Journal of King Saud University – Computer and Information Sciences (2018) **30**, 291–319

King Saud University

**Journal of King Saud University – Computer and Information Sciences**

www.ksu.edu.sa
www.sciencedirect.com

# A survey on Internet of Things architectures

**P.P. Ray**

*Department of Computer Applications, Sikkim University, Sikkim 737102, India*

Received 4 July 2016; revised 24 September 2016; accepted 3 October 2016
Available online 8 October 2016

**KEYWORDS**

Internet of Things (IoT);
Architecture;
Cyber physical system

**Abstract** Internet of Things is a platform where every day devices become smarter, every day processing becomes intelligent, and every day communication becomes informative. While the Internet of Things is still seeking its own shape, its effects have already stared in making incredible strides as a universal solution media for the connected scenario. Architecture specific study does always pave the conformation of related field. The lack of overall architectural knowledge is presently resisting the researchers to get through the scope of Internet of Things centric approaches. This literature surveys Internet of Things oriented architectures that are capable enough to improve the understanding of related tool, technology, and methodology to facilitate developer's requirements. Directly or indirectly, the presented architectures propose to solve real-life problems by building and deployment of powerful Internet of Things notions. Further, research challenges have been investigated to incorporate the lacuna inside the current trends of architectures to motivate the academics and industries get involved into seeking the possible way outs to apt the exact power of Internet of Things. A main contribution of this survey paper is that it summarizes the current state-of-the-art of Internet of Things architectures in various domains systematically.


**Contents**



E-mail address: ppray@cus.ac.in
Peer review under responsibility of King Saud University.

ELSEVIER Production and hosting by Elsevier

http://dx.doi.org/10.1016/j.jksuci.2016.10.003

## 1. Introduction

Internet of Things (IoT) refers to the stringent connectedness between digital and physical world (Atzori et al., 2010; Sterling, 2005; Internet Reports, 2005). Various researchers have described IoT in multitude forms:

- "*a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual 'Things' have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network*" (Kranenburg, 2008).
- "*3A concept: anytime, anywhere and any media, resulting into sustained ratio between radio and man around 1:1*" (Srivastava, 2006).
- "*Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts*" (Networked Enterprise & RFID & Micro & Nanosystems, 2008). The semantic meaning of "*Internet of Things*" is presented as "*a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols*".

We will consider the definition provided by the ITU:

- "*A global infrastructure for the information society enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies*" (ITU work on Internet of things, 2015).

As per Gartner, 25 billion devices will be connected to the internet by 2020 and those connections will facilitate the used data to analyze, preplan, manage, and make intelligent decisions autonomously. The US National Intelligence Council (NIC) has embarked IoT as one of the six "Disruptive Civil Technologies" (National Intelligence Council, 2008). In this context, we can see that service several sectors, such as: transportation, smart city, smart domotics, smart health, e-governance, assisted living, e-education, retail, logistics, agriculture, automation, industrial manufacturing, and business/process management etc., are already getting benefited from various architectural forms of IoT (Gubbia et al., 2013; Miorandi et al., 2012; Giusto et al., 2010).

IoT architecture may be treated as a system which can be physical, virtual, or a hybrid of the two, consisting of a collection of numerous active physical things, sensors, actuators,

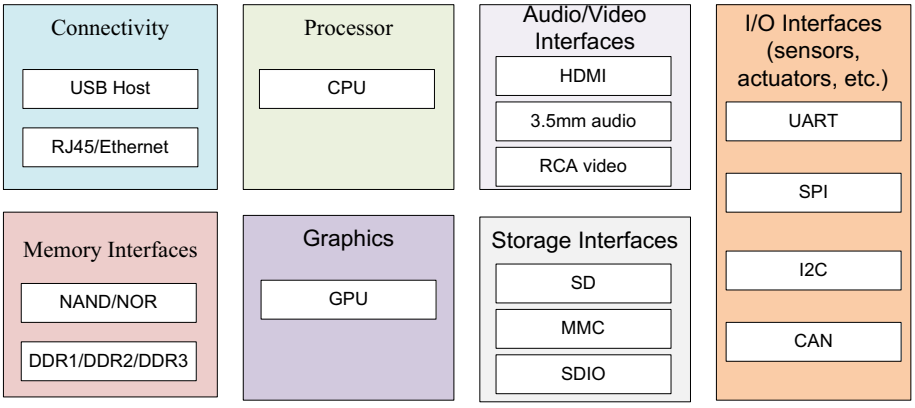


**Figure 1** IoT device components.

**Table 1** Comparison of the existing IoT supported hardware platforms.

| Parameters | Arduino Uno | Arduino Yun | Intel Galileo Gen 2 | Intel Edison | Beagle Bone Black | Electric Imp 003 | Raspberry Pi B+ | ARM mbed NXP LPC1768 |
|---|---|---|---|---|---|---|---|---|
| Processor | ATMega328P | ATmega32u4, and Atheros AR9331 | Intel® Quark™ SoC X1000 | Intel® Quark™ SoC X1000 | Sitara AM3358BZCZ100 | ARM Cortex M4F | Broadcom BCM2835 SoC based ARM11 76JZF | ARM Cortex M3 |
| GPU | - | - | - | - | PowerVR SGX530 @520 MHz | - | VideoCore IV® Multimedia@ 250 MHz | - |
| Operating voltage | 5V | 5V, 3V | 5V | 3.3V | 3.3V | 3.3V | 5V | 5V |
| Clock speed (MHz) | 16 | 16,400 | 400 | 100 | 1 GHz | 320 | 700 | 96 |
| Bus width (bits) | 8 | 8 | 32 | 32 | 32 | 32 | 32 | 32 |
| System memory | 2kB | 2.5 kB, 64 MB | 256 MB | 1 GB | 512 MB | 120 KB | 512 MB | 32 KB |
| Flash memory | 32 kB | 32kB, 16 MB | 8 MB | 4 GB | 4 GB | 4 Mb | - | 512 KB |
| EEPROM | 1 kB | 1 kB | 8 kB | - | - | - | - | - |
| communication supported | IEEE 802.11 b/g/n, IEEE 802.15.4, 433RF, BLE 4.0, Ethernet, Serial | IEEE 802.11 b/g/n,IEEE 802.15.4, 433RF, BLE 4.0, Ethernet, Serial | IEEE 802.11 b/g/n,IEEE 802.15.4, 433RF, BLE 4.0, Ethernet, Serial | IEEE 802.11 b/g/n,IEEE 802.15.4, 433RF, BLE 4.0, Ethernet, Serial | IEEE 802.11 b/g/n, 433RF, IEEE 802.15.4, BLE 4.0, Ethernet, Serial | IEEE 802.11 b/g/n,IEEE 802.15.4, 433RF, BLE 4.0, Ethernet, Serial | IEEE 802.11 b/g/n,IEEE 802.15.4, 433RF, BLE 4.0, Ethernet, Serial | IEEE 802.11 b/g/n,IEEE 802.15.4, 433RF, BLE 4.0, Ethernet, Serial |
| Development environments | Arduino IDE | Arduino IDE | ArduinoIDE | Arduino IDE, Eclipse, Intel XDK | Debian, Android, Ubuntu, Cloud9 IDE | Electric Imp IDE | NOOBS | C/C++ SDK, Online Compiler |
| Programming language | Wiring | Wiring | Wiring, Wyliodrin | Wiring, C, C++, Node.JS, HTML5 | C, C++, Python, Perl, Ruby, Java, Node.js | Squirrel | Python, C, C++, Java, Scratch, Ruby | C, C++ |
| I/O Connectivity | SPI, I2C, UART, GPIO | SPI, I2C, UART, GPIO | SPI, I2C, UART, GPIO | SPI, I2C, UART, I2S, GPIO | SPI, UART, I2C, McASP, GPIO | SPI, I2C, UART, GPIO | SPI, DSI, UART, SDIO, CSI, GPIO | SPI, I2C, CAN, GPIO |

cloud services, specific IoT protocols, communication layers, users, developers, and enterprise layer. Particular architectures do act as a pivot component of IoT specific infrastructure while facilitating the systematic approach toward dissimilar components resulting solutions to related issues. A well defined form of IoT architecture is currently available for knowledge purpose:

– "*a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual 'Things' have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network*" (Kranenburg, 2008).

### *1.1. IoT functional blocks*

An IoT system is comprised of a number of functional blocks to facilitate various utilities to the system such as, sensing, identification, actuation, communication, and management (Sebastian and Ray, 2015a). Fig. 1. presents these functional blocks as described below.

- Device: An IoT system is based on devices that provide sensing, actuation, control, and monitoring activities. IoT devices can exchange data with other connected devices and application, or collect data from other devices and process the data either locally or send the data to centralized servers or cloud based applications back-ends for processing the data, or perform some tasks locally and other tasks within IoT infrastructure based on temporal and space constraints (i.e. memory, processing capabilities, communication latencies, and speeds, and deadlines). An IoT device may consist of several interfaces for communications to other devices, both wired and wireless. These include (i) I/O interfaces for sensors, (ii) interfaces for Internet connectivity, (iii) memory and storage interfaces, and (iv) audio/video interfaces. IoT devices can also be of varied types, for instance, wearable sensors, smart watches, LED lights, automobiles and industrial machines. Almost all IoT

**Table 2** Comparison of the existing communication technologies.

| Parameters | WiFi | WiMAX | LR-WPAN | Mobile communication | Bluetooth | LoRa |
|---|---|---|---|---|---|---|
| Standard | IEEE 802.11 a/c/b/d/g/n | IEEE 802.16 | IEEE 802.15.4 (ZigBee) | 2G-GSM, CDMA 3G-UMTS, CDMA2000 4G-LTE | IEEE 802.15.1 | LoRaWAN R1.0 |
| Frequency band | 5–60 GHz | 2–66 GHz | 868/915 MHz, 2.4 GHz | 865 MHz, 2.4 GHz | 2.4 GHz | 868/900 MHz |
| Data rate | 1 Mb/s–6.75 Gb/s | 1 Mb/s–1 Gb/s (Fixed) 50–100 Mb/s (mobile) | 40–250 Kb/s | 2G: 50–100 kb/s 3G: 200 kb/s 4G: 0.1–1 Gb/s | 1–24 Mb/s | 0.3–50 Kb/s |
| Transmission range | 20–100 m | < 50Km | 10–20 m | Entire cellular area | 8–10 m | < 30 Km |
| Energy consumption | High | Medium | Low | Medium | Bluetooth: Medium BLE: Very Low | Very Low |
| Cost | High | High | Low | Medium | Low | High |

devices generate data in some form of the other which when processed by data analytics systems generate leads to useful information to guide further actions locally or remotely, For instance, sensor data generated by a soil moisture monitoring device in a garden, when processed can help in determining the optimum watering schedules.

- Communication: The communication block performs the communication between devices and remote servers. IoT communication protocols generally work in data link layer, network layer, transport layer, and application layer.
- Services: An IoT system serves various types of functions such as services for device modeling, device control, data publishing, data analytics, and device discovery.
- Management: Management block provides different functions to govern an IoT system to seek the underlying governance of IoT system.
- Security: Security functional block secures the IoT system by providing functions such as, authentication, authorization, privacy, message integrity, content integrity, and data security.
- Application: Application layer is the most important in terms of users as it acts as an interface that provides necessary modules to control, and monitor various aspects of the IoT system. Applications allow users to visualize, and analyze the system status at present stage of action, sometimes prediction of futuristic prospects.

### *1.2. Utilities of IoT*

IoT may be characterized as the holder of key utility factors as given below (Sebastian and Ray, 2015a).

(1) Dynamic and self adapting: IoT devices and systems should have the capability to dynamically adapt with the changing contexts and take actions based on their operating conditions, user's context, or sensed environment. For example, consider a surveillance system comprising of a number of surveillance cameras. The surveillance cameras can adapt their modes (to normal or infra-red night modes) based on whether it is day or night. Cameras could switch from lower resolution to higher resolution modes when any motion is detected and alert nearby cameras to do the same. In this example, the surveillance system is adapting itself based on the context and changing (e.g., dynamic) conditions.

(2) Self-configuring: IoT devices may have self-configuring capability, allowing a large number of devices to work together to provide certain functionality (such as weather monitoring). These devices have the ability to configure themselves (in association with IoT infrastructure), setup the networking, and fetch latest software upgrades with minimal manual or user intervention.

(3) Interoperable communication protocols: IoT devices may support a number of interoperable communication protocols and can communicate with other devices and also with the infrastructure.

(4) Unique identity: Each of IoT device has a unique identity and unique identifier (such as IP address or URI). IoT systems may have intelligent interfaces which adapt based on the context, allow communicating with users and environmental contexts. IoT device interfaces allow users to query the devices, monitor their status, and control them remotely, in association with the control, configuration and management infrastructure.

(5) Integrated into information network: IoT devices are usually integrated into the information network that allows them to communicate and exchange data with other devices and systems. IoT devices can be dynamically discovered in the network, by other devices and/or network, and have the capability to describe themselves (and their characteristics) to other devices or user applications. For example, a weather monitoring node can describe its monitoring capabilities to another connected node so that they can communicate and exchange data. Integration into the information network helps in making IoT systems "smarter" due to the collective intelligence of the individual devices in collaboration with the infrastructure. Thus, the data from a large number of concerned weather monitoring IoT nodes can be aggregated and analyzed to predict the weather.

**Table 3** Comparison of the IoT cloud platforms may be used for agricultural domains: a case study.

| IoT cloud platforms | Real time data capture | Data visualization | Cloud service Type | Data analytics | Developer cost |
|---|---|---|---|---|---|
| Xively (https://xively.com/) | Yes | Yes | Public (IoTaaS) | No | Free |
| ThingSpeak (https://thingspeak.com/) | Yes | Yes (Matlab) | Public | Yes | Free |
| Plotly (https://plot.ly/) | Yes | Yes (IPython, Matlab, Rstudio) | Public | Yes | Free |
| Carriots (https://www.carriots.com/) | Yes | Yes | Private (PaaS) | No | Limited up to: 10 devices |
| Exosite (https://exosite.com/) | Yes | Yes | IoTSaaS | Yes | 2 devices |
| GroveStreams (https://grovestreams.com/) | Yes | Yes | Private | Yes | Limited up to: 20 stream, 10,000 transaction, 5 SMS, 500 Email |
| ThingWorx (www:thingworx.com/) | Yes | Yes | Private (IaaS) | Yes | Pay per use |
| Nimbits (www.nimbits.com/) | Yes | Yes | Hybrid | No | Free |
| Connecterra (www.Connecterra.io/) | Yes | Yes | Private | Yes | Pay per use |
| Axeda (www.axeda.com) | Yes | Yes | Private | Yes | Pay per use |
| Yaler (https://yaler.net) | Yes | Yes | Private (CaaS) | Yes | Pay per use |
| AMEE (www.amee.com) | Yes | Yes | Private | Yes | Pay per use |
| Aekessa (www.arkessa.com) | Yes | Yes | Private (CaaS) | Yes | Pay per use |
| Paraimpu (https://www.paraimpu.com/) | Yes | Yes | Hybrid | No | Limited up to: 4 things, 500 data items/thing |
| Phytech (http://www.phytech.com/) | Yes | Yes | Private | Yes | Pay per use |

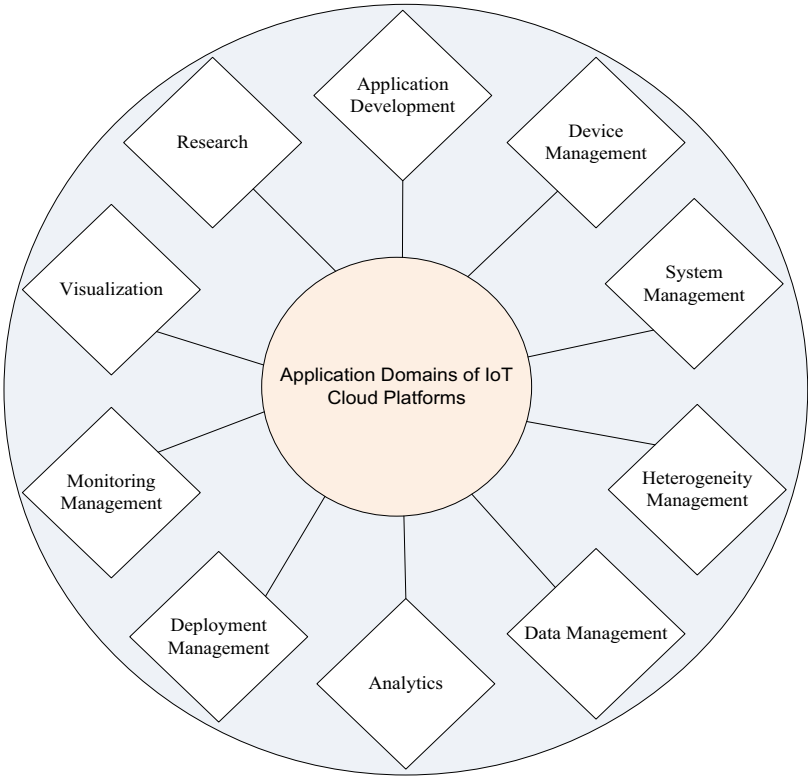


**Figure 2** Application domains of IoT cloud platforms.

(6) Context-awareness: Based on the sensed information about the physical and environmental parameters, the sensor nodes gain knowledge about the surrounding context. The decisions that the sensor nodes take thereafter are context-aware (Yang et al., 2014).

(7) Intelligent decision making capability: IoT multi-hop in nature. In a large area, this feature enhances the energy efficiency of the overall network, and hence, the network lifetime increases. Using this feature, multiple sensor nodes collaborate among themselves, and collectively take the final decision.

### 1.3. IoT supported technologies

This section discusses various IoT technologies such as, hardware platforms, and wireless communication technologies used in different agricultural applications. Different IoT cloud service providers that are being popularly used in current market are also studied.

### 1.4. Hard ware platforms

Table 1 presents the existing hardware platforms classified according to key parameters such as: Processor, GPU, Operating Voltage, Clock Speed, Bus Width, System Memory, Flash Memory, EEPROM, Communication Supported, Development Environments, Programming Language, and I/O Connectivity. The comparative study shows how these platforms are encouraging the growth of IoT by utilizing constraint behavior.

### 1.5. Wireless communication standards

Communication Protocols form the backbone of IoT systems and enable network connectivity and coupling to applications. Communication protocols allow devices to exchange data over the network. The protocols define the data exchange formats, data encoding, addressing schemes for devices and routing of packets from source to destination. Other functions of the protocols include sequence control, flow control, and retransmission of lost packets. Table 2 compares different wireless communication technologies with respect to various parameters.

#### 1.5.1. 802.11 – WiFi

IEEE 802.11 is a collection of Wireless Local Area Network (WLAN) communication standards. For example, 802.11a operates in the 5 GHz band, 802.11b and 802.11 g operate in the 2.4 GHz band, 802.11n operates in the 2.4/5 GHz bands, 802.11ac operates in the 5 GHz band and 802.11ad operates in the 60 GHz band. Theses standards provide data rates from 1 Mb/s to 6.75 Gb/s. WiFi provides communication range in the order of 20 m (indoor) to 100 m (outdoor).

#### 1.5.2. 802.16 – WiMax

IEEE 802.16 is a collection of wireless broadband standards. WiMAX (Worldwide Interoperability for Microwave Access) standards provide data rates from 1.5 Mb/s to 1 Gb/s. The recent update (802.16 m) provides data rate of 100 Mb/s for mobile stations and 1 Gb/s for fixed stations. The specifications are readily available on the IEEE 802.16 working group website (IEEE 802.16, 2014).

#### 1.5.3. 802.15.4 – LR-WPAN

IEEE 802.15.4 is a collection of Low-Rate Wireless Personal Area Networks (LR-WPAN) standards. These standards form the basis of specifications for high level communications protocols such as ZigBee. LR-WPAN standards provide data rates from 40 Kb/s to 250 Kb/s. These standards provide low-cost and low-speed communication to power constrained devices. It operates at 868/915 MHz and 2.4 GHz frequencies at low and high data rates, respectively. The specifications of 802.15.4 standards are available on the IEEE802.15 working group website (IEEE 802.15, 2014).

#### 1.5.4. 2G/3G/4G – mobile communication

There are different generations of mobile communication standards including second generation (2G including GSM and CDMA), third generation (3G-including UMTS ad CDMA2000) and fourth generation (4G-including LTE). IoT devices based on these standards can communicate over cellular networks. Data rates for these standards range from 9.6 Kb/s (2G) to 100 Mb/s (4G) and are available from the 3GPP websites.

#### 1.5.5. 802.15.1 – BlueTooth

Bluetooth is based on the IEEE 802.15.1 standard. It is a low power, low cost wireless communication technology suitable for data transmission between mobile devices over a short range (8–10 m). The Bluetooth standard defines a personal area network (PAN) communication. It operates in 2.4 GHz band. The data rate in various versions of the Bluetooth ranges from 1 Mb/s to 24 Mb/s. The ultra low power, low cost version of this standard is named as Bluetooth Low Energy (BLE or Bluetooth Smart). Earlier, in 2010 BLE was merged with Bluetooth standard v4.0.

#### 1.5.6. LoRaWAN R1.0 – LoRa

LoRaWAN is a recently developed long range communication protocol designed by the LoRa™ Alliance which is an open and non-profit association. It defines Low Power Wide Area Networks (LPWAN) standard to enable IoT. Mainly its aim is to guarantee interoperability between various operators in one open global standard. LoRaWAN data rates range from 0.3 kb/s to 50 kb/s. LoRa operates in 868 and 900 MHz ISM bands. According to Postscapes, LoRa communicates between the connected nodes within 20 miles range, in unobstructed environments. Battery life for the attached node is normally very long, up to 10 years.

### 1.6. Cloud solutions

IoT cloud solutions pave the facilities like real time data capture, visualization, data analytics, decision making, and device management related tasks through remote cloud servers while implying "pay-as-you-go" notion. Various cloud service providers are gradually becoming popular in the several application domains such as agriculture. Table 3 presents comparative study between agriculture specific IoT cloud service providers as a case study. Following sub section describes how IoT clouds may be placed appropriately according to their applicability in several domains of importance.

### 1.7. Application domains

IoT cloud platforms are designed to be meant for particular application specific domains such as, application development, device management, system management, heterogeneity management, data management, analytics, deployment, monitoring, visualization, and finally research purpose (see Fig. 2). It is obvious that there are many more platforms currently present in the market, most popular 26 of these are

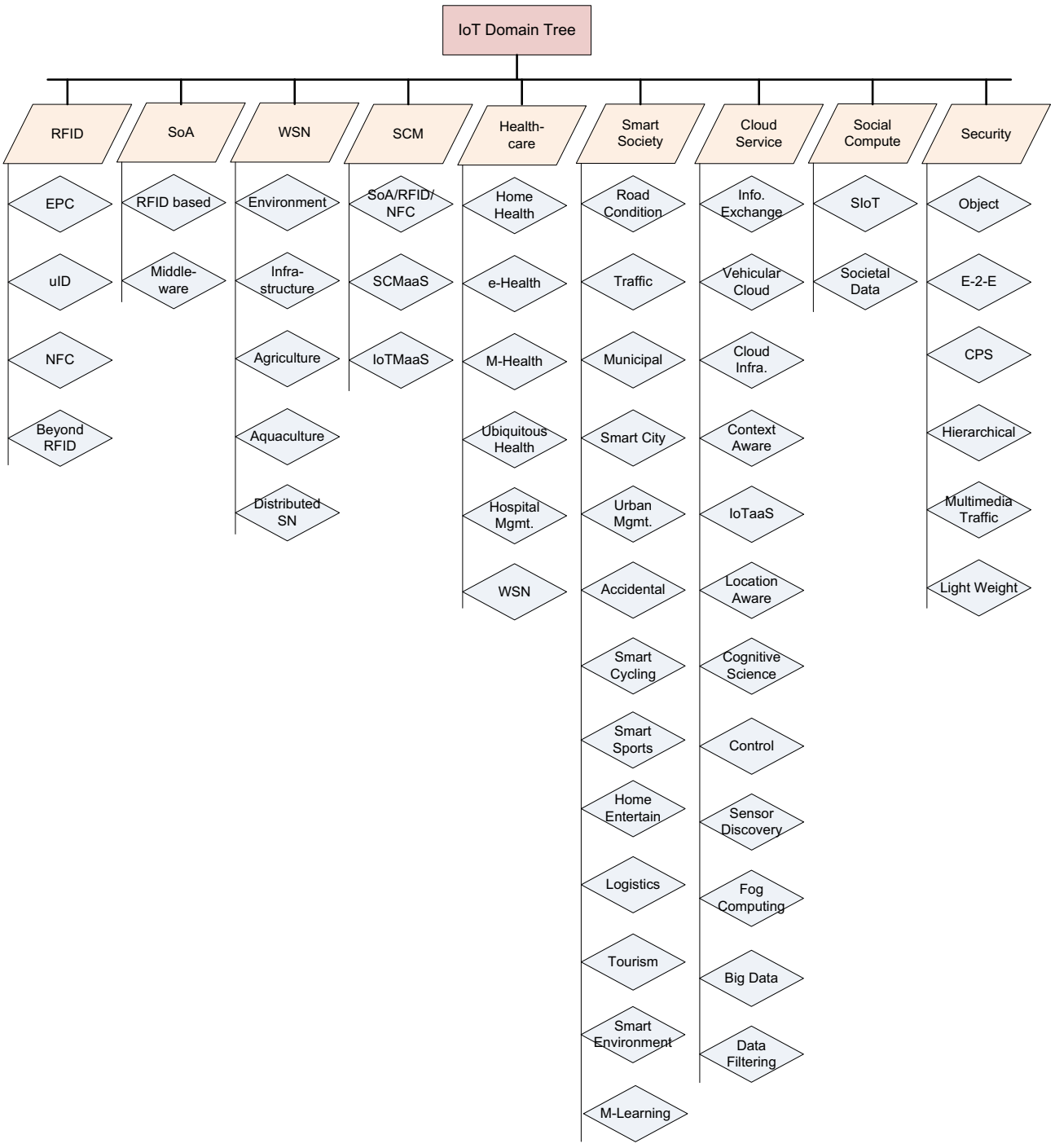


**Figure 3** Application domains of IoT cloud platforms.

chosen. Further, based on applicability and suitability preferences in several domains the IoT cloud platforms have been revisited. 10 different domains are selected based on which most of IoT cloud platforms are currently evolving into the IT market. Management wise few technological sectors are envisioned where these platforms do best fit into such as: Device, System, Heterogeneity, Data, Deployment, and Monitoring. Similarly, Analytics, Research and Visualization fields are chosen where rest of the platforms may be accommodated.

### *1.8. Contributions*

The exponential growth of low cost mobile devices and MEMS technology have pushed up the growth of IoT and allied technologies in a multitude form. It is expected that actual representation of IoT is going to blink around 2025. The graphical notion representing the growth is devised by International Telecommunication Union (ITU) on its meeting held in March, 2015 in Geneva. The full fledged exploration of wearable technology, cognitive computing, and artificial

intelligence seem to come very later on the graph, presented in this occasion.

Available architectures explore multiple opportunities to seek the advantageous part of IoT while encouraging the developer and user groups to get application specific solutions. But, the central issue of these architectures is the lack of full interoperability of interconnected things in abstraction level. This leads to invoke many proclaimed problems, such as: degraded smartness of high degree, less adaptability, limited anonymity, poor behavior of the system, reduced trust, privacy, and security. IoT architectures do pose several network oriented problems due to its limitation of homogeneity approach. Several institutions, standardization bodies, and researchers are currently engaged with the development of bringing uniformity in the architectures to fulfill the required technological needs. This paper presents a precise picture of the present state-of-the-art in the IoT architectures based on 129 research papers selected for this purpose. More specifically, this article:

- Educates the reader with a state-of-the-art description of domain specific IoT architectures;
- Presents the trends in several sectors of practices;
- Identifies research problems that researchers shall face in near future;
- Provides future directions.

The remainder of the paper is organized as follows. Section 2 presents domain specific state-of-the-art in IoT. Section 3 presents the open research issues associated to IoT architectures and futuristic road map showing Io<*> (Internet of *) concept, on which researchers should focus more in near future.

## 2. Survey on domain specific IoT architectures

This section prescribes the works done so far by the scientists around the globe (Intel research). Various domain specific architectures based on the broad areas, such as: RFID (Marrocco et al., 2009), service oriented architecture, wireless sensor network, supply chain management, industry, healthcare, smart city, logistics, connected living, big data, cloud computing, social computing, and security are described in this section. The selection of theses domains depends upon current scenario of IoT applicability. It is has been tried to incorporate as much directions into this article, but due to the size constraints, present limitations have been made. The key methodology behind the survey depends on few factors of importance where earlier mentioned domains are deeply investigated based on their respective sub domains. This survey is performed to evaluate a number of segregated sub domains to gain and provide significant knowledge on the following: architectural structure, applicability, associativity, deployability, and incorporation measure. A precise, concrete and concise conclusion is made at the end of this article based on the surveyed perception. The overall method behind the survey describes how IoT is applied to the sub domains using particular architectures. Fig. 3 presents the domain tree showing all its leaves as sub domains.

### 2.1. RFID

#### 2.1.1. EPC

The term "IoT" was initially proposed to refer to uniquely identifiable interoperable connected objects with Radio-Frequency IDentification (RFID) technology (Ashton, 2009). Later on researchers did relate IoT with other technologies, such as: sensors, actuators, GPS devices, and mobile devices. The "*thing*" oriented approach of the IoT is in fact attributed by the Auto-ID Labs in early 2000s where IoT has got its original shape. Since its inception, Auto-ID along with EPCglobal targeted to architect the actual model of the IoT. These institutions have normally focused their works on the development of the Electronic Product Code™ (EPC) to necessitate and support the wide spread usage of RFID tags in modern trading network. Industry driven standard such as the EPCglobal Network™ is the outcome of this business. The primary purpose of this kind of industry standard is mainly to get well designed so as to have improvement over the object visibility particularly the location and status aware objects. This is obviously not only the single button of the shirt but from a larger point of view, IoT should not be an infrastructure where an EPC system shall persist just containing RFIDs as the only devices; these are only the tip of the burg, the complete story lies far away!

#### 2.1.2. uID

Unique/Universal/Ubiquitous IDentifier (uID) architecture is another alternative in IoT, the central idea of which is just the incorporation and development of middleware aware (Issarny et al., 2011) deliverables. As per my intervention, the RFID based item traceability as well as addressability is not the notion of the IoT, further it should pave more stringent tasks in case of different objects (Sakamura, 2006).

#### 2.1.3. NFC and other technologies

As per Presser and Gluhak (2009), it has been perceived that the RFID still holds the driving force for IoT. Due to low cost and small size, RFID has dominated the marketing strategy since its origin. However, the authors state that huge pool of heterogeneous devices and network protocols will soon cover up the IoT. As of them, Near Field Communications (NFC), Wireless Sensor and Actuator Networks (WSAN), Wireless Identification and Sensing Platforms (WISP), and RFID together will show a new horizon toward IoT. A United Nations (UN) report has recently informed the fact that mankind is approaching toward a new decade of RFID enabled ubiquitous systems where human being shall be dwarfed by internet oriented objects as they are going to be the majority in number (Botterman, 2009).

Appropriate IoT based modeling may solve the situation by storing and communicating in valuable ways (Toma et al., 2009). In this context, RFID readers and tags (Finkenzeller, 2003) shall consist of new holistic system where each tag may be characterized by a unique identity. These forms of tags are appropriate for monitoring of cattle in far house and for personification of man. RFID reader broadcasts a signal into its periphery that activates the nearby tags to reply using its unique key. Real-time information passing may help in

implementation of rigorous stratification between objects of interest (Kos et al., 2012). RFID tag acts as an ID of concern device where it is attached in form of an adhesive sticker (Jules, 2006). Smaller versions of RFID tags are being currently produced by many manufacturers. Hitachi has developed the smallest version of RFID tag as: 0.15 mm × 0.15 mm × 7.5 μm in dimension recently.

#### 2.1.4. Beyond RFID

Consortium of CASAGRAS has envisaged the concept of IoT to go beyond the concept of RFID in future. As per their published report, things could benefit human being if they are submerged with networks while allowing communicating with other digital devices in the world. CASAGRAS consortium strongly believes in two statements: (a) IoT connects physical and/or virtual objects, and (b) proliferation of IoT into traditional networking systems (Dunkels and Vasseur, 2008). At this point, I apprehend their thought about IoT which shall become an institution which shall perform autonomous services by capturing data from interoperable and transparent networking media. Authors of Broll et al. (2009) propose to integrate NFC around the posters or panels, which provide valuable information about the description, cost, and schedule about transportation system to induce digital marker with help of mobile phones by knowing the facts, such as: ticket availability, seat availability, real-time stoppage information etc. RFID enablement is a keen component of IoT invasion. Which is seconded by Zhangm et al. (2011), that presents RFID based EPC network enabled Representational State Transferful (RESTful) i.e., software architecture for distributed hypermedia systems, IoT platform architecture to validate the usage of REST in IoT domain.

### 2.2. Service oriented architecture

Service oriented architecture (SOA) is an approach which is used to create architecture based on the use of system services. The inbuilt SoA approach is currently being invoked in IoT domain, utilizing the concept of middleware i.e., a software layer superimposed between application and technology layer which hides the unnecessary pertinent details from the developed hence reducing the time of product development, helping the design workflow be simpler to ease the process of marketing the commercial outcomes in short time duration (Deugd et al., 2006).

#### 2.2.1. RFID Involvement

Researchers have developed an RFID-SN i.e., RFID enabled Sensor Network, Buettner et al. (2008) comprising of RFID tag, reader, and computer system for understanding system behavior. *Fosstrak one* has developed a novel RFID related application based on SoA management (Foss track). Scientists have proposed an EPC network (Floerkemeier et al., 2007) configured RFID reader based system by catering multiple data related services on its application layer e.g., aggregation, filtering, lookup and directory service, tag identifier management, and privacy, utilizing the SoA paradigm.

#### 2.2.2. Middleware enablement

A RFID based 3 layered middleware architecture relies on three associative functionalities such as: tag association, the place association, and the antenna association with user (Welbourne et al., 2009). A holistic IoT architecture is proposed that consists of heterogeneous devices, Embedded Internet Systems (EIS), standard communication protocols, and SoA paradigm which utilizes the CoAP protocol and standard services by enabling the exchange of sensor data with an IoT based cloud and a private cloud, while disseminating web based human–machine interface for configuration, monitoring and visualization of structured sensor data (Pereira et al., 2013). The INOX platform (Clayman and Galis, 2011) advocates similar approach which consists of three layers, such as: (a) Service layer – supports and contains the services using APIs, (b) Platform layer – contains necessary management and

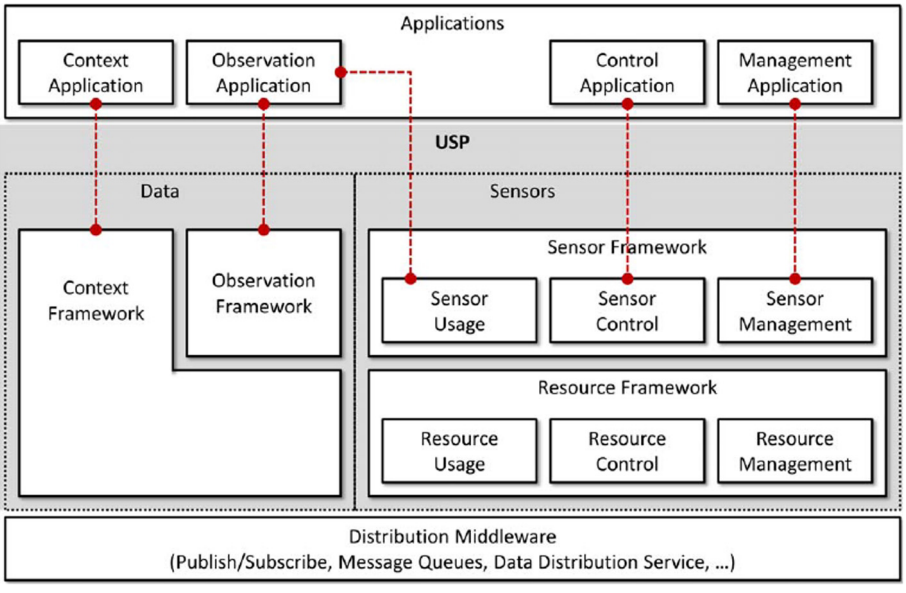


**Figure 4** Stratification in the USP architecture.

orchestration to deploy services and the virtualization technologies enriching hardware layer; and (c) Hardware layer – contains of sensors and smart objects. Article (Pasley, 2005) advocates to reuse inbuilt techniques while composing of hardware and software together at the time of implementing a SoA in the concern setup. A common linkage between the SoA and a middleware has been proposed with an integrated architectural approach, leveraging the advantages of the SoA through enhancement of device functionality, communications, and integrated services (Spiess et al., 2009). An SoA based 5 layered IoT-middleware architecture is shown in Buckl et al. (2009), where objects do lie at the bottom and the object abstraction, service management (provides services like: dynamic discovery, status monitoring, and service configuration of the objects. Semantic (Wahlster, 2008; Vázquez, 2009) operations such as: QoS, lock, police and context management are also performed (Hydra Middleware Project), service composition and application layers are placed just consecutive above of each other. Furthermore a domotic infrastructure which is based on SoA oriented IoT, is developed in the literature where sensor and actuator based automatic energy consumption logic has been implied. In this perspective, the authors of Spiess et al. (2009) and Buckl et al. (2009) have used two advanced computer languages, such as: *Business Process Execution Language* (*BPEL*) (defined as: business processes that interact with external entities through Web Service operations (Web Service Definition Language (WSDL)) (OASIS)) and *Jolie* (target application, specific set of objects or limited geographical scenario) to implement the SoA enabled middleware.

### 2.3. Wireless Sensor Network

Wireless Sensor Network (WSN) (Xia, 2009; Yaacoub et al., 2012) is one of the key parts of IoT system. It consists of a finite number of sensor nodes (mote) mastered by a special purpose node (sink) by employing multi layered protocols organization (Akyildiz et al., 2002). Primarily energy efficiency, scalability, reliability, and robustness etc. parameters are sought when designing a WSN powered system.

#### 2.3.1. Systems

Mostly used WSN systems do incorporate IEEE 802.15.4 protocol for provisioning *Wireless Personal Area Networks* (*WPAN*) for communication purpose (IEEE 802.15). The top layers of inbuilt protocol stacks do necessitate IPv6 addressing facility to enhance the controlling ability of vast number of nodes, while increasing the size of the payload in transmitted packets along with maximized lazy time (sleep) of nodes. It has already been demonstrated by Duquennoy et al. (2009), that implements embedded TCP/IP stacks into the objects e.g., TinyTCP, mIP, and IwIP, which in turn transmits information to a remote server through proxy like interface by employing web sockets.

#### 2.3.2. Environment monitoring

The *e-SENSE* project has employed a WSN by a 3 layered logical approach to provide intelligent support to the user group by application, middleware, and connective measures (Arsénio et al., 2014). *UbiSec&Sens* is another example of WSN based supportive system which is similar to the *e-SENSE* but security layer is added as extra on top of it. Functional design and implementation of a complete WSN platform can be used for monitoring of long-term environmental monitoring based IoT applications (Lazarescu, 2013). The objectives of this design satisfy numerous parameters, such as: cheap structure, enablement of pool of sensors, fast deployment, longevity of device, less maintenance, and high Quality of Service. WSN based application has been devised on agriculture and forestry where IoT plays a key role (Bo and Wang, 2011). An architectural design across the middleware, hardware, and network layer results in a unique WSN platform – "*Sprouts*", which is versatile, open source, and multi-standard in nature (Kouche, 2012). Studies have found the challenges related to the usage of mobile phones as spontaneous gateways of WSNs in IoT systems, by showing the usage of a name-based *Future Internet Architecture* (FIA), while delivering the information of a temperature sensor data from an Android phone directly to multiple applications via in-network multicast over the same network test bed (Li et al., 2013).

#### 2.3.3. Infrastructure Monitoring

IoT based dam safety application – *Tailings Dam Monitoring and Pre-alarm System* – (*TDMPAS*) has been developed and implemented which incorporates cloud services to accomplish with the real-time monitoring of the saturated water line, water level and dam deformation (Enji et al., 2012). *TDMPAS* helps the engineers to acquire cautious alarm information remotely, prior to actual accident which would have been occurred. *Unified Sensing Platform* (*USP*) (Gazis et al., 2013) has been designed as the blueprint of what enables the seamless integration of multi-dissimilar objects and their efficient use by efficient, reusable and context aware way. Authors also present

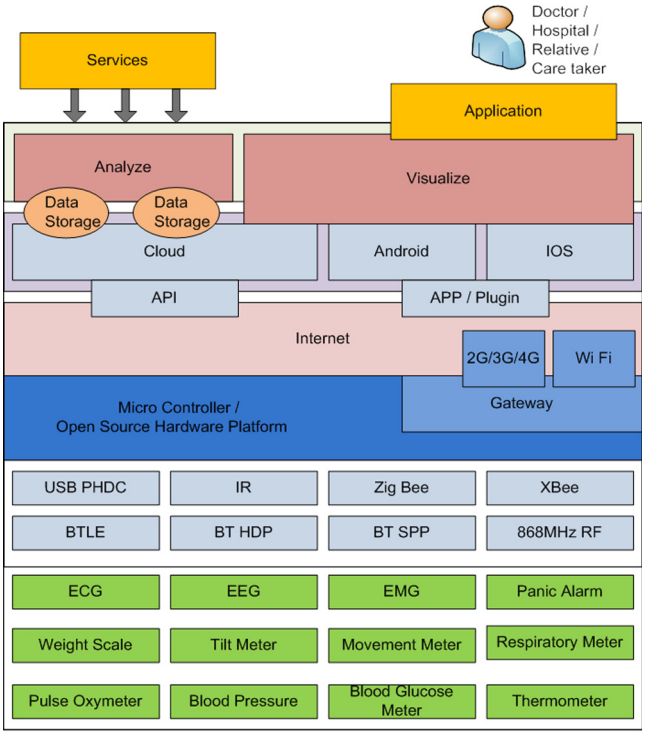


**Figure 5** Home Health Hub IoT ($H^3$IoT) platform.

the 3 layered (distribution middleware, *USP*, and application) *USP* architecture (see Fig. 4) which stratifies publish/subscribe, message queues, data distribution services etc., through data and sensor based *USP* layer. Sensor and resource frameworks perform sensor oriented usage and control operations by efficient resource management catering contextual observation toward various top level applications.

#### 2.3.4. Agriculture

Agriculture based IoT is envisaged by developing a prototype platform (Zhao et al., 2010) that controls network information integration to study the actual situation of agricultural production while operating from a remote location. This study employs WSN as the backbone of the implementation. A recent work has proposed a 6 layered agriculture architecture that incorporates WSN as a subsidiary element to enhance multi-culture analysis, user experience, and predictive analysis (Ray, 2015a).

#### 2.3.5. Aquaculture

An IoT based aquaculture while providing real-time information system called "*E-Nose*" has been developed to pursue the information of water quality via mobile internet and WSN to the users. The system performs forecasting of the change of the trend of water quality based collected data (Ma et al., 2012).

#### 2.3.6. Distributed sensor network

*Emergent Distributed Bio-Organization* (*EDBO*) model is conceived to harness emergent phenomena in *Artificial Distributed Systems* (*ADS*) (Eleftherakis et al., 2015). EDBO nodes are represented by agents – "BioBots" which use two-way relationships to form an overlay network. Each BioBot is capable to handle a limited number of relationships to other BioBots in an autonomous environment. BioBot serves as a wrapper for abstracting, data, functionality, and services based on user queries. It facilitates the propagation of queries through the network in an autonomous manner where its behavior is based on several bio-inspired heuristic mechanisms that helps to participate in decision making. The architecture leverages the combination of multiple BioBot empowered by cyber physical system (CPS) nodes positioned in distributed locations. Users can invoke their requests upon the EDBO which is then processed by collective decisions made by the BioBot with intervention of CPS nodes.

### 2.4. Supply Chain Management and industry

Supply Chain Management (SCM) may be defined as the flow of goods and services while including the movement and storage of raw materials, work-in-process inventory, and finished goods from point of origin to point of consumption.

#### 2.4.1. SoA, RFID, and NFC Integration

SCM related visionary works (Yuan et al., 2007; Dada and Thiesse, 2008) incorporating SoA architecture have been performed where sensor based applications are made in the field of supply chain market providing the quality based perishables items in smarter way. Metro has implemented a commodity based retail support to the customers by integrating RFID technology on top of SoA enabled SCM (METRO Group Future Store Initiative). Research has been started to gain real-time access in SCM empowered ERP systems by involving RFID based NFC solutions (Karpischek et al., 2009). An IoT based real-time sharing architecture for manufacturing industry has been proposed which includes SCM as the central building block (Sun et al., 2011). For instance, Sun et al. (2011) is an IoT based warehouse inventory and SCM information sharing platform system that includes: RFID based storage, position and handheld readers, RFID tags, and similar kind of devices. Supplier, manufacturer, and dealer information oriented servers communicate with loading and inventory workers through the pre-installed database system which occupies the central position in the devised system. A 3 layered (such as: perception layer, network layer, and service layer) IoT based e-commerce architecture is devised to consider active, personalized, and intelligent features to disseminate the user's need and services (Shang et al., 2012). Article Ilic et al. (2009) presents the impact analysis about the efficient Supply Chain Management over the cost of perishable goods at retail. The authors have investigated a novel way to lower down the carbon foot prints in retails by inclusion of sensor based systems into the perishables goods.

#### 2.4.2. SCM as service

*IoT Mashup-as-a-Service* (*IoTMaaS*) (Janggwan et al., 2013) is proposed to comply with heterogeneity of devices by obliging the model driven architecture facilitating SCM for the purpose of making harmony with stakeholders like end users, device manufacturers, and cloud computing providers (Guinard and Vlad, 2009). EPC global object service oriented *Resource Name Service* (*RNS*) (Tian et al., 2012) platform provides equitable name service for the IoT employing resource locating service, auxiliary authentication service, and anti-counterfeiting service to enhance open loop information sharing between numerous IoT components in industry and related applications, especially for SCM framework. *Business Operation Support Platforms* (*BOSP*) have been developed which focuses on carriers that play lead role in IoT industry chain. The given 3 layered architecture is made of access layer, devices management layer, and ability formation layer; fulfilling the technicalities such as multi network, device control, application specific jobs orientation to the system (Xiaocong and Jidong, 2010).

### 2.5. Health care

Recently, smart healthcare system development and dissemination has become possible by the convergence of various IoT architectures.

#### 2.5.1. Home health care

Authors have proposed *iHome Health-IoT platform* for in-home health care services based on the IoT; illustrating a 3 layered open-platform based *intelligent medicine box* (*iMedBox*) to pursue various medical facilities integrated with sensors, devices, and communicate by means of WAN, GPRS, and/or 3G (Yang et al., 2014). Services like *intelligent pharmaceutical packaging* (*iMedPack*) is enabled by RFID and actuation capability which are enabled by functional materials, flexible, and wearable *bio-medical sensor device* (*Bio-Patch*). Bio-Patch takes decision when to call remote physician, emergency center, hospital, test clinic, and supply chain medicine retailers.

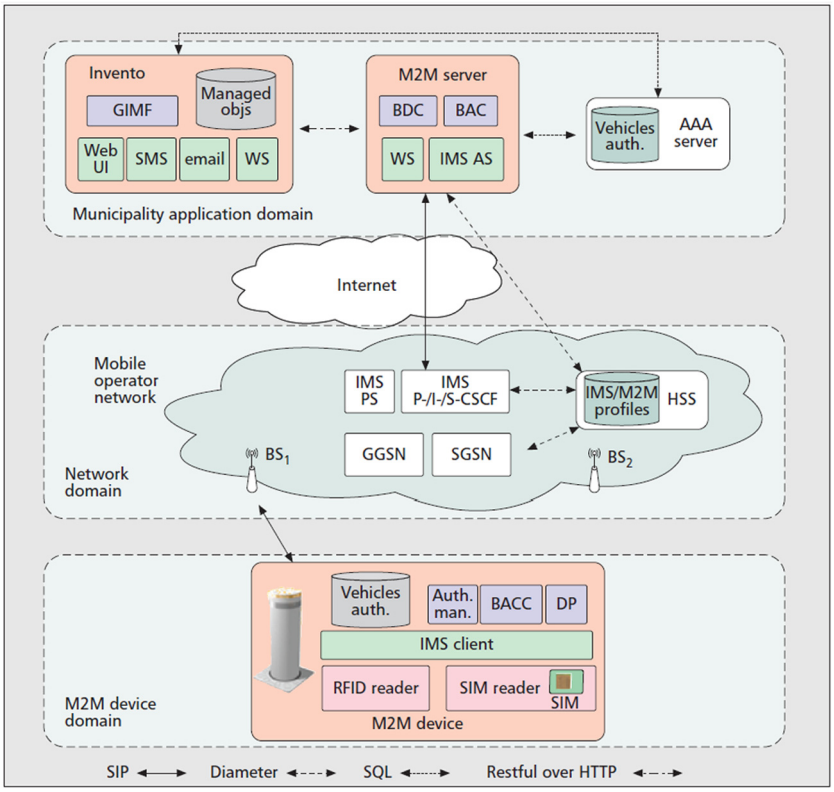


**Figure 6** M2M-based distributed architecture.

Sebastian and Ray (2015a) presents a novel IoT based architecture for finding home health status by informing residents the critical notions of the house. Few frameworks monitor health of elderly people by utilizing standardized technologies is presented (Ray, 2014a,b).

Sebastian and Ray (2015b) elaborates the architecture of IoT in sports especially based on soccer where heath care is given the most priority. Model driven tree and generalized domain model architectures are consecutively appeared in Ray et al. (2013) and Rai et al. (2013) to solve heath and related issues in real life.

Home Health Hub Internet of Things ($H^3$IoT) is designed to disseminate the health care of elderly people at home (see Fig. 5) (Ray, 2014a). It is a 5-layered approach (i.e. Physiological Sensing Layer (PSL), Local Communication Layer (LCL), Information Processing Layer (IPL), Internet Application Layer (IAL), and User Application Layer (UAL)) to assess and monitor the physiological changes of elderly and take subsequent actions for further health check up by doctor and acre givers.

### 2.5.2. e-Health

A privacy preservation framework (Ukil et al., 2012) provides a negotiation based architecture to find a solution for utility-privacy trade-off in IoT data management, especially in *e-health* domain. Authors also report on the usage of the MB2 abstractions and how the implementation needs to be evolved over time to the current design to tackle with health issues (Blackstock et al., 2010).

### 2.5.3. m-Health

An amalgamated concept of *Internet of m-health Things* (*m-IoT*) is provided by introducing the 4G based health applications for non-invasive glucose level sensing with advanced opto-physiological assessment technique and diabetes management (Istepanian et al., 2011).

### 2.5.4. Ubiquitous health

Investigation toward a semantic data model to store and interpret IoT data on a resource-based data accessing method (*UDA-IoT*), to acquire and process medical data ubiquitously to improve the accessibility to IoT data resources have been made (Boyi et al., 2014). The presented concept is studied around the emergency medical services scenario. Various paths for conjugation between cloud computing and IoT for efficient managing and processing of sensor data by wearable health care sensors are in practice that demonstrates IoT application on pervasive health care (Doukas and Maglogiannis, 2012).

### 2.5.5. Hospital management

IoT based architecture (Yu et al., 2012) of smart hospital is implemented to improve efficacy of present hospital information system, such as: fixed information point, inflexible networking mode, and related parameters. *Automating Design Methodology* (*ADM*) system for smart rehabilitation of old age population is devised by a group of researchers (Fan et al., 2014). Such kind of ontology based platform creates a rehabilitation strategy and reconfigures the medical resources

according to patients' specific requirements quickly and automatically.

#### 2.5.6. WSN integration

A WSN based remote identification system has been designed using the *Android Study of Internet of Things* (*HCIOT*) platform in "Community Health" to employ the concept of IoT together with an improved *Particle Swarm Optimization* (*PSO*) method to efficiently enhance physiological multi-sensors data fusion measurement precision (Sung and Chiang, 2012).

### 2.6. Smart Society

Present world can be molded into a well connected smart society by leveraging innovative architectural concepts of IoT. This section unfolds the research works performed to carry the world into a smart place to live through smart city, developed logistics and smart living formulations.

#### 2.6.1. Road condition monitoring

Road condition monitoring and alert generation (Ghose et al., 2012) has been done using the in-vehicle Smartphone as connected sensors, to an IoT platform, while providing a novel e nergy-efficient-phone-orientation-agnostic accelerometer analytics in phone authentic road condition mapping employing privacy concern. At the same time, the HyperCat IoT catalog specification (Blackstock and Lea, 2014) is prescribed as the tool to adapt an IoT platform by providing an IoT hub focused on the highways industry called "*Smart Streets*" which paves a new dimension to set an interoperable IoT ecosystem in near future.

#### 2.6.2. Traffic management

Investigations have been conformed (Foschini et al., 2011) to seek the possibility of implementing Machine-to-Machine (M2M) solutions in the field of road traffic management that integrates *IP Multimedia Subsystem* (*IMS*) i.e., it realizes the advanced service management platforms able to integrate different infrastructures and service components according to specific application domain requirements, based service infrastructure. Vehicular network using IoT based middleware (Wang et al., 2011) has been introduced to efficiently manage on road vehicles.

#### 2.6.3. Municipal involvement

A 3 layered M2M-based management platform (see Fig. 6) based distributed architecture is proposed for municipality application domain (Foschini et al., 2011). Authors have truly utilized numerous terms to mention the architecture, such as: *GIMF*: Geospatial information management framework, *Web UI*: Web user interface, BAC: Bollard authorization component, *IMS PS*: IMS presence server, *IMS P-/I-/S-CSCF*: IMS proxy-/interrogating-/serving-call session control function, *BN*: Base node, *SGSN*: Serving GPRS support node, *BACC*: Bollard actuator control component, *WS*: Web services, *BDC*: Bollard diagnosis component, *IMS AS*: IMS application server, HSS: Home subscriber server, *GGSN*: Gateway GPRS support node, and *DP*: Diagnosis procedure. Device, network and application layers cumulate the overall concept behind their approach. Session Initiation Protocol (SIP) (extensions specified by the Internet Engineering Task Force (IETF) and 3GPP IMS-related standards) controls the IMS client as the session control endpoint, and participates in session setup and management.

#### 2.6.4. Link data for society

Peer focus has been kept on the communication and networking aspects of the devices that are used for sensing and measurement of the real world objects (De et al., 2012; Kortuem et al., 2010). The presented semantically modeled linked data architecture performs the connectivity between IoT instances of objects to the web resources which supports the publication of extensible and interoperable descriptions in the form of linked data.

#### 2.6.5. Smart city

A smart city experiment (Sancheza et al., 2014) describes the deployment and experimentation architecture of the large scale IoT experimentation at the "Santander city". The same has been presented as a three-tier architecture consisting of an *IoT device tier*, an *IoT gateway* (*GW*) tier and server tier to facilitate the *SmartSantander* infrastructure. The *IoT node tier* consisting of IoT devices with less resource, less processing power and less power consumable capability. The *IoT gateway node tier* links the IoT devices at the edges of the network to a core network infrastructure in a remotely programmable manner. The devices in this layer are more resource oriented but lesser than the server layer. The *server tier* hosts data repository functionality. This layer is most powerful of all three, in terms of heavy computing machineries, capability for real world data mining, knowledge engineering, and visualization in cloud infrastructure.

An evaluation framework for IoT platforms has recently been devised by using the publicly available information about the platforms' features and supporting services for smart city (Mazhelis and Tyrvainen, 2014). To enable the implementation of a generalized smart city solution, an M2 M communication platform is addressed to comply with the requirements and design aspects of a reference as an enabler for Smart Cities (Elmangoush et al., 2013). An IoT centric novel model of smart city has been introduced (Ganche et al., 2013) where a top-down architectural principle is followed to mandate the overall uniformity. A recent publication introduces a federated S*mart City Platform* (*SCP*) developed in the context of the ALMANAC FP7 EU project. The article further discusses on the lessons learned during their initial experimental application of the SCP to a smart waste management scenario in a European city (Bonino et al., 2015). The ALMANAC SCP is aimed at integrating IoT, capillary networks, and metro access to deliver smart services to the citizens of the subject area. The key element of the employed SCP is a "middleware" that supports functionalities, such as: semantic interoperability between heterogeneous resources, devices, services, and data management. The proposed platform is built upon a dynamic federation of private and public networks while supporting *End-to-End* security that enables the integration of services.

#### 2.6.6. Urban management

A novel IoT-LAB test bed (Papadopoulos et al., 2013) highlights the experimentations that can significantly improve the

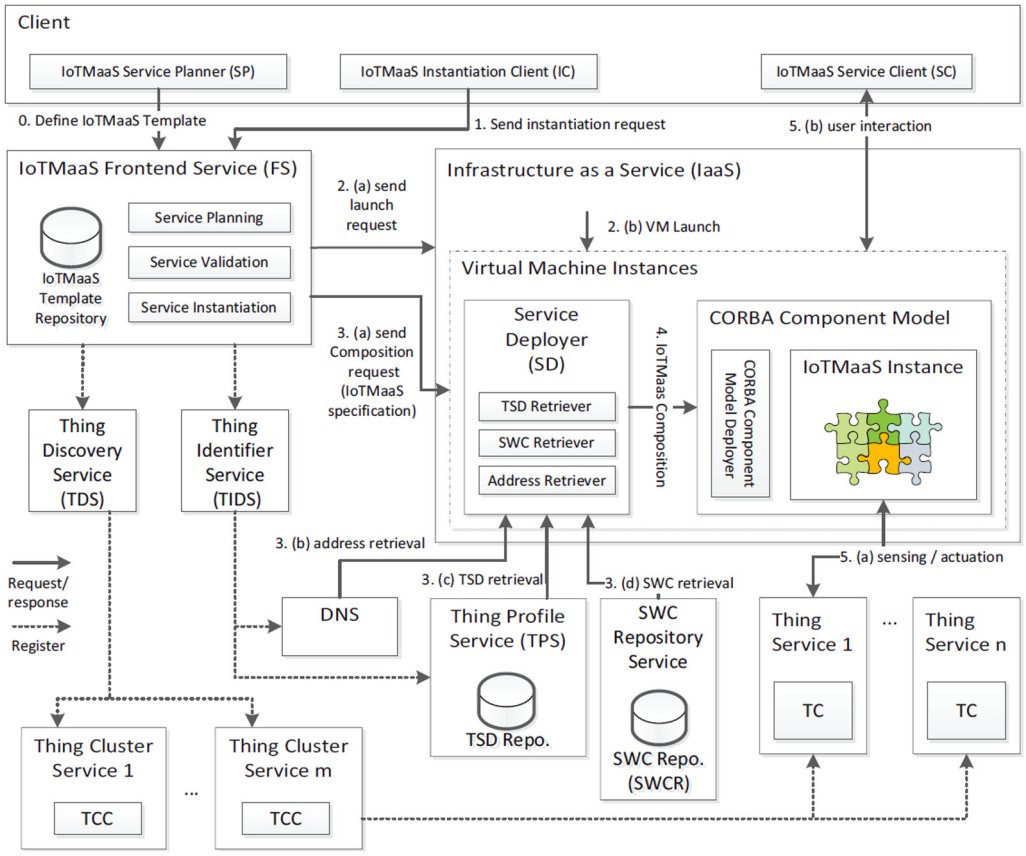


**Figure 7** An architecture to serve IoTMaaS.

value of performance evaluation campaigns through the experiments satisfying proof-of-concept validator. The main target is to test the significance of the underlying architecture whether it is suitable for smart employability or not. *Urban Information System* (*UIS*) (Jina et al., 2014) is a platform for the realization of IoT based smart cities enabled with smart sensors and networking support materialized through data management and cloud based integration to form a transformational part of the existing cyber physical system while employing noise mapping in proper fashion. Researchers have developed a unified smart platform based on the "Google Map" to integrate a Geo-IoT application – Remote Digital Home Control (Dayu et al., 2010).

### 2.6.7. *Accidental measures*

An IoT based emergency management system has been proposed (Zhang and Anwen, 2010) which handles the catastrophic events in a specialized way.

### 2.6.8. *Smart cycling*

SENSAPP (Mosser et al., 2012) is designed as a prototypical cloud open-source service based application to store and exploit data collected by the IoT. The coarse-grained point of view clearly states that sensor architect and data miner software process the IoT data collected from sensor attached with a bi-cycle. The database and functional registry system cope up with notification related tasks. User can easily access and utilize the information remotely using third party software.

### 2.6.9. *Smart sports*

A generic Internet of Things architecture for smart sports-"Internet of Things Sport" has been proposed to facilitate integrated interactions between sports persons, sports objects, team owner, medical teams, and followers (Ray, 2015b).

### 2.6.10. *Home entertainment*

Television is a media of entertainment at home. A group of researchers (Kos et al., 2013) have developed a system for generating lightning fast reports from intelligent IoT based network communication platform, correlating the real-time DSL access line and IPTV together. A RESTful Web Service having unique URI address to implement applications like: environmental perception and vehicular networks implying physical and virtual objects. IoT enabled real-time multimedia often use User Data Protocol (UDP) for transmission of data which makes huge amount of packet loss due to network congestion and channel noise. To counter this (Jiang and Meng, 2012) has developed an IoT oriented architectural platform to solve the front end bandwidth using a novel multimedia transmission protocol over UDP. An open source solution has also been proposed (Lin, 2013) where Arduino based hardware platform is used for proper functioning of a smart home, which is an example of a typical cyber physical system, consists of input, output and energy monitoring activities. IoT cloud platform is also integrated with the implemented setup.

#### 2.6.11. Smart logistics

Railways are the heart of any logistics. An IoT based intelligent identification system for railway logistics has been proposed for efficient logistics management (Guoa et al., 2012).

#### 2.6.12. Smart tourism

Tourism and smart city have come together with help of IoT in China as presented in a recent literature (Guo et al., 2014). Architectural concept behind IoT based tourism is a novel approach which is artistically evolved from it.

#### 2.6.13. Smart environment

Authors (López-de-Ipiña et al., 2007) have observed the interaction between objects of spatial regions with pertinent mobile devices, while enabling multi-modal human to environment interaction for sake of advanced context-aware (location, identity, preferences) data and service discovery. This also implies on the filtering and consumption within both indoor and outdoor environments by fostering web as an application programing platform where external parties may create mash-ups while mixing the functionality offered by users.

A recent research has demonstrated a novel architectural approach to acquire and analyze thermal comfort of a human by means of MISSENARD Index (Ray, 2016).

#### 2.6.14. m-Learning

A functional model is proposed to cater the needs of futuristic mobile-learning (m-learning) through IoT (Yang et al., 2011). While discussing, authors envisage a technology transfer model that may be leveraged by 4 factors, such as:

(a) Creating optimal learning environment for m-learning, (b) providing mass resources for m-learning, (c) making individual service of m-learning, and (d) enriching evaluation method. *m-learning mode based on Internet of Things*(*IOT-ML*) architecture is given by the authors that has the capabilities to perform several tasks like: preliminary analysis, creation of learning situation, acquiring learning resources, and evaluating the learning infrastructure by taking rigorous feedback and push/pull based learning environment.

### 2.7. Cloud service and management

This section provides the architectural solutions paved to encounter cloud computing and big data problems. Cloud computing provides platform, infrastructure, and software as a service to the client systems for managing, accessing, and processing purpose ordinarily in form of pay-as-you go, or free (Islam et al., 2013; Rao et al., 2012).

#### 2.7.1. Information exchange cloud

A recently deployed IoT broker system (Leu et al., 2013) functions as an information exchange center, relaying periodic messages from heterogeneous sensor devices to IoT clients to enhance shortest processing time (SPT) algorithm for scheduling web based IoT messages by implementing priority queue model.

#### 2.7.2. Vehicular cloud

A newly proposed vehicular cloud platform provides vehicular cloud data services incorporating an intelligent parking cloud service and a vehicular data mining cloud service for vehicle warranty analysis (He et al., 2014).

#### 2.7.3. Cloud infrastructure

The Global ICT Standardization Forum for India (GISFI) Sivabalan et al., 2013 while designing of IoT framework pressurized on well defined Reference Architecture (RA) for enhancing interoperability between various devices and application in multi-vendor scenario incorporating distributed cloud infrastructure.

#### 2.7.4. Context aware services

A data acquisition and integration platform (Chen and Chen, 2012) based on IoT is proposed where context-oriented approaches have been used to collect sensor data from various sensor devices. Authors have developed to a mechanism to produce context data with help of the devised context broker, which retrieves data from the IoT repository as a contextual portfolio, which is annotated with semantic description. It

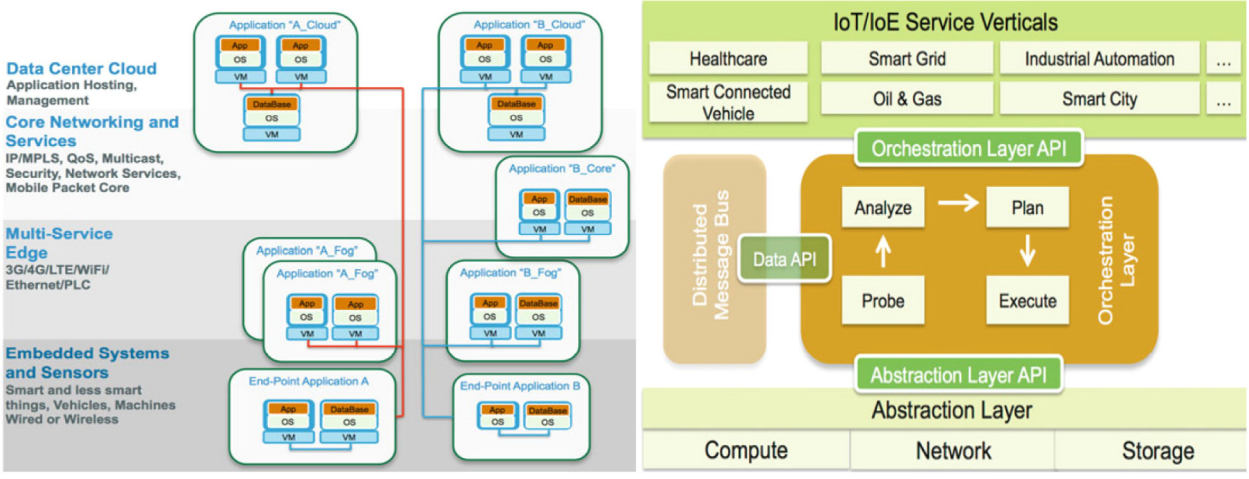


**Figure 8** Distributed IoT/IoE applications on the fog infrastructure (left), and components of fog architecture (right).

depicts the interrelationship between clients, thing server, thing cluster, IoTMaaS Frontend Service, IaaS, and VMI whereas device identifier services are keen to hold the request/response and registry enrollment activities. CORBA component model and service deployment are the heart of VMI which caters the sensing, SWC and TDS retrieval (see Fig. 7).

#### 2.7.5. IoT as a Service

*IoT Platform as a Service* (*IoTPaaS*) framework (Fei et al., 2013) provides essential platform services for IoT solutions by providing efficient delivery to the extend the virtual vertical services by leveraging core computing resources and advanced middleware (Katasonov et al., 2008) services on the cloud. Collected sensor data is transmitted to remote IoT cloud platforms through a gateway which is a layer of various network protocols. Retail billing and related financial processes can easily be metered with IoT PaaS by consisting a nexus of application context management which is governed by allowing data flow, monitored by event processing, data services, and tenant management. An IoT based ETSI M2M (Lin et al., 2013) architecture-compliant service platform has been developed which charters the users with the tasks of developing various M2M applications on OpenMTC (from FOKUS) to investigate the usefulness of the service platform for IoT/M2M. Unique addressing schemes and unified communication mechanism are two basic issues for any IoT structure.

#### 2.7.6. Location aware service

Domain mediators and IoT resource management services are responsible for transferring of devices massages, monitoring of object status, and registering into the system. The *Mobility First Future Internet Architecture* (*MFFIA*) is an ideal platform for realizing pervasive computing (location awareness) in IoT. Particularly when it is necessary to build proper blocks of applications in terms of identity based routing, overloaded identities, content caching, and in network compute plane (Li et al., 2012).

#### 2.7.7. Cognitive service

IoT based Cognitive management framework paves the ability of self-management functionality and knowledge acquisition through machine learning motivated by designating objectives, constraints, and rules (Foteinos et al., 2013). Web2.0 enabled ubiquitous "*Living Lab*" platform necessitates rich and complex ecosystem sensor-based information sources and mobile services to the users (Tang et al., 2010).

#### 2.7.8. Control service

Along with condition, advent of IoT along with cheap sensor enabled devices, huge amount of heterogeneous sensor data are being generated each and every moment of time. This had led scientists to develop *Service-Controlled Networking* (*SCN*) (Sowe et al., 2014) with cloud computing as its core, so as to pave the practical use of the collected sensor data and manage the IoT communities to search, find, and utilize their sensor data on the system dashboard.

#### 2.7.9. Sensor discovery service

Recently a "*SmartLink*" (Perera et al., 2014) has been proposed that can be used to discover and configure sensors by discovering in a particular location. Further, it establishes a direct connection between the sensor hardware and cloud-based IoT middleware using plug-in based approach. Researchers have employed "*TOSCA*" cloud service to

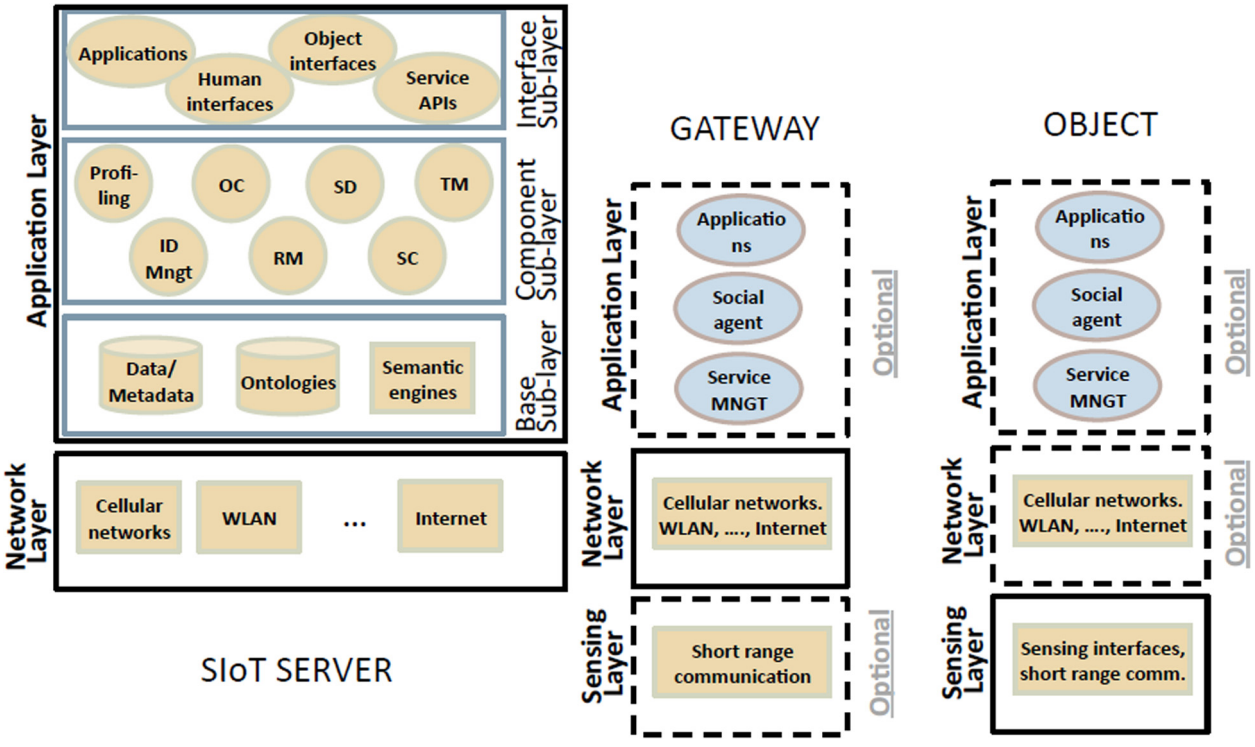


**Figure 9** Social IoT architecture, following the three layer model made of the sensing, network, and application layer.

systematically specify the components and configurations of IoT applications which can be automated in heterogeneous IoT system environments (Fei et al., 2013). In this context, the *Web Ecosystem of Physical Devices* (*EcoDiF*) platform (Pires et al., 2014) integrates heterogeneous physical devices in order to provide support to real-time data control, visualization, processing, and storage. EcoDiF uses web protocols such as: HTTP, REST, EEML, and EMML while implementing the underneath structure.

#### *2.7.10. Fog computing*

Fig. 8 (see Left) presents multi tenant IoT-Fog architecture (Bonomi et al., 2014) with suitable applications A and B. Distributed application for A has one cloud and two "Fog" (Bonomi et al., 2012) components. Similarly, the application for B has one cloud component, one core component and a "Fog" component. Both the parts are connected by a virtual network complying computing, storage (Virtual File System, Virtual Block/Object Store) and networking (Network Virtualization Infrastructure). Fig. 5 (see Right) is the diagrammatic orientation of a 3 layered "Fog" architecture. Abstract layer is specific to the computing, networking and storage activities leveraging abstraction API which communicates with orchestration layer consisting of distributed massage bus structure talks to it via probing, analyzing, planning and executing. The top most is the service layer, designed for user purposes culminating various applications, such as: smart healthcare, grid, and vehicle etc.

#### *2.7.11. Big data*

IoT architectures generate different types of data in large volume at very high speed. This "Big Data" problem is suitably encountered by a recent development (Jiang et al., 2014). It proposes a data storage framework to store integrating both structured and unstructured IoT dependent data. The novel architecture combines "Hadoop" along with multiple other databases to create a distributed file repository to store and efficiently manage various types of data collected by sensors and RFID readers. This architecture technically incorporates the Big Data concept in its backbone. The 6 layered architecture places heterogeneous devices which reside at the bottom whereas database systems, such as: Hadoop, NoSQL, and Relational database cover the next higher layer. Data and file repositories are placed on top of it, leveraging multi tenant and version management, object mapping along with database connectivity. Resource configuration nodule layer configures various resource accessories and meta models. Service management layer provides service generation activities besides RESTful API and URIs. The top most layer is the application layer which caters the direct user experience with the contents collected by devices and represented in knowledge oriented manner to the users.

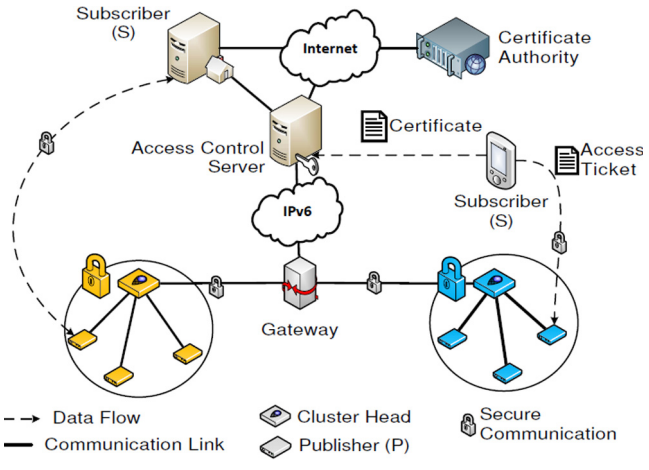


**Figure 10** DTLS employed End-to End security architecture.

#### *2.7.12. Data filtering*

Now the problem is how to manage the data generated from large number of sensors in and IoT based system? The answer is provided by a group of researchers by means of addressing the contextual parameters along with the particular data for which the analytics if necessary (Narendra et al., 2015). Authors propose an architecture that aggregates data filtering, transforming, and integration approach together. They present a warehouse-based data model for specifying the data needed at particular points of granularity and frequency that drive data storage and representation which is aligned with the defined Semantic Sensor Network (SSN) *Ontology*.

### *2.8. Social computing*

These sections present different aspects of social computing currently being sought by IoT. Social IoT is a novel area of research that seeks to indentify and harness the qualitative and behavioral values from robotic things while implementation social rules upon them.

#### *2.8.1. SIOT*

Social Internet of Things-SIoT (Girau et al., 2013; Atzori et al., 2012) is proposed to seek various functionalities, such as: registration for a new social object to the platform, managing the system creation of new relationships, and creation of devices groups. This is innovative approach to integrated IoT with societal elements. Similar comprehension is seen through an open service framework for the Internet of Things which facilitates the IoT-related mass market by establishing a global IoT ecosystem with use of IoT devices and software (Kim and Lee, 2014). Atzori et al. (2011) has designed an architecture of social network of intelligent objects-Social Internet of Things (SIoT), where objects establish social relationships among each other by enabling the capability of discovery, selection, and particular services.

#### *2.8.2. Societal data service*

An open community-oriented platform has been investigated to support *Sensor Data-as-a-Service* (*SDaaS*) featuring interoperability and reusability of heterogeneous sensor data and data services (Zhang et al., 2013). The concept behind virtual sensors and virtual devices are also identified to stream data continuously or discretely by scalable and context aware reconfigurable sensor data and services. A three layer architectural model for IoT is presented in Buckl et al. (2009) (see Fig. 9). It consists of: (a) the sensing layer, which is devoted

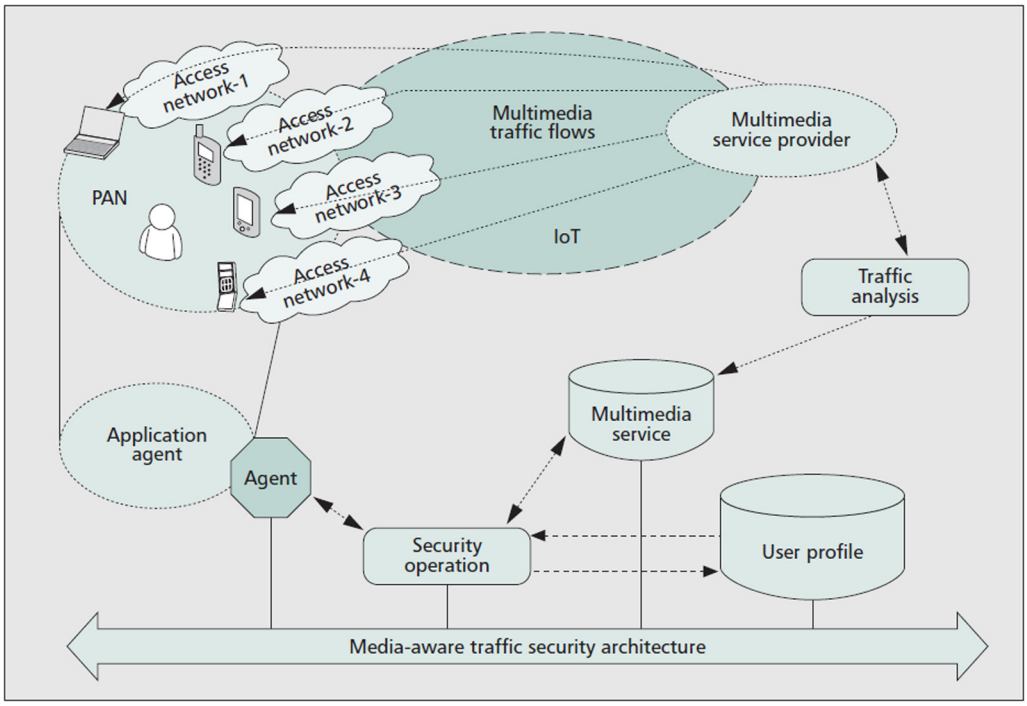


**Figure 11** MTSA architecture.

to the data acquisition and node collaboration in short range and local networks; (b) the network layer, which is aimed at transferring data across different networks; and (c) the application layer, where the IoT applications are deployed together with the middleware functionalities. The Component Sublayer includes the important tools to implement the core functionality of the SIoT system. The ID management is aimed at assigning an ID used to universally identify all the possible categories of objects. The profiling is targeted at configuring manual and semi-automatic information about the objects. The Owner Control (OC) module enables the definition of the activities that can be performed by the object. The relationship management (RM) is a key module since the objects do not have the intelligence of humans in selecting the friendships. Main task of this component is to allow objects to begin, update, and terminate their relationships with other objects. The Service Discovery (SD) is aimed at finding objects that can provide the required service in the same way humans seek for friendships and for any information in the social networking services. The service composition (SC) module enables the interaction between objects. The main potential in deploying SIoT is its capability to foster such an information retrieval. Leveraging on the object relationships, the service discovery procedure finds the desired service, which is then activated by means of this component. The Trustworthiness Management (TM) component is aimed at understanding how the information provided by other members shall be processed. Reliability is built on the basis of the behavior of the object and is strictly related to the relationship management module. Trustworthiness can be estimated by using notions well-known in the literature which are crucial in social networks. The third sub-layer is the Interface Sub-layer that is located where the third party interfaces to objects, humans, and services are located.

### *2.9. Security*

Security issue has always been an area where network related researchers are continuously striving to get through. IoT is not out of its scope. In this section a few relevant works are presented to cope up with architectural issues in IoT based security.

#### *2.9.1. Object security*

Vucinic et al. propose an architecture that leverages the security concepts both from content-centric and traditional connection-oriented approaches (Vučini'c et al., 2014). It relies on secure channels established by means of (D)TLS for key exchange, without inclusion of the "state" among communicating entities. *Object-based Security Architecture* (*OSCAR*) supports facilities such as: caching and multicast, and does not affect the radio duty-cycling operation of constrained objects while providing a mechanism to protect from replay attacks by coupling DTLS scheme with the CoAP. Authors evaluate OSCAR in two cases: (a) 802.15.4 Low Power enabled Lossy Networks (LLN), and (b) Machine-to-Machine (M2M) communication for two different hardware platforms and MAC layers on a real test bed using the Cooja emulator. The architecture has been evaluated under a smart city paradigm.

#### *2.9.2. End-to-End security*

An End-to-End two way authentication security architecture for the IoT, using the Datagram Transport Layer Security (DTLS) protocol has been evaluated (Kothmay et al., 2012). The proposed security architecture (see Fig. 10) is based on the most widely used public key cryptography technique (RSA), and works on top of standard low power communica-

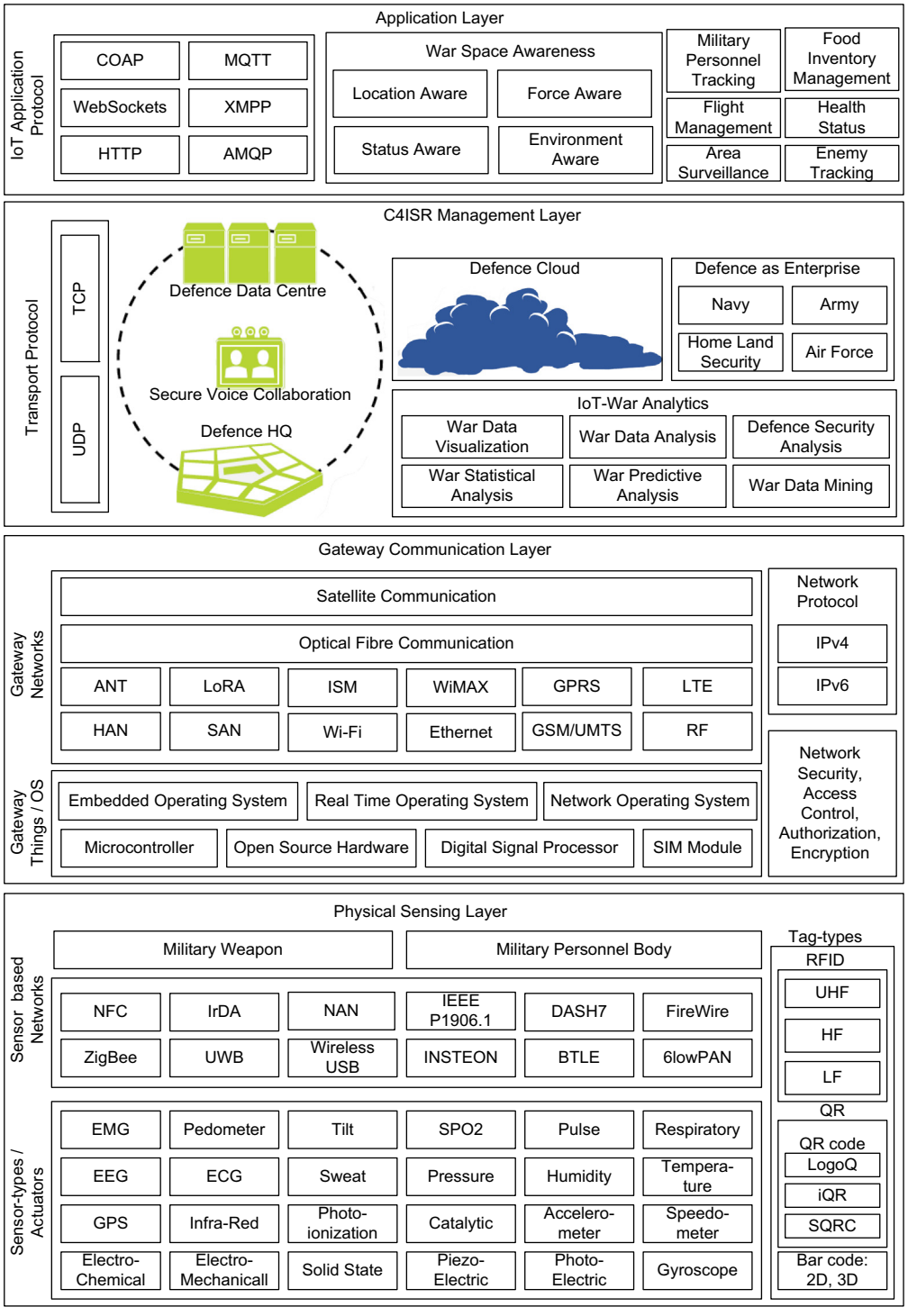


**Figure 12** IoTNetWar architectural framework.

tion stacks. Internet is connected by IPv6 in the near future, and parts of it run the 6LoWPAN. The transport layer in 6LoWPAN is UDP which can be considered unreliable; the routing layer is RPL, or Hydro. Hydro is used for routing, because of its similarity to RPL and its availability as part of the TinyOS 2.x distribution. IEEE 802.15.4 is used for the physical and MAC layer. Based on this protocol stack DTLS is chosen as the key security protocol. This places it in the application layer on top of the UDP transport layer. The prescribed architecture elaborates the underlying data and communication flow between subscriber, gateway, access control server, and internet enabled certificate authority.

### *2.9.3. Cyber-physical-social security*

A cyber-physical-social based security architecture (IPM) is proposed to deal with Information, Physical, and Management

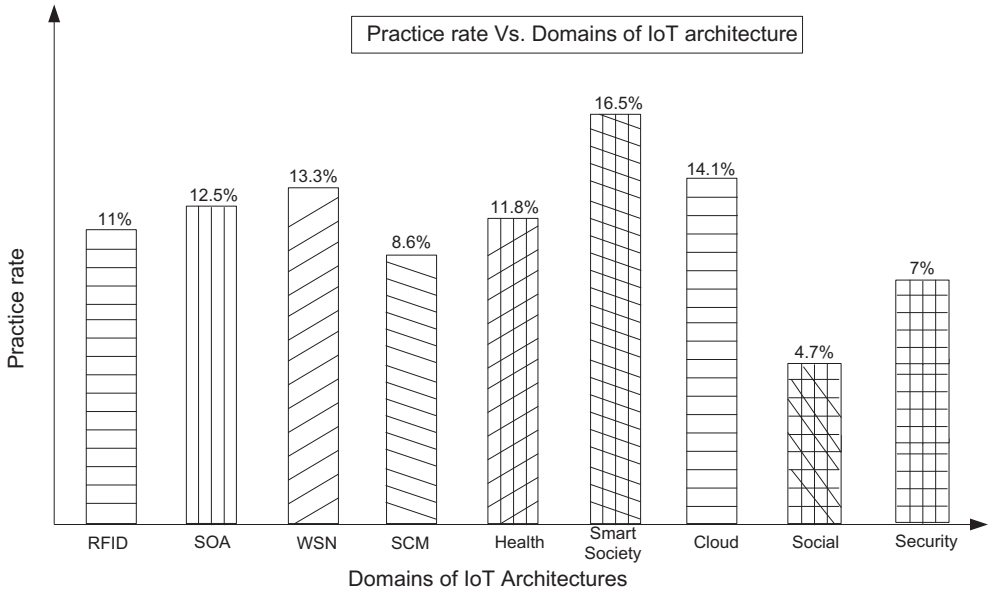


**Figure 13** Practice chart of domains of IoT.

security perspectives (Ning and Liu, 2012). The IPM architecture is empowered by the *Unit IoT and Ubiquitous IoT* (*U2IoT*) architecture. U2IoT acts as the core of IPM provisioning three key supports, such as: establishing information security model to describe the mapping relations among U2IoT, security layer, and security requirement in which social layer and additional intelligence and compatibility properties are infused into IPM; referring physical security to the external context and inherent infrastructure are inspired by artificial immune algorithms; and suggesting recommended security strategies for social management control.

### *2.9.4. Hierarchical security*

Authors propose hierarchical security architecture to protect against inherent openness, heterogeneity, and terminal vulnerability. The proposed architecture aims to improve the efficiency, reliability, and controllability of the entire security system. Authors investigate several types of attacks and threats that may diffuse the architecture. To oppose vulnerability, a coarse-grained security cell is designed that along with a refined secure subject protects the IoT enabled system in the form of information, data, control, and behavior. The 3-layered architecture devises a vertical division that narrows down the complexity of the cross-layer security interaction, and the transverse division based on data flow while clearing the processing logic of the security mechanism (Zhang and Qu, 2013).

### *2.9.5. Multimedia traffic security*

An efficient *Media-aware Traffic Security Architecture* (*MTSA*) is proposed that facilitates various multimedia applications in the Internet of Things (Zhou and Chao, 2011). MTSA sacrifices unconditional secrecy to facilitate a normalized multimedia security solution for all genres of sensors in IoT. In particular, MTSA employs a visual secrecy measure which degrades proportionally to the number of shares in a possession of an eavesdropper. MTSA is enabled with perceived multimedia distortion (Zhao et al., 2009; Kundur et al., 2008) techniques. The MTSA reduces the complexity of multimedia computations and decreases the size of the shares (see Fig. 11). MTSA is inherited from a context-aware multimedia service based security framework (Zhou et al., 2010).

### *2.9.6. Light wight security*

A recent article presents comprehensive and lightweight security architecture to secure the IoT throughout the lifecycle of a device – "HIMMO". HIMMO relies on the lightweight scheme as its building block. It is not only efficient resource-wise, but also enables advanced IoT protocols and deployments. HIMMO based security architecture can be easily integrated in existing communication protocols such as IEEE 802.15.4, or OMA LWM2M while providing a number of advantages such as: performance and operation. HIMMO is featured by a few advancements such as: full collusion resistance, device and back-end authentication and verification, pair-wise key agreement, support for multiple TTPs and key escrow, or protection against DoS attacks (Morchon et al., 2016).

### *2.9.7. Defense*

A novel architectural approach-IoTNetWar (see Fig. 12) has been proposed of inculcating advanced network based technologies into the defense (Ray, 2015a). This is a 4-layered (i.e. Physical Sensing Layer, Gateway Communication Layer, C4ISR Management Layer, and Application Layer) invasion designed to assimilate IoT based integrated military communication, intellectual intelligence, and C4ISR command under one roof. C4ISR Layer is the most crucial of all that specifically monitors the interactions between defense head quarter with its data center through voice collaborative support.

**Table 4** Conglomeration of domain specific architectures.

| Domains | Architecture references | | | | | | |
|---|---|---|---|---|---|---|---|
| RFID (Marrocco et al., 2009) | EPC (Auto-Id Labs; The EPCglobal Architecture Framework, 2009; Ashton, 2009) | uID (Sakamura, 2006; Issarny et al., 2011) | | NFC and Other Technologies (Presser and Gluhak, 2009; Botterman, 2009; Toma et al., 2009; Finkenzeller, 2003; Jules, 2006; Kos et al., 2012) | | Beyond RFID (Dunkels and Vasseur, 2008; Broll et al., 2009; Zhangm et al., 2011) | |
| Service Oriented Architecture (Deugd et al., 2006) | RFID Involvement (Buettner et al., 2008; Foss track; Floerkemeier et al., 2007) | Middleware Enablement (Wahlster, 2008; Vázquez, 2009; Pasley, 2005; Spiess et al., 2009; Buckl et al., 2009; OASIS; Middleware Project; Welbourne et al., 2009; Pereira et al., 2013; Clayman and Galis, 2011) | | | | | |
| Wireless Sensor Network (Middleware Project; Xia, 2009; Yaacoub et al., 2012) | Systems (IEEE 802.15; Duquennoy et al., 2009) | Environment Monitoring (e-Sense; Ubi e-Sense; Lazarescu, 2013; Bo and Wang, 2011; Kouche, 2012; Li et al., 2013; Arsénio et al., 2014) | | Infrastructure Monitoring (Enji et al., 2012; Gazis et al., 2013) | Agriculture (Zhao et al., 2010, Ray, 2017) | Aquaculture (Ma et al., 2012) | Distributed Sensor Network (Eleftherakis et al., 2015) |
| Supply Chain Management and Industry | SoA, RFID, and NFC Integration (Yuan et al., 2007; Group Future Store Initiative; Karpischek et al., 2009; Broll et al., 2009; Ilic et al., 2009; Dada and Thiesse, 2008; Sun et al., 2011; Shang et al., 2012; Metro) | | | | SCM as Service (Guinard and Vlad, 2009; Xiaocong and Jidong, 2010; Janggwan et al., 2013; Tian et al., 2012) | | |
| Health Care | Home Health Care (Sebastian and Ray, 2015a,b; Ray, 2014a, b; Ray et al., 2013; Rai et al., 2013; Yang et al., 2014) | e-Health (Ukil et al., 2012; Blackstock et al., 2010) | m-Health (Istepanian et al., 2011) | Ubiquitous Health (Boyi et al., 2014; Doukas and Maglogiannis, 2012) | Hospital Management (Yu et al., 2012; Fan et al., 2014) | | WSN Integration (Sung and Chiang, 2012) |
| Smart Society | Road Condition Monitoring | Traffic Management (Foschini et al., 2011; Wang et al., 2011) | | Municipal Involvement (Foschini et al., 2011) | Link data for Society (De et al., 2012; Kortuem et al., 2010) | Smart City (Sancheza et al., 2014; Mazhelis and Tyrvainen, 2014; Elmangoush et al., 2013; Ganche et al., 2013; Bonino et al., 2015) | Urban Management (Papadopoulos et al., 2013; Jina et al., 2014; Dayu et al., 2010) |
| | Accidental Measures (Zhang and Anwen, 2010) | Smart Cycling (Mosser et al., 2012) Smart Sports (Ray, 2015b) | Home Entertainment (Lin, 2013; Kos et al., 2013; Jiang and Meng, 2012) | Smart Logistics (Guoa et al., 2012) | Smart Tourism (Guo et al., 2014) | Smart Environment (López-de-Ipiña et al., 2007) | m-Learning (Yang et al., 2011) |
| Cloud Service and Management (Islam et al., 2013; Rao et al., 2012) | Information Exchange Cloud (Leu et al., 2013) | Vehicular Cloud (He et al., 2014) | | Cloud Infrastructure (Sivabalan et al., 2013) | | Context Aware Services (Chen and Chen, 2012) | |
| | Location Aware Service (Li et al., 2012) | IoT as a Service (Katasonov et al., 2008; Fei et al., 2013; Lin et al., 2013) | | Cognitive Service (Foteinos et al., 2013; Tang et al., 2010) | | Control Service (Sowe et al., 2014) | |
| | Sensor Discovery Service (Perera et al., 2014; Fei et al., 2013; Pires et al., 2014; EEML; EMML) | Fog Computing (Bonomi et al., 2012, 2014) | | Big Data (Jiang et al., 2014; URI) | | Data Filtering (SSN; Narendra et al., 2015) | |
| Social Computing Security | SIOT (Girau et al., 2013; Kim and Lee, 2014; Atzori et al., 2011, 2012) | | | Societal Data Service (Buckl et al., 2009; Zhang et al., 2013) | | | |
| | Object Security (Vučini'c et al., 2014; Cooja) | End-to-End Security (Kothmay et al., 2012; RPL;Tiny OS; Hydro) | | Cyber-Physical-Social Security (Ning and Liu, 2012) | | Hierarchical Security (Zhang and Qu, 2013) | |
| | Multimedia Traffic Security (Zhou and Chao, 2011; Zhao et al., 2009; Kundur et al., 2008; Zhou et al., 2010) | | | Light Wight Security (Morchon et al., 2016) Defense (Ray, 2015a) | | | |

### 2.10. Observation

In earlier sub sections, several domain specific IoT based architectural works have been discussed. While reviewing different areas of implementations, it is found that smart city related practices are dominant over other segments. Fig. 13 illustrates the graphical representation of the rate of practice versus domains of IoT architectures. On the basis of 130 research papers included in this survey, the graph has been plotted; where RFID and health related architectural studies are getting equally popular around at 11%. SoA based architectural research is gradually coming forwards faster than RFID and health sectors, making its mark at 12.5%. WSN being a common area of practice has secured 13.3% among all. As mentioned in earlier section, smart city and related applications are gaining popularity in recent days. The result shows that 16.5% of overall research has been performed collectively toward the development for in smart society only. Indeed the smart society approach touches the highest point on the plot. Cloud computing based research and practices seem to be just beyond of WSN i.e., 14%. SCM and industrial approaches are subsequently marking its position in IoT specific world. SCM secures 8.6% on the graph. Security and privacy issues are very important by its own virtue; hence researchers are coming up with novel architectural concepts to facilitate the IoT. 7% investigations are made on its behalf. Social computing based research is still at nascent stage. Very few and specific explorations have been made on this ground. It has attained only 4.7%. The graphical representation of current trends in IoT based architectural research shows that more facilitation to be incurred in several domains, such as: e-learning, defense (Ray, 2015a), rural management, and robotics (Ray, submitted for publication) are yet to be touched (not shown on the graph). Table 4 combines all discussed architectures in earlier section as a tabular form. The representation of this table conglomerates different types of architectural frameworks as per their sub-domain. This will help the researchers to go into the depth of what is described in this paper as the sub-domains or domains as a whole, that need to be searched and paved in future.

## 3. Open research issues and future direction

Although the architectures described in earlier section make IoT concept practically feasible, a large research effort is still required in this direction. This section reviews technical problems associated with current IoT architectures. Later on, a novel concept Io<*> or (Internet of *) is presented so as to meet all necessary parts that are missing in existing architectures.

### 3.1. Technical challenges

It is broadly accepted that the IoT technologies and applications are still in their infancy (Xu, 2011). There are still many research challenges for industrial use such as technology, standardization, security and privacy (Atzori et al., 2010). Future efforts are needed to address these challenges and examine the characteristics of different industries to ensure a good fit of IoT devices in the human centric environments. A sufficient understanding of industrial characteristics and requirements on factors such as cost, security, privacy, and risk are indeed required before the IoT will be widely accepted and deployed in all the domains (Gershenfeld et al., 2004). Let discuss a few problems in this regard:

(i) Design of Service oriented Architecture (SoA) for IoT is a big challenge where service-based objects may face problems from performance and cost related issues. SoA needs to handle a large number of devices connected to the system which phrases scalability issues. At this moment, challenges like: data transfer, processing, and management become a matter of burden overheaded by service provisioning (Vermesan et al., 2009).

(ii) IoT is a very complicated heterogeneous network platform. This, in turn enhances the complexity among various types devices through various communication technologies showing the rude behavior of network to be fraudulent, delayed, and non-standardized. Bandyopadhyay and Sen (2011) has clearly pointed out the management of connected objects by facilitating through collaborative work between different things e.g., hardware components and/or software services, and administering them after providing addressing, identification, and optimization at the architectural and protocol levels is a serious research challenge.

(iii) If we look from the viewpoint of network services, it seems clear that there is always a lack of a Service Description Language (SDL). Otherwise, it would make the service development, deployment, and resource integration difficult by extending the product dissemination time causing loss in market. Hence, a commonly accepted SDL should be constructed so as the powerful service discovery methods and object naming services be implemented (Vermesan et al., 2009). Novel SDL may be developed to cope with product dissemination after validating the requite SDL specific architecture.

(iv) As of now, IoT is degenerated on a traditional network oriented ICT environment. It is always affected by whatever connected to it. Here, a need of unified information infrastructure is to be sought. Huge number of connected devices shall produce real-time data flow which must be governed by high band width frequency path. Hence, a uniform architectural base is to be created to cater the infrastructure needs sophistically.

(v) The originated data may be too much large in size that current database management system may not handle in real-time manner. Proper solutions need to be idealized. IoT based data would be generated in a rapid speed. The collected data at receivers end shall be stored in efficient way which current RAID technology is incapable of. Here, an IoT based data service centric architecture need to be revised to handle this problem.

(vi) Different devices attached to the IoT will put down data of variety in type, size and formation. These variations should be occupied with the futuristic technology which may involve multi-varied architectural notion for its ideal indentation. Researcher should come forward with novel Big IoT Data specific design where data can efficiently handled.

(vii) Data is a raw fact that generally does not conform to non-relevant handouts. Here in case of IoT, data play the massive role in decision making. The value of data

is only achievable after filtering process is performed on the pool of data. This meaningful information can only be obtained by orientation of mining, analysis, and understand it. Big data problem is sufficient for handling similar regression. Relevant architectural framework is in evident that can hale data mining, analytics, and hence decision making services. Big Data approach could be aggregated herewith.

(viii) In addition, industries must seek the challenges of hardware software coexistence around IoT. Variety of devices combined with variety of communication protocols through TCP/IP or advanced software stacks would surely manipulate web services which shall be deployed by various middleware solutions (Wang et al., 2013). Particular architecture leveraging the facilitation of heterogeneous protocols shall be devised.

(ix) The IoT is envisaged to include an incredibly high number of nodes. All the attached devices and data shall be retrievable; here in such context, the unique identity is a must for efficient point-to-point network configuration. IPv4 protocol identifies each node through a 4-byte address. As it is well known that the availability of IPv4 numbered addresses is decreasing rapidly by reaching zero in next few years, new addressing policies shall be countered where IPv6 is a strong contender. This is an area where utmost care is needed to pursue device naming and identification capability, where appropriateness of architectural proficiency is a must.

(x) Standardization is another clot which may precisely be operated for growth of IoT. Standardization in IoT signifies to lower down the initial barriers for the service providers and active users, improvising the interoperability issues between different applications or systems and to perceive better competition among the developed products or services in the application level. Security standards, communication standards and identification standards need to be evolved with the spread of IoT technologies while designing emerging technologies at a horizontal equivalence. In addition, fellow researchers shall document industry-specific guidelines and specify required architectural standards for efficient implementation of IoT.

(xi) From the viewpoint of service, lack of a commonly accepted service description language makes the service development and integration of resources of physical objects into value-added services difficult. The developed services could be incompatible with different communication and implementation environments (Atzori et al., 2010). In addition, powerful service discovery methods and object naming services need to be developed to spread the IoT technology (Sundmaeker et al., 2010). Scientists should pave novel architectures to cater with these difficulties.

(xii) The widespread applicability of IoT and associated technologies shall largely depend on the network cum information security and data privacy protection. Being highly complex and heterogeneous in nature, IoT always faces severe security and privacy threats. Deployment, mobility, and complexity are the main challenges that restrict IoT to be damn safe (Roman et al., 2011). As per Roman et al. (2011), Li (2013), Ting and Ip (2013), privacy protection in IoT environment is more vulnerable than in traditional ICT network due to the large number of presences of attack vectors on IoT entities. Say for an example, IoT based health care monitoring system will collect patient's data (e.g., heart rate, pulse, body temperature, respiration etc.) and later on send the information directly to the doctor's office or hospital via network. As the time of data transfer over the network, if patient's data is stolen or misplaced serious risk may arise which can cause even death to the user. In such situation, it is noticed that most of the architectures do not include privacy, and security aspects into the respective concept which is drawback that needs to be clarified. Though, existing network security technologies enable IoT to get protected from such threats, more work still needs to be considered. A reliable, effective and powerful security protection mechanism for IoT is on the top most priority at the moment. Authors Xu et al. (2014) have depicted following topics where research should be carried on: (a) Definition of security and privacy from the social, legal, and culture point of view, (b) trust and reputation management, (c) end-to-end encryption, (d) privacy of communication and user data, and (e) security on services and applications. It is further understood that although existing network security technologies provide a basis for privacy and security in IoT, more work still need to be performed. A reliable security protection mechanism for IoT needs to be researched from the following aspects: (a)The definition of security and privacy from the viewpoint of social, legal and culture; (b) trust and reputation mechanism; (c) communication security such as end-to-end encryption; (d) privacy of communication and user data; (e) security on services and applications (Xu et al., 2014).

### 3.2. Direction toward Io<*>

This section prescribes typical application specific approaches, which are absent in the aforementioned review work or have not been touched at all by the research communities. The Io<*> refers to Internet of Any architecture (where, '*' is normally assumed to be 'all' in computing). Architectures are continuously gaining importance and soon it will hold the underneath foundation of IoT. From a viewpoint of an architect/developer, the first and foremost job while designing a novel philosophy, far ahead of implementing in practice, is to establish a fundamental model which shows the layered components and how they are connected to each other. Research should be made possible to elaborate new thing based framework to complement the following particulars such as: mining, sports, tourism, governance, social, robotics, automation, and defense. As IoT is still in its nascent stage, we should be motivated to Io<*> where any architecture could be well suited. Smart healthcare, domotics, transportation, environment and agriculture are currently being sought in terms of IoT. Academics are constantly in the process to successfully cope up with the necessary platforms to solve these problems in near future. Io<*> concept shall revolutionize the way we see through the IoT technologies by combing the untouched areas with the cumulated

ones. This shall hold the horizontal, vertical, and diagonal crisscross among all the core components of the IoT to the generalized applications. Io < * > is completely a hypothetical concept that must be tracked on. Analog, digital, and hybrid objects shall be the 'things' part. Not only solid but also liquid, semi-liquid, and crystallized type of materials may be the part of it. Integrated chips (IC), system on lab, lab on chip, FPGA, ASIC, and flexible electronics elements shall miniaturize the distance between digital and pure digital mechanism. Standard OSI network model is to be revisited for advanced layer based Io < * >. All the network protocols shall appropriately be utilized on its layers. 6LowPAN (Hui et al., 2009), CoAP, MQTT, websockets, XMPP, SOAP, RESTful, and IPv6 are to be integrated in a novel way where scripted web based pages would talk to the < * > portion by leveraging NoSQL, SPARQL, Graph database, parallel database, Hadoop, Hbase, RDF, OWL oriented set ups. On top of it, data analytics, risk analysis, graphical visualization, resource management, service coordinator, task manager, APP based Plug-in enabler, API moderator, storage monitor, and predictive analyzer shall be mounted to improvise Io < * >-as-a-Service (Io < * > aaS). Unlimited applications are to be roofed up the layer to mitigate the user experience to a new height. Smart transportation, logistics, assisted driving, mobile ticketing, environment monitoring, augmented maps, health track, data collection, identification and sensing, comfortable home, smart plant, intelligent museum, social networking, theft monitoring, loss apprehension, historical queries, smart taxi, smart city, governance, and enhanced game environment etc. shall be cherished by human being. Mining sites are to be covered up by Io < * >; besides, sports, travel and tourism, and defense mechanisms are to be connected by. AES, 3-DES, RSA, and SHA-3 algorithms need to be revised to get fitted into the resource constrained < * >. Multimedia may be lid onto Io < * > by apprehending streaming algorithms where as discrete messages be appended after payloads of transmitted packets. "Sensor Model Language" (SensorML) shall be revisited to provide a robust and semantically-tied means of defining processes and processing components, associated with the pre-measurement and post-measurement transformation of observations (Open geospatial). The main objective of SensorML will be to enable the interoperability by using ontologies and semantic mediation. This could be done at the syntactic level and semantic level consecutively; resulting sensors and processes be better understood, utilized, and shared by machines, in complex workflows, and between intelligent sensor web nodes respectively. As of now most of the digital and hybrid devices of traditional network come along contemporary "Operating Systems" (OS). Very few OS are released in market for IoT invasion. IoT operating systems such as Contiki-OS, RIOT-OS are the most prevalent versions available in the market, though they lack in hardware interoperability and semantic means. In this perspective, more work shall be carried to develop new variants of universal IoT-OS. Actuator layer may be another valuable part of Io < * > which has never been seen in any literature till date. In relation to the sensor, actuators are going to increase in exponential rate. The need of a central monitoring and controlling environment is required, Io < * > shall occupy the gap.

## 4. Conclusion

The Internet has proved its existence in our lives, from interactions at a virtual level to social relationships. The IoT has added a new potential into internet by enabling communications between objects and human, making a smarter and intelligent planet. This has led the vision of "*anytime, anywhere, anyway, anything*" communications practically in true sense.

To this end, it is observed that the IoT should be considered as the core part of the existing internet relying on its future direction, which is obvious to be exceptionally different from the current phase of internet what we see and use in our lives. Hence, the architectural concept comes in the picture. Architecture is a framework of technology enabled things to interconnect and interact with similar or dissimilar objects by imposing human to be a layer on it. In fact, it is clear that the current IoT paradigm, which is supportive toward M2M communications, is now getting limited by a number of factors.

New formulations are inevitable for sustenance of IoT which is a strong notation for the researcher to come up with. From the above survey, it is found that publish/subscribe based IoT is flourishing now a days and being successively used in many applications. In this perspective, it should be understood that people are solemnizing their thoughts in terms of vertical silos of architectures. If this trend continues for next few years, it is mandatory that IoT may not achieve its goal related to flexibility, interoperability, concurrency, scalability, and addressability issues. Crowed sourcing may be incorporated into the architectural conciseness. Defense, military, intelligence services, robotics etc. fields do still undercover by IoT. Tourism, education, multimedia, governance, social aware, and context aware IoT architectures have not been functional at all. Vertical silos must be coincided with the horizontal perspective for affective measures of the IoT.

In this article, firstly the background and definition of IoT are given. Secondly, thorough discussions on fundamentals behind IoT architectures are elaborated. Next, several key domains where IoT based research works are currently going on are visited. Afterward, detailed analyses of the research challenges are mentioned. Resulting graph attains the state-of-the-art research based motives on the aforementioned domains. A novel concept-"Io < * >" is also proposed that is based on various theoretical nomenclature and external inputs. Different from other IoT survey papers, a main contribution of this paper is that it focuses on area specific architectures of IoT applications and highlights the challenges and possible research opportunities for future IoT researchers who would work in architectural as well as in IoT as a whole.

## References

Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E., 2002. Wireless sensor networks: a survey. Comput. Netw. 38 (4), 393–422.

Arsénio, A., Serra, H., Francisco, R., Nabais, F., Andrade, J., Serrano, E., 2014. Internet of intelligent things: bringing artificial intelligence into things and communication networks. Stud. Comput. Intell. 495, 1–37.

Ashton, K., 2009. Internet of things. RFID J.

Atzori, L., Iera, A., Morabito, G., 2010. The internet of things: a survey. Comput. Networks 54 (15), 2787–2805.
Atzori, L., Iera, A., Morabito, G., 2010. The internet of things: a survey. Comput. Netw. 54 (15), 2787–2805.
Atzori, L., Iera, A., Morabito, G., 2011. SIoT: giving a social structure to the internet of things. IEEE Commun. Lett. 15 (11), 1193–1195.
Atzori, L., Iera, A., Morabito, G., Nitti, M., 2012. The social internet of things (SIoT) when social networks meet the internet of things: concept, architecture and network characterization. Comput. Networks 56 (16), 3594–3608.
Auto-Id Labs, <http://www.autoidlabs.org/>.
Bandyopadhyay, D., Sen, J., 2011. Internet of things: applications and challenges in technology and standardization. Wireless Personal Commun. 58 (1), 49–69.
Blackstock, M., Lea, R., 2014. IoT interoperability: a hub-based approach. In: Proceedings of International Conference on the Internet of Things (IOT), pp. 79–84.
Blackstock, M., Kaviani, N., Lea, R., Friday, A., 2010. MAGIC Broker 2: an open and extensible platform for the internet of things. Proc. Internet Things, 1–8. ISBN: 978-1-4244-7415-8.
Bo, Y., Wang, H., 2011. The application of cloud computing and the internet of things in agriculture and forestry. In: Proceedings of International Joint Conference on Service Sciences (IJCSS), pp. 168–172.
Bonino, D., Alizo, M.T.D., Alapetite, A., Gilbert, T., Axling, M., Udsen, H., Soto, J.A.C., Spirito, M., 2015. ALMANAC: internet of things for smart cities future. In: International Conference on Internet of Things and Cloud (FiCloud), pp. 309–316.
Bonomi, F, Milito, R., Zhu, J., Addepalli, S., 2012. Fog computing and its role in the internet of things. In: Proceedings of MCC, Helsinkini, Finland.
Bonomi, F., Milito, R., Natarajan, P., Zhu, J., 2014. Fog computing: a platform for internet of things and analytics. In: Big Data and Internet of Things: A Roadmap for Smart Environments. Studies in Computational Intelligence, vol. 546, pp. 169–186.
Botterman, M., 2009. For the European Commission Information Society and Media Directorate General, Networked Enterprise & RFID Unit – D4, Internet of Things: An Early Reality of the Future Internet, Report of the Internet of Things Workshop, Prague, Czech Republic.
Boyi, X., Xu, L.D., Cai, H., Xie, C., Hu, J., Bu, F., 2014. Ubiquitous data accessing method in IoT-based information system for emergency medical services. IEEE Trans. Industr. Inf. 2 (10), 1578–1586.
Broll, G., Rukzio, E., Paolucci, M., Wagner, M., Schmidt, A., Hussmann, H., 2009. PERCI: pervasive service interaction with the internet of things. IEEE Internet Comput. 13 (6), 74–81.
Buckl, C., Sommer, S., Scholz, A., Knoll, A., Kemper, A., Heuer, J., Schmitt, A., 2009. Services to the field: an approach for resource constrained sensor/actor networks. In: Proceedings of WAINA, Bradford, United Kingdom.
Buettner, M., Greenstein, B., Sample, A., Smith, J.R., Wetherall, D., 2008. Revisiting smart dust with RFID sensor networks. In: Proceedings of ACM HotNets, Calgary, Canada.
Chen, Y.S., Chen, Y.R., 2012. Help working with abstracts context-oriented data acquisition and integration platform for internet of things. In: Proceedings of Conference on Technologies and Applications of Artificial Intelligence, pp. 103–108.
Clayman, S., Galis, A., 2011. INOX: a managed service platform for inter-connected smart objects. In: Proceedings of the workshop on Internet of Things and Service Platforms.
CoAP, www.coap.technology.
Contiki OS, www.contiki-os.org.
Cooja, www.contiki-os.org.
Dada, A., Thiesse, F., 2008. Sensor applications in the supply chain: the example of quality-based issuing of perishables. In: Proceedings of Internet of Things, Zurich, Switzerland.
Dayu, S., Huaiyu, X., Ruidan, S., Zhiqiang, Y., 2010. A GEO-related IOT applications platform based on Google Map. In: Proceedings of IEEE 7th International Conference on e-Business Engineering (ICEBE), pp. 380–384.
De, S., Elsaleh, T., Barnaghi, P., Meissner, S., 2012. An internet of things platform for real-world and digital objects. Scalable Comput.: Pract. Exp. 13 (1), 45–57.
Deugd, D.S., Carroll, R., Kelly, K., Millett, B., Ricker, J., 2006. SODA: service oriented device architecture. IEEE Pervasive Comput. 5 (3), 94–96.
Doukas, C. Maglogiannis, I., 2012. Bringing IoT and cloud computing towards pervasive healthcare. In: Proceedings of Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), pp. 922–926.
Dunkels, A., Vasseur, J.P., 2008. IP for Smart Objects, Internet Protocol for Smart Objects (IPSO) Alliance, White Paper, <http://www.ipso-alliance.org>.
Duquennoy, S., Grimaud, G., Vandewalle, J. J., 2009. The web of things: interconnecting devices with high usability and performance. In: Proceedings of ICESS, HangZhou, Zhejiang, China.
EEML, www.eeml.org.
Eleftherakis, G., Pappas, D., Lagkas, T., Rousis, K., Paunovski, O., 2015. Architecting the IoT paradigm: a middleware for autonomous distributed sensor networks. Int. J. Distrib. Sens. Network 2015, 1–17.
Elmangoush, A., Coskun, H., Wahle, S., Magedanz, T., 2013. Design aspects for a reference M2M communication platform for Smart Cities. In: Proceedings of International Conference on Innovations in Information Technology, pp. 204–209.
EMML, https://en.wikipedia.org/wiki/Enterprise_Mashup_Markup_Language.
Enji, S., Zhanga, X., Lib, Z., 2012. The internet of things (IOT) and cloud computing (CC) based tailings dam monitoring and pre-alarm system in mines. Saf. Sci. 50 (4), 811–815.
e-Sense, <http://www.ist-e-sense.org>.
Fan, Y.J., Yin, Y.H., Xu, L.D., Zeng, Y., 2014. IoT-based smart rehabilitation system. IEEE Trans. Industr. Inf. 10 (2), 1568–1577.
Fei, L., Vogler, M., Claessens, M., Dustdar, S., 2013. Towards automated IoT application deployment by a cloud-based approach. In: Proceedings of IEEE 6th International Service-Oriented Computing and Applications (SOCA), pp. 61–68.
Fei L., Voegler, M., Claessens, M., Dustdar, S., 2013. Efficient and scalable IoT service delivery on cloud. In: Proceedings of IEEE Sixth International Conference on Cloud Computing (CLOUD), pp. 740–747.
Finkenzeller, K., 2003. RFID Handbook. Wiley.
Floerkemeier, C., Roduner, C., Lampe, M., 2007. RFID application development with the Accada middleware platform. IEEE Syst. J. 1 (2), 82–94.
Foschini, L., Taleb, T., Corradi, A., Bottazzi, D., 2011. M2M-based metropolitan platform for IMS-enabled road traffic management in IoT. IEEE Commun. Mag. 49 (11), 50–57.
Foss track, <http://www.fosstrak.org>.
Foteinos, V., Kelaidonis, D., Poulios, G., Stavroulaki, V., Vlacheas, P., Demestichas, P., Giaffreda, R., Biswas, A.R., Menoret, S., Nguengang, G., Etelapera, M., Cosmin, N.S., Roelands, M., Visintainer, , Moessner, K., 2013. A cognitive management framework for empowering the internet of things. Future Internet Lect. Notes Comput. Sci. 7858, 187–199.
Ganche, I., Ji, Z., O'Droma, M., 2013. A generic IoT architecture for smart cities. In: Proceedings of 25th IET Irish Signals & Systems Conference, pp. 196–199.
http://www.gartner.com/newsroom/id/2905717 [Accessed on 21 June, 2015].
Gazis, V., Sasloglou, K., Frangiadakis, N., Kikiras, P., 2013. Architectural blueprints of a unified sensing platform for the internet of things. In: Proceedings of 22nd International Confer-

ence on Computer Communications and Networks (ICCCN), pp. 1–5.
Gershenfeld, N., Krikorian, R., Cohen, D., 2004. The internet of things. Sci. Am. 291 (4), 76–81.
Ghose, A., Biswas, P, Bhaumik, C., Sharma, M., 2012. Road condition monitoring and alert application: using in-vehicle Smartphone as Internet-connected sensor. In: Proceedings of Pervasive Computing and Communications Workshops (PERCOM Workshops), pp. 489–491.
Girau, R., Nitti, M., Atzori, L., 2013. Implementation of an experimental platform for the social internet of things. In: Proceedings of Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), pp. 500–505.
Giusto, D., Iera, A., Morabito, G., Atzori, L. (Eds.), 2010. The Internet of Things. Springer.
Graph database, http://www.neo4j.com/developer/graph-database/.
METRO Group Future Store Initiative, <http://www.futurestore.org/>.
Gubbia, J., Buyya, R., Marusica, B.S., Palaniswamia, M., 2013. Internet of things (IoT): a vision, architectural elements, and future directions. Future Gener. Comput Syst. 29 (7), 1645–1660.
Guinard, D., Vlad, T., 2009. Towards the web of things: web mashups for embedded devices In: Proceedings of the International World Wide Web Conference, Madrid.
Guo, Y., Liu, H., Chai, Y., 2014. The embedding convergence of smart cities and tourism internet of things in china: an advance perspective. Adv. Hospitality Tourism Research (AHTR) 2 (1), 54–69.
Guoa, Z., Zhanga, Z., Lib, W., 2012. Establishment of intelligent identification management platform in railway logistics system by means of the internet of things In: Proceedings of International Workshop on Information and Electronics Engineering (IWIEE), pp. 726–730.
Hadoop, https://hadoop.apache.org/.
Hbase, https://hbase.apache.org.
He, W., Yan, G., Xu, L.D., 2014. Developing vehicular data cloud services in the IoT environment. IEEE Trans. Industr. Inf. 10 (2), 1587–1595.
Hui, J., Culler, D., Chakrabarti, S., 2009. 6LoWPAN: incorporating IEEE 802.15.4 Into the IP Architecture – Internet Protocol for Smart Objects (IPSO) Alliance, White Paper, <http://www.ipso-alliance.org>.
Hydra Middleware Project, FP6 European Project, <http:// www.hydramiddleware.eu>.
Hydro, www.cs.berkeley.edu/~stevedh/pubs/smartgrid10hydro.pdf.
IEEE 802.15, <http://ieee802.org/15>.
Ilic, A., Staake, T., Fleisch, E., 2009. Using sensor information to reduce the carbon footprint of perishable goods. IEEE Pervasive Comput. 8 (1), 22–29.
Intel research, <http://seattle.intel-research.net/wisp/>.
National Intelligence Council, 2008. Disruptive Civil Technologies – Six Technologies with Potential Impacts on US Interests Out to 2025 – Conference Report CR 2008–07 http://www.dni.gov/nic/NIC_home.html.
ITU Internet Reports, 2005. The Internet of Things.
IPv6, www.ipv6forum.com.
Islam, M.M., Hung, P.P., Hossain, A.A., Aazam, M., Morales, M.A. G., Alsaffar, A.A., Lee, S.J., Huh, E.N., 2013. A framework of smart internet of things based cloud computing. Res. Notes Inf. Sci. (RNIS) 14, 646–651.
Issarny, V., Georgantas, N., Hachem, S., Zarras, A., Vassiliadist, P., Autili, M., Gerosa, M.A., Hamida, A.B., 2011. Service-oriented middleware for the future internet: state of the art and research directions. J. Internet Serv. Appl. 2 (1), 23–45.
Istepanian, R.S.H., Hu, S., Philip, N.Y., Sungoor, A, 2011. The potential of Internet of m-health Things "m-IoT" for non-invasive glucose level sensing. In: Proceedings of: IEEE Engineering in Medicine and Biology Society, EMBC, pp. 5264–5266.
ITU work on Internet of things, 2015. ICTP workshop. [Accessed on March 26, 2015].
Janggwan, I., Seonghoon K., Daeyoung K., 2013. IoT mashup as a service: cloud-based mashup service for the internet of things. In: Proceedings of IEEE International Conference on Services Computing (SCC), pp. 462–469.
Jiang, W., Meng, L., 2012. Design of real time multimedia platform and protocol to the internet of things. In: Proceedings of IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 1805–1810.
Jiang, L., Xu, L.D., Cai, H., Jiang, Z., 2014. An IoT-oriented data storage framework in cloud computing platform. IEEE Trans. Industr. Inf. 10 (2), 1443–1451.
Jina, J., Gubbib, J., Marusicb, S., Palaniswamib, M., 2014. An information framework of creating a smart city through internet of things. IEEE Internet Things J. 1 (2), 112–121.
Jules, A., 2006. RFID security and privacy: a research survey. IEEE J. Sel. Areas Commun. 24 (2), 381–394.
Karpischek, S., Michahelles, F., Resatsch, F., Fleisch, E., 2009. Mobile sales assistant – an NFC-based product information system for retailers. In: Proceedings of the First International Workshop on Near Field Communications, Hagenberg, Austria.
Katasonov, A., Kaykova, O., Khriyenko, O., Nikitin, S., Terziyan, V., 2008. Smart semantic middleware for the internet of things. In: Proceedings of Fifth International Conference on Informatics in Control, Automation and Robotics, Funchal, Madeira, Portugal.
Kim, J., Lee, J.W., 2014. OpenIoT: an open service framework for the Internet of Things. In: Proceedings of IEEE World Forum on Internet of Things (WF-IoT), pp. 89–93.
Kortuem, G., Kawsar, F., Fitton, D., Sundramoorthy, V., 2010. Smart objects as building blocks for the internet of things. IEEE Internet Comput. 14 (1), 44–51.
Kos, A., Pristov, D., Sedlar, U., Sterle, J., Volk, M., Vidonja, T., Bajec, M., Bokal, D., Bešter, J., 2012. Open and scalable IoT platform and its applications for real time access line monitoring and alarm correlation. Internet Things Smart Spaces Next Gener. Networking Lect. Notes Comput. Sci. 7469, 27–38.
Kos, A., Sedlar, U., Sterle, J., Volk, M., 2013. Network monitoring applications based on IoT system. In: Proceedings of 18th European Conference on and Optical Cabling and Infrastructure (OC&i) Network and Optical Communications (NOC), pp. 69–74.
Kothmay, T., Schmitt, C., Hu, W., Bŕunig, M., Carle, G., 2012. A DTLS based end-to-end security architecture for the internet of things with two-way authentication. In: Proceedings of IEEE 37th Conference on Local Computer Networks Workshops (LCN Workshops), pp. 956–963.
Kouche, A.E., 2012. Towards a wireless sensor network platform for the Internet of things: sprouts WSN platform. In: Proceedings of IEEE International Conference on Communications (ICC), pp. 632–636.
Kranenburg, R.V., 2008. The Internet of Things: A Critique of Ambient Technology and the All-Seeing Network of RFID, Institute of Network Cultures.
Kundur, D., Luh, W., Okorafor, U.N., Zourntos, T., 2008. Security and privacy for distributed multimedia sensor networks. Proc. IEEE 96 (1), 112–130.
Lazarescu, M.T., 2013. Design of a WSN platform for long-term environmental monitoring for IoT applications. IEEE J. Emerg. Select. Top. Circuits Syst. 3, 45–54.
Leu, J.S., Chen, C.F., Hsu, K.C., 2013. Improving heterogeneous SOA-based IoT message stability by shortest processing time scheduling. IEEE Trans. Serv. Comput. 7 (4), 575–585.
Li, L., 2013. Technology designed to combat fakes in the global supply chain. Bus. Horiz. 56 (2), 167–177.
Li, J., Shvartzshnaider, Y., Francisco, J.A., Martin, R.P., Raychaudhuri, D., 2012. Enabling internet-of-things services in the mobility first future internet architecture. In: Proceedings of IEEE Interna-

tional Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM).
Li, J., Zhang, Y., Chen, Y.F., Nagaraja, K., 2013. A mobile phone based WSN infrastructure for IoT over future internet architecture. In: Proceedings of IEEE International Conference on and IEEE Cyber, Physical and Social Green Computing and Communications (GreenCom), pp. 426–433.
Lin, H.T., 2013. Implementing smart homes with open source solutions. Int. J. Smart Home 7 (4), 289–296.
Lin, F.J., Ren, Y., Cerritos, E., 2013. A feasibility study on developing IoT/M2M applications over ETSI M2M architecture. In: Proceedings of International Conference on Parallel and Distributed Systems (ICPADS), pp. 558–563.
López-de-Ipiña, D., Vazquez, J.I., Abaitua, J., 2007. A Web 2.0 platform to enable context-aware mobile mash-ups. Ambient Intell. Lect. Notes Comput. Sci. 4794, 266–286.
Ma, D., Ding, Q., Li, Z., Li, D., Wei, Y., 2012. Prototype of an aquacultural information system based on internet of things E-Nose. Intell. Autom. Soft Comput. 18 (5), 569–579.
Marrocco, G., Occhiuzzi, C., Amato, F., 2009. Sensor-oriented passive RFID. In: Proceedings of TIWDC, Pula, Italy.
Mazhelis, O., Tyrvainen, P., 2014. A framework for evaluating Internet-of-Things platforms: application provider viewpoint. In: Proceedings of IEEE World Forum on Internet of Things (WF-IoT), pp. 147–152.
Metro, www.metrogroup.de.
Miorandi, D., Sicari, S., Chlamtac, I., 2012. Internet of things: vision, applications and research challenges. Ad Hoc Netw. 10 (7), 1497–1516.
Morchon, O.G., Rietman, R., Sharma, S., Tolhuizen, L., Arce, J.T., 2016. A comprehensive and lightweight security architecture to secure the IoT throughout the lifecycle of a device based on HIMMO. In: Algorithms for Sensor Systems. Lecture Notes in Computer Science, vol. 9536, pp. 112–128.
Mosser, S., Fleurey, F., Morin, B., Chauvel, F., 2012. SENSAPP as a reference platform to support cloud experiments: from the internet of things to the internet of services. In: 14th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC), pp. 400–406.
MQTT, www.mqtt.org.
Narendra, N., Ponnalagu, K., Ghose, A., Tamilselvam, S., 2015. Goal-driven context-aware data filtering in IoT-based systems. In: IEEE 18th International Conference on Intelligent Transportation Systems (ITSC), pp. 2172–2217.
Networked Enterprise & RFID & Micro & Nanosystems, 2008. In: Proceedings of Co-operation with the Working Group RFID of the ETP EPOSS, Internet of Things in 2020, Roadmap for the Future.
Ning, H., Liu, H., 2012. Cyber-physical-social based security architecture for future internet of things. Adv. Internet Things 2, 1–7.
NoSQL, www.nosql-database.org/.
OASI, 0000. Web Services Business Process Execution Language Version 2.0, Working Draft, <http://docs.oasis-open.org/wsbpel/2.0/wsbpelspecificationdraft.pdf>.
Open geospatial, http://www.opengeospatial.org/ standards/sensorml [Accessed on 8 July, 2015].
OWL, http://www.w3.org/TR/owl-semantics/.
Papadopoulos, G.Z., Beaudaux, J., Gallais, A., Noël, T., Schreiner, G., 2013. Adding value to WSN simulation using the IoT-LAB experimental platform. In: Proceedings of IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), pp. 485–490.
Parallel database, www.codex.cs.yale.edu/avi/db-book/db5/slide-dir/ch21.ppt.
Pasley, J., 2005. How BPEL and SOA are changing web services development. IEEE Internet Comput. 9 (3), 60–67.
Pereira, P.P., Eliasson, J., Kyusakov, R., Delsing, J., 2013. Enabling cloud connectivity for mobile internet of things applications. In: Proceedings IEEE 7th International Symposium on Service Oriented System Engineering (SOSE), pp. 518–526.
Perera, C., Jayaraman, P.P., Zaslavsky, A., Georgakopoulos, D., 2014. Sensor discovery and configuration framework for the internet of things paradigm. In: Proceedings of IEEE World Forum on Internet of Things (WF-IoT), pp. 94–99.
Pires, P.F., Cavalcante, E., Barros, T., Delicato,, F.C., 2014. A platform for integrating physical devices in the internet of things. In: Proceedings of 12th IEEE International Conference on Embedded and Ubiquitous Computing (EUC), pp. 234–241.
Presser, M., Gluhak, A., 2009. The Internet of Things: Connecting the Real World with the Digital World, EURESCOM mess@ge – The Magazine for Telecom Insiders 2. <http://www.eurescom.eu/message>.
Rai, R., Lepcha, C., Ray, P.P., Chettri, P., 2013. GDMA: generalized domain model architecture of internet of things. In: Proceedings of National Conference on Applied Electronics (NCAE), AIT Kolkata, pp. 65–68.
Rao, B.P., Saluia, P., Sharma, N., Mittal, A., Sharma, S.V., 2012. Cloud computing for internet of things sensing based applications. In: Proceedings of 2012 Sixth International Conference on Sensing Technology (ICST), pp. 374–380.
Ray, P.P., 2014a. Home health hub internet of things (H3IoT): an architectural framework for monitoring health of elderly people. In: Proceedings of IEEE ICSEMR, Chennai.
Ray, P.P., 2014. Internet of things based physical activity monitoring (PAMIoT): an architectural framework to monitor human physical activity. In: Proceedings of CALCON, Kolkata, pp. 32–34.
Ray, P.P., 2015a. Towards an internet of things based architectural framework for defence. In: Proceedings of IEEE International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), pp. 411–416. 2015.
Ray, P.P., 2015b. A generic internet of things architecture for smart sports. In: Proceedings of IEEE International Conference on Control, Instrumentation, Communication and Computational Technologies, pp. 405–410. 2015.
Ray, P.P., 2016. Internet of things cloud enabled MISSENARD index measurement for indoor occupants. Measurement 92, 157–165. Elsevier.
Ray, P.P., submitted for publication. Internet of Robotic Things.
Ray, P.P., 2017. Internet of Things for Smart Agriculture: Technologies, Practices and Future Road Map. Journal of Ambient Intelligence and Smart Environments – IOS Press (in press).
Ray, P.P., Sharma, A., Rai, R., 2013. MDTRM: abstraction to model driven tree reference model of internet of things. In: Proceedings of National Conference on Applied Electronics (NCAE), AIT Kolkata, pp. 61–64.
RDF, https://www.w3.org/RDF.
RESTful, www.restapitutorial.com.
Roman, R., Najera, P., Lopez, J., 2011. Securing the internet of things. Computer 44 (9), 51–58.
RPL, https://tools.ietf.org/html/rfc6550.
Sakamura, K., 2006. Challenges in the age of ubiquitous computing: a case study of T-engine – an open development platform for embedded systems. In: Proceedings of ICSE, Shanghai, China.
Sancheza, L., Muñoza, L., Galachea, J.A., Sotresa, P., Juan, R., Gutierreza, V., Ramdhanyb, R., Gluhakc, A., Krcod, S., Theodoridise, E., Pfistererf, D., 2014. SmartSantander: IoT experimentation over a smart city testbed. Comput. Netw. 61 (14), 217–238.
Sebastian, S., Ray, P.P., 2015. Development of IoT invasive architecture for complying with health of home. In: Proceedings of I3CS, Shillong, pp. 79–83.
Sebastian, S., Ray, P.P., 2015. When soccer gets connected to internet, In: Proceedings of I3CS, Shillong, pp. 84–88.
Shang, X., Zhang, R., Chen, Y., 2012. Internet of things (IoT) service architecture and its application in E-Commerce. J. Electron. Commerce Org. (JECO) 10 (3), 44–55.

Sivabalan, A., Rajan, M.A., Balamuralidhar, P., 2013. Towards a lightweight internet of things platform architecture. J. ICT Standardization 1, 241–252.
SOAP, www.w3.org/TR/soap.
Sowe, S.K., Kimata, T., Mianxiong, Dong, Zettsu, K., 2014. Managing heterogeneous sensor data on a big data platform: IoT services for data-intensive science. In: Proceedings of IEEE 38th International Computer Software and Applications Conference Workshops (COMPSACW), pp. 295–300.
SPARQL, www.w3.org/TR/rdf-sparql-query.
Spiess, P., Karnouskos, S., Guinard, D., Savio, D., Baecker, O., Souza, L., Trifa, V., 2009. SOA-based integration of the internet of things in enterprise services. In: Proceedings of IEEE ICWS, Los Angeles, Ca, USA.
Srivastava, L., 2006. Pervasive, ambient, ubiquitous: the magic of radio. In: Proceedings of uropean Commission Conference "From RFID to the Internet of Things, Bruxelles, Belgium.
SSN, www.w3.org/2005/Incubator/ssn/ssnx/ssn.
Sterling, B., 2005. Shaping Things – Mediawork Pamphlets. The MIT Press.
Sun, Z., Li, W., Song, W., Jiang, P., 2011. Research on manufacturing supply chain information platform architecture based on internet of things. Adv. Mater. Res. 314–316, 2344–2347.
Sundmaeker, H., Guillemin, P., Friess, P., 2010. Vision and challenges for realizing the Internet of Things, European Commission.
Sung, W.T., Chiang, Y.C., 2012. Improved particle swarm optimization algorithm for android medical care IOT using modified parameters. J. Med. Syst. 36 (6), 3755–3763.
Tang, T., Wu, Z., Karhu, K., Hämäläinen, M., Ji, Y., 2010. An internationally distributed ubiquitous living lab innovation platform for digital ecosystem research. In: Proceedings of International Conference on Management of Emergent Digital EcoSystems, pp. 159–165.
The EPCglobal Architecture Framework, 2009. EPCglobal Final Version 1.3, <www.epcglobalinc.org>.
Tian, Y., Liu, Y., Yan, Z., Wu, S., 2012. RNS-a public resource name service platform for the internet of things. In: Proceedings of IEEE International Conference on Green Computing and Communications (GreenCom), pp. 234–239.
Ting, S.L., Ip, W.H., 2013. Combating the counterfeits with web portal technology. Enterprise Inf. Syst. 9 (7), 661–680.
Tiny OS, www.tinyos.net.
Toma, I., Simperl, E, Hench, G., 2009. A joint roadmap for semantic technologies and the internet of things. In: Proceedings of the Third STI Road mapping Workshop, Crete, Greece.
Ubi e-Sense, <http://www.ist-ubisecsens.org>.
Ukil, A., Bandyopadhyay, S., Joseph, J., Banahatti, V., Lodha, S., 2012. Negotiation-based privacy preservation scheme in internet of things platform. In: Proceedings of International Conference on Security of Internet of Things, pp. 75–84.
URI, https://www.w3.org/Addressing.
Vázquez, I., 2009. Social Devices: Semantic Technology for the Internet of Things, Week@ESI, Zamudio, Spain.
Vermesan, O., Friess, P., Guillemin, P., (2009), Internet of things strategic research roadmap, The Cluster of European Research Projects, available from http://www.internet-of-things-research.eu/pdf/IoT Cluster Strategic Research Agenda 2009.pdf.
Vučini'c, M., Tourancheau, B., Rousseau, F., Duda, A., Damon, L., Guizzett, R., 2014. OSCAR: object security architecture for the internet of things. arXiv:1404.7799v1.
Wahlster, W., 2008. Web 3.0: Semantic Technologies for the Internet of Services and of Things, Lecture at the 2008 Dresden Future Forum.
Wang, M., Fan, C., Wen, Z., Li, S., 2011. Implementation of internet of things oriented data sharing platform based on RESTful web service. In: Proceedings of 7th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM), pp. 1–4.
Wang, S., Zhang, Z., Ye, Z., Wang, X., Lin, X., Chen, S., 2013. Application of environmental Internet of Things on water quality management of urban scenic river. Int. J. Sustainable Dev. World Ecol. 20 (3), 216–222.
Websockets, https://w3c.github.io/websockets/.
Welbourne, E., Battle, L., Cole, G., Gould, K., Rector, K., Raymer, S., Balazinska, M., Borriello, G., 2009. Building the internet of things using RFID: the RFID ecosystem experience. IEEE Internet Comput. 13 (3), 48–55.
Xia, F., 2009. Wireless sensor technologies and applications. Sensors 9 (11), 8824–8830.
Xiaocong, Q., Jidong, Z., 2010. Study on the structure of "internet of things (IOT)" business operation support platform. In: Proceedings of 12th IEEE International Conference on Communication Technology (ICCT), pp. 1068–1071.
XMPP, www.xmpp.org.
Xu, L., 2011. Enterprise systems: state-of-the-art and future trends. IEEE Trans. Ind. Inf. 7 (4), 630–640.
Xu, L.D., He, W., Li, S., 2014. Internet of THINGS IN INDUSTRIES: A SURVEY. IEEE Trans. Indus. Inf. 10 (4), 2233–2243.
Yaacoub, E., Kadri, A., Dayya, A.D., 2012. Cooperative wireless sensor networks for green internet of things. In: Proceedings of the 8h ACM Symposium on QoS and Security for Wireless and Mobile Networks, pp. 79–80.
Yang, B., Nie, X., Shi, H., Gan, W., 2011. M-learning mode research based on internet of things. In: Proceedings of International Conference on Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC), pp. 5623–5627.
Yang, G., Li, X., Mäntysalo, M., Zhou, X., Pang, Z., Xu, L.D., Walter, S.K., Chen, Q., Zheng, L., 2014. A health-IoT platform based on the integration of intelligent packaging, unobtrusive biosensor and intelligent medicine box. IEEE Trans. Ind. Inf. 10 (4), 2180–2191.
Yu, L., Lu, Y., Zhu, X.J., 2012. Smart hospital based on internet of things. J. Networks 7 (10), 1654–1661.
Yuan, R., Shumin, L., Baogang, Y., 2007. Value Chain Oriented RFID System Framework and Enterprise Application. Science Press, Beijing.
Zhang, J., Anwen, Q., 2010. The application of internet of things (IOT) in emergency management system in China. In: Proceedings of IEEE International Conference on Technologies for Homeland Security (HST), pp. 139–142.
Zhang, W., Qu, B., 2013. Security architecture of the internet of things oriented to perceptual layer. Int. J. Comput. Consumer Control (IJ3C) 2 (2), 37.
Zhang, J., Iannucci, B., Hennessy, M., Gopal, K., Xiao, S., Kumar, S., Pfeffer, D., Aljedia, B., Ren, Y., Griss, M., Rosenberg, S., Cao, J., Rowe, A., 2013. Sensor data as a service – a federated platform for mobile data-centric service development and sharing. Proc. IEEE Int. Services Comput. (SCC), 446–453. ISBN: 978-0-7695-5046-6.
Zhangm, X., Wen, Z., Yuexin, W., Zou, J., 2011. The implementation and application of the internet of things platform based on the REST architecture. In: Proceedings of International Conference on Business Management and Electronic Information, pp. 43–45.
Zhao, H.V., Lin, W.S., Liu, K.J.R., 2009. A case study in multimedia fingerprinting: behavior modeling and forensics for multimedia social networks. IEEE Signal Process. Mag. 26 (1), 118–139.
Zhao, J.C., Zhang, J.F., Feng, Y., Guo, J,X., 2010. The study and application of the IOT technology in agriculture. In: Proceedings of 3rd IEEE International Conference on Computer Science and Information, Technology (ICCSIT), vol. 2, pp. 462–465.
Zhou, L., Chao, H.C., 2011. Multimedia traffic security architecture for the internet of things. IEEE Network, 35–40.
Zhou, L., Naixue, X., Shu, L., Vasilakos, A., Yeo, S.S., 2010. Context-aware multimedia service in heterogeneous networks. IEEE Intell. Syst. 25 (2), 40–47. PP(99).