significant need of providing schemes for managing the sensors to make use of sensor resources in an efficient manner. There are no generalized application scenarios which uses all types of physical sensors all the time. In [35] a mechanism is proposed to appropriately choose the physical sensors for the specific application scenario. However, sensor services can support a variety of applications if it moved to the cloud [36, 37]. The cloud sensor architecture must satisfy two major requirements: (1) The network should be scalable and energy efficient and (2) It should be able to provide open ended application development system [38].

Broadly, three layered architecture can be visualized for the sensor cloud [14]. The physical sensors are present at the lowest layer of the architecture of sensor cloud. The multiple sensors which are deployed in the application scenarios collect and upload the data to the sensor cloud which is present in the second layer of the sensor cloud architecture in a standardized format. The data uploaded in a standardized format allow users to use the services of the sensor cloud without having concern over protocols and formatting of the uploaded data. The sensor cloud is present at the second layer of the architecture which procreates the virtual sensors defined by the sensor owners based upon the service templates. Finally, at the top layer application developers use these virtual sensors into their respective applications. The three layer architecture is shown in the figure 3.1. The transmission of sensed data to the sensor cloud is done through physical entities or logical entities. The logical entities use the concept of virtualization, which is nothing but the logical abstraction of the physical entities for efficient utilization of resources. For the logical abstraction or to cover the virtualization aspect, a channel is required for the communication between the physical resources and virtual resources.

The two key components of sensor cloud infrastructure are: (1) Resource host (2) Sensor cloud platform.

1. **Resource Host:** Resource host covers the lowest layer of the sensor cloud infrastructure which consists of [39]:
   (a) **Physical sensors:**Physical sensors are the devices that are distributed to the various application domains and have the capability of sensing the data from the deployed region. On the basis of their sensor readings and the actual distance from the events, the physical sensors are ranked [39]. The authors proposed a FIND technique [39] to find the faulty node in the system by finding the mismatch between the actual distance rank and sensor rank; if there is a mismatch, the node is faulty. Each physical sensor deployed in application scenarios has a unique resource id and shares a common power unit hosted by the sensor coordinators. The physical sensors are XML encoded so that the services provided by these sensors can be utilized on heterogeneous platforms without having the concern over the conversion of these services on various platforms [36].
   (b) **Sensor Coordinators:** The physical sensors do not have the capability to transmit the data; rather it only senses the environment where it is deployed. It is the responsibility of the sensor coordinators to transmit the sensed data to the sensor cloud. Based on the transmission capabilities the sensor coordinators which have unique resource id, can be locally or globally identified. The locally identifiable coordinators transmit the sensed data from the physical sensors to the sensor cloud through a sensor gateway, whereas the globally identifiable coordinators transmit the sensed

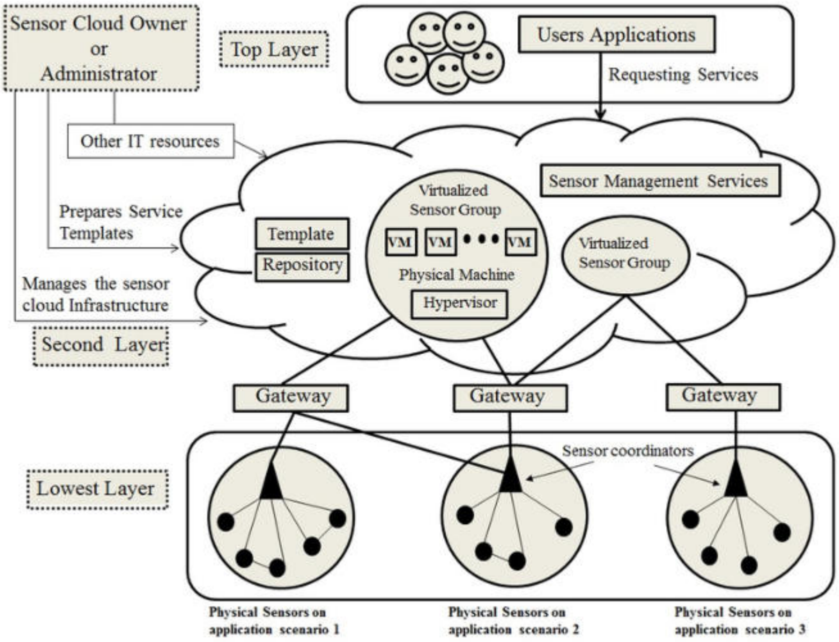
Sensor Cloud Owner or Administrator
Top Layer
Users Applications
Requesting Services
Other IT resources
Sensor Management Services
Prepares Service Templates
Template
Repository
Virtualized Sensor Group
VM
VM
VM
Physical Machine
Hypervisor
Virtualized Sensor Group
Manages the sensor cloud Infrastructure
Second Layer
Gateway
Gateway
Gateway
Sensor coordinators
Lowest Layer
Physical Sensors on application scenario 1
Physical Sensors on application scenario 2
Physical Sensors on application scenario 3

Fig. 3.1: Sensor Cloud Architecture.

data directly to the sensor cloud platform. There are three different topologies a physical sensor can attach to the sensor coordinators [39]:

i. **Fixed:** In this topology, the sensor coordinator is attached to a fixed set of sensors and they cannot be plugged in/out in any way.

ii. **Mobile:** In this topology, sensor coordinators are attached with a variable set of physical sensors that can be plugged in/out in any case. This type of topology supports the mobility of both physical sensor and sensor coordinator as the connection of the physical sensor with the sensor coordinator can either be wired or wireless.

iii. **Variable:** In this type of topology, the sensor coordinator has always been fixed and is attached with a fixed set of physical sensors in a timely slotted manner.

(c) **Sensor Gateway:** The sensed and aggregated data are sent from physical sensors to the cloud platform through sensor gateways. The locally identifiable coordinators sent the data to the cloud platform through the sensor gateway which acts as an interface between the sensor cloud platform and locally identifiable coordinators. The sensor coordinators and various intermediate devices between the coordinator and sensor gateway act intelligently to route the data packets to the sensor gateway. The sensor gateways then take these data traffic and send it to the cloud platform for further processing.

2. **Sensor Cloud Platform:** The sensor cloud platform is the second layer of the sensor cloud architecture which consists of following major components:

(a) **Templates:** The sensor cloud infrastructure procreates the virtual sensors and provides it to the user applications when required in such a way that the end user has the illusion that the service instances are the part of resources, such as disk storage, CPU, memory, etc. [41]. The service instance creation is done by using the appropriate templates defined by the cloud owners; the end users also make requests of these service instances via the interface by selecting appropriate service templates.

(b) **Sensor management services:** This manages the services provided by the cloud owner. The service provider manages the sensor cloud templates and can modify the services of the template as per the requirement of the user application and services [37]. The delivery time of the services to the end users is improved by the automation of services which is an important factor in providing the cloud computing services to the user applications [42]. As human intervention in providing the services has an adverse effect on the system; hence, automation of services proves to improve the flexibility and efficiency of the system [14].

(c) **Virtual sensor:** The virtual sensor abstracts the physical sensor and the concept of virtualization, which will be discussed in subsequent sections of this paper in detail, virtualizes the physical sensors and frees the user from the concern of knowing the status of the connected physical sensors with the sensor cloud infrastructure; it only concerns the status of the virtual sensor. However, the user of the sensor cloud infrastructure should also concern the status of the physical sensors along with the status of the virtual sensor for getting accurate results [14].

The sensor cloud infrastructure is a three layered architecture in which sensor owners are free to register or unregister their physical sensors, and can join the sensor cloud infrastructure. After the registration of the physical sensors, the corresponding IT resources will become operational and templates for the virtual sensors and virtualized sensor groups are created. The service templates are created as a catalogue menu service and the users can create new services for the existing sensors service instances [14]. Once the templates for the service instances are created, the virtual sensors can share the sensor data and user application can request virtual sensors for their use by appropriately selecting the service templates. Further, the service templates are discarded once they become useless to reduce the utilization charges for the corresponding resources [37].

4. Sensor virtualization. The most pertinent technology for cloud computing is virtualization; which hides the heterogeneous platforms, infrastructure, and data from the user applications without giving the details about the underlying hardware implementation for seamless operation. The key idea behind virtualization is resource sharing and collaboration. The virtualization basically partitions the physical server into multiple logical servers which in turn behaves like an independent physical server that are able to run the operating system and applications. The virtual server encapsulates the virtualization software called a hypervisor, which runs multiple server instances or virtual machines on a single host by the encapsulating guest version of the operating system. It emulates the physical hardware resources and increases the utilization of resources by reducing the need of physical hardware systems. There are two types of hypervisors that virtualization software uses, to manage multiple virtual machines on a single host machine:

Type 1 or bare-metal hypervisors: The type 1 hypervisors are installed directly on to the server to control the physical hardware and hence, provide higher efficiency, stability and are ideal for larger operations. The following are the Type 1 hypervisors; Nutanix AHV, AntsleOs, Xen, XCP-ng, Oracle VM Server for SPARC, Microsoft Hyper-V, Oracle VM Server for x86, , Xbox One system software, and VMware ESXi.

Type 2 or hosted hypervisors: The type 2 hypervisors are not installed directly onto the server; instead, it is installed on top of the server's operating system. It is easier to install and are ideal for small operations. Following are the examples of type-2 hypervisors: Microsoft virtual PC, VMware Workstation, VMware Player, VirtualBox, Oracle Solaris Zones.

Many companies like VMWare, Microsoft, IBM, Citrix, RedHat, and Oracle, etc., provide virtualization services for storage and computations to the user requesting for services. The virtual server indeed proved to be cost-effective and less time consuming when compared to traditional methods for storing and computing the data. Hence, the benefits of hypervisors made the sensor cloud environment to incorporate the virtual sensors.

The virtual sensor is software that abstracts the physical sensors deployed in the application domain. The physical sensors convert the collected data, from electromagnetic signals into digital form in a standardized format and send it to the virtual sensors.The need of a virtual sensor is not to replace the physical sensor; instead it facilitates, adds further functionalities and can create the additional module if required for the physical sensors at the software-computing level for efficient resource utilization [39]. The virtual sensor can be placed and accessed from anywhere which improves the coverage parameter of physical sensors and hence enhance the performance of physical sensors with limited resources [39]. The group of virtual sensors has unique identities that are mapped to an IP. APIs at the IaaS level are used for virtual sensor allocation and enable the user application to establish the connection, uploading data to the cloud, register and deregister with the virtual sensor, etc. After the allocation of virtual sensors to a particular virtual machine, it can communicate with the physical sensors present at the lowest layer of the sensor cloud architecture. The virtualization technique helps to manage the physical sensor management services through the hypervisor. The physical sensors have the ability to sense, process the data, store, and communicate with the system. These abilities of the physical sensors are the four modules of the system which are distributed at various levels (physical sensor level, sensor gateway, or cloud) of the sensor cloud architecture [39]. The virtual sensor interacts with the system which consists of four modules of the physical sensor interacting with each other. The sensor module is placed at the sensor coordinator or sensor gateway which is the lowest level of the sensor cloud architecture. The sensor module is closest to the physical devices where data is being aggregated [39]. The processing module processes the data aggregated from the physical devices and can be further subdivided to handle various other individual tasks. It is basically placed at the cloud platform and works at the IaaS or PaaS level [39]. Another important module of the system attached to the virtual sensor, is a storage module that stores the aggregated and processed data.

The main limitation with the sensor device is storage as it has memory constraints. Hence, the storage module of the system solves the issue by mapping the sensor memory to cloud storage. A virtual sensor can also represent temporal data [39]. The communication module of the system helps in the transmission and reception of the data. The source port of the virtual sensor aggregates the data from the physical device coordinator through sensor gateway and destination port of the virtual sensor transmit this data to the cloud or forward it to the other virtual sensor for further processing or transmit to the user applications if required [39]. An error-free data must be provided by the virtual sensor; for that, the virtualization aspect of the sensor should monitor the system. The APIs of virtual sensor management services, monitor network connectivity and bandwidth availability, control the events, report data redundancy etc., for efficient and error-free data availability [39].

5. Challenges and Constraints. There are various challenges and constraints associated with the sensor cloud infrastructure which make sensor cloud to be limited in certain scenario of applications; removal of such challenges and constraints will make the sensor cloud infrastructure into a different level, which allows the user to be more flexible regardless of the security and other concerns. Following are the challenges that need to be considered before wide acceptability of sensor cloud infrastructure [14]:

1. **Design issues:** The continuous transfer of data must be guaranteed between the sensor devices and the server for reliable and fault-tolerant communication. The designer needs to focus on these issues to avoid accumulation errors which can be occurred in applications like medical health care monitoring, hospitals, etc. Such types of applications require continuous transfer of data as the patient or the person concerned moves frequently, in and out from the coverage area of the smart device gateways [43, 44].
2. **Storage issues:** Storage of data is done at the server side and there is lots of data processing that creates bursty data processing and needs to be avoided because of the simultaneous connection of multiple clients with the system. To deal with the problem, a predictive storage concept has been introduced [45] in which data at some remote sensors of the sensor cloud infrastructure are archived and predictive caching is used at the proxies of the systems.
3. **Authorization issues:** Privacy issues can be dealt with by giving authorization to different entities that communicate with the system and authenticate the entities via a web interface.
4. **Power issues:** Power issue is a critical issue that should be dealt with when the mobile phone gateway is connected with the sensor cloud infrastructure [46]. The continuous transfer of data and data processing drains out the battery of mobile phones.
5. **Event management:** The data come from heterogeneous sensors and the sensor cloud infrastructure needs to deal with different data abstraction models from different vendors. The infrastructure should develop the APIs, standard format and design new database mechanisms to deal with the event query coming from the users, for the large real-time data.
6. **Service level agreement violation:** The infrastructure should be able to provide quality services

to the users and if it fails to do so the cloud provider violates the service level agreement. Opting the best possible cloud provider in terms of cost, QoS, time is the biggest challenge [47].

7. **Efficient information dissemination:** Efficient dissemination of information is a critical challenge as the data sets and their respective access services are geographically distributed and it is difficult to provide the data and services to the appropriate user applications.
8. **Security and privacy issues:** Security and privacy is an important concern for any network. With a sensor cloud platform the data comes from a diverse range of physical devices and it is the responsibility of the infrastructure to secure the sensitive data and create better privacy policies to maintain privacy [47, 48].
9. **Real time multimedia content processing issue:** The availability of real time multimedia data from the large data sources in the cloud and to classify real time multimedia and contents to provide appropriate services to users at their location is another challenge for the sensor cloud infrastructure [24].
10. **Energy efficiency issue:** The constant transmission of data from the sensor devices to the cloud consumes lots of energy as the sensor nodes have power constraints and also they have less storage and processing capabilities. Therefore, there is an ultimate need for the transmission of the sensed data to the cloud for further processing and hence the nodes consume power in sensing and transmission. So, one solution to this problem is to add a smart gateway to the middleware [49] that can do some pre-processing and compression of data and can reduce the transmission load. The reduction in transmission load and compression of data can ultimately reduce energy consumption and can improve memory usage.
11. **Bandwidth limitation and network access management:** The number of connected devices in a sensor network and the cloud users is large. So, to manage these devices in terms of bandwidth utilization is a big challenge for the sensor cloud infrastructure [50]. The efficient access management of the number of the connected network in the sensor cloud infrastructure helps in bandwidth utilization [51].

6. Integration of IoT with sensor cloud. The Internet of Things (IoT) and sensor cloud are two broad and distinct technologies. The integration of sensor cloud and IoT has opened the door for future internet and benefits the real world problems. The seamless integration of sensor cloud and the Internet of things make the sensor cloud platform reachable and also solve the storage and computing limitation of IoT. The applications of both technologies are becoming viable, low cost, approachable, and robust and are extremely pervasive. There are two components involved in the integration of sensor cloud and IoT: (1) Sensor cloud infrastructure and (2) IoT system. The sensor cloud infrastructure provides the platform for the IoT system and mitigates its storage and computational limitations whereas the IoT system provides the interoperable and lightweight procedures for exchanging the data and information with the sensor cloud infrastructure. The architecture of IoT is still under construction enabling the future technologies, but is mainly divided into three layers: (1) Perpetual layer (2) Network layer (3) Application layer. Further, in some literature [52] [53] researchers have added two more layers: (1) Middleware layer and (2) Business layer. The five layer architecture is described in Fig. 6.1.

The lowest layer of the IoT architecture is the perception layer consisting of data sensors, RFID tags, actuators, GPS, Bluetooth, camera, barcode labels, etc. The perception layer is the physical layer that identifies the unique things and perceives the data from the environment. The layer deals with the gathered and sensed data from the environment and sends it to the network layer. The network layer of the IoT architecture consists of one or more gateway with interfaces through which the gathered and sensed data are sent to the internet. The layer is responsible for connecting to the other network devices, servers, smart things, and performs the network management of the architecture. The next layer of the IoT architecture is the middleware layer also called as processing layer; it receives the information from the network layer. The middleware layer is responsible for storing, analysing, and processing the huge amount of information and takes decisions on the processed information. It provides and manages various services to underlying layers by employing various technologies like databases, big data processing modules, cloud computing etc. [54]. The processed information is then sent to the application layer which provides various applications and services to the users. The information received from the application layer is then utilized for creating various services for the business. The business layer deals with processing or moulding the information for providing various services to users.

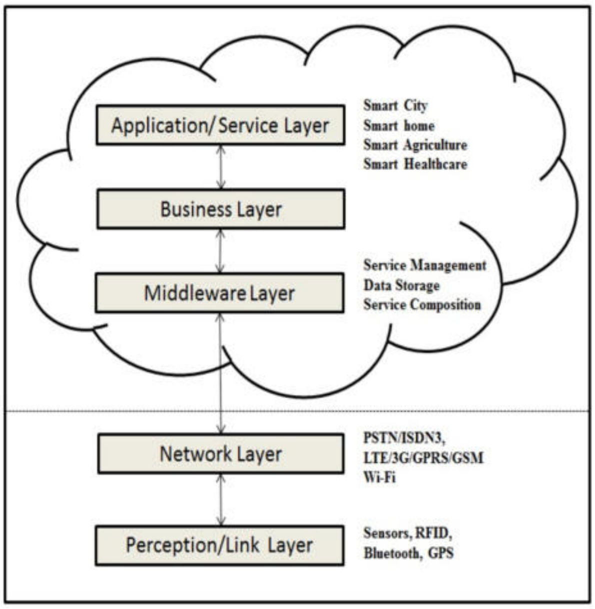

Fig. 6.1: Layers of Internet of Things.

6.1. Significance of integrating IoT with sensor cloud. The ensembling of IoT and sensor cloud can be seen as the potential solution to the limitations of the IoT. The sensor cloud provides an open, flexible, scalable and reconfigurable environment for various monitoring and controlling applications which makes it easier to enable with IoT. Following are the significance of integrating the IoT with sensor cloud:

1. **Physical sensors:** The physical sensors which are used to sense the environment has difficulty in tracking the objects. Hence, the integration of unique identifiers with the physical sensors provides a reasonable addition to the network and the objects of the network become trackable with the sensing capabilities [55]. Moreover, this integrated architecture will be able to support heterogeneous platforms as the physical sensors are XML encoded to support several services on various platforms [36].
2. **Mobility:** The sensor nodes in sensor networks are usually stationary whereas in IoT the nodes are mobile with unique identities which help to identify the nodes. By integrating the two networks, the integrated system can be able to support applications which require mobility.
3. **Communications:** The physical sensors in the sensor network provide multi-hop communication and the unique identifiers like barcodes, serial numbers, RFID helps to identify and track the objects in the integrated system [56] which will offer an effective solution to track, connect and manage the things from anywhere and anytime.
4. **Cost:** By replacing some of the physical sensors of the sensor network with small and cheap RFID tags, the integrated system becomes more economical [55].
5. **Storage:** The IoT has a large amount of structured and unstructured data from various information sources [57], but has limited storage capability; hence integrating IoT with sensor cloud improves the storage capability of the integrated system.
6. **Computation:** The IoT nodes deal with limited data processing and energy resources and need another more powerful node for data processing and aggregation of data. The sensor cloud solves this issue by offering unlimited processing capabilities. Hence, the integrated system offers large processing capabilities and saves time and energy.
7. **Security and Privacy:** The sensor network provides multi-hop communication. In multi-hop communication the sensed data are sent to the sensor cloud platform through the sensor coordinator. The

attached physical devices with the sensor coordinator are seen as a black box to the outer layer and provide more security and privacy to the IoT network [10].

8. **Scalability:** The integrated architecture of IoT with sensor networks allows the IoT system to be more scalable, as only cloud is not enough to support various physical devices; the cloud requires various data centres which are comparatively costly.
9. **Visualization:** The visualization API of sensor cloud infrastructure helps the users to predict future trends through visualization tools with the stored sensed data from various physical devices [48].
10. **Resource Optimization:** As the sensor-cloud provides resource optimization which enables the system to share the resources for various applications [48]; integrating sensor-cloud with IoT makes the integrated system utilize the shared resources which reduce the resource cost of the system and provide wider range of applications and services.

7. Possible ensemble architecture of the IoT and sensor cloud. The ensembling of IoT and sensor cloud is guaranteed to serve a variety of real-world applications as they make use of their respective advantages to provide better services to the users. In essence, the ensemble architecture of IoT and sensor cloud contains numerous elements, such as IoT sensors and actuators, sensor coordinators, protocols, gateways, sensor cloud, and data center. The ensemble architecture of IoT and sensor cloud as shown in Fig. 7.1 which consists of two main components: (1) Unique identifiers, IoT sensor, and actuators and (2) Sensor cloud platform.

The IoT devices are present in the lowest layer of the architecture which consists of unique identifiers to identify the physical objects and sensors to sense the physical environment. The identifier is a pattern of characters and numbers that is used to identify physical or virtual entities within a single context. In IoT standards, identifiers are divided into distinct categories [58]: (1) object identifiers (Object Ids) (2) communication identifiers (Communication IDs) and (3) application identifiers (Application IDs). The object identifiers are used to identify physical or virtual objects [58], like barcodes, RFIDs, Uniform Resource Locator (URL) and Uniform Resource Identifiers (URI), MAC, serial numbers, etc. The communication identifiers are used when the devices or nodes in the network needed to be uniquely identified [58]. IPV4, IPV6, and (Domain Name System) DNS etc., comes under communication IDs. The application IDs are used to identify the services provided by the application layer like URL and URI are application layer identifiers [58]. Besides these, there are several universal identification schemes, such as Electronic Product Code (EPC), International Mobile Equipment Identity (IMEI), Universal Unique Identifier (UUID), Universal Product Code (UPC), OID (Object identifier), etc [59, 60]. After unique identification of the physical entities, the IoT sensors and actuators are used to sense the physical environment. The IoT sensor changes the physical parameter into electrical signals and reliable, accurate sensors are utilized in various applications in miniaturized packages, health care, packages for harsh environments, multi sensor modules and led the foundation for engineers to apprehend the diverse properties of applications. As against IoT sensors, actuators are used to control or alter the physical changes; they convert the electrical signals into physical output, like heat or motion. For example, actuators can be utilized in laser, LED, loudspeaker, solenoid, motor controllers, etc. The sensed information from the sensors and actuators are then sent to the sensor coordinators which is locally or globally identified in the network; for the transmission of the data to the sensor cloud through sensor gateways or directly to the sensor if sensor coordinators are globally identified, for further processing as discussed in Section 3.

The sensor gateways are smart physical device or software program that acts as a bridge between the sensor cloud and sensor coordinators, intelligent devices, etc., and are provided with little extra computational functionality; so that they can decide when to upload the data to the sensor cloud depending upon the application scenarios. The physical devices generate the sensed data when they are connected to the network, but at some point in time, the sensed data is no longer required. The uploading of sense data to the sensor cloud and synchronization of devices becomes unnecessary depending upon the application scenarios; and needs to be stopped for a while for preserving the energy, sensor cloud, and network resources [61]. Apart from uploading the necessary data to the cloud infrastructure, the smart gateways also perform various other tasks, like pre-processing of sensed data from the IoT enabled devices, filtering and restructuring the data into a useful form, keep checks on the physical device and energy constraints of the devices, provide security and privacy to the IoT network and physical devices, etc [10]. The multiple IoT devices connected to a network can directly send their data to the smart gateway which is possible in single hop communication or they can send the data

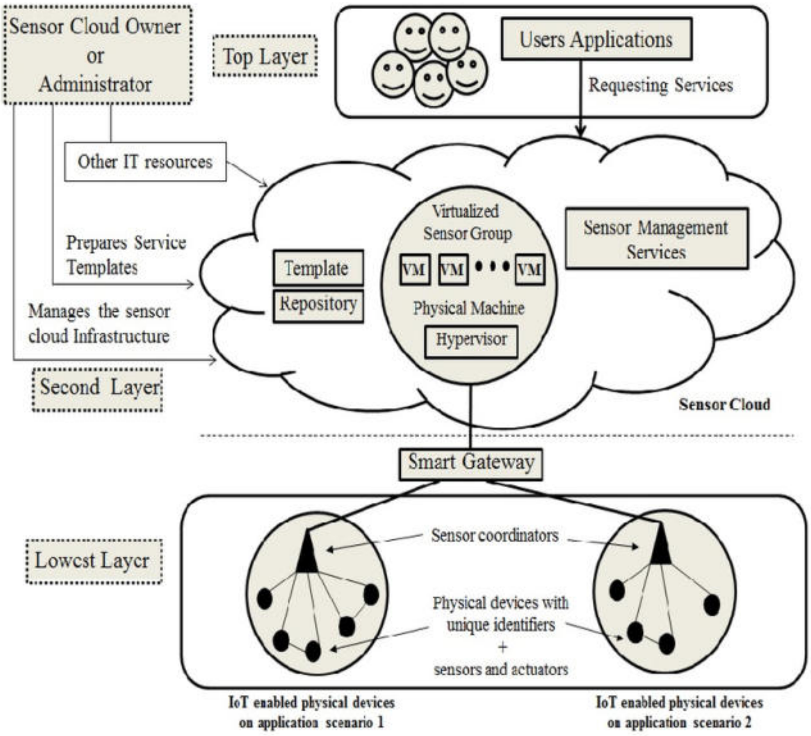
Sensor Cloud Owner or Administrator
Top Layer
Users Applications
Requesting Services
Other IT resources
Prepares Service Templates
Manages the sensor cloud Infrastructure
Second Layer
Template
Repository
Virtualized Sensor Group
VM
VM
VM
Physical Machine
Hypervisor
Sensor Management Services
Sensor Cloud
Smart Gateway
Lowest Layer
Sensor coordinators
Physical devices with unique identifiers + sensors and actuators
IoT enabled physical devices on application scenario 1
IoT enabled physical devices on application scenario 2

Fig. 7.1: Ensemble architecture of IoT and sensor cloud.

through their sensor coordinators in multi-hop communication. The multi-hop communication scenario allows the IoT network to be more scalable, with a diverse range of physical devices and heterogeneous data which requires extensive data analysis and pre-processing from the smart gateways [10]. In multi-hop communication with the smart gateways, the sensor coordinators make their underlying physical devices as a black box to the outer layer; which in turn adds additional security to the IoT network, and hence security can be customized according to the sensor and IoT network [10]. Once the sensed data is pre-processed the restructured data from the smart gateways are then sent to the sensor cloud for further processing as discussed in Section 3. The data from the sensor cloud are then utilized for making various applications and services for users. The application layer deals with the utilization of services and applications for users. The IoT and sensor cloud has a diverse range of applications and integration of these two promising network paradigms promised to offer a variety of real world applications. The applications of the IoT system are based on network availability, coverage, scalability, heterogeneity, repeatability, and user involvement [62]. The most common application of these types of infrastructure can be in health monitoring, battlefield monitoring, telematics, agricultural and irrigation control, earth observation, wildlife monitoring.

8. Research challenges and constraints for ensembling IoT through sensor cloud. Following are the challenges that need to be addressed properly for the proliferation of the efficient enabling of IoT through sensor cloud:

1. **Unique identifiers:** Despite the availability of various identification schemes discussed in Section 7, there is no universal unique identification scheme for the heterogeneous platform for IoT applications. Various IoT platforms use globally unique identification schemes [63, 64] or have their own unique identification schemes to identify the IoT platforms, but the diverse nature of physical devices and the heterogeneous IoT platforms with the absence of de facto standards for naming and addressing, pose

a key challenge over interoperability of different identifiers [65, 66] and need to be addressed. The commercial and the political difference between the standard bodies; which provide the specifications, and framework for the IoT platforms, create the problems of having unique identification schemes [67]. A new universal identification mechanism for the heterogeneous IoT platforms should be created for the interoperability of the different IoT platforms, but moving IoT platforms supporting a diverse range of IoT applications to a whole new universal identification scheme is also quite challenging and poses several issues.

2. **Infrastructure difference:** The presence of infrastructural differences between the sensor cloud and IoT system makes the difficulty in balancing and managing the sensor cloud environment and IoT requirements. Hence, while integrating these two technologies, balancing, and management of the two platforms should be taken care of.
3. **Smart gateway:** Integration of IoT and sensor cloud requires a smart gateway which pre-processes, filters, and restructures the collected data from the IoT devices and transfers the useful data to the sensor cloud; which is not possible with the light IoT devices and sensors. The gateway should be smart and intelligent enough to do the tasks, such as data management, device management. Different types of gateway works at different levels in the protocol layers and the seamless integration of enabling technologies with the smart gateway makes the IoT system smarter to deal with things.
4. **Mobility:** As IoT nodes are mobile; there is a constant disruption of services when the nodes move from one gateway to another depending upon the application scenarios. Hence, it is another issue and needs to be taken into consideration while integrating the IoT with the sensor cloud. There is an ultimate need of designing an efficient mobility management scheme for these kinds of networks where they are a requirement of the constant interaction of IoT nodes for providing the services to the users. Researchers have proposed various mobility models for the various types of network so that the network can be utilized for various real world applications. A resource mobility scheme [68] was proposed which operates in two modes: caching and tunneling; for providing services in continuity to users and allow the application to use the sensed data when the resources are temporarily unavailable during mobility of the nodes. The scheme shows a 30% reduction in service loss in the mobility scenarios. An efficient mobility management scheme should be designed to support heterogeneous devices and platforms. A feasible group mobility management scheme [69] was proposed, in which the nodes with similar mobility behavior stored at their location database are grouped and the leader of that group will manage the mobility on behalf of other nodes of the group which in turn try to mitigate the signalling congestion problem. One more approach [70] exists in the literature that maintains the continuity of services of the migrating sensor nodes in a framework which is based on the concept of a Web of Things. Several other group mobility models for mobile ad hoc networks [71-73] were proposed that manage the mobility pattern of the nodes, inspired by the social behavior of the natural systems.
5. **Standardization:** Standardization of cloud infrastructure is also a key challenge when integrating the IoT with sensor cloud. The cloud interoperates with various cloud vendors where each cloud vendor supports their standardized formats. The integration of IoT with sensor cloud has to deal with the diverse standardized format for the cloud interfaces, resources, and for managing the networks. The interoperability of cloud infrastructure to enable the underlying technologies is very important and needs to be addressed [74, 75].
6. **Performance:** The performance evaluation of the IoT network is an open issue that needs to be addressed when integrating it with other technologies. The performance evaluation of the IoT network is dependent on the performance of various underlying technologies and several other factors, as the network is built from various elements. So thorough evaluation of these networks is a tedious task and is not much reported in the literature, but needs to be addressed for the efficient and wide deployment of the integrated IoT system in real world scenarios.
7. **Energy management:** The sensor nodes consume lots of energy while communicating with the cloud infrastructure. The sensor nodes consist of sensing, transmission, processing, and power unit. The presence of sensors in physical devices to sense the physical environment consumes lots of energy; the temporary power unit, like batteries in a network of billions of physical devices may not be sufficient and

Table 9.1: Characteristics of sensor cloud, IoT and IoT enabled sensor cloud

Characteristics	**Sensor cloud**	**IoT**	**IoT enabled sensor cloud**
Storage capability	Virtually Unlimited	Limited	Virtually Unlimited
Computational Power	Virtually Unlimited	Limited	Virtually Unlimited
Displacement	Centralized	Ubiquitous	Centralized
Data	Generate and manages the unlimited data	Generates lots of data	Generate and manages the unlimited data
Reachability	Pervasive	Limited	Extensive
Mobility of physical devices	Mostly stationary	Mobile	Mobile
Resource Optimization	High	Low	High
Implementation cost	High	Moderate	Low

needs permanent energy supplies from the environment, like mechanical motion, solar energy, radiation, thermal gradient, and light [76, 77]. These renewable energy sources can be used in the sensor nodes [78, 79] to curb the energy limitations of the network. An efficient mechanism should be addressed for the utilization of energy. Integrating fog computing with the IoT system can bring cloud resources locally [80] and can save lots of energy.

8. **Resource allocation:** Resource allocation to IoT devices by the sensor cloud is another challenge that needs to be addressed when enabling IoT with sensor cloud. Resource allocation to the physical entity is a challenging issue as it is difficult to decide how much or whom to give resources when resources are in demand by several physical entities. Depending upon the application scenarios the requirement of resources is decided. One solution to this problem is to bring for computing as middleware to manage resources to the underlying physical devices [10].
9. **Bandwidth usage and network access management:** The drastic increase in physical devices and sensor-cloud users pose great difficulty in the allocation of proper bandwidth to each device and sensor-cloud users despite having the presence of various bandwidth allocation methods in the literature. Providing the proper bandwidth to such a huge infrastructure which is using various networks to deal with its applications is a difficult task, but with proper network access management schemes, the link performance can be improved and can have optimized bandwidth usage [51].

9. Analysis and discussion:. This section analyses the ensemble system of IoT and sensor cloud. There are various literature which showcases the integration of IoT system with other technologies, such as fog computing [81, 82], big data [83, 84], software defined networks [85, 86], machine learning [87], and many more. The adaptability of these integrated IoT systems with other technologies in real world scenarios provides interoperability with a diverse range of systems and is proved to be economically viable. In particular, the seamless integration of IoT and sensor cloud is very significant in terms of their applicability to the diverse range of applications. The characteristics of the sensor cloud, IoT and IoT enabled sensor cloud is presented in Table 9.1. As can be seen, the characteristics of sensor cloud and IoT are complementary to each other and these are some reasons why researcher are showing more interest in integrating these two promising technologies. The integration of the IoT and the sensor cloud will fill the gaps of each other; the IoT will have the benefit of virtually large storage, improved processing capabilities, communication, and resource optimization from the sensor cloud to limit its technological constraints. On the other hand, the sensor-cloud can extend its scope to deal with various physical devices in a dynamic and distributed manner, and become approachable to a diverse range of real world scenarios for providing new services to the users. The sensor cloud in the integrated system provide the intermediary layer between the physical devices and the user applications to hide the complexities and functionalities which will later benefit the implementation of the technologies and will impact the future application development.

The motivation towards the integration of the IoT and sensor cloud lies in the storage, communication, and computation. The properties of IoT, such as interconnectivity, heterogeneity, dynamism, data privacy and security, etc., demand the requirement of connecting heterogeneous things or objects in a dynamic manner with a secured ecosystem containing physical devices, internet, and the end users. The sensor network is identified as main enabler of IoT [88]. Technical advances made low powered, efficient, low cost devices, to be used in large scale applications. The physical devices are enabled with a variety of sensors and are deployed in variety of application domains despite being suffering from various technical constraints, such as energy, processing power, reliability, mobility, etc. With this context, the timely processing of the huge amount of collected data along with making sensor energy efficient, small and reliable; the ensemble system poses several challenges [89]. Integrating sensor data with the cloud provides new opportunities in large coverage, and relevancy, but affects the data privacy and security [89]. Cross platform of IoT is another challenging issue. The manufacturers have to set the specifications of the sensors, actuators, and controllers and are essential for them to incorporate cross-platform solutions to customize requirements for diverse range of applications [90]. Collaborating with other organizations for building the IoT products will reduce the system complexity of the solutions and be more energy efficient, cost effective and reliable, as it is difficult to provide and meet all the requirements of the IoT product by a single organization or company [91].

The integration of IoT and sensor cloud is considered a vital footprint for mitigating various limitations and challenges of both the integrated drivers. These drivers contribute to the ensemble architecture by (1) publishing/subscribing the sensed information: The sensed information from the multiple sensor networks are published and is subscribed by the applications based on their requirements and on-demand basis [87], (2) collaborating with different manufacturers: The IoT devices require cross-platform design and integration of heterogeneous sensors in terms of hardware, communication and sensing range, communication protocols, and standards [90]. Hence, collaboration with different manufacturers and organizations will give ease in the manufacturing the IoT devices, (3) on-demand resource scalability at application runtime and providing customized query processing to the end users and (4) visualizing sensor: The sensor cloud platform provides an API to the end-users for managing the sensors on their own [49]. The end user can perform variously customized operations like addition or deletion of a sensor, selection of sensors based on their current services etc. The sensor visualization is very important for IoT platform as it provides interfaces to customers for issuing the queries and it can be present anywhere like, in smartphones, laptops, and other digital assistants [90]. The ensemble system of IoT and sensor-cloud is making significant improvements and contributing immensely to the proliferation of the IoT system.

10. Future Directions. This section presents the future research direction for the ensemble system of IoT and sensor cloud. Following are the scope where there is a requirement of putting additional research efforts to make use of the whole capacity of the integrated system:

1. **Network virtualization:** Network virtualization is an important aspect of research and many applications of integrated system of IoT and sensor cloud will take benefit from this field. The efficient utilization of network and resources can be done by logically isolating the network partition from the globally distributed network infrastructure.
2. **Common open API and standard formats:** The common API and standard format will make the integrated system more flexible and efficient. It also provides various business opportunities for providing a common open service platform environment for the integrated IoT and sensor cloud system.
3. **Multi-networking:** The ensemble system should support handover and location management. As the mobility is high in IoT enabled sensor cloud and is dynamic in nature; it is necessary to maintain and improve the network reliability, QoS, and fault tolerance.
4. Enabling the ensemble system with other technologies like fog computing and software defined networking will also serve a great benefit to the ensemble system.
5. **Identification:** A unique identification, addressing and naming of the physical device in the integrated system is very important for supporting diverse devices and to handle their mobility.
6. **Optimal gateway selection:** The selection of optimal gateway to serve the user request in IoT enabled sensor cloud environment is important for real time monitoring systems. The mapping of service request to the optimal gateway support variety of applications and make an efficient and reliable integrated system.

11. Conclusion. The internet technology has flourished with the arrival of the IoT and has witnessed a revolution in enabling IoT with the emerging technologies. The limitations of the IoT system can be efficiently handled by seamlessly integrating IoT with other technologies which in turn offer a variety of services and applications. This paper summarizes the concept of IoT and sensor cloud with their challenges and architectures.

Further, the paper reviews the possible ensemble architecture of the IoT and the sensor cloud. Enabling IoT with sensor cloud makes the integrated system cost-effective, flexible, scalable, and provides better computation power and storage. The significance and research challenges of the ensemble system are also being reviewed. The paper analyses and discusses the motivation, and need behind the integration of the IoT and sensor cloud. Moreover, future research directions are also identified in order to exploit the full potential of the integrated system. The integrated system provides a wide variety of advantages and applications which will continue to evolve in years to come.

REFERENCES

[1] J. Verma, *Internet of Things*,Everyman's Science,12 (2018), pp. 12-14.

[2] C. Zhu , V.C Leung, J. J. Rodrigues, L. Shu, L. Wang, and H. Zhou, *Social sensor cloud: framework, greenness, issues, and outlook*, IEEE Network, 32(5) (2018), pp. 100-105, http://www.disca.upv.es/misan/mobmodel.htm, page accessed on October 15th 2017.

[3] https://ietf.org/topics/iot/, Accessed 30 March 2020.

[4] https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/, Accessed 2 April 2020.

[5] P. Mell, and T. Grance,*The NIST definition of cloud computing*, (2011).

[6] A. R. Biswas, and R. Giaffreda, *IoT and cloud convergence: Opportunities and challenges*, in IEEE World Forum on Internet of Things (WF-IoT) , IEEE, 2014.

[7] M.P. Andersen,G. Fierro, and D. E. Culler, *Enabling synergy in iot: Platform to service and beyond*, Journal of Network and Computer Applications, 81 (2017), pp. 96-110.

[8] Q. Zhang, L. Cheng, and R. Boutaba, *Cloud computing: state-of-the-art and research challenges*, Journal of internet services and applications, 1(1) (2010), pp. 7-18.

[9] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, *Fog computing and its role in the internet of things*, in Proceedings of the first edition of the MCC workshop on Mobile cloud computing, ACM, August 2012, pp. 13-16.

[10] M. Aazam, and E. N. Huh, *Fog computing and smart gateway based communication for cloud of things*, in 2014 International Conference on Future Internet of Things and Cloud, IEEE, August 2014, pp. 464-470.

[11] A. Botta, W. De Donato, V. Persico, and A. Pescapé, *Integration of cloud computing and internet of things: a survey*, Future generation computer systems,56 (2016), pp. 684-700.

[12] S. K. Dash, S. Mohapatra, and P. K. Pattnaik, *A survey on applications of wireless sensor network using cloud computing*, International Journal of Computer Science & Emerging Technologies,1(4) (2010), pp. 50-55.

[13] C. S. R. Murthy, and B. S. Manoj, *Ad hoc wireless networks: Architectures and protocols*, Pearson Education, India, 2004.

[14] A. Alamri, W. S. Ansari, M. M. Hassan, M. S. Hossain, A. Alelaiwi, and M. A. Hossain, *A survey on sensor-cloud: architecture, applications, and approaches*, International Journal of Distributed Sensor Networks, 9(2) (2013), pp. 917-923.

[15] L. Atzori, A. Iera, and G. Morabito, *The internet of things: A survey*, Computer networks, 54(15) (2010) , pp. 2787-2805.

[16] J. Minlan, L. Jingyuan, and Z. Xiaokang, *Research on algorithm of three-dimensional wireless sensor networks node localization*,Journal of Sensors (2016).

[17] M. Khelifi, I. Benyahia, S. Moussaoui, F. Naït-Abdesselam, *An overview of localization algorithms in mobile wireless sensor networks*, in 2015 International Conference on Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS), IEEE, July 2015, pp. 1-6.

[18] J. S. Miller, P. A. Dinda, and R. P. Dick, *Evaluating a basic approach to sensor network node programming*, in Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems, ACM, November 2009, pp. 155-168.

[19] G. Fortino, R. Giannantonio, R. Gravina, P. Kuryloski, and R. Jafari, *Enabling effective programming and flexible management of efficient body sensor network applications*, IEEE Transactions on Human-Machine Systems, 43(1) (2012), pp. 115-133.

[20] L. Mottola, and G. P. Picco, *Programming wireless sensor networks: Fundamental concepts and state of the art*, ACM Computing Surveys (CSUR), 43(3) (2011), pp. 19.

[21] S. Biswas, R. Das, and P. Chatterjee, *Energy-efficient connected target coverage in multi-hop wireless sensor networks*, in Industry interactive innovations in science, engineering and technology, Springer, Singapore, 2018, pp. 411-421.

[22] Y. Ma, L. Wang, P. Liu, R. Ranjan, *Towards building a data-intensive index for big data computing–A case study of Remote Sensing data processing*, Information Sciences, 319 (2015), pp. 171-188.

[23] L. Hang, L., W. Jin, H. Yoon, Y. Hong, and D. Kim, *Design and Implementation of a Sensor-Cloud Platform for Physical Sensor Management on CoT Environments*, Electronics, 7(8) (2018), pp. 140.

[24] http://www.ntu.edu.sg/intellisys, Accessed 4 April 2020.

[25] K. T. Lan, *"What's next? Sensor + Cloud?"*, in Proceedings of the 7th International Workshop on Data Management for Sensor Networks, ACM Digital Library, 2010, pp. 978-971.

[26] N. Kurata, M. Suzuki, S. Saruwatari, and H. Morikawa, *Actual application of ubiquitous structural monitoring system using wireless sensor networks*, in Proceedings of the 14th World Conference on Earthquake Engineering (14WCEE), October 2008, pp. 1-9.

[27] G. Demiris, B. K. Hensel, M. Skubic, and M. Rantz, *Senior residents' perceived need of and preferences for "smart home" sensor technologies*, International journal of technology assessment in health care, 24(1) (2008), pp. 120-124.

[28] A. Alexe, and R. Ezhilarasie., *Cloud computing based vehicle tracking information systems*, International journal of technology assessment in health care, IJCST, 2(1 (2011)), pp. 49-52.

[29] B. P. Rao,P. Saluia, N. Sharma, A. Mittal, S. V. Sharma, *Cloud computing for Internet of Things & sensing based applications*, in 2012 Sixth International Conference on Sensing Technology (ICST), IEEE, December 2012, pp. 374-380.

[30] R. Katsuma,Y. Murata, N. Shibata, K. Yasumoto, K., and M. Ito, *Extending k-coverage lifetime of wireless sensor networks using mobile sensor nodes*, in 2009 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, IEEE, December 2012, pp. 48-54.

[31] K. Matsumoto, R. Katsuma, N. Shibata, K. Yasumoto, and M. Ito, *Minimizing localization cost with mobile anchor in underwater sensor networks*, in Proceedings of the Fourth ACM International Workshop on UnderWater Networks, ACM, November 2009, pp. 14.

[32] S. Madden, and M. J. Franklin, *Fjording the stream: An architecture for queries over streaming sensor data*, icde, 2 (2002), pp. 555.

[33] O. Gnawali, R. Fonseca, K. Jamieson, D. Moss, and P. Levis, *Collection tree protocol*, in Proceedings of the 7th ACM conference on embedded networked sensor systems, ACM, Novemberr 2009, pp. 1-14.

[34] A. Rowe, V. Gupta, and R. R. Rajkumar, *Low-power clock synchronization using electromagnetic energy radiating from ac power lines*, in Proceedings of the 7th ACM conference on embedded networked sensor systems, ACM, November 2009, pp. 211-224.

[35] M. Gaynor, S. L. Moulton, M. Welsh, E. La Combe, A. Rowan, and J. Wynne, *Integrating wireless sensor networks with the grid*, IEEE Internet Computing, 8(4) (2004), pp. 32-39 .

[36] M. Yuriyama, T. Kushida, and M. Itakura , *A new model of accelerating service innovation with sensor-cloud infrastructure*, in 2011 Annual SRII Global Conference, IEEE, March 2011, pp. 308-314.

[37] M. Yuriyama, T. Kushida, *Sensor-cloud infrastructure-physical sensor management with virtualized sensors on cloud computing*, in 2010 13th International Conference on Network-Based Information Systems, IEEE, September 2010, pp. 1-8.

[38] Y. Xu, and A.Helal, *Scalable cloud–sensor architecture for the Internet of Things*, IEEE Internet of Things Journal, 3(3) (2015), pp. 285-298

[39] S. Bose, A. Gupta, S. Adhikary, and N. Mukherjee, *Towards a sensor-cloud infrastructure with sensor virtualization*, in Proceedings of the Second Workshop on Mobile Sensing, Computing and Communication, June 2015, pp. 25-3).

[40] S.Guo, Z, Zhong, and T. He *FIND: faulty node detection for wireless sensor networks*, in Proceedings of the 7th ACM conference on embedded networked sensor systems, November 2009, pp. 253-266.

[41] R. S. Ponmagal, and J. Raja, *An extensible cloud architecture model for heterogeneous sensor services*, International Journal of Computer Science and Information Security, 9(1) (2011), pp. 147-155.

[42] 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 2010 Second International Conference on eHealth, Telemedicine, and Social Medicine, IEEE, Februrary 2010, pp. 95-99.

[43] J. Biswas, J. Maniyeri, K. Gopalakrishnan, L. Shue, J. E. Phua, H. N. Palit, and X. Li, *Processing of wearable sensor data on the cloud-a step towards scaling of continuous monitoring of health and well-being*, in 2010 annual international conference of the IEEE engineering in medicine and biology, IEEE, August 2010, pp. 3860-3863.

[44] G. Singh, J. O'Donoghue, and C. K. Soon, *Telemedicine: issues and implications*, Technology and Health Care, 10(1) (2002), pp. 1-10.

[45] M.Islam, M. M. Hassan, G. W. Lee, and E. N. Huh, *A survey on virtualization of wireless sensor networks*, Sensors, 12(2) (2012), pp.2175-2207.

[46] K. Lee, D. Murray, D. Hughes, and W. Joosen, *Extending sensor networks into the cloud using amazon web services*, in 2010 IEEE International Conference on Networked Embedded Systems for Enterprise Applications, IEEE, November 2010, pp. 1-7.

[47] X. H. Le, S. Lee, P. T. H. Truc, A. M. Khattak, M. Han, D. V. Hung, and E. N. Huh, *Secured WSN-integrated cloud computing for u-life care*, in 2010 7th IEEE Consumer Communications and Networking Conference, IEEE, January 2010, pp. 1-2.

[48] C.Doukas, and I. Maglogiannis, *Managing wearable sensor data through cloud computing*, in 2011 IEEE Third International Conference on Cloud Computing Technology and Science, IEEE, Novemeber 2011, pp. 440-445.

[49] L. D. Kumar, S. S. Grace, A. Krishnan, V. M. Manikandan, R. Chinraj, and M. R. Sumalatha ,*Data filtering in wireless sensor networks using neural networks for storage in cloud*, in 2012 International Conference on Recent Trends in Information Technology, IEEE, April 2012, pp. 202-205.

[50] Y.Xu, S. Helal, M. Thai, M. Scmalz, *Optimizing push/pull envelopes for energy-efficient cloud-sensor systems*, in Proceedings of the 14th ACM international conference on Modeling, analysis and simulation of wireless and mobile systems, ACM, October 20111, pp. 17-26.

[51] F.Ge, H. Lin, A. Khajeh, C. J. Chiang, M. E. Ahmed, W. B. Charles, and R. Chadha, *Cognitive radio rides on the cloud*, in 2010-MILCOM 2010 MILITARY COMMUNICATIONS CONFERENCE, IEEE, October 2010, pp. 1448-1453.

[52] , W. Qun, *Research on architecture of Internet of Things and construction of its simulation experiment platform [J]*, Experimental Technology and Management, 10 (2010).

[53] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, *Future internet: the internet of things architecture, possible applications and key challenges*, in 2012 10th international conference on frontiers of information technology, IEEE, December 2012, pp. 257-260.

[54] P.Sethi, and S. R. Sarangi, *Internet of things: architectures, protocols, and applications*, Journal of Electrical and Computer Engineering, 2017.

[55] H. Liu, M. Bolic, A. Nayak, and I. Stojmenovic, *Taxonomy and challenges of the integration of RFID and wireless sensor networks*, IEEE network, 22(6) (2008), pp. 26-35.

[56] C. Englund, and H. Wallin, *RFID in wireless sensor network*, Doctoral dissertation, Chalmers tekniska högsk, Doctoral dissertation, Chalmers tekniska högsk.

[57] *EC–European Commission, Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination*, Final report, (2014).

[58] C.Pastrone, D. Rotondi, A. Skarmeta, H. Sundmaeker, O. Vermesan, S. Ziegler, and L. Yang, *Internet of things*, eu-china joint white paper on internet-of-things identification. Tech. Rep., European Research Cluster on the Internet of Things.

[59] A.Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, *Internet of things: A survey on enabling technologies, protocols, and applications*, IEEE communications surveys & tutorials, 17(4) (2015), pp. 2347-2376.

[60] Z.Yan, N. Kong, Y. Tian, and Y. J. Park, *A universal object name resolution scheme for IoT*, in 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, IEEE, August 2013, pp. 1120-1124.

[61] M. Aazam, I. Khan, A. A. Alsaffar, and E. N. Huh, *Cloud of Things: Integrating Internet of Things and cloud computing and the issues involved*, in Proceedings of 2014 11th International Bhurban Conference on Applied Sciences & Technology (IBCAST) Islamabad, Pakistan, IEEE, January 2014, pp. 414-419.

[62] A.Gluhak, S. Krco, M. Nati, D. Pfisterer, N. Mitton, and T. Razafindralambo, *A survey on facilities for experimental internet of things research*, IEEE Communications Magazine, 49(11) (2011), pp. 58-67.

[63] R.Ma, Y. Liu, C. Shan, X. L. Zhao, and X. A. Wang, *Research on Identification and Addressing of the Internet of Things*, in 2015 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), IEEE, November2015, pp. 810-814.

[64] G.Roussos, and P. Chartier, *Scalable id/locator resolution for the iot*, in 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, IEEE, October 2011, pp. 58-66.

[65] C. H. Liu, B. Yang, and T. Liu, *Efficient naming, addressing and profile services in Internet-of-Things sensory environments*, Ad Hoc Networks, 18 (2014), pp. 85-101.

[66] L.Roalter, M. Kranz, and A. Möller, *A middleware for intelligent environments and the internet of things*, in International Conference on Ubiquitous Intelligence and Computingpp, Springer, Berlin, Heidelberg, October 2010, pp. 267-281.

[67] H. Aftab, K. Gilani, J. Lee, L. Nkenyereye, S. Jeong, and J. Song, *Analysis of identifiers on IoT platforms*, Digital Communications and Networks, (2019).

[68] F. Ganz, R. Li, P. Barnaghi, and H. Harai, H, *A resource mobility scheme for service-continuity in the Internet of Things*, in 2012 IEEE International Conference on Green Computing and Communications, IEEE, November 2012, pp. 261-264.

[69] H. L. Fu, P. Lin, H. Yue, G. M. Huang, and C. P. Lee, *Group mobility management for large-scale machine-to-machine mobile networking*, IEEE Transactions on Vehicular Technology, 63(3) (2013), pp. 1296-1305.

[70] T.Elsaleh, A. Gluhak, and K. Moessner, *Service continuity for subscribers of the mobile real world Internet*, in 2011 IEEE International Conference on Communications Workshops (ICC), IEEE, June 2011, pp. 1-5.

[71] S. Misra, and P. Agarwal, *Bio-Inspired Group Mobility Model for Mobile Ad hoc Networks based on Bird-Flocking Behavior*, Soft Computing, 16(3) (2012), pp. 437-450.

[72] J. Verma, and N. Kesswani, *BIGM: A Biogeography Inspired Group Mobility Model for Mobile Ad Hoc Networks*, International Journal of Wireless Information Networks, 25(4) (2018), pp. 488-505.

[73] J. Verma, and N. Kesswani, *AMIGM: Animal Migration Inspired Group Mobility Model for Mobile Ad hoc Networks*, Scalable Computing: Practice and Experience, 20(3) (2019), pp. 577-590.

[74] E. B. Gürsel, and A. Tarek, *Analysis of Interoperability In Cloud Computing*, in Proceedings of the 2019 5th International Conference on Computer and Technology Applications, April 2019, pp. 189-192.

[75] , G. Lewis, *The Role of Standards in Cloud-Computing Interoperability*, CMU/SEI-2012-TN-012, Software Engineering Institute, Carnegie Mellon University, (2012).

[76] S. Kim, R. Vyas, J. Bito, K. Niotaki, A. Collado, A. Georgiadis, M. M. Tentzeris, *Ambient RF energy-harvesting technologies for self-sustainable standalone wireless sensor platforms*, in Proceedings of the IEEE, 102(11) (2014), pp. 1649-1666.

[77] P. D.Mitcheson, E. M. Yeatman, G. K. Rao, A. S. Holmes, and T. C. Green, *Energy harvesting from human and machine motion for wireless electronic devices*, in Proceedings of the IEEE, 96(9) (2008), pp. 1457-1486.

[78] , C.Botteron, D. Briand, B. Mishra, G. Tasselli, P. Janphuang, F. Haug, and P. A. Farine, *A low-cost UWB sensor node powered by a piezoelectric harvester or solar cells*, Sensors and Actuators A: Physical, 239 (2016), pp. 127-136.

[79] B.Gusarov, E. Gusarova, B. Viala, L. Gimeno, S. Boisseau, O. Cugat, and B. Louison, *Thermal energy harvesting by piezoelectric PVDF polymer coupled with shape memory alloy*, Sensors and Actuators A: Physical, 243 (2016), pp. 175-181.

[80] D.Evans, *The internet of things: How the next evolution of the internet is changing everything*, CISCO white paper, 1(2011), pp. 1-11.

[81] R. Z. Naeem, S. Bashir, M. F. Amjad, H. Abbas, and H. Afzal, *Fog computing in internet of things: Practical applications and future directions*, Peer-to-Peer Networking and Applications, 12(5) (2019), pp. 1236-1262.

[82] C. Puliafito, E. Mingozzi, F. Longo, A. Puliafito, and O. Rana, *Fog computing for the internet of things: A Survey*, ACM Transactions on Internet Technology (TOIT), 19(2) (2019), pp. 1-41.

[83] B. P. Sutjiatmo, A. Erwinsyah, E. Laxmi Lydia, K. Shankar, P. T. Nguyen, W. Hashim, and A. Maseleno *Empowering internet of things (IoT) through big data*, (2019).

[84] X. Xu, Q. Liu, Y. Luo, K. Peng, X. Zhang, S. Meng, L. Qi, *A computation offloading method over big data for IoT-enabled*

cloud-edge computing, Future Generation Computer Systems, 95 (2019), pp. 522-533.

[85] P. Throrat, S. Singh, A. Bhat, V. L. Narasimhan, G. Jain, *SDN-Enabled IoT: Ensuring Reliability in IoT Networks Through Software Defined Networks*, in Towards Cognitive IoT Networks, Springer, Cham, (2020), pp. 33-53.

[86] K. Sood, S. R. Pokhrel, K. Karmakar, V. Vardharajan, and S. Yu, *SDN-Capable IoT Last-Miles: Design Challenges*, in 2019 IEEE Global Communications Conference (GLOBECOM), IEEE, December 2019, pp. 1-6.

[87] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, *Machine learning in IoT security: current solutions and future challenges*, arXiv preprint arXiv:1904.05735,(2019).

[88] A.Zaslavsky, C. Perera, and D. Georgakopoulos, *Sensing as a service and big data*, arXiv preprint arXiv:1301.0159, (2013).

[89] F. Zhao, *Sensors meet the cloud: Planetary-scale distributed sensing and decision making*, in 9th IEEE International Conference on Cognitive Informatics (ICCI'10), IEEE, July 2010, pp. 998-998.

[90] S. Misra, S. Sarkar, and S. Chatterjee, *Sensors, Cloud, and Fog: The Enabling Technologies for the Internet of Things*, CRC Press (2019).

Edited by: Dana Petcu
Received: May 15, 2021
Accepted: Nov 16, 2021