ISSN: 0975-766X
CODEN: IJPTFI
Available Online through **Research Article**
www.ijptonline.com

INTERNET OF THINGS (IOT): A SURVEY ON EMPOWERING TECHNOLOGIES, RESEARCH OPPORTUNITIES AND APPLICATIONS

S.Sankar[1], Dr.P.Srinivasan[2]
[1]Research Scholar, School of Computer Science and Engineering, VIT University, Vellore-632014, Tamilnadu.
[2]Associate Professor, School of Information Technology and Engineering, VIT University, Vellore-632014, Tamilnadu, India.
Email: India;sankar.s@vit.ac.in

Received on 25-10-2016 *Accepted on 02-11-2016*

Abstract:

Background and Objective: The Internet of Things (IoT) has intended for enabling the physical devices to connect over the internet, that's able to exchange the data between the physical devices in heterogeneous wireless sensor network environment. IoT paradigm is the integration of several technologies such as wireless sensor, actuator networks, identification and tracking technologies, distributed intelligence, enhanced a communication protocol which provides the communication solution among the objects. **Materials and Methods:** The combination of the emerging technologies and Internet transform physical objects into smart objects, able to learn, understand and react to their environment by itself. In coming years, IoT is expected to introduce the new technologies and applications for connection between the physical objects and intelligent decision-making. **Conclusion:** This paper presents the detailed summary of the Internet of Things introduction, visions, enabling technologies, Architectural details, protocols and its standard specification, research opportunities and challenges and application related issues.

Keywords: Internet of things (IoT), Internet Engineering Task Force (IETF), European Telecommunication standards institute (EISI), Institute of Electrical & Electronics Engineers (IEEE), Near Field Communication (NFC), Social Internet of Things (SIoT)

1. Introduction:

In 1999, “Internet of Things” the word initially coined by Kevin Ashton while he was working at Auto-ID Labs[1].The physical devices that are connected over the Internet, that able to exchange the data from one device to another device with less human intervention. CISCO Internet Business Solutions Group (IBSG) points out the physical things were connected to Internet than the people population. The things connected to the internet were 12.5

billion in 2010. Estimating 50 billion things will be connected to the internet in 2020.In 2025, the Internet of things going to connect everything in our life stated by The US National Intelligence Council [2],[4].

The ordinary world transforms into a smart world because the physical things are connected to the Internet which can share the information between the objects and take the decision without human involvement.

Now a day, thousands and millions of sensor enabled devices are connected to the Internet. Internet Protocol is used to perform the data communications over a packet switched network. Internet Assigned Numbers Authority (IANA) is managing the Internet Protocol version4. IPv4 uses 32-bit IP address and they are used to assign the unique addresses maximum 4.3 billion devices. It has been exhausting in Feb 1st, 2011. In IoT scenario, large numbers of devices needs to connect with Internet. So the next generation internet protocol known as IPV6, which is introduced by IETF IPng in 1999. It is used to assign the unique addresses maximum up to 2 64 devices [2], [3].

Establishing the connection between the object is not enough, beyond that objects can learn it and take the decision automatically. In IoT scenario, the things transform into smart object using the technologies such as communication technologies, sensor networks, ubiquitous computing and pervasive computing [4].

A word “ubiquitous” came from the Latin language. It gives the meaning as “everywhere”. In 1991, the computer scientist, Marc Weiser coined the term “ubiquitous computing”. He pointed out the computer devices will be embedded with everyday objects, invisibly it communicate with the environment. The vision of ubiquitous computing is “anywhere, anytime, by anything and anyone”. Now a day, users can communicate at any time and any place. In coming years, the global networks not only connect the human, electronic components and presents with the physical objects. The physical objects are able to share the information between them. Due to the technological revolution, the scenario will be totally changed. The physical devices able communicate with other devices at anytime, anywhere, by anyone and anything in an Internet of things on ubiquitous network connectivity [5]. The new dimension of telecommunication environment for connecting things as shown in figure 1.

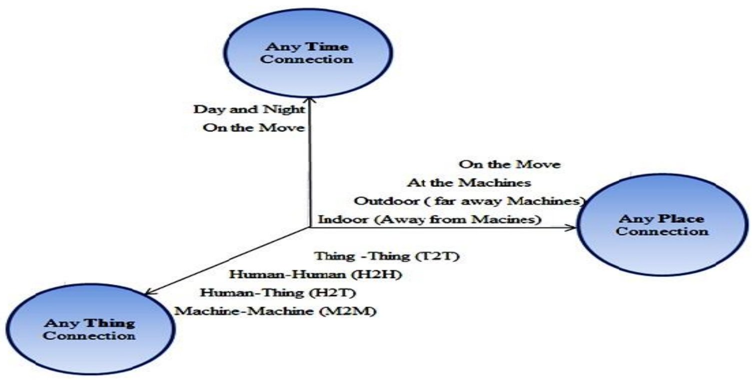

Figure1. New dimension of telecommunication environment for connecting things.

This paper is organized as follows: The Section2 provides the IoT visions. The Section 3 discusses enabling & empowering technologies. Section 4 discusses an Architecture of IoT. Section 5 provides the detail of IoT protocol standards. Section 6 provides the detail of IoT research opportunities and challenges. Section 7 discusses the IoT Application. Section 8 presents the summary of this paper in the conclusion.

2. IoT Vision

The Internet of things (IoT) is a new paradigm will play a vital role in the near future. IoT enables the heterogeneous communication in wired and wireless network [6]. It can be mainly categorized into three paradigms such as things-oriented vision, Internet-oriented vision and semantic-oriented vision [7],[8]. The vision of the Internet of things (IoT) paradigm is shown in figure2.

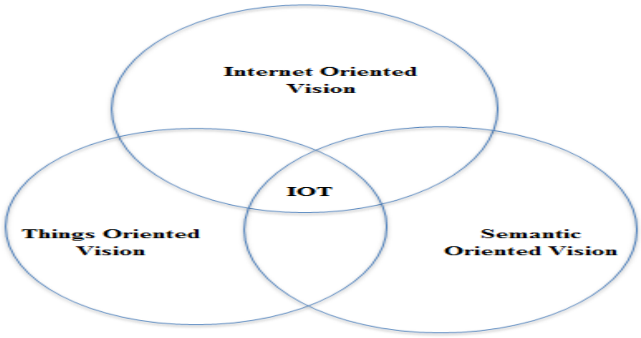

Figure 2. Three visions of IoT paradigm.

2.1. Things oriented vision

In things oriented vision, it performs the tracking or monitoring the object using sensors and the ubiquitous technologies. In earlier days, Electronic Product Code (EPC) used to uniquely identify the objects and these techniques extended into sensors. It is very important for the future Internet.

2.2. Internet oriented vision

In Internet oriented vision, the physical object is converted into a smart object. Internet Protocol is assigned to an object which is used to access the object uniquely. The sensor-enabled object converts into smart, which is identified uniquely and it is continuously monitored.

2.3. Semantic Oriented Vision

In Semantic Vision, huge amount of sensor-enabled physical devices connected over the Internet. The sensors continuously monitor and generate the massive data. The generated data are possibly redundant and in the form of homogeneous and heterogeneous. Semantic vision helps to process the data meaningfully and take the necessary action or decision appropriately.

3. Enabling and Empowering Technologies:

In a real world, communication between the physical devices is possible through mitigating of several enabling technologies. Now a day, many physical devices are connected to the Internet. Establishing the communication, maintain and provide the Quality of Service between the physical devices is a challenging task. The emerging technologies improve the IoT scenario. They mainly categorized in two ways such as software technologies and hardware technologies.

3.1 Software Technologies

The IoT mainly uses software technologies such as RIOT OS, Contiki OS, Tiny OS, Lite OS and etc [4].

RIOT OS

RIOT OS is a Real-time operating for IoT devices. It supports for 6LoWPAN, IPv6, RPL, UDP and TCP. It follows the C and C++ programming standards [4].

Contiki OS

Contiki is an operating system for the IoT devices. It connects low-cost and tiny devices, low-power micro controllers to the Internet. Contiki is a toolbox for making complex wireless systems[4].

Tiny OS

Tiny operating is an embedded and component-based operating system for wireless sensor network environment. It follows the nesC programming standards[4].

Lite OS

Linux Lite is a Linux operating system. It is developed by Debian and Ubuntu team. It is used for wireless network environment. It was initially developed and designed to attract Windows OS users [4].

Middleware

Middleware is software that provides an interface between the components of IoT. The objective of Middleware is able to make heterogeneous computing and communication devices and support the interoperability within the services and application. The recent middleware architecture follows the Service Oriented Architecture (SOA) approach. SOA based middleware technology allows for decomposing the complex and monolithic system into eco-friendly, simple and well-defined parts [9].

Cloud Computing: Cloud computing provides the new mechanism for storing the data and extraction of knowledge from the big data. Integration of Cloud computing with IoT is not an easy task. The cloud computing integrating into

IoT causes some problem such as synchronization, standardization, balancing, reliability, management, enhancement and etc. IoT uses various cloud platforms, namely such as ThingsWorx, Open , Google Cloud, Amazon, GENI and etc[4]. Xively is an open source public cloud services for the Internet of Thing platform. It offers the hosting service provider for sensor data. It is open source, freeware and easily accessible application programming interface (API's) [10]. Nimbits is an open source cloud software and it provides the platform as a service (PaaS) for smart embedded devices to the cloud [11].

Aneka is a .Net based application development and it provides the platform as a service. It is open source and freeware. It can used to compute and storage resources of both private and public cloud services [12].

3.2. Hardware Technologies

IoT prerequisite is hardware technology. Now a day, many companies are involved to develop the hardware for standardization of IoT.

RFID

Radio Frequency Identification (RFID) consists of one reader, several tags and antenna. The tag helps to find the object uniquely. The RFID reader propagates the radio waves through an antenna. The antenna has a small microchip and it responsible for sending and receiving a tag id. In 2003, Hitachi developed a tag with dimensions specified as 0.4 mm x 0.4mm x 0.15mm. It works on 13.56 GHz and coverage area is 10 meters. The RFID system can monitor the object in real-time[8].

WSN: Wireless sensor network (WSN) spatially distributes the sensor node to check the physical or environmental condition and cooperatively pass the data to the destination via sink node [8].

Quick Response Code: The Quick Response code is printed on the product. The QR code recognition application installed in a smart phone. It recognizes the QR code based on high-resolution camera using image processing techniques. The QR code recognition application extracts the text, image, URI information from the product. The QR code mainly uses various things including newspaper, billboard, magazine, shopping mall and etc [13].

Near Field Communication: NFC is a wireless technology for short range communication between the devices. The coverage distance is 4 cm. NFC operates at 13.56 MHZ. It is a subset within the family of RFID [14].

Bluetooth Low Energy: Bluetooth Low Energy (BLE) is a wireless technology for personal area networks (PAN). BLE is mainly used for very low power devices. Bluetooth Special Interest Group (SIG) designed and marketed the Bluetooth low energy. The application areas are security, healthcare, beacons, home entertainment and industries[15].

6LoWPAN

IPV6 over low power wireless personal area network (IPv6) is developed and standardized by IETF. The main aim of 6LoWPAN can assign the internet protocol for low power, small devices and take part in the scenario[4],[8],[16].

The IoT enabling hardware technologies and standards and other features are shown in the Table-1

Table-1. IoT Enabling Hardware technologies and standards.

Technology	Range	Standard	Frequency
RFID	10 m	RFID tag- 150 11784 (134KHz) RFID Air interface Protocol: ISO- 11785(13.56 MHz) RFID Payment System and Contactless Smart Card: ISO - 14443/15693 (13.56 MHz) Mobile RFID ISO/IEC- 18092 ISO/IEC- 29143 ISO 18000-1– Generic Parameters for the Air Interface for Globally Accepted Frequencies ISO 18000-2 (< 135 kHz) ISO 18000-3 (13.56 MHz) ISO 18000-4 (2.45 GHz) ISO 18000-6 (860 to 960 MHz) ISO 18000-7 (433 MHz)	13.56 MHz
Sensor	100 m	ISO/IEC- JTC1 SC31 and ISO/IEC Sensor Interfaces- IEEE 1451.x, EPC global, ISO TC 211, IEC, SC 17B, ISO TC 205 JTC1-WG7	900 and 2400 MHz
Quick response code	10:1 in inches	AIM , UPC Barcode, JIS, ISO	5- 1002 MHz or 1002-1218 MHz
Near Field Communication	4 cm	ISO/ IEC: 18000-3	13.56 MHz
Bluetooth Low Energy	100 m	IEEE 802.15.1	2.4GHz
6LoWPAN	20 m	IETF	900 and 2400 MHz
Z-Wave	30 m	Z-Wave Alliance (ZAD12837 / ITU-T G.9959)	900MHz for (ISM)
WiFi	50 m	802.11n	2.4GHz and 5GHz
Cellular	35 Km	GSM/GPRS/EDGE (2G), LTE (4G), UMTS/HSPA (3G),	900/1800/ 1900/2100MHz
Zigbee	10- 20 m	IEEE 802.15.4	2.4 GHz

4. Architecture:

IoT is capable of interconnecting billions of objects through Internet. It is very difficult process to manage entire objects in the internet. So there exists a need for the standardized layered architecture. Quite a number of architectures are proposed but still there is no standardized architecture [4],[17]. The design of IoT architecture depends on different factors such as communication, security, networking, business models, scalability and interoperability among homogeneous and heterogeneous devices are taken into consideration [18],[19],[20]. In IoT architecture initially proposed three layer architecture [4],[21]and the latter introduced four layers [21]and five layer architecture [4], [21],[26]. The categories of IoT architecture is shown in below.

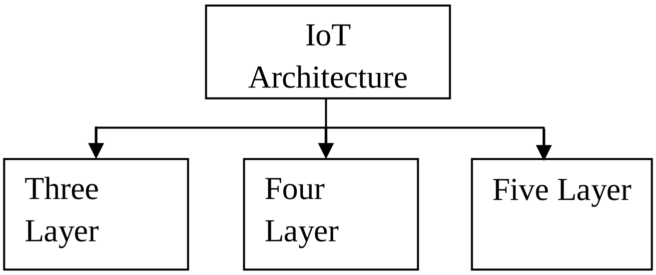

Figure 3. Categories of IoT Architecture.

4.1 Three Layer Architecture

Three layer (3-layer) architecture comprises of three layers namely: perception layer, network layer and application layer. Three layer (3-layer) architecture representation as shown in figure 4.

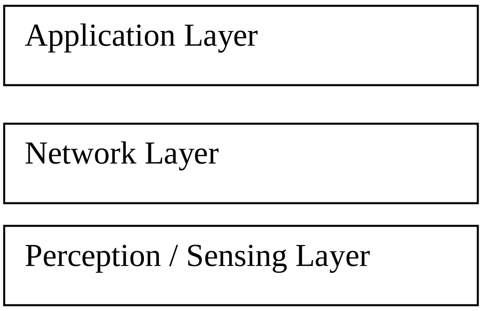

Figure 4. IoT Three Layer Architecture

Perception or Sensing Layer

Perception layer is a sensory organ of IoT. The Perception Layer mainly has things with RFID tags and reader-writers, 2D Bar code labels and readers, GPS, sensors, camera and other terminals. It senses the data from the environment. The physical layer considers the following factors such as

- Cost, size, resource, and energy consumption.
- Heterogeneity
- Deployment
- Communication
- Network
- Energy efficiency
- Protocols

Network Layer

The network layer responsible for obtain the data from sensor device. Sensor enabled devices connected to exchange the data via the network layer. It is capable of aggregating the data into own data base or cloud storage.

Application Layer or User Interface Layer

The user interface layer or application layer contains the interaction methods with user's applications.

4.2. Four Layer Architecture or Service Oriented Architecture

Shancang Li et'al proposed a service oriented architecture. It has totally four layers (4-layer) such as sensing layer, network layer, service layer, interface layer [18]. The service oriented architecture representation as shown in figure 5.

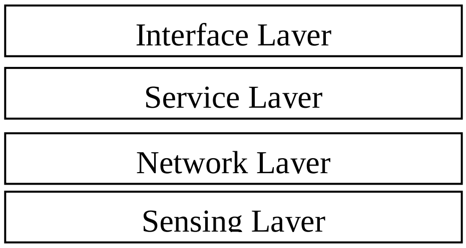

Figure5. IoT Four Layer Architecture

Sensing Layer

In sensing layer, RFID tags, Near Field and sensor are able to automatically collect and exchange the data from devices.

Network Layer: Network Layer is capable of collecting or aggregating data from devices or things to be stored in local database or cloud storage.

Service Layer: Middleware technology involves in service layer. It provides the services based on the user requirement. The service layer provides the services namely: data sharing and storage, data management, service discovery and composition.

Interface Layer

Interface layer provides the interaction method with user application among heterogeneous devices.

4.3 Five Layer Architecture

The recent internet of things application follows the five layer architecture. The three layer architecture can't provide all kinds of services and features of Internet of Things. So the researchers analyzed and introduced a new architecture, which based on the standard of the Internet and Telecommunications Management Network [22]. Miao Wu et' al and Luigi A et'al are proposed the five layer architecture.

Miao Wu et' al proposed the five layer (5- layer) architecture in 2010. Five layer (5-layer) architecture consists of Business Layer, Application Layer, Processing Layer, Transport Layer and Perception Layer. Miao Wu et'al proposed five layer (5-layer) architecture as shown in figure 6 [22].

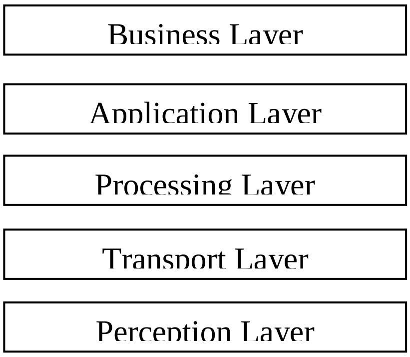

Figure 6. IoT Five Layer Architecture

Perception Layer

The perception layer is to observe or perceive the physical properties of objects namely: GPS, RFID, sensor, bar code and etc. It perceives the information in the form of Digital signal which is used to send over network.

Transport Layer or Network Layer

Transport layer or Network layer is responsible for transmitting data from the perception layer through various network namely: local area network (LAN), 3G, 4G,Wifi, Bluetooth, Zigbee, infrared, UMB, FTTx and etc. Now a day, internet of things planned to use IPV6 protocol in transport layer.

Processing Layer: The processing layer responsible for store, analyse, process the data from transport layer. Processing layer receives the massive volume of data and it can be stored in local database or cloud storage.

Application Layer:

Application layer provides the user interaction method and it processes the data from process layer. Application layer develops the various applications such as intelligent transportation, identity authentication, location-based services and etc. Application layer is very important role in IoT, which helps to increase the scale of the IoT in the entire aspects .

Business Layer

Business layer manages the application, business relevant model and some other business model in IoT.

4.4. Ala Al-Fuqaha et'al five layer (5-Layer) IoT architecture

Ala Al-Fuqaha et'al proposed five layer (5-Layer) IoT architecture and it referred from the network stack in 2015. Ala Al-Fuqaha et'al proposed architecture as shown in figure7.

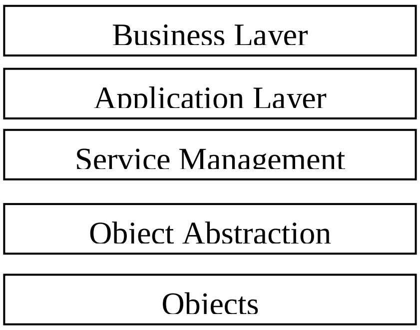

Figure 7. IoT Five layer Architecture.

Objects Layer

Physical devices unable to communicate directly with each other. In IoT scenario, the physical devices or objects attached to sensors or RFID Tags and uniquely assigned the IP address. The perception layer collects the information from sensors such as query location, temperature, soil moisture, vibration, humidity and etc. The plug and play architecture introduced and automatically configures the sensors. The sensor generates the digitized data and it transfers to the object abstraction layer [4], [23], [26].

Object Abstraction Layer

Object abstraction layer gets the information from object layer and send to service management layer. This layer is mainly using technologies namely: Bluetooth Low Energy, RFID, 3G, WiFi, GSM, GPS, Zigbee, 4G, 6LoWPAN and etc [4], [23].

Service Management Layer

Service management layer ensures to provide the services based on the demand of the user in a heterogeneous network environment [4], [23].

Application Layer: The application layer responsible to provide the services based on the customer need. The application layer covers different applications namely: smart city, intelligent transportation, health care, Smart Agriculture, smart home, etc [4].

Business Layer

The business layer responsible to manage the overall activities and business models. It helps to build a graph, flow chart, business model, decision-making and etc[4].

4.5. Middleware based Architecture

The middleware based IoT architecture representation as shown in figure 8.

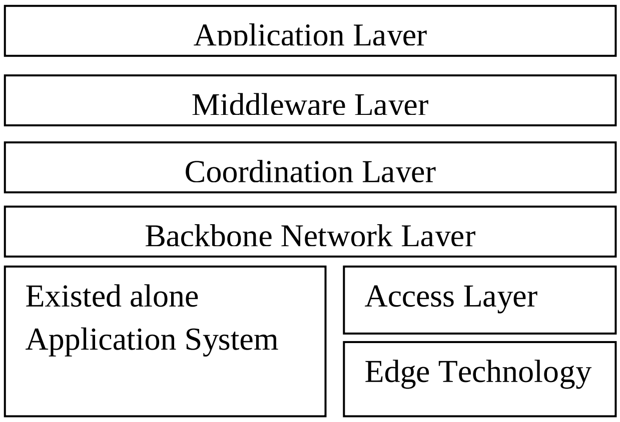

Figure 8: Middleware Based IoT Architecture

Edge technology Layer

Edge technology layer is a sensing layer, which is made up of embedded system and hardware devices. This layer has the responsibility to sense the data from the environment.

Access Layer

An access gateway layer responsible to manage the data and it is used for publishing and subscribing the services and communication between platforms.

Existed Alone Application System

The standardization of Internet of Things for enabling the interoperability that doesn't affect between existed application and new deployment object.

Backbone Network Layer

A backbone network is a computer network that exchanges the data from sensor devices in a heterogeneous network environment.

Coordination Layer

The co-ordination layer responsible for aggregating the data from different network.

Middleware layer

Middleware layer responsible for aggregate the data from hardware devices through backbone network layer.

Application layer

Application layer provides the different application services between the middleware layer and user applications.

5. IoT Protocols:

Many research working group proposed various standards. Some research working groups namely EPC global, Internet Engineering Task Force (IETF), European Telecommunication standards institute (EISI), Institute of

Electrical & Electronics Engineers (IEEE), World Wide Web Consortium (W3C) involves for Standardize the protocol. The standardized layer and its protocols as shown in figure 9.

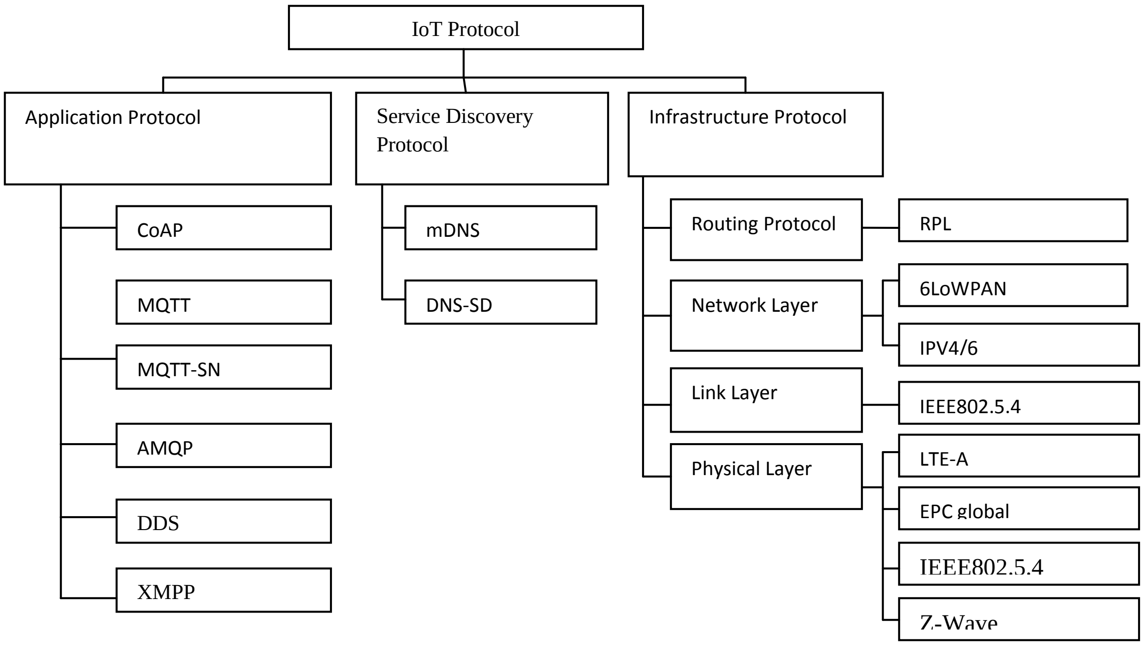

Figure 9. Standardization of IoT Protocols.

5.1. Application Protocol

Application layer provides the user interaction method and process the data from process layer. Application protocol used in application layer. The major application protocols such as CoAP, MQTT, DDS, AMQP, MQTT-SN and XMPP used in application protocol.

CoAP

Constrained Application Protocol (CoAP) is developed by IETF Constrained RESTful Environments (CoRE) Working Group. Coal is mainly used for application layer[4]. CoAP protocol objective is to allow smaller devices and computer capabilities to utilize RESTful communication. Constrained application protocol follows the synchronous Request and Response application layer protocol [24].

MQTT

In 2013, Nipper of Arcom and Andy Stanford Clark of IBM proposed Message Queue Telemetry Transport protocol(MQTT). It aims to connect the embedded devices and network with application and middleware. It runs over TCP. MQTT is mainly used for LAN communication over internet. MQTT consists of three components namely: 1. Publisher 2. Broker 3. Subscriber. A device act as subscriber. A subscriber informs to the broker. The broker sends the request to publisher. The publisher publishes the data based on the subscriber request. The publisher generated data send to subscriber through broker [25].

MQTT-SN

MQTT-SN specifically designed for sensor network. MQTT-SN is known as MQTT Version1.2. Zigbee Alliance developed the MQTT-SN Protocol. Z-Wave and etc. It mainly used for remote monitoring or controlled from cloud. MQTT-SN messages are light weight than MQTT messages [4].

Advanced Message Queuing Protocol

Advanced Message Queuing Protocol (AMQP) is an application layer protocol that mainly used for message oriented environments. It provides the reliable communication via message delivery protocol. AMQP uses the TCP protocol and exchange the information from one device to another device over internet. In wire protocol, AMQP uses two main components namely: exchanges and message queues.

The sensor device generates the data. Exchanges responsible to route the message queues. Message queues responsible to receive the messages or data. Rule based approach is used to route between the message queue and exchanges. The messages stored in the message queue and finally appropriate receiver receives the corresponding message [4], [26].

Data Distribution Service

Data Distribution service (DDS) follows the publish and subscribe protocol. Object Management Group (OMG) developed the Data Distribution Service protocol [27]. It contrasts to other publish and subscribe protocol such as AMQP, MQTT, MQTT-SN.

DDS based on broker less architecture, which uses multicasting services. In DDS is well suited for M2M communication. During the communication, DDS supports 23 Quality of services like security, reliability, durability and etc.

Extensible Messaging and Presence Protocol (XMPP)

XMPP is an Internet Engineering Task Force (IETF) instant messaging (IM) standard. Jabber open source community developed Extensible Messaging and Presence Protocol (XMPP). This protocol mainly used for voice & video calling and multi-party chatting.

XMPP allows the user to converse with each other to send a instant messages (IM) through all kind of operating system [4], [28]. XMPP allows Instant Message application to achieve access control, authentication, encryption and compatibility with other protocols [4], [29].

The Internet of Things application protocol features and properties are represented in Table-2.

Table-2 IoT Application Protocol Features and Properties.

Application Protocol	RESTful	Transport	Publish/ Subscribe Architecture	Request/ Response	Security	QoS	Header Size	Standard	Application
CoAP	Yes	UDP	Yes	Yes	DTLS	Yes	4	IETF	Mobile and Social network
MQTT	No	TCP	Yes	No	SSL	Yes	2	OASIS	Face book Messenger, health care, monitoring, Energy meter
MQTT-SN	No	TCP	Yes	No	SSL	Yes	2	OASIS	Remote monitoring
XMPP	No	TCP	Yes	Yes	SSL	No	-	Open Standard	Multi- party chatting, voice and video calling
AMQP	No	TCP	Yes	No	SSL	Yes	8	OASIS	Message Oriented Environment
DDS	No	TCP UDP	Yes	No	SSL DTLS	Yes	-	OMG	Multicasting
HTTP	Yes	TCP	No	Yes	SSL	No	-	IETF & W3C	Client-Server Information System

5.2 Service Discovery Protocol

In IoT Scenario increasing the number of devices requires a resource management scheme that able to enable the resources and manage the services dynamic way. Service discovery has two important protocols are namely: multicast DNS and DNS service discovery for discovering the resources and services in devices [4], [30].

5.3 Infrastructure Protocol

Network infrastructure is comprised of software and hardware resources of whole network that enable the network connectivity, communication, operations and management of the network. The infrastructure protocol can be used to enable the devices. The important infrastructure protocols such as, IPV6 over low power wireless personal area network, IEEE 802.15.4, Bluetooth Low Energy, Routing protocol for Low Power and Lossy Networks (RPL), EPC global, Long Term Evolution-Advanced (LTE-A) and Z-Wave [4].

6. Research Opportunities:

Now a day, many researchers are doing their research in IoT. Internet of Things is a blooming technology. In Near Future, Everything will be connected over the internet. Everything can be communicated to any things. In thissection presents the IoT research Opportunities based on most of the ongoing successful research work. IoT research opportunities are Ambient Services and Event monitoring, Context Aware and Sensor Search, Cipher-Physics System, Energy Management, Quality of Service (QoS), remote controlling, Resource Allocation, Routing, Scalable and Reliable, Security and Privacy, Service Oriented Architecture based , Social , Traffic Maintenance, Trustworthiness and etc.

Ambient Services and Event monitoring

Ambient intelligence deals with the electronic environment. It observes and response to the person's present in the environment. Ambient intelligence technologies are applied in Ambient Assisted Living (AAL) for handicapped or elderly people live their environment comfortable way.

KINOPTIM is one of the ambient assisted living Application which is mainly used for patient or elderly people monitoring in healthcare. An event monitoring system proposed a new service oriented user centred and event aware framework can be performed the services monitoring and handle the automatically occur events in Ambient environments[31].

Context Aware and Sensor Search

Now a day, people are expecting for smart life to move towards Internet of Things. In IoT system, the sensors continuously generate large quantities of raw data. Context aware computing is used to get more information about the surrounding in sensor data [32]. Charith perara et al implemented CASSARAM simulator that addressed the problem of context aware sensor selection, sensor search and sensor ranking model. CASSARAM is used to select the part of sensor information from a large set of sensory information with similar functionalities and the capacity [33].

Context aware applications are remote and continuous monitoring, elderly care support, and chronic disease management [34].

Cipher-Physical System

Computer based algorithm able to control the collection of computation, networking and physical processes that tightly integrated with the internet and its end-user. A cipher physical system consists of two levels, namely cipher level and physical level. Physical level consists of sensors and communication protocols. Cipher level consists of data management and storage. The cipher physical system helps to check the environment condition or ambient condition through remotely [35], [36].

Quality of Service

Quality of Service (QoS) evaluates the network performance. The Internet of things has many numbers of devices connected in heterogeneous networks. Each device makes different QoS need and difficult to satisfy the services. The conventional QoS attributes such as throughput, delay or jitter. These parameters are not enough for it. In, more QoS attributes are included, such as information accuracy, network resource needed, energy consumption and coverage [4]. Quality of Service is used to utilize the resources efficiently in the system [37].The development of energy- centered and QoS aware service selection algorithm (EQSA) for improve the QoS in IoT system. QoS is a major parameter in EQSA Algorithm. This algorithm is used to reduce the energy consumption of service but does't affect the user satisfaction [38].

Resource Allocation

The massive number of Machine to Machine (M2M) devices connects in the IoT scenario. Resource allocation is a challenging task in IoT. The random access method initially introduced for getting the service over the network. This method causes random access collisions and delays of the network connection establishment. Initially addressed two algorithms, namely: enhanced access barring (EAB), access class barring (ACB) for dynamic resource allocation, but both methods are not efficient. Yuan-chi pang et al proposed a context-aware dynamic resource allocation (CADRA) mechanism to resolve the random access contention. This mechanism improves the resource efficiency and also decreases the delay of connection establishment [39].

Routing: Routing is a process of selecting the best path among multiple paths in a network. The huge numbers of physical devices are connected to the internet. The sensor generates the massive amount data. The generated data to be stored in a local server or data center. So data center plays a vital role to store the sensor data. In recent years, novel server centric network structures based on the tree structure. Dynamic programming based routing mechanism provides the optimal solution for data centers [40].

Zhezhuang Xu et al proposed a joint clustering and routing (JCR) protocol for proficient and reliable data collection in Wireless Sensor Network. JCR adopts gradient routing and backoff timer to generate the proficient intercluster topology for maximum transmission range [41]. Ahmed Bader et al proposed uncoordinated power control mechanism for multi hop networking in the context of Internet of Things. This mechanism randomly adjust the transmit power level from blind cooperative cluster of each device. Each device should infer about neighborhood requirement of power utilization [42].

Ruonan Zhang et al proposed a hybrid approach called mobile collectionandnode density based clustering, futherly to combine theMobile elementand hierarchical routing data collection for collecting the data from large scale Wireless Sensor Network [43].

Security, Privacy and Trust Management

Security is a crucial role in IoT. The IoT system is vulnerable for few reasons such as wireless communication between the physical devices, low capabilities of components [8], [44]. Datagram Transport layer security (DTLS) initially used for system. DTLS protocol is suitable for lightweight components but it is not suitable for large scale devices [44]. Shahid Raza et al proposed a security concept for large scale and followed symmetric key Architecture[45]. Prasanta Gope et'al proposed a secure based modern health care system using body sensor network. It provides the security services and preserves the patient privacy [46]. Security and privacy applied for most of the application areas such as social Internet of things, Healthcare, Education, smart cities, smart home and etc.

Trust management plays avital role in for trustworthy data or information exchange between the devices. Trust is not only consider the security, but also follows some other factorsnamely: ability, goodness, strength, reliability and other characters of an entity [47].

Social Internet of Things (SIoT)

Social Internet of Things comprises of Internet of Things and social networking concepts. Social internet of things (SIoT) is a paradigm in which object is capable of establishing the social relationship and improve the scalability in information and service discovery.

The implementation of the social internet of Ihings raises the major issues related to information and service discovery in things. Luigi Atzori et'al provided the possible solution as how the social internet of things provides the information to objects, capable of devices and humans to discover select the objects and use objects with their services in IoT scenario[8], [48].

Major Research Challenges in IoT: In this part discusses the major research related issues in Internet of Things in table-3.

Table-3. Research challenges in IoT.

Issues	**Challenges**
Architecture	Many researchers proposed various architecture still not yet standardized the Architecture
Interoperability	Machine to Machine (M2M) communication
Security	i. The entire communication between the physical device is wireless communication ii. low capability devices participates in .
Privacy	Profile access operations between devices without interferences are difficult
Availability	Ability to provide the anytime, anywhere, anything services are challenge.
Scalability	Ability to add new devices doesn't affect the Quality of Service is a challenge in .
Mobility	The connecting user or devices can be getting the services while on the move is a challenge.

7. Applications: There is several application areas are widely used in Internet of Things (IoT). In This paper presents the application based on the current usages of the people. The applications are smart Home, Wearable, Industrial internet, smart city, connected health, smart grid, smart retail, connected car, smart farming, smart supply chain.

7.1 Smart Home

A smart home is a home or living environment that comprises of technology to allow home appliances connected to the internet for control & monitor automatically [49]. Smart home minimizes the user involvement to monitor the home object or devices and controlling the home appliances [50]. The smart home technologies such as Radio Frequency Identification (RFID) [51], micro controller enabled sensor and actuator [52], all kinds of sensors, like temperature sensor, humidity sensor and etc[52]. Implementation of the smart home can be divided into three layers namely: network layer, sensing and actuating layer and application layer. The sensing and actuating layer responsible for collecting the data from sensor enabled physical devices such as temperature, humidity, gas and etc.. Network layer responsible for transferring the data using Zigbee, WiFi, through the internet. Application layer provides the user required information to the user [53].

7.2 Wearable

Wearable technology responsible for tracking the activity using wearable devices in IoT scenario. Wearable devices are part of the wireless network of physical objects embedded with sensor, software,electronics and connectivity to enable the objects to share the information for operator and other connected devices without human involvement. Recently, Wearable technology is mainly used in the healthcare sector. Wearable sensors can be monitored and track the human activity, health condition, fitness condition, human behaviours and etc [54].

7.3 Smart City

A smart city is combining the IoT and information and communication technology (ICT) solution s to enrich the facilities and sophisticated life provides to the human being. Smart city another name is called as Urban. Smart city provides the public services namely: transport and parking, school and salubrity of hospitals surveillance and maintenance of public areas, lighting, and preservation of cultural heritage [55], [56], [57].The aim of smart city is to increase the quality of services (QoS), better use of public resources to offer the citizens, reducing the cost of the public administration.

7.4 Smart Grid

A smart grid is an electrical grid that consists of various energy measures, smart meters, smart appliances, renewable energy resources and energy efficiency resources. The smart grid technologies are distribution automation, substation automation, supervisory control and data acquisition (SCADA), demand response, energy management systems, power-line carrier communications, wireless mesh networks and fibre-optics. The significant features of the smart grid are flexibility, reliability, in network topology, load adjustment, sustainability efficiency, load balancing, and etc [58].

7.5 Industrial Internet

The industrial internet is a third wave of revolution in industries. The industrial revolution technologies are open computing and communication system, emerging technology to accelerate the productivity and enrich the human work experience. Many industries realized the potential of internet based technology. An intelligent decision system represents the physical world of machine; wireless networks can merge the connectivity [59].

7.6 Connected Car

A connected car is a car that has internet access to Wireless Local Area Network (WLAN)]. The connected car can exchange the information between the devices and other devices. This core enables new technologies to give the added benefits to drivers. The example features of connected car are notification of speeding and safety alerts, automatic notification of crashes helps to find parking or gas stations [60].

7.7 Connected Health

Connected Health is a revolution in the medical field.The patient fixes the sensor devices like fit bit healthcare sensors in their body. Body sensor collects the information and store into cloud storage. Then the doctor or patient family members can check the patient health information in remotely [61].

7.8 Smart Retail

The retail is the process of sale the commodities in small quantities directly to consumers. Smart Retail automates complex interactions from multiple sources such as collecting critical consumer data, alerts management of deviations from the global goals and monitor staff activity [2].

7.9 Smart Supply Chain

Supply Chain Management process of consider innovative strategies and deploy solutions that can help our organisation retain the customers in better way. It is a process of combining the business process from end-user through original supplier that creates a name based on product, service and information. Now a day, Internet of Things introduces to smart supply chain, especially logistics for improving the customer values for the specific product development company [62].

7.10 Smart Farming

Food is an important factor in our everyday life. Now a day, Most of the agriculture-based countries are decreasing their yield of the food production. Reasons of decreasing the food producers are population growth, climate change, pest attack and etc. The food and agricultural organization of the United Nation (FAO) predicts that the overall population will reach 8 billion people by 2025 and increases 9.6 billion people by 2050. The food production rate must increase 70% by 2050. Smart / precision farming system plays a critical role for improving farm activities. Modern farm management system adopts to replace the already existing farm management techniques. The lattest trend enables these technologies and controlled over internet. Internet of Things based farming techniques enables and expects to produce much food production in this current era [63], [64].

8. Conclusion:

In coming years, IoT is going to rule the world which is an extension of internet technology. Inter networking of physical object connected over the internet, that able to exchange the information between them. Now days, physical objects converts into smart objects, that can be learn and take the decision automatically by itself. The IoT objective is to improve the quality of life by connecting many smart objects, and technologies. This paper surveyed recent progresses on the Internet of Things from the aspect of IoT visions, enabling technologies, architecture, protocols, research opportunities and challenges and its applications.

References:

1. Ashton K. That ‘internet of things’ thing. RFID Journal. 2009 Jul 22;22(7):97-114.
2. Gubbi J, Buyya R, Marusic S, Palaniswami M. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems. 2013 Sep 30;29(7):1645-60.
3. Stankovic JA. Research directions for the internet of things. IEEE Internet of Things Journal. 2014 Feb;1(1):3-9.
4. Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M. Internet of things: A survey on enabling technologies, protocols, and applications. IEEE CommunicationsSurveys & Tutorials. 2015 Nov 18;17(4):2347-76.
5. Tan L, Wang N. Future internet: The internet of things. In2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE) 2010 Aug 20 (Vol.5, pp. V5-376). IEEE.
6. Mainetti L, Patrono L, Vilei A. Evolution of wireless sensor networks towards the internet of things: A survey. InSoftware, Telecommunications and Computer Networks (SoftCOM), 2011 19th International Conference on 2011 Sep 15 (pp. 1-6). IEEE.
7. Singh D, Tripathi G, Jara AJ. A survey of Internet-of-Things: Future vision, architecture, challenges and services. InInternet of things (WF-IoT), 2014 IEEE world forum on 2014 Mar 6 (pp. 287-292). IEEE.
8. Atzori L, Iera A, Morabito G. The internet of things: A survey. Computer networks. 2010 Oct 28;54(15):2787-805.
9. Razzaque MA, Milojevic-Jevric M, Palade A, Clarke S. Middleware for internet of things: a survey. IEEE Internet of Things Journal. 2016 Feb;3(1):70-95.
10. Verma DC, Verma P. Techniques for Surviving Mobile Data Explosion. John Wiley &Sons; 2014 Feb 28.
11. Nimbits,Sep. 25, 2014. [Online]. Available: http://www.nimbits.com/
12. Wei Y, Sukumar K, Vecchiola C, Karunamoorthy D, Buyya R. Aneka cloud application platform and its integration with windows azure. arXiv preprint arXiv:1103.2590. 2011 Mar 14.

13. Coetzee L, Eksteen J. The Internet of Things-promise for the future? An introduction. InIST-Africa Conference Proceedings, 2011 2011 May 11 (pp. 1-9). IEEE.
14. Want R. Near field communication. IEEE Pervasive Computing. 2011;3(10):4-7.
15. Gomez C, Oller J, Paradells J. Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology. Sensors. 2012 Aug 29;12(9):11734-53.
16. Shelby Z, Bormann C. 6LoWPAN: The wireless embedded Internet. John Wiley & Sons;2011 Aug 17.
17. Khan R, Khan SU, Zaheer R, Khan S. Future internet: the internet of thingsarchitecture, possible applications and key challenges. InFrontiers of InformationTechnology (FIT), 2012 10th International Conference on 2012 Dec 17 (pp. 257-260).IEEE.
18. Da Xu L, He W, Li S. Internet of things in industries: A survey. IEEE Transactions on Industrial Informatics. 2014 Nov;10(4):2233-43.
19. Looy AV, Backer MD, Poels G. A conceptual framework and classification of capability areas for business process maturity. Enterprise Information Systems. 2014 Mar 4;8(2):188-224.
20. Ulmer JS, Belaud JP, Le Lann JM. A pivotal-based approach for enterprise business process and IS integration. Enterprise Information Systems. 2013 Feb 1;7(1):61-78.
21. Krčo S, Pokrić B, Carrez F. Designing IoT architecture (s): A European perspective. InInternet of Things (WF-IoT), 2014 IEEE World Forum On 2014 Mar 6 (pp. 79-84). IEEE.
22. Wu M, Lu TJ, Ling FY, Sun J, Du HY. Research on the architecture of Internet of things. In2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE) 2010 Aug 20 (Vol. 5, pp. V5-484). IEEE.
23. Yang Z, Yue Y, Yang Y, Peng Y, Wang X, Liu W. Study and application on the architecture and key technologies for IOT. InMultimedia Technology (ICMT), 2011 International Conference on 2011 Jul 26 (pp. 747-751). IEEE.
24. Zouganeli E, Svinnset IE. Connected objects and the Internet of things—A paradigm shift. In2009 International Conference on Photonics in Switching 2009 Sep 15 (pp. 1-4). IEEE.
25. Hunkeler U, Truong HL, Stanford-Clark A. MQTT-S—A publish/subscribe protocol for Wireless Sensor Networks. InCommunication systems software and middleware and workshops, 2008. comsware 2008. 3rd international conference on 2008 Jan 6 (pp. 791-798). IEEE.

26. Godfrey R, Ingham D, Schloming R. OASIS Advanced Message Queuing Protocol (AMQP) Version 1.0; OASIS Standard.
27. Data distribution services specification, V1.2, Object Manage. Group(OMG), Needham, MA, USA, Apr. 2,2015. [Online]. Available: http://www.omg.org/spec/DDS/1.2/.
28. Saint-Andre P. Extensible messaging and presence protocol (XMPP): Core.
29. Jones MT. Meet the extensible messaging and presence protocol (xmpp). IBM developerWorks, Markham, ON, Canada. 2009.
30. Jara AJ, Ladid L, Gómez-Skarmeta AF. The Internet of Everything through IPv6: An Analysis of Challenges, Solutions and Opportunities. JoWUA. 2013 Sep;4(3):97-118.
31. Yachir A, Amirat Y, Chibani A, Badache N. Event-Aware Framework for DynamicServices Discovery and Selection in the Context of Ambient Intelligence and Internet of Things. IEEE Transactions on Automation Science and Engineering. 2016 Jan;13(1):85-102.
32. Perera C, Zaslavsky A, Christen P, Georgakopoulos D. Context aware computing for theinternet of things: A survey. IEEE Communications Surveys & Tutorials. 2014 Jan 1;16(1):414-54.
33. Perera C, Zaslavsky A, Christen P, Compton M, Georgakopoulos D. Context-aware sensor search, selection and ranking model for internet of things middleware. In2013IEEE 14th International Conference on Mobile Data Management 2013 Jun 3 (Vol. 1, pp.314-322). IEEE.
34. Mortazavi B, Pourhomayoun M, Ghasemzadeh H, Jafari R, Roberts CK, Sarrafzadeh M.Context-Aware Data Processing to Enhance Quality of Measurements in Wireless Health Systems: An Application to MET Calculation of Exergaming Actions. IEEE Internet of Things Journal. 2015 Feb;2(1):84-93.
35. Mois G, Sanislav T, Folea SC. A Cyber-Physical System for Environmental Monitoring. IEEE Transactions on Instrumentation and Measurement. 2016 Jun;65(6):1463-71.
36. Sha L, Gopalakrishnan S, Liu X, Wang Q. Cyber-physical systems: A new frontierInMachine Learning in Cyber Trust 2009 (pp. 3-13). Springer US.
37. Nef MA, Perlepes L, Karagiorgou S, Stamoulis GI, Kikiras PK. Enabling qos in the internet of things. InProc. of the 5th Int. Conf. on Commun., Theory, Reliability, and Quality of Service (CTRQ 2012) 2012 (pp. 33-38).
38. Khanouche ME, Amirat Y, Chibani A, Kerkar M, Yachir A. Energy-Centered and QoS-Aware Services Selection for Internet of Things.

39. Pang YC, Lin GY, Wei HY. Context-Aware Dynamic Resource Allocation for Cellular M2M Communications. IEEE Internet of Things Journal. 2016 Jun;3(3):318-26.
40. Xie J, Lyu L, Deng Y, Yang LT. Improving Routing Performance via Dynamic Programming in Large-Scale Data Centers. IEEE Internet of Things Journal. 2015 Aug;2(4):321-8.
41. Xu Z, Chen L, Chen C, Guan X. Joint Clustering and Routing Design for Reliable and Efficient Data Collection in Large-scale Wireless Sensor Networks.
42. Bader A, Alouini S. Localized Power Control for Multihop Large-Scale Internet of Things.
43. Zhang R, Pan J, Xie D, Wang F. NDCMC: A Hybrid Data Collection Approach for Large-Scale WSNs Using Mobile Element and Hierarchical Clustering.
44. Alam S, Chowdhury MM, Noll J. Interoperability of security-enabled internet of things.Wireless Personal Communications. 2011 Dec 1;61(3):567-86.
45. Raza S, Seitz L, Sitenkov D, Selander G. S3K: Scalable Security With Symmetric Keys—DTLS Key Establishment for the Internet of Things.
46. Gope P, Hwang T. BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network. IEEE Sensors Journal. 2016 Mar 1;16(5):1368-76.
47. Yan Z, Zhang P, Vasilakos AV. A survey on trust management for Internet of Things. Journal of network and computer applications. 2014 Jun 30;42:120-34.
48. Geetha S. Social Internet of Things. World Scientific News. 2016 Jan 1;41:76.
49. Bing K, Fu L, Zhuo Y, Yanlei L. Design of an Internet of things-based smart home system. InIntelligent Control and Information Processing (ICICIP), 2011 2ndInternational Conference on 2011 Jul 25 (Vol. 2, pp. 921-924). IEEE.
50. Soliman M, Abiodun T, Hamouda T, Zhou J, Lung CH. Smart home: Integrating internet of things with web services and cloud computing. InCloud Computing Technology andScience (CloudCom), 2013 IEEE 5th International Conference on 2013 Dec 2 (Vol. 2, pp.317-320). IEEE.
51. Darianian M, Michael MP. Smart home mobile RFID-based Internet-of-Things systemsand services. In2008 International conference on advanced computer theory and engineering 2008 Dec 20 (pp. 116-120). IEEE.
52. Jie Y, Pei JY, Jun L, Yun G, Wei X. Smart home system based on IOT technologies. InComputational and Information Sciences (ICCIS), 2013 Fifth International Conference on 2013 Jun 21 (pp. 1789-1791). IEEE.

53. Li B, Yu J. Research and application on the smart home based on component technologies and Internet of Things. Procedia Engineering. 2011 Dec 31;15:2087-92.

54. Hiremath S, Yang G, Mankodiya K. Wearable Internet of Things: Concept, architecturalcomponents and promises for person-centered healthcare. InWireless Mobile Communication and Healthcare (Mobihealth), 2014 EAI 4th International Conference on 2014 Nov 3 (pp. 304-307). IEEE.

55. Zanella A, Bui N, Castellani A, Vangelista L, Zorzi M. Internet of things for smart cities. IEEE Internet of Things Journal. 2014 Feb;1(1):22-32.

56. Theodoridis E, Mylonas G, Chatzigiannakis I. Developing an IoT Smart City framework.InIISA 2013 Jul 10 (pp. 1-6).

57. Hernández-Muñoz JM, Vercher JB, Muñoz L, Galache JA, Presser M, Gómez LA, Pettersson J. Smart cities at the forefront of the future internet. InThe Future Internet Assembly 2011 May 17 (pp. 447-462). Springer Berlin Heidelberg.

58. Berger LT, Schwager A, Escudero-Garzás JJ. Power line communications for smart grid applications. Journal of Electrical and Computer Engineering. 2013 Jan 1;2013:3.

59. Jeschke S, Brecher C, Meisen T, Özdemir D, Eschert T. Industrial Internet of Things and Cyber Manufacturing Systems. InIndustrial Internet of Things 2017 (pp. 3-19). Springer International Publishing.

60. Zouganeli E, Svinnset IE. Connected objects and the Internet of things—A paradigm shift. In2009 International Conference on Photonics in Switching 2009 Sep 15 (pp. 1-4). IEEE.

61. Gope P, Hwang T. BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network. IEEE Sensors Journal. 2016 Mar 1;16(5):1368-76.

62. Cooper MC, Lambert DM, Pagh JD. Supply chain management: more than a new namefor logistics. The international journal of logistics management. 1997 Jan 1;8(1):1-4.

63. Kaloxylos A, Eigenmann R, Teye F, Politopoulou Z, Wolfert S, Shrank C, Dillinger M, Lampropoulou I, Antoniou E, Pesonen L, Nicole H. Farm management systems and the Future Internet era. Computers and electronics in agriculture. 2012 Nov 30;89:130-44.

64. Rupanagudi SR, Ranjani BS, Nagaraj P, Bhat VG, Thippeswamy G. A novel cloud computing based smart farming system for early detection of borer insects in tomatoes. InCommunication, Information & Computing Technology (ICCICT), 2015 International Conference on 2015 Jan 15 (pp. 1-6). IEEE.