Wireless Personal Communications (2020) 112:1383–1429
https://doi.org/10.1007/s11277-020-07108-5

A Survey on Architecture, Protocols and Challenges in IoT

C. C. Sobin[1]

Published online: 25 January 2020

Abstract
Internet of Things (IoT) is an emerging paradigm which aims to inter-connect all smart physical devices, so that the devices together can provide smart services to the users. Some of the IoT applications include smart homes, smart cities, smart grids, smart retail, etc. Since IoT systems are built up with heterogeneous hardware and networking technologies, connecting them to the software/application level to extract information from large amounts of data is a complex task. In this paper, we have surveyed various architecture and protocols used in IoT systems and proposed suitable taxonomies for classifying them. We have also discussed the technical challenges, such as security and privacy, interoperability, scalability, and energy efficiency. We have provided an in-depth coverage of recent research works for every mentioned challenge. The objective of this survey is to help future researchers to identify IoT specific challenges and to adopt appropriate technology depending on the application requirements.

Keywords Internet of Things · Architecture · Protocols · Challenges · Security

1 Introduction

Internet of Things (IoT) is a technology that connects any possible objects/things, so that the things start communicating among themselves to provide better services for users in an unimaginable way and makes their life easier. Intelligent things could be set of sensors, actuators, smart phones, etc. Some of the applications of IoT include, smart home, smart city, smart agriculture, smart retail and smart health, etc. The idea IoT was first introduced by Kevin Ashton in 1999, when he was working with Auto-ID Center to develop network of objects using Radio-frequency Identification (RFID). Today, there are more connected objects to Internet than humans. A recent study shows that the number of connected devices in earth will reach up to 20 million by 2020.

Along with the enormous growth of IoT, there are many issues and challenges to be addressed while developing IoT applications. Since, IoT is able to connect every physical object, heterogeneity comes into picture, where IoT must be operated on large number of heterogeneous devices. So a unifying architecture/middleware is needed to implement IoT,

✉ C. C. Sobin
sobincc@gmail.com

[1] Department of CSE, SRM University, Amaravati, AP, India

although there are many reference models [1–3] for creating IoT architecture and middleware [4–7] for implementing IoT on current Internet architecture.

Interoperability is another challenge where different devices must be able to communicate. Although there are many standard protocols developed for different IoT applications, a unifying protocol structure is still required. Quality of service parameters such as, security must be taken care since anyone will be able to access the data by accessing the device or accessing data during transmission, in both cases the data must be secured. So, authentication is very important, and the user's identity must not be revealed and during communication between devices user data must not be tapped.

Scalability is another challenge to be addressed. Since, the number of devices being connected is large in number, scalability must be considered while designing routing protocols and data storage mechanisms. Energy efficiency must be also taken care, since IoT devices have limited resources and battery power. Routing protocols designed for communication between IoT devices must take care of congestion, since number of devices must be communicated are huge in number. Another interesting research area is exploring social side of IoT. Although there are many surveys have been proposed in literature, our survey is different from others, in the view of covering every aspects of IoT, such as, architecture, protocols, security and privacy, scalability and energy efficiency, etc., and describing the most recent research works associated with them. So, our survey can be considered as the most recent and comprehensive survey on IoT. We have also identified some of the futuristic application domains of IoT, such as Social IoT, Opportunistic IoT, etc., and applicability of emerging network architectures, like Content Centric Networking (CCN), Named Data Network (NDN), etc. in IoT.

The rest of this paper is organized as follows, Sect. 2 describes the applications of IoT and Sect. 3 mentions the requirements of IoT. In Sect. 4, we have discussed the enabling technologies used by IoT applications. Section 5 describes existing taxonomy and the proposed taxonomy are described in Sect. 6. Section 7 describes the IoT architecture and the middleware developed for IoT till now. Section 8 describes the communication protocols used in IoT applications. Section 9 describes auxiliary issues associated with IoT applications, such as security and privacy, energy efficiency, scalability and social networking with IoT. Performance comparison of some of the existing IoT based applications in Sect. 10. The open problems identified as part of the study is listed in Sect. 11. Finally, we conclude in Sect. 12.

2 Applications of IoT

There are numerous applications of IoT in various fields such as home, health care, industries, retail, transportation, surveillance, etc. as shown in Fig. 1.Some of the applications of IoT is listed below.

- *Smart Health Care*: Integrating IoT features to medical devices will improve the quality of the services to the patients, particularly to elderly people who require constant supervision. IoT can be used to monitor old people for fall detection, to monitor temperature conditions inside refrigerator, which stores medicines, vaccines, and to monitor the patient's condition in hospitals and home. Today main focus on smart healthcare solutions is to develop wearable devices which will help to capture the medical data. An example of a smart health scenario is described in Fig. 2, in

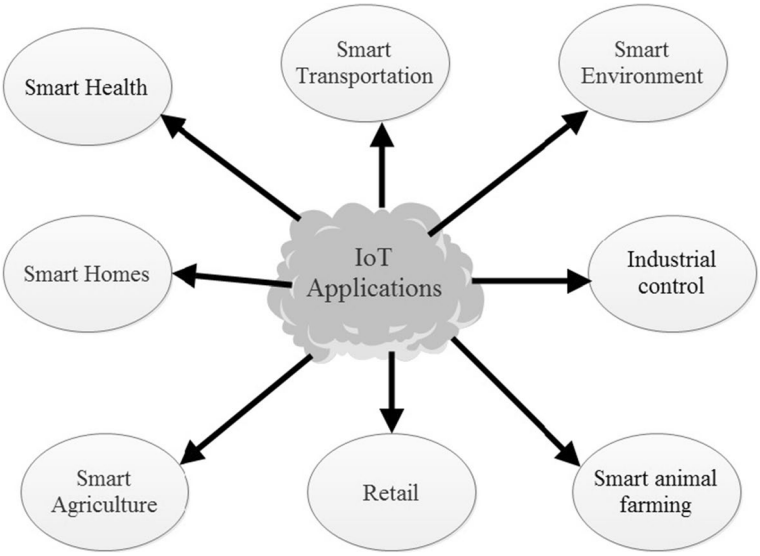

Fig. 1 Applications of Internet of Things

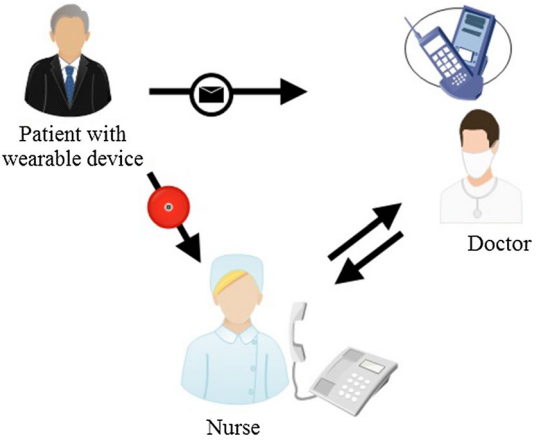

Fig. 2 Example of a smart health scenario

which a wearable device is attached to the patient, which will send notifications to nurses or doctors directly, when there is an abnormal behaviour of the patient health. Although the expansion of IoT in healthcare sector is a promising area, there are some issues also to be considered related to data privacy and security.

- *Smart Homes*: In smart homes, we will have the ability to control any device of home using a laptop or smart phone, and devices talk to each other to provide us useful services. Using smart meters, we can measure the energy consumption, and temperature. As in Fig. 3, a smart home consists of several smart things, like light control, temperature control, remote control, camera surveillance, high-speed Internet, smart appliances, smart media, etc., to ensure smart living for people.

Fig. 3 Smart home scenario

- *Retail*: IoT can be used for tracking of products, for monitoring storage conditions of products. It can be used to give suggestions to customers in shopping based on their habits, and also can be used in automatic restocking process by helping in control and rotation of products in shelves and warehouses of the stores.
- *Smart Transportation*: IoT is used in finding the location of items in big warehouses or harbours, checking quality conditions during shipment of goods, controlling routes followed for delicate goods such as gold, medical drugs, etc. Example of a smart vehicular environment is shown in Fig. 4, in which the various sensors help to analyze traffic patterns and notify traffic jams, accidents, available parking slots, etc. Such information helps the passengers for a smart and intelligent driving.
- *Industrial Control*: In industries IoT is used to monitor air quality, temperature, ozone presence, and sending alarm in case of emergencies. One example is the baggage handling machine used in the airports, where the sensors sense whether the baggage is

Fig. 4 Smart vehicular environment

moving on the conveyor belt and stops if none are moving. Baggage is identified based on the barcodes.

- *Smart Agriculture*: IoT can be used to monitor soil moisture, control climatic conditions in order to maximize fruit production, controlling humidity and temperature levels to prevent fungus. IoT can monitor weather conditions to predict rain, ice formation, drought, etc. A real-life example of such smart agriculture system is a smart cattle farm in which the information about cattle movement, behaviour, fertility, and lactation are available to the owners using smart phones, which helps to increase the productivity.
- *Smart Environment*: In order to detect and prevent natural disasters like earthquakes, landslides, etc., IoT can be used in monitoring environmental conditions. For detecting CO2 emissions by factories and cars, and to detect fire in forest, etc., IoT can be used.

3 Requirements of IoT

IoT is facing several hindrances on its way of being implemented as a global technology. There are many open issues that need to be addressed for efficient implementation of IoT. Some of them are, lack of standard architecture and standard protocols, security and privacy, device heterogeneity, scalability, energy efficiency, interoperability and data management (Fig. 5).

- *Identification and Scalability*: Overall scope of IoT is much larger than Internet of computers. As the number of objects being interconnected is huge in number, scalability issues arise at different levels.

(a) Naming & addressing: As numbers of devices that are going to be connected are huge in number, address space should be large enough to accommodate all the devices.
(b) Data communication: A large number of devices are connected with high-level of interconnection, so scalability arises for data communication.
(c) Information management: The data generated by the vast number of sensors is enormous. Proper information extraction mechanisms must be used in order to extract useful information from the data, and to store data.
(d) Service provisioning and management: Massive numbers of services are available with IoT.

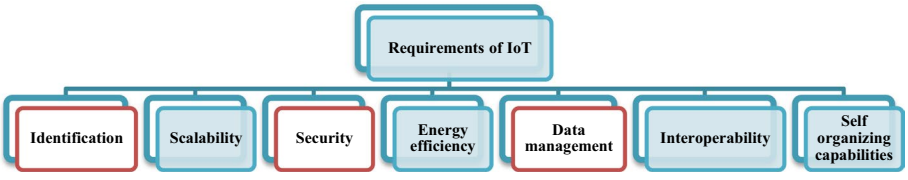

Fig. 5 Requirements of IoT

- *Self-organizing Capability*: Unlike computers which need users to configure, smart objects need to organize, configure, adapt to situations without requiring human intervention. In order to meet the scale and complexity of IoT, devices need to manage themselves without external intervention. There is a need for distributed intelligence in IoT, allow the smart objects able to autonomously react to a wide range of different situations, thereby minimizing human intervention. Self-organization capabilities include automatic service discovery, automatic device discovery without requiring external trigger and the ability to adaptively tune to protocols behavior.
- *Interoperability*: In IoT different kinds of smart objects have different capabilities in terms of computation, communication, bandwidth, energy available, etc. To facilitate communication and cooperation between these different types of devices, common standard is required.
- *Data Management*: In IoT environment, sensor networks generate large amounts of data, which will be stored on central nodes or servers. Every device may need some service, finding the server which provides the requested service must be done in an efficient manner. Generating useful information from raw sensor data might be useful for finding energy consumption or helps in many businesses.
- *Security and Personal Privacy*: Security is the key requirement that can ensure wide adoption of IoT technology. Security must be considered as a key system-level priority for IoT and has to be taken into account in architecture of IoT. In a wireless IoT context, due to weakness of radio signals eavesdropping kind of security attacks are possible, and due to heavily constrained nature of the devices and limited bandwidth makes it highly challenging to implement security policies in IoT. Security algorithms must be simple and there should be a minimum number of message exchanges due to limited bandwidth.
- *Energy Efficiency*: Energy in its three phase's energy harvesting, energy conservation and energy consumption are a major issue to be addressed in IoT, as the devices of IoT are constrained in nature, which implies they have limited battery power. For all IoT entities, minimizing energy to be spent in computing/communication is a primary constraint.

    (a) Energy harvesting techniques: piezoelectric materials, thermos-electric, micro solar panels.
    (b) Energy conservation techniques: Batteries, fuel cells, polymer batteries.

4 Enabling Technologies

The concept of IoT is implemented using several enabling technologies such as RFID, Wireless Sensor Network (WSN), and Machine-to-Machine (M2M) communication, etc., RFID technology makes objects uniquely identifiable, whereas, sensor nodes used in WSNs are widely used for sensing different environmental conditions.

4.1 Radio Frequency Identification (RFID)

RFID is playing a predominant role as an identifying technology of IoT. RFID is becoming more popular and is expected to replace the bar code technology in the near future. RFID is a means of storing and retrieving data through electromagnetic transmission, i.e.,

using radio waves. RFID includes an RFID tag, reader, antenna, and a back-end database server. RFID Reader reads data from the tags and then forwards it to the back-end server, from which users can access data. RFID operates in different radio frequencies, such as *low frequency*, *high frequency*, *ultra-high frequency*, and *microwave* depending on the requirements of the applications they support. There are three types of RFID tags depending on whether they use battery or not. Passive tags use battery power for communication and sensing, which are more suitable in case of IoT, as battery replacement is a costly operation. However, they lead to lower quality sensing and work with only short ranges. Semi-Passive tags use power generating circuits for powering the RF components on chip and battery power to maintain internal volatile memory. Active tags depend completely on battery power. They have more memory, more range in comparison to semi-passive tags. Normally passive tags transmit all the frequencies, where the active tags transmit only the high frequency. The components as part of RDIF based IoT applications (Fig. 6) are listed below.

- Tag: It contains a microchip for storing the identification number. The microchip has an antenna which helps exchange data with readers. A tag is attached to an object and gives a unique identification number to the object. The tag can store and read data and has some amount of computational capability.
- Antenna: It acts as tag detector which creates a magnetic field.
- Reader: It exchanges information from tags which are in its proximity. It consists of transmitter, receiver and memory and control units. Using transmitter and receiver it exchanges information between antenna attached to tag and itself.
- Back-end database server: It stores the mapping between the tag ID and the actual object attached to it.

Each object in IoT should be uniquely identifiable when objects are connected in a network. In some scenarios, objects instead of being uniquely identified, they may be identified as an object of particular class ('e.g., this object is a pen, regardless of which pen it is'). This identification can be done in many ways such as RFID, IP, QR codes, etc. If object is given a physical RFID tag, then object can be read by an RFID reader. Reader

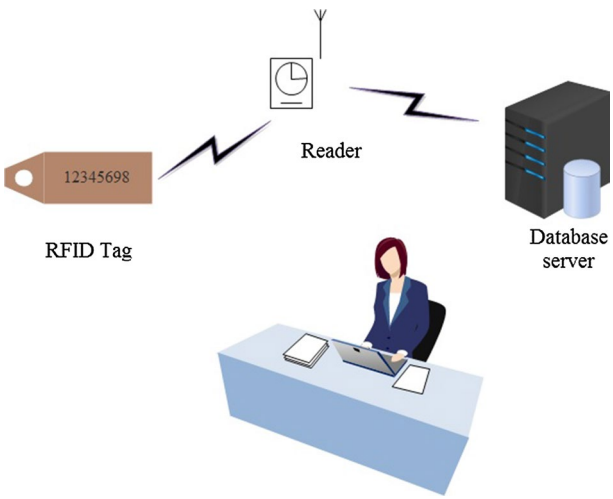

Fig. 6 Components of an RFID based IoT Application

gives the identification number of the device. In this way we can track location of items in logistics, warehouse, etc. Other way is to provide unique description for each device, i.e., every device is uniquely identifiable by its own. RFID technology suffers from large size of tag; also, hardware needed increases since RFID readers must be present to read data from tags. Therefore, for every set of RFID tag, a reader must be present. Different objects designed by different companies may use different coding schemes, and they won't be willing to change to some new identification scheme. So, to use EPC code, uCode and other coding schemes a global identification scheme must be designed, which is backward compatible with the coding schemes that are currently being used by industries.

Although RFID is the most popular technology used in many of the IoT applications such as home automation, supply chain management, etc., there are some issues associated with employing RFID tags. By simply using RFID tags only the identification procedure can be exploited, for making things "smart", sensors have to be integrated with IoT for sensing surrounding environment and making decisions accordingly. Also, the use of RFID without any security measures will help the malicious users to read/modify the tags remotely. A most common issue with RFID systems is the collision due to simultaneous tag responses, which may result in wastage of resources such as bandwidth energy, etc., and the increased delay in retrieving the objects. Another issue is the need for a single communication protocol to ensure interoperability. Also, in the case of active tags, the battery life is a crucial aspect to be considered for developing long lasting IoT applications.

Even with the aforementioned issues, there are still scope for using RIFD as enabling technology for many of the future smart IoT applications. Consider the scenario of a smart shopping, in which the tags associated with the items will communicate directly with the people, by introducing themselves, which, will make the shopping smarter. Another example is the case of a smart supply chain management in which the tags associated with the items communicates with the staff in charge to put new tags or replace old tags, etc.

4.2 Wireless Sensor Network (WSN)

Wireless Sensor Network (WSN) is a set of sensor nodes distributed spatially and are used for monitoring environmental conditions. WSNs have used in many of the IoT applications, such as air pollution monitoring, battlefield surveillance, water quality monitoring, natural disaster prevention, etc. An example of deployment of wireless sensors in battlefield is

Fig. 7 Example scenario of sensors deployed in battlefield

shown in Fig. 7, where sensor nodes are deployed in no-man's land or in border areas to collect strategic information. In such a network, sensors are having self-organizing capability and are able to detect and classify multiple targets using the acoustic and magnetic signals. In order to make the sensors unobtrusive, the resources associated with sensor nodes, such as battery power, memory, etc., are very small and also there is no provision to reuse them, which will cause some of the sensors to die out completely and stops functioning. So, for a WSN based IoT applications, the resource-constrained nature of sensor nodes has to be considered while designing the distributed algorithms and communication protocols.

Sensor nodes can exchange data among themselves. There are two types of WSNs, namely centralized, decentralized. In centralized WSN, data from all sensor nodes are transmitted to a single system, which does process and communication. This has drawbacks of single point of failure and also load on a single system will be too high. In distributed WSN, sensor nodes can retrieve process and provide data to other sensor nodes or end users. WSN contains two kinds of entities; they are sensor nodes, and end users. Sensor nodes of two different local networks communicate using gateways. There are three different ways of connecting WSNs to the Internet. In the first approach, WSNs can be connected to the Internet using a single gateway. Another approach is a hybrid network, while some of the sensors can directly access the Internet using different gateways. The final approach is based on WLAN structure and forming an IEEE 802.15.4 access point network, where sensors can access Internet in one hop.

Although WSNs are more suitable to be used as the integrating technology for IoT based applications, there are some issues that have to considered, which are summarized below.

- Security: There are some security related issues related to sensor nodes. In order to prevent the physical attack on the deployed sensors, particularly for military applications, the sensors should be unobtrusive from enemies, which is very difficult to achieve, as only solution is to reduce the size of the sensors, which will limit their resources. Self-organizing nature of sensor nodes may cause some of the nodes to behave maliciously and will disrupt the functioning of the WSNs. Presently the solution to security related issues is deploying cryptographic solutions, like encryption, etc., but due to the less energy and memory associated with the sensor makes the task difficult.
- Energy efficiency: As mentioned earlier, due to the nature of the area where the sensors deployed (e.g., no-man's land, border areas, etc.) there may not have provision for recharging the batteries. So, designing energy efficient algorithms for WSNs is still an open area of research.
- Quality of Service (QoS) requirements: Ensuring QoS requirements as with Internet or traditional wired architecture are not yet achieved with WSNs used for many of the applications. Because of the mobility and varying network topology the sensor nodes may not be able to achieve the strict QoS requirements related to many of the real-time IoT applications.

4.3 Machine-to-Machine Communication

The most important part in IoT is the interconnection between machines or objects. M2M communication enables the communication between machines. M2M enables Machine-to-Machine, Machine-to-Mobile and Machine-to-Man communication through the transmission of wireless network. The main functionality of the M2M communication is the remote monitoring because, it has wide use in many of the IoT applications

such as supply chain management, traffic control, telemedicine and many other logistic services. The main components of an M2M communication (Fig. 8) includes, short-range communication technologies such as RFID, Wi-Fi, Bluetooth, etc., cellular communication links and a local server, which are able to analyze the data and take decisions. The European Telecommunication standard Institute (ETSI) is focused on M2M communication. Please refer to the technical report [8] for more details on M2M communication.

AlthoughM2M communication is a key aspect of many of the smart IoT applications, there are some issues to be considered.

- Lack of standardization: There is no standardization currently available for M2M communication, which leads to design application-specific or device-specific platforms. So, the manufacturers need to agree up on developing common standards for device-to-device communications.
- Naming and addressing: Another aspect is related to naming and addressing. M2M communication should be able to support more than one naming schemes, and more than one device (or a group of devices) with a single name to support multicasting.
- Security: Although M2M communication is having less human intervention, proper security measures has to be taken to prevent many of security threats such as, unauthorized access, physical tampering, etc. The remote management functionality provided in many of the M2M applications require proper use of firmware to prevent malicious attacks.

In this section, we have summarized some of the key enabling technologies used for IoT applications, such as RFID, WSN and M2M communications.

5 Existing Taxonomies of IoT

In this section, we study the existing taxonomies on IoT that have been so far listed in the literature. A timeline of the existing surveys is listed in Fig. 9. Here, we have covered the existing taxonomies in the existing literature classified them based on different domains they addressed (Fig. 10).

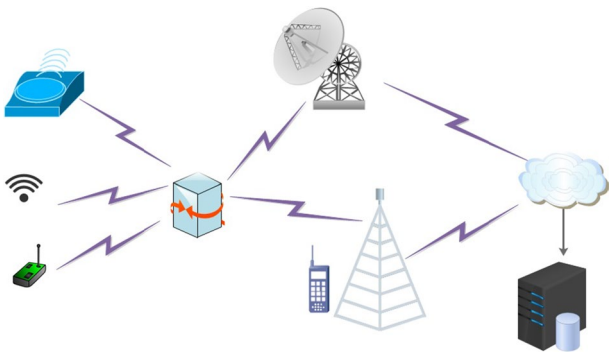

Fig. 8 Components of M2M communication

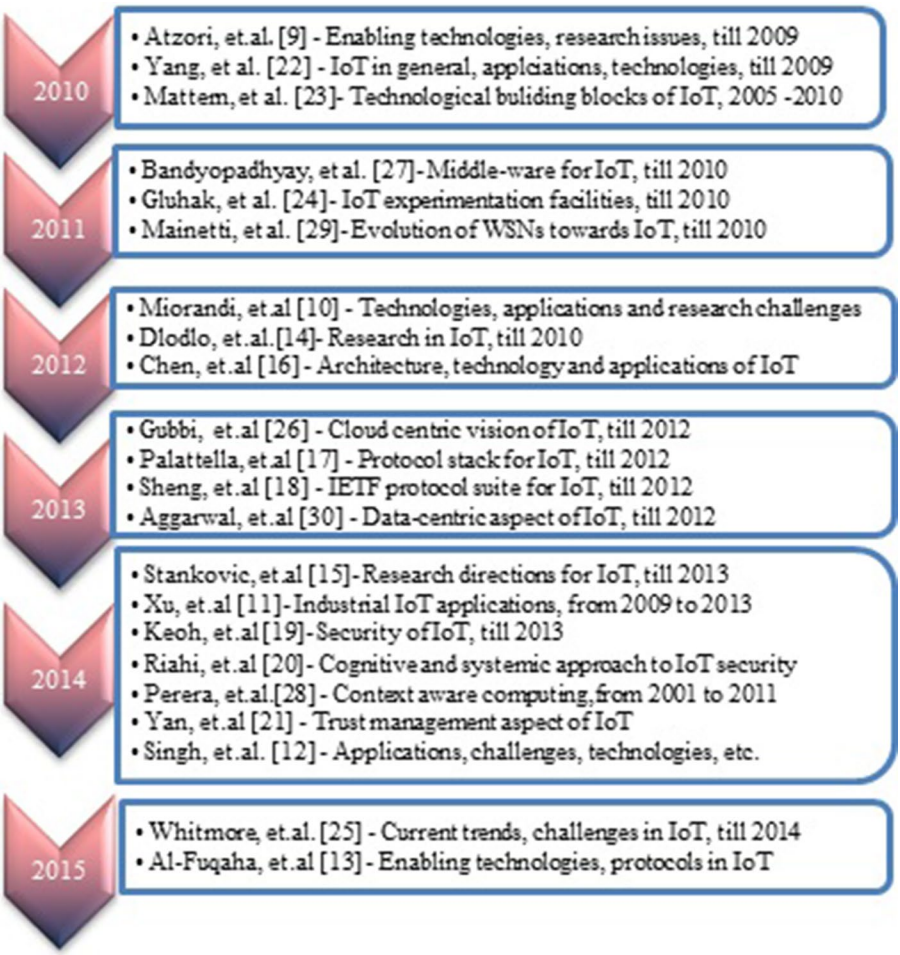

Fig. 9 Timeline of existing IoT surveys

5.1 Applications and Enabling Technologies

In a popular survey on IoT, Atzori et al. [9], outlined state-of-the art in IoT till 2009. The major focus on the survey is the vision of the IoT paradigm, enabling technologies, and major research issues associated with IoT. Authors have mentioned that IoT paradigm is convergence of different visions, like things-oriented vision, Internet-oriented vision and semantic-oriented vision. A taxonomy of major application domains is also listed in the paper. To help future researchers in the domain, authors have identified a set of open research issues. Miorandi et al. [10], discussed the application fields, enabling technologies and research challenges in IoT. The authors have also discussed the vision and concept of IoT in *Information and Communication Technologies* (ICT) sector and the possibility of adoption of recent content-centric network architecture in IoT. The ongoing projects in IoT are also discussed in the paper. The authors have also provided a list of open research areas relevant to IoT for the benefit of future researchers.

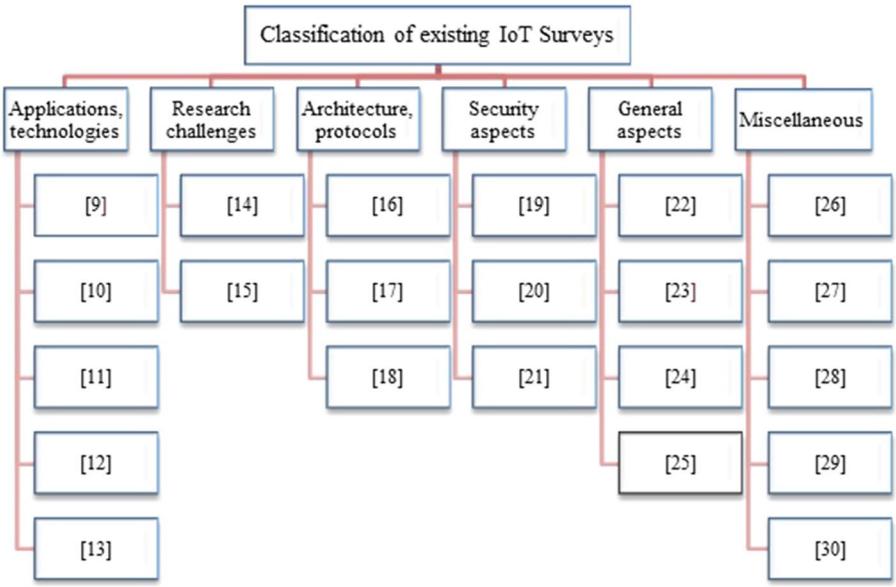

Fig. 10 Classification of existing taxonomies on IoT

Xu et al. [11], provided a survey on industrial IoT applications, which includes the current research from 2009 to 2013.The applicability of service-oriented architecture (SOA) in IoT is also discussed. The SOA for IoT consists of four layers, namely, sensing layer, networking layer, service layer and interface layer. Authors have also discussed the design considerations for industrial IoT applications. To help future researchers in this domain, research challenges and future trends in industrial IoT also listed in the paper. Singh et al. [12], have discussed the applications, services, visual aspect and challenges for IoT. The authors classified three major versions of IoT as (1) Things oriented version, (2) Internet oriented version and finally (3) the semantic oriented version. They have also discussed the challenges faced by Wireless Sensor Networks (WSNs) for developing IoT communication networks. A smart semantic framework is also introduced to encapsulate the data collected by the sensors in the network. In a very recent survey, Al-Fuqaha et al. [13], emphasized the enabling technologies, protocols and application issues related to IoT. Compared to other surveys, authors have provided a horizontal view of IoT, in-depth about the technical details and research challenges, which will help the future researchers in this domain. Authors also have also discussed the relation between IoT and other futuristic technologies such as big data, cloud and fog computing. The time span of the survey is from 2004 to 2014.

5.2 Research Challenges

Dlodlo et al. [14], discussed the different places across the globe, where research on IoT is going on. The authors have also discussed application domains, technologies used in IoT. The methodology of IoT research work is also described which includes the main contributors and emerging patterns and trends in IoT research. Stankovic et al. [15], provided

a specific survey on future research directions of IoT. The authors have presented various research challenges, such as scaling, architecture and dependencies, creating knowledge and big data, robustness, openness, security privacy and finally human in-the-loop systems.

5.3 Architecture and Protocols

Chen et al. [16], described IoT architecture and technologies used in IoT, like RFID, Electronic Product Code (EPC), and ZigBee, etc. They have also proposed a framework of digital agriculture application based on IoT. Palattella et al. [17], described protocols of Physical layer, Link layer, Network layer, Routing layer, Application layer. It described IEEE 802.15.4, power saving link layer-IEEE 802.15.4E, in which it focused on scheduling, synchronization, channel hoping issues. IETF 6LOWPAN and IETF ROLL and other application layer protocols such as COAP were described in brief. In [18], Sheng et al. have discussed the standards, challenges and opportunities for IETF protocol suite for IoT. The authors have provided in-depth details about the IETF communication standards in layer-wise manner and discussed the technical challenges in implementing the standards based on the requirements imposed by IoT applications. Authors have also mentioned some of the research opportunities for future researchers in this domain.

5.4 Security Aspects

Keoh et al. [19], listed the efforts by Internet Engineering Task Force (IETF) for the standardization of securing IoT. They have described in detail about the security solutions used with CoAP protocol used by IoT applications. The standardization efforts used to adapt the latest Datagram Transport Layer Security (DTLS) protocol for IoT applications are also discussed. In a recent survey, Riahi et al. [20], provided a cognitive and systemic approach to IoT security. Authors have added a new *cognitive* dimension to the existing two-dimensional systemic approach for IoT security, which helps to analyze different situations and provide measures to guarantee security and reliability. The proposed approach consists of four nodes: person, people, technology and intelligent object. Authors have referred the connections among the nodes as *tensions* and presented possible research issues for each tension. Yan et al. [21], discussed the trust management aspect of IoT. They have discussed in detail about the trust, objectives of trust management and existing literature on trustworthy IoT. A system model for IoT is described with three layers, physical, network and application. The goals that the trust management should achieve are also described based on the proposed system model. Authors have also mentioned some of the open issues in the related domain.

5.5 IoT in General

Yang et al. [22], provided the state-of-art of IoT, mainly focusing on enabling technologies for IoT, such as RFID systems, sensor networks, and intelligence in smart objects, etc. The applications of IoT are also discussed together with some of the open issues to be addressed by the future researchers. The time span of the survey is from 2005 to 2009. In an earlier survey on IoT, Mattern et al. [23], discussed the vision, use case scenarios, challenges, and mostly focused on RFID and other technological building blocks of IoT. They have also mentioned some important aspects like, Web of things, IP for things and social

and political issues related to IoT as part of the survey. The time span of the survey is from 2005 to 2010.

Gluhak et al. [24], surveyed the requirements for next generation IoT experimentation facilities. The authors have discussed existing publicly available test beds for IoT experimentation and provided taxonomy of test beds based on their features and capabilities. The discussion on experimentation facilities required by the future IoT applications help the IoT researchers in their future endeavors. Whitmore et al. [25], surveyed current literature on IoT based on the current trends, challenges and reported open research questions to help future research endeavors in the area. Authors have classified the existing literature into following categories: *technology, applications, challenges, business models, future directions* and *overview/survey*.

5.6 Miscellaneous

Gubbi et al. [26], have discussed the cloud centric vision of IoT with a focus on enabling technologies and application domains which will drive future of IoT research. They have presented a cloud implementation using *Aneka* cloud platform based on the interaction of private and public cloud. Authors have mentioned that the convergence of WSNs, Internet and distributed computing will be the most important aspect future researchers have to consider in their future endeavors. The paper includes the current research till 2012. Bandyopadhyay et al. [27], proposed a survey of middleware systems for IoT. Since, in IoT, heterogeneous domains applications communicate over heterogeneous interfaces, developing middle-ware solutions is an important aspect to consider. In this perspective, authors have provided a brief discussion of existing IoT middle-wares and categorized them based on different features, like interoperation, device management, platform portability, context awareness, security and privacy.

Perera et al. [28], proposed a survey on context aware computing in an IoT perspective. The time span of the survey is from 2001 to 2011 and covered almost 50 projects. Authors have proposed taxonomy by identifying features, models, techniques, functionalities and approaches used by the projects at higher levels. Based on experience from context aware computing, authors have mentioned some future challenges in IoT that has to be addressed by future researchers. Mainetti et al. [29], described the existing literature on standards and solutions for WSNs as part of IoT. Authors also proposed a framework, which will be able to harmonize between new and legacy installations to migrate to an all-IP environment. Aggarwal et al. [30], proposed a survey on IoT based on data-centric perspective. Authors have mentioned that *scalability*, *distributed processing*, and *real time analytics* are the important factors to be considered in the perspective of data centric IoT applications.

In this section, we have discussed the existing survey papers on IoT. As in Fig. 10, most of the surveys on IoT described different aspects, such as, IoT applications and enabling technologies [8, 9, 12, 27, 30], research challenges [16, 23], IoT architecture [11, 14, 24], security aspects [17, 19, 29], general aspects on IoT [10, 26, 28] and some other specific areas [15, 18, 20, 22, 25], etc. However, none of them provided on a comprehensive study on IoT covering all the aspects, such as architecture, protocols, security and privacy, scalability and energy efficiency, etc. Also, we have identified some of the emerging application areas of IoT, such as social networking with IoT, incorporating delay tolerance in IoT and applicability of emerging network architectures, like CCN, NDN, etc. In this survey, we have described about some of the recent developments on integrating IoT applications with such emerging technologies. Since, many of the researchers studied IoT for more than

a decade, incorporating emerging network architectures and technologies should be further area of research. In this aspect, we have also identified some of the promising research challenges in this survey to help the future researchers.

6 A Novel Taxonomy of IoT

As discussed in previous section, the existing taxonomies on IoT various aspects, such as applications, technologies, research challenges, architecture, protocols, security, etc. In this paper, we focus on a comprehensive study of IoT covering all the aspects such as protocols, architecture, security, scalability, social networking, energy efficiency and inter-operability (Fig. 11). Compared to other surveys, our objective is to provide a complete picture of every aspect related to IoT and describing the most recent research works done with them, which makes our survey as most recent and comprehensive survey. In this section, we will discuss in detail about our taxonomy in detail.

In Fig. 12, we have classified the topics covered in the proposed taxonomy. We broadly classify the literature on IoT into architecture, protocols and auxiliary issues, which consists of security and privacy, scalability, energy efficiency and social IoT. Although IoT architecture is covered in some of the existing surveys, we have provided a classification based on architecture from existing system and dedicated IoT architecture. Protocols used in IoT are classified into WSN based protocols and IoT specific protocols. Finally, apart from the existing surveys, we have listed some of the auxiliary issues, which are very important factor to be considered while designing IoT applications.

IoT can be applied in several areas such as, logistics, searching and tracking, industrial sectors, smart homes and many others. IoT is facing several hindrances on its way of being implemented as a global technology. There are many open issues that need to be addressed for efficient implementation of IoT that are, lack of standard architecture and standard protocols, security and privacy, energy efficiency, and scalability are limiting the wide-range deployment of IoT.

Challenges in security and privacy, energy efficiency, and scalability are limiting the wide-range deployment of IoT. Security risks in IoT arises out of the fact that innumerable devices can be connected to the IoT without proper identity verification and they can harm the system objective if they have malicious intent. Scalability is another big issue which has to be addressed because billions and billions of smart physical objects are interconnected with each other to provide smooth services. Energy-efficiency is related to the

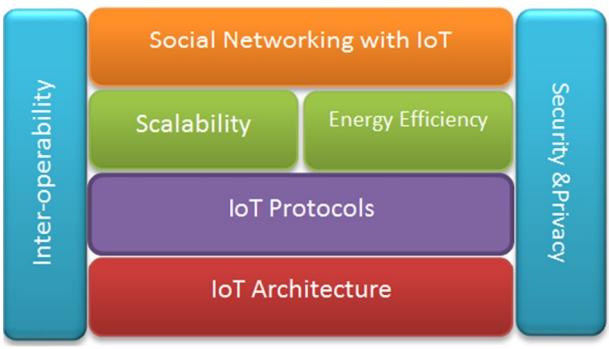

Fig. 11 Topics covered in this paper

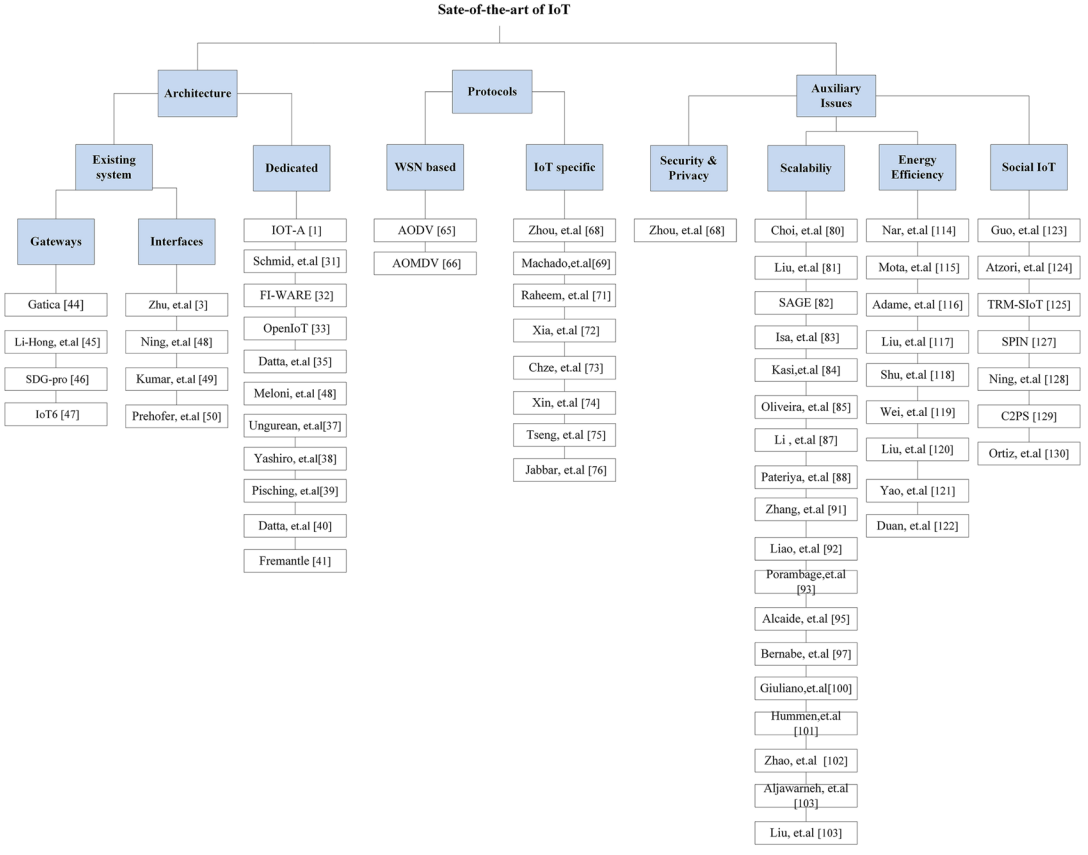

Fig. 12 Proposed taxonomy of IoT literature

resource-constraint of smart physical objects which may soon die out disconnecting the network prematurely.

7 IoT Architecture

There are many architectures that are being developed for independent applications of IoT. Current architectures which are providing communication between heterogeneous devices, gave inappropriate models and they do not address security and privacy concerns and scalability issues. A unifying architecture is still needed for IoT.

7.1 Dedicated IoT Architecture

IoT-A [1], is a project that provides an architectural reference model that addresses interoperability and efficient integration into a service layer of the future Internet. IoT-A created an architecture reference model, whose main objective is to provide a coherent unifying IoT architecture, creating a holistic approach to implement IoT. This reference model contains domain model, information model, communication model, trust, security and privacy model. Domain model defines concepts of IoT and relationships among them. Information model explicitly represents domain model concepts. Communication model provides communication among IoT concepts. Trust, security and privacy ensures secure and privacy preserving communications among domain concepts of IoT.

Schmid et al. [31], proposed big IoT architecture to establish IoT ecosystems and to provide interoperability between IoT platforms. The proposed architecture consists of a web API, semantic descriptions of the resources and services and finally a marketplace. The big IoT architecture contains overall eight IoT platforms, in which six are cloud/infrastructure level platforms and two are device-level platforms. FI-WARE [32], is another IoT framework developed with semantic based enablers to address the issue of interoperability. In OpenIoT [33], authors proposed open source IoT platform with interoperability support for the IoT services in the cloud. The W3 Semantic Sensor Networks (SSN) ontology as part of the openIoT which act as a middleware among physical and virtual sensors. Yu et al. [34], have proposed, WISE, a web of object architecture for building web based IoT applications and services. The main purpose of WISE is to provide cooperation between services with various things with a focus on smart home and building services.

Datta et al. [35], have provided an IoT architecture, which provides a real-time interaction between mobile clients and sensors using wireless gateway. The proposed architecture consists of three layers: (1) sensing layer, (2) gateway API layer and finally the application layer. Initially devices used in the M2M communication and the endpoint users' needs to register in the Wireless Gateway (WG) and after that, they can establish a connection to the WG (discovery phase). After the discovery phase, users can communicate directly with the sensors. Meloni et al. [36], proposed IoT architecture for wide area measurement systems, which focused on virtualization aspect in Smart Grids (SG). The proposed architecture ensures the interoperability, reusability and flexibility of the SG services.

Ungurean et al. [37], proposed an IoT architecture based on OPC.NET specifications in the perspective of an industrial environment. The proposed architecture consists of two modules, (1) data server: collects data from sensors, which are used as the field buses and send those data to the actuators. (2) HMI application performs the client-side operations and uses OPC.NET for connecting to the Internet. Yashiro et al. [38], have proposed an

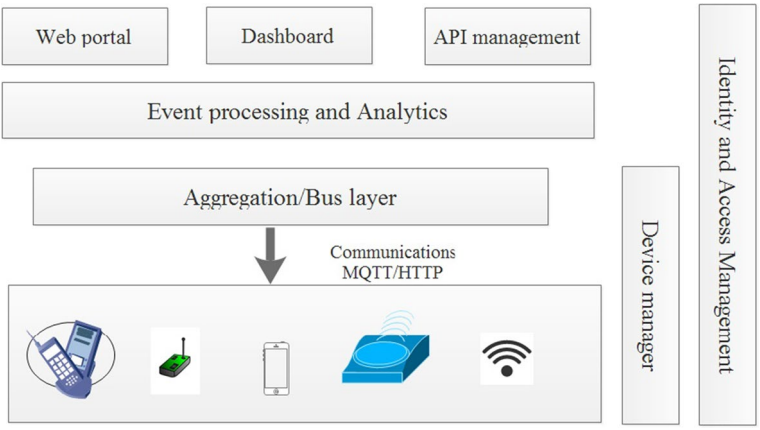

Fig. 13 Reference architecture for IoT proposed in [41]

IoT architecture, namely, *uID-CoAP*, for integrating existing embedded applications to IoT network. The uID-CoAP framework combines Constrained Application Protocol (CoAP) with Ubiquitous ID (uID) architecture to build an IoT network based on RESTful services and semantic knowledge based uID database. Recently, Pisching et al. [39], proposed an architecture based on IoT and cyber physical systems for supporting the communication between things and machines in the scenario of fourth Industrial Revolution (I4.0). Datta et al. [40], proposed an IoT architecture for enabling digital services. The functional elements as part of the architecture includes (1) Stimuli Generation: represents sensors, which are capable of producing stimuli capture from the environment (2) Stimuli Processing and Storage: raw stimuli generated is converted into high level abstraction and store in local storage. (3) Consumable device: represents the application logic such as mobile phones, tablets, etc. Fremantle et al. [41], proposed reference architecture for IoT based on following requirements.

- Connectivity and communications: The constraints on memory and power of the devices used in IoT initiates the need of simple and binary protocol, which is having the ability to connect across the gateways
- Device management: There are many requirements for managing the devices connected to the IoT application, such as software updates, enabling security features, remote device management, etc.
- Data collection analysis and actuation: There is a huge requirement of managing large number of devices as well as highly scalable storage system which can handle massive data generated by many of the IoT applications.
- Scalability: The architecture should be highly scalable and able to deploy in cloud infrastructure
- Security: Any IoT application required to handle inherent security threats of Internet, specific security risks of the devices and finally the safety of the devices.

Based on the above requirements authors have proposed a reference architecture for IoT, as in Fig. 13.

The layers as part of the reference architecture are:

- Device layer: is the bottom layer of the architecture, which represents the devices, such as mobile phones, sensors, Bluetooth, Wi-Fi, etc., which are used in the IoT applications and are connected to Internet either directly or indirectly using some communication links.
- Communication layer: the layer which supports the connectivity among the devices using protocols such as HTTP, MQTT, CoAP, etc.
- Aggregation/Bus layer: the layer responsible the HTTP/MQTT brokers to connect to the devices and aggregates and combines the communications from different devices to route to gateways. The layer is also responsible for bridging among different protocols.
- Event processing and Analytics layer: the layer responsible for collecting the events from the bus and provide actions based on the events.
- External communications layer: provide interactions with the systems outside the network using M2M communications using APIs.

RFID technology is based on simple operational principal, yet deployment and installation of RFID require great effort. RFID technology consists of multiple readers and several tags operating for different application in heterogeneous environment. To solve this problem a middleware is needed to abstract heterogeneous readers and generate specific application-oriented events. "ASPIRE" (Advanced Sensors and lightweight Programmable middleware for Innovative RFID Enterprise applications) [2] project will change the current RFID deployment techniques. The main goal of ASPIRE is to develop a middleware platform for building RFID solutions. This project gave a middleware for low cost hardware and reduces the efforts for management and development of applications. This middleware provides services for deployment, development and improvement of RFID solutions. The middleware provided by ASPIRE is lightweight, intelligent, programmable, standards compliant, scalable, and privacy friendly.

An EPC based IoT architecture [42] was developed which helps in automatic registration of IoT devices into the network, and communication between IoT devices using standard protocols that are used for Internet. Here, sensor node contains RFID for identification, ZigBee for communication and a microcontroller (MCU). RFID contains electronic product code (EPC) of the thing and it acts as ID. MCU reads static information about the thing without using reader. These nodes communicate to gateway through ZigBee sink node. It uses CoAP as the application layer protocol of IoT devices and to communicate with applications of the internet that uses HTTP, gateways are used to making them communicable. An overview of an ideal IoT architecture is described in [43].

7.2 From Existing Systems

In IoT we are joining different heterogeneous components together, so a middleware is needed to abstract the technical details of lower layers for upper layer applications, so programmers can develop applications without worrying about the lower layer technologies. The middleware should provide interoperability among different applications. SOA-based architecture and Ubiquitous service-Discovery Service (ubiSD-S) are some of APIs that are used in middleware to provide interoperability. Below is some middleware that is developed for IoT.

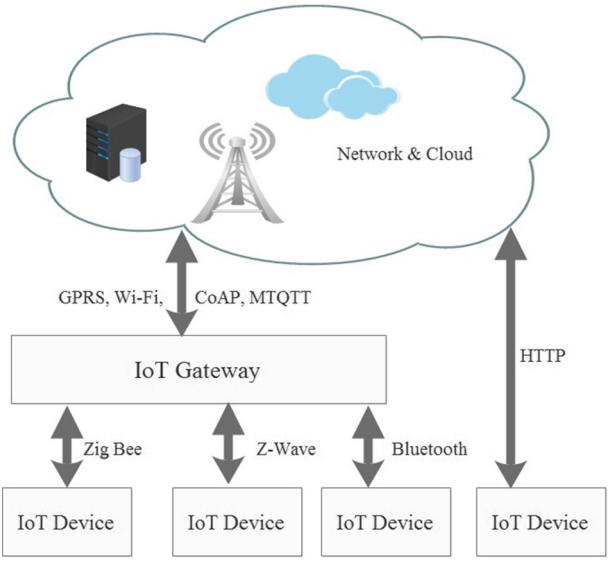

Fig. 14 Example of IoT gateway

7.3 IoT Gateways

There is a need of gateway for interoperability between constrained environment and regular network that can map current protocols to constrained protocols stack. The goal of IoT gateway is to resolve with the heterogeneity between sensor nodes and Internet and fill the gap between traditional network and IoT network (Fig. 14). So IoT gateways are used for the integration of WSN into Internet. It also helps in the management and control of WSNs. The main problems that are faced by IoT gateway system is the diversity of protocols and sensor technologies in the WSN.

Gatica [44] is a middleware which enrich the raw sensed data generated by the sensors with annotations and then transforms and exposes them in RFID triplets and finally streams the RDIF objects to the endpoint users. Principal Component Analysis (PCA) is used to cluster the data and to execute queries over streaming sensed data to discover hidden patterns using analytic interfaces. Li-Hong, [45], proposed a sensor access scheme based on IoT gateways. The authors have used Lightweight Directory Access Protocol (LDAP) to provide information storage scheme for sensor access. SDG-Pro [46] is a framework for software defined IoT cloud gateways. SDG-Pro provides a programming model, which can provide a unified and programmable view of the development process as part of the IoT applications.

IoT network can make use of standard network protocol, IPv6 for network communications. IPv4 is not viable for it since its address space cannot accommodate the huge number of IoT devices, so IPv6 could be used in future Internet, due to its large address space. IoT6 [47] is a project that focused about IPv6 protocol and its features like addressing, mobility, security and auto configuration. These IPv6 features can be used for IoT paradigm. The main focus of IoT6 was to develop an IoT architecture based on IPv6 that can support scalability and interoperability. Then in future internet, two types of networks exist, one is current IPv4 based networks (non-IPv6 based networks) and the IoT networks which are IPv6 based. In order to make both networks compatible for communication, gateways need to be deployed between these two types of networks.

To exchange information between people and WSNs, traditional Internet and mobile networks can be used. However, it is difficult to connect WSN to Internet or mobile communication network because there are no standardized, uniform protocols and data from WSN cannot be transmitted to long distance. Therefore, with the development of IoT there is a need for gateway, which acts as a bridge between traditional network and sensor network and address the heterogeneity between them. In [3], the authors have developed a gateway to act as a bridge between traditional communication networks or Internet and WSN and provides the functionality of protocol conversion and device management. IoT gateway is in between physical layer/sensor layer and application layer. It receives data from sensor nodes and transmits to the application layer and also IoT gateway manages data forwarding and protocol conversion between different traditional network and WSN.

IoT devices are soon to be deployed in every field so there is a need of IoT deployment with the current network. Merging with current Internet devices is possible through low-cost, transparent gateways [4]. Interconnection at the application level is required between HTTP and CoAP and at network layer between IP and 6LoWPAN. There is a need of mapping between current TCP protocol stack and IoT protocols.

7.4 Interfaces

There is a need for a common interface in IoT for the things to identify themselves and share data according to end user's needs. The architecture of IoT contains sensor layer, network layer and application layer. In IoT sensor layer use many kinds of sensor technology that are not uniform. This non-uniform sensor technology causes the upper application being restricted. If sensor technology changes or modified this upper application have to adjust according to them. So IoT middleware is needed. Zhu et al. [3], discussed a middleware technology in the application system –'SmartScene'. RFID is used for identifying objects with assigning unique electronic product code to each object, but it cannot give accurate real time location of objects. ZigBee is a wireless technology that can obtain precise real time information of objects. So, in 'SmartScene', both ZigBee and RFID are used to include features of both RFID and ZigBee. At sensor layer two different technologies are used, so data at application layer have two different formats. So, there is a need of middleware that provides common services interface for upper application and hides complexity of lower layer.

Devices that are connected to the Internet are increasing and they use different ways to connect to the traditional network. However, the rigidity of current network infrastructure administrator has to manually implement high-level network policies through command line interface (CLI). And the traditional network infrastructure and protocols are not adaptable to this high-level of scalability, high traffic and mobility. Software Defined Networking (SDN) [7] is a network architecture that eliminates the rigidity present in traditional networks and allows networks to be more adaptable and flexible. Besides, its centralized design allows important information to be collected from the network and used to improve and adapt their policies dynamically. SDN proposes some changes to today's networks. In SDN, data plane and control plane are separated, so that evolution and development are independent for both. Secondly, it has centralized control plane for a global view of the network. Finally, SDN establishes open interfaces between the control plane and data plane. Ning et al. [48], proposed two architectures representing human neural system. (1) Unit IoT architecture and (2) Ubiquitous IoT architecture. In unit IoT, there is a single management and data server and it collects data from all sensor nodes and acts as centralized server. In

modified unit IoT there are many data servers to manage data. Ubiquitous IoT is a combination of many unit IoTs.

Recently, Kumar et al. [49], have proposed a lightweight method to integrate IoT interface with a web browser. Such integration helps to control any IoT device through a web browser independent of the operating system used. The proposed system works based on the features in-built to the browser, such as bookmarks, authentication, etc., so that the need for a centralized server-based solution is eliminated. Prehofer [50], have modeled the complex IoT system with sensors and actuators and provided RESTful interfaces for IoT systems, which can be used for the discovery, reading and manipulation of IoT resources. Abidin et al. [51], focused on IoT in agriculture environment and proposed a web-based interface to support the operation of automated fertigation system. There is also a provision of emergency access to the fertigation system through web site to stop the current operation. Serrano et al. [52], addressed the issues related to interoperability of information in IoT applications using linked data techniques. Authors have also described challenges for IoT in deploying future Internet.

8 IoT Protocols

IoT Protocols must follow below requirements, consume low power, should be highly reliable and devices must be able to connect to Internet. Below is the protocol stack and set of protocols used in each layer. IoT covers a huge number of devices, so for communication between devices standard protocols are needed that must consume low power, must be highly reliable and devices must be able to connect to the Internet. Below is the protocol stack and set of protocols used in each layer.

The protocols for different layers of IoT are listed below [17, 53].

- Physical layer

  (a) *IEEE802.15.4 PHY*: This protocol is defined by IEEE 802.12.4 for the physical layer of it. It supports low-power devices at physical layer or sensor layer. The main purpose of the protocol is to define the physical and MAC layer for the operation of Low Rate Wireless Personal Area Networks (LR-WPAN). It supports many of the upper layer protocols, such as ZigBee, TSMP, etc. The transfer rate of the basic framework is 250 KB/s supporting 10–100 m communication range. Additional features of the standard include, CSMA/CD for collision avoidance, reservation of guaranteed time slots for supporting real-time communications, and security aspects, etc. [54]. The types of devices generally are: (1) Full Function Devices (FFD), which supports any topology and have full functionalities, like routers, coordinators, etc. (2) Reduced Function Devices (RFD), which can only use star topology and is having with limited functionality, so cannot function as coordinator and sleeps when there is no activity [55]. IEEE802.15.4 PHY is mostly used low-end devices of limited hardware support (Fig. 15).

- MAC layer

Fig. 15 Protocol stack

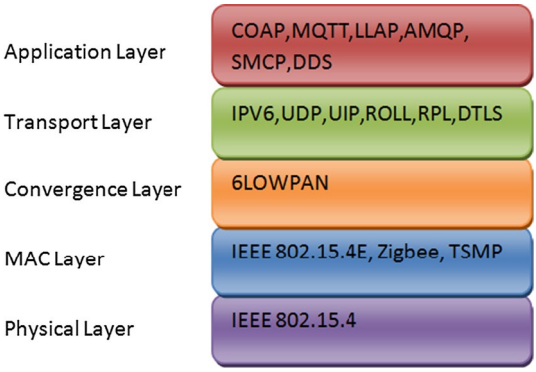

Fig. 16 IEEE802.15.4-2006 header [3]

Type (3)	Security enabled (1)	Packet pending (1)
Acknowledgment requested (3)	Pan ID compressed (1)	Reserved (3)
Destination address mode (2)	Frame version (2)	Source address mode (2)

Fig. 17 XBee Series 2/ZigBee

(a) *IEEE802.15.4E MAC*: This protocol is defined for MAC layer of IoT, which can transmit the frames through IEEE802.15.4 PHY channel. There are two modes of operation supported by IEEE802.15.4E MAC layer: (1) Beacon-mode, in which synchronization is achieved with the help of super frames and CSMA-CA mechanism and achieves dedicated bandwidth and low power consumption (2): Non-beacon-mode, which is the traditional multiple access system and uses CSMA-CA for collision avoidance. The detail of the IEEE802.15.4-2006 header is given below (Fig. 16). The 3-bit field, type is used to identify different frames such as, beacon, data, command and acknowledgement. There are four flags, namely, security enables, packet pending (not used), acknowledgement requested (set to 1, if requires acknowledgement) and finally, PAN ID compressed (same for source and destination). Normally, beacon frames are not used in IEEE802.15.4E [56].

(b) *ZigBee*: is a wireless technology developed to create Personal Area Networks (PAN), with low-power, low-cost and low-bandwidth devices, which can be used for developing IoT applications. ZigBee (Fig. 17) can be used for creating mesh

networks, in which multiple paths exist among nodes in the network. Such a topology allows nodes to configure dynamically and provide ad-hoc routing capability to the nodes in the network.

(c) *Time Synchronized Mesh Protocol (TSMP)*: a communication protocol used by *motes*, which are the wireless devices having self-organizing capability. SMP is able to achieve synchronization and the communication among the motes is using the time slots similar to TDMA. Unlike ZigBee, TSMP is designed to operate in a noise environment and uses channel hopping to eliminate interferences. TSMP is mainly used for reliable and long-lasting applications.

- Convergence layer

(a) *6LoWPAN*: is an IPv6 variant of low power wireless PAN, which allows send/receive IPv6 packets over IEEE 802.15.4 based networks [57]. For backward compatibility to IP network 6LoWPAN protocol is proposed to bring IPv6 in IoT. 6LoWPAN enables IPv6 to be used for IoT so that current network can be easily deployed in IoT. 6LoWPAN is mainly used for the application scenarios, such as home automations, smart meters, etc. As pointed out in [55], there are so many advantages of using 6LoWPAN: (1) Since, IPv6 is the next generation Internet, integrating IPv6 with LR-WPAN will help to design next generation IoT applications. (2) The vast address space in IPv6 compared to IPv4, meets the requirements of today's IoT and Big data applications. (3) The feature of stateless and auto-configuration will help the nodes to read the MAC addresses automatically.

- Transport layer

(a) *User Datagram Protocol (UDP)*: UDP is a datagram-oriented protocol for the transport layer. UDP is suitable for applications, which can establish low-latency fault-tolerant connections. UDP supports port numbers, for distinguishing different user requests and checksum to verify the received data [58]. It includes minimum overhead, but with loss of reliability.

(b) *IPV6*: is a recent IP protocol developed for packet-switched inter networking. In order to provide unique identification for each object in IoT network, existing IP addresses may not be sufficient. IPv6will provide 4.3 billion addresses since it is having 128-bit address space. Apart from the address space, IPv6 permits hierarchical address allocation methods, there by resolving the issue related to expansion of routing tables.

(c) *uIP (micro IP)*: The uIP is a small implementation of TCP/IP developed by Adam Dunkels [59] for embedded systems, which uses with tiny 8- and 16-bit microcontrollers. The main motivation for developing uIP is to minimize the memory and code. The basic protocols implemented over uIP are IP, ICMP and TCP, although the other protocols, like ARP, SLP and PPP can also be implemented.

(d) *ROLL*: ROLL stands for routing over Low Power, Lossy Network (LPLN). In IoT, routing issues are difficult to solve because of low-power and lossy networks. Existing routing protocols, such as, AODV, OSPF, etc., cannot be directly applied

to LPLNs. So, Internet Engineering Task Force (IETF) working group ROLL have developed a new routing protocol, namely, RPL for IoT environment.

(e) *RPL*: is the routing protocol developed for low power and lossy networks. RPL supports multipoint-to-point traffic in IoT networks [60]. For multipoint-to-point traffic, RPL creates a Destination Oriented Directed Acyclic Graph (DODAG) used for routing. RPL also have optional security features to support message authentication using advanced encryption standard (AES) and RSA signatures for data integrity.

(f) *DTLS*: provides privacy during communications, for datagram protocols (i.e., protocols using UDP) such as eavesdropping, forgery and tampering of messages, etc. Basically, DTLS is a datagram version of stream-oriented Transport Layer Security protocol (TLS) and provide security support in the situations of packet loss or reordering. Unlike in TLS, DTLS does not suffer from the delays, but there are issues related to loss of datagram's, oversized datagram's, and packet ordering.

- Session/Application layer

(a) *CoAP*: Like HTTP, CoAP is document transfer protocol. However, this is used for constrained devices (devices that have low resources in terms of energy, memory and computation), examples include sensor nodes in WSNs, which helps to get the values read by the sensors, similar to the value retrieved from Web APIs. CoAP uses UDP at Transport layer, unlike TCP/IP. CoAP is even can be used in micro-controllers with low resources such as 10 KB RAM [61]. CoAP also supports multicasting, which is very important for many of the IoT applications. There is also a provision to map CoAP with HTTP using application-agnostic cross-protocol proxies.

(b) *MQTT*: MQTT is an open message protocol based on pub/sub paradigm and used for lightweight M2M communications. MQTT employs a client/server model and collects data from objects (sensors) and send it to the server (broker) over TCP. MQTT allows one–one, one-to-many and many-to-many communication possibilities. There are various application domains supported by MQTT, where bandwidth constraints and interruptions in connectivity used to occur. Although MQTT support light-weight communications, there are some limitations of MQTT. Firstly, it supports only TCP, which is a limitation for networks, where packet loss occurs most of the time. Secondly, the naming used in MQTT are quite long, which is impractical for IEEE802.15.4 [62].

(c) *DDS*: Data-Distribution Service (DDS) is a middleware standard developed which supports publish/subscribe paradigm for real-time systems. In the pub/sub communication paradigm, producers can publish the information (topics of interest) to the broker. When the subscribers show an interest on the topics then the broker the delivers the topics to them. Such pub/sub model eliminates the need for developing complex methods in a distributed environment. There are also some open standards available for DDs, called as Open DDS [63]

(d) *AMQP*: Advanced Message Queuing Protocol (AMQP) is an application layer protocol, which is used for sending information between applications or organi-

zations. AQMP is a wire-oriented protocol, where the data are sent as stream of bytes and used the underlying protocol as TCP and supports reliability, flow control, authentication, etc.

(e) *SMCP*: is a CoAP stack written in C language. SMCP supports fully asynchronous I/O, both BSD sockets and UIP [64].

(f) *LLAP*: It stands for Lightweight Local Automation Protocol. The main feature of LLAP is that it can send the short messages across objects over any of the communication medium.

8.1 WSN Routing Protocols

Efficient routing protocols are required to transmit data generated in IoT applications. However, the IoT or WSN characteristics of constrained resources and lossy wireless links create many challenges in designing of efficient routing protocols. The existing routing protocols being developed for WSNs can be categorized into three types based on the network structure, as (1) flat routing, (2) location-based routing, and (3) hierarchical routing. In flat routing all nodes are the same or homogeneous, they have common functionality. In case of location-based routing, routing of data is determined based on position of the nodes, and position of nodes can be determined by received signal strength. Finally, in hierarchical routing different nodes have different functionalities. Nodes with higher resource can be used for routing purpose and other nodes are used only for sensing. Below, we discuss some of the routing protocols developed for IoT applications.

Ad hoc On Demand (AODV) [65] is the most widely used routing protocol for ad-hoc mobile networks. Ad hoc networks do not depend on existing infrastructure for routing. In AODV routes are determined dynamically (i.e., on demand), when a node wants to communicate information to another node of the network. This routing protocol does not depend on periodic advertisements by routers, so resource usage (i.e., bandwidth and energy of node) is less compared to traditional routing protocols. The protocol has two phases, namely route discovery and route maintenance. In the route discovery phase, the node that wants to communicate firstly checks in its routing table for the desired destination, if it is available, then communication starts immediately in that selected path, otherwise a route request (RREQ) packet is broadcast in the network, the node, which is having path to the desired destination sends a route reply (RREP) packet to the source and makes entry in its routing table for backward path. In route maintenance phase, every router tries to maintain the latest information about routes such as removing node entry from routing table if it gets disconnected from the network. If source node moves out, it starts new discovery process, and if the destination or intermediate moves out, then route error (RERR) message is sent to the source. Source node receiving RERR will start new route discovery. The drawback of this routing protocol is, a single route is chosen in the route discovery process and if that route is unavailable, then again route discovery procedure has to be started by the source node, which is wasting some amount of energy of constrained devices of it.

As an improvement to AODV, Adhoc On Demand Multipath Distance Vector (AOMDV) [66] routing protocol is developed, in which, multiple paths are chosen in route discovery and route reply procedures, unlike in AODV where single path is chosen. AOMDV ensures loop freedom by maintaining sequence numbers and advertised hop-counts. The term, "advertised hop-count" indicates the maximum hop-count of the multiple paths to the destination, available from the source node. Once maximum hop-count is reached, then the advertised hop-count remains the same for the current sequence number. Only routes

with lower hop-count are allowed. In nutshell, in routing table entry, hop-count in AODV is replaced by advertised hop-count for AOMDV. Also, the RREQ request is embedded with a first hop field to indicate the first hop it has taken. Each node also keeps a first hop, indicating the list of neighbor nodes the corresponding RREQ request have been traveled. With these two modifications, the link disjointness of multiple path is achieved in AOMDV compared to AODV. However, compared to the AODV, the proposed AOMDV, additional computational overhead is required for computing multiple paths. Zhou et al. [67] also proposed a new on-demand routing protocol, which is a variation of existing AODV protocol.

8.2 Dedicated IoT Routing Protocols

The routing protocols for IoT are mostly developed using AOMDV. Since the routing protocols of it should be lightweight, variants of AOMDV are used in developing dedicated IoT protocols.

Zhou et al. [68], proposed a Routing protocol, AODV based on Node State (NS-AOMDV). In NS-AODV, as part of the route discovery phase, for each path, the node weight is calculated and sorted in decreasing order. For data transmission, path having largest weight is selected. To avoid the congestion in the network, the nodes with heavy load is delayed in forwarding the RREQ requests. So, the node having lighter load will participate in establishing the connection initially. In order to achieve energy efficiency, the nodes with energy level below a threshold are excluded in forwarding of RREQ requests. Machado et al. [69], developed a routing protocol, namely, *REL*, for IoT applications, in which the path to destination is selected based on end-to-end link quality, residual energy and hop count. The proposed REL protocol also able to perform load balancing and achieves energy efficiency. Similar to the [69], an energy efficient routing protocol, (EBR) for opportunistic networks have been proposed in [70], in which nodes with lower energy level and storage space are excluded in message forwarding. Opportunistic networks are a special category of ad-hoc networks, where there may not exist end-to-end path among some parts of the network and in such scenarios, routing is performed based on opportunistic contacts.

Raceme et al. [71], analyzed the security issues while deploying location/ID split protocol in IoT. The analysis was performed on X.25 security standard framework. Based on the experiments, the authors have identified various security vulnerabilities.

Xia et al. [72], addressed the network congestion in WSNs and proposed a routing protocol based on *Stackelberg* game. In the proposed method based on the transmission rate, the nodes may sleep to reduce the network congestion. Chze et al. [73], proposed a routing protocol for supporting secure communication of IoT devices. In the proposed protocol, combines the authentication in the routing procedure itself. A node has to authenticate with a specific set of parameters before forming or joining a network. The simultaneous process of authentication and routing improves the security of the communication among IoT devices. Xin et al. [74], proposed a Routing Protocol for Internet of Things with High-speed Mobile Nodes. In this paper, the authors proposed an REAODV protocol for the scenario with high-speed mobile nodes. It used the reverse broadcast RREP and adds an energy restriction to achieve less network delay, higher throughput and energy consumption overweight improvement in fast-changing network.

Apart from the variations of AOMDV protocol, Tseng et al. [75] have recently proposed a dedicated routing protocol for IoT, namely, Multipath Load Balancing (MLB).

The MLB protocol consists of two main components, LAYER_DESIGN and LOAD_BALANCE. In case of LAYER_DESIGN, nodes are assigned to inner and outer layers based on their distance towards IoT gateway. The LOAD_BALANCE allows the nodes to decide which inner layer nodes are having least traffic load, which is selected as the next hop to IoT gateway. With these two components, MLB allows multipath routing with load balancing and achieves robustness and reliability. Jabbar et al. [76] have evaluated the energy consumption of the existing routing protocols, such as, Multi-Path-Optimized Link State Routing (MP-OLSR) and the Dynamic MANET On-demand (DYMO) for a smart city environment. The simulation results show that the MP-OLSR is having lower energy consumption compared to DYMO.

9 Auxiliary Issues

In this section, we will discuss the auxiliary issues, such as security and privacy, scalability, energy efficiency and social networking associated with IoT applications development.

9.1 Security and Privacy

Security and privacy are the most important challenges of implementing IoT. Since any one in IoT network can access the data of other devices in the network, the data must be kept secure, during the transmission and also proper authentication is needed before accessing any device. In IoT context, we cannot use complex algorithms for providing security and privacy, due to limited computing, memory, and communication capabilities of IoT devices. The designed algorithms should be simple enough to be applied in IoT devices.

Since IoT widely adopts wireless medium for the transmission of data, there is possibility of eavesdropping, message forgery and tampering attacks. Therefore, there is a need to secure the data during communication between devices. Although we can reuse some of the existing IP-based security solutions, the resource-constrained nature of IoT devices have to be considered. Therefore, recently, many IP based security protocol variants are developed, like Datagram TLS (DTLS) [77], HIP Diet Exchange (DEX) [78], and minimal IKEv2 [79].

Choi et al. [80], addressed the issues related to eavesdropping in Machine Type Communications (MTC), using secret key generation method. The authors have proposed a method that generates sequence of random numbers, based on Channel Dependent Signature (CDS) for secret key generation in Orthogonal Frequency Division Multiplexing (OFDM) system. In the proposed method, for confusing the eavesdroppers, incorrect symbols are transmitted, whereas, the legitimate users can receive the correct symbols using shared secret of channel state information (CSI) together with a legitimate transmitter. Liu et al. [81], have proposed secure key establishment method using Elliptic Curve Cryptography (ECC), and an access control mechanism using Role-Based Access to prevent eavesdropping attack in IoT systems. For each execution, different session keys are generated, and the method does not allow to generate future session keys based on the previous session keys. This is because; the session key is calculated as one-way has function and session secrets. SAGE [82], is a privacy preserving system developed against global eavesdropping e-Health IoT

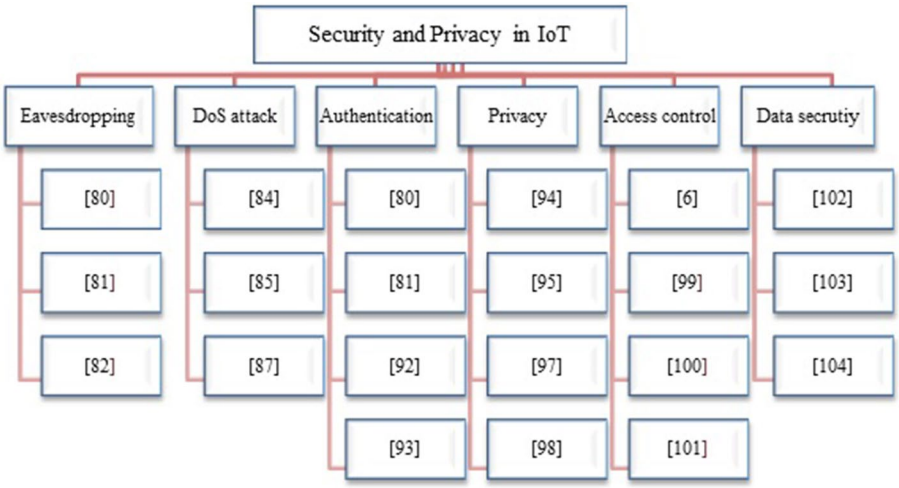

Fig. 18 Various Security Attacks in IoT

systems. In SAGE, the privacy threats of the patients are categorized into content orient and contextual privacy and both are proven against provable security techniques (Fig. 18).

A lightweight and secure TFTP protocol [83] is an enhancement of security protocol for bulk data transfer (TFTP) among embedded devices (ex: Wi-Fi access points). They used lightweight symmetric encryption for data, and asymmetric encryption protocols for key exchange, in TFTP. Kasinathan et al. [84], described a Denial of Service (DoS) detection architecture for 6LoWPAN. In the proposed method, Intrusion Detection System (IDS) is integrated into the network framework used in *ebbit* project. With the help of IDS probe, 6LoWPAN network traffic is analyzed and IDS send alerts to the DoS protection manager, when an Intrusion is detected. Oliveira et al. [85], provided a solution to prevent DoS attack for 6LoWPAN. The proposed approach is based on neighbor discovery protocol used in edge routers for mitigating DoS attack from Internet. In a nutshell, the edge routers in the neighbor discovery phase add extra information, such as, (a) transport layer protocol accepted, (b) whether the node accepts connections from Internet and (3) the maximum client request rate-shape limit, to the Address Registration Option (ARO) message to verify the address uniqueness, which helps to prevent DoS attacks. Bonetto et al. [86], have developed security procedures for IoT devices considering the resource-constrained nature of the IoT devices. The authors have developed a lightweight method which implements authentication and encryption for protecting IoT devices. Li et al. [87], developed PKI-like Protocol for the Internet of Things. They have proposed PKI like security mechanism, including PKI-security foundation architecture and PKI-like protocol. The problem with these variants is they use public key encryption as method of securing communications. Public key operations involve a considerable amount of transmissions and computation time. As a result, in constrained devices, when cryptographic operations are being performed normal CPU operations cannot be done in parallel. Therefore, a single opponent can make use of these costly operations in order to slow down the system by sending many handshake packets in short duration of time which is nothing but a DoS attack. Current DOS mechanisms are not sufficient to defend against such attacks. This is an open issue for the future development of IoT.

Authentication is the process of verifying the identity of the user who wishes to access the system. In IoT context, a user could be sensor node or an end user. Basic enabling technologies of IoT are wireless sensor networks (WSN), and Radio Frequency Identification (RFID). Authentication protocols can be classified into three categories, namely simple, lightweight, and ultra-lightweight. Simple uses standard symmetric cryptographic techniques such as AES, DES, etc.

Lightweight protocols use random number generators, cyclic redundancy check, etc., but not hash function. In RFID, due to its radio transmission nature, the information travelling in the air could be eavesdropped by an adversary. Hence, security appears to be one of the biggest challenges in designing RFID systems. Authentication and privacy are two important issues that have to be considered for RFID security. Ultra-lightweight protocols use simple bit-wise operations. Pateriya et al. [88], proposed an Ultra Lightweight Mutual Authentication Protocol for Low Cost RFID Tags. It used X-OR manipulation as the encryption method. In [89, 90], authentication protocols have been developed for RFID, but they do not provide mutual authentication, forward security and scalability. Zhang et al. [91], proposed an authentication protocol, which ensures forward security, but lacks scalability and mutual authentication. In [92], RFID authentication scheme is designed which used ECC based principles. They used elliptic curve cryptosystems (ECC) among PKC algorithms due to a small key size and efficient computations. It achieves mutual authentication and satisfy requirements of RFID system, there are other protocols for ensuring authentication in RFID, but they all fail to ensure mutual authentication because they considered reader to tag authentication, but the reader's authentication is not done in those protocols, this ECC based mutual authentication protocol ensures privacy, forward security, scalability and mutual authentications.

In WSN, in order to establish an end to end secure connectivity, proper authentication must be provided. Authentication protocols must not only be resistant against security attacks, they must be lightweight in order to be deployed in resource constrained devices of WSN. Porambage et al. [93], have developed an authentication protocol for ensuring security in WSN. The proposed protocol establishes secure connections because it is ECC based (ECC is inherently secured due to its basic principle ECDLP). This protocol is free from DOS attacks because CA checks the identity of the requested node after receiving a first hello packet, if identity is fake no further communication is done. After that all messages are exchanged by encrypting with common authentication key, so illegal data modifications are not possible, so data integrity is preserved. Since certificates require less amount of memory, it ensures scalability.

Privacy specifies that user's identity must not be revealed in IoT network. The user must be known as anonymous to IoT network. Following are some implementations for providing security and privacy In IoT implementations. Palomar et al. [94], addressed the issue of preserving privacy in IoT applications and proposed a decentralized anonymous authentication protocol. In the proposed protocol, the nodes form ad-hoc community and nodes are issued the authentication credentials which help them to interact with each other by preserving the anonymity.

Alcaide et al. [95], have proposed an anonymous authentication protocol using de-centralized approach, which can be used for preserving privacy in IoT applications. The basic idea is that, a private key is generated and distributed based on (t,n) threshold protocol. The (t,n) threshold protocol allows at most t pairs to be compromised without key get compromised. The users use Anonymous Access Credential (AAC), for authenticating to data collector entities, which collects data from authorized users. Later, Lin et al. [96], have the protocol proposed in [95], is insecure, by proving that a data collector can be cheated

by an adversary by impersonating as a legitimate user. Bernabe et al. [97] provided a privacy preserving IoT security framework as part of SOCIOTAL EU project. The proposed framework is based on Architecture Reference Model (ARM) used in IoT-A EU project. The privacy of the user is achieved by an identity management system, which stores and taken care of the credentials used by the objects and the users in a privacy-preserved fashion. Recently, Celdran et al. [98], provided, SeCoMan, a framework for privacy-preserving and context-aware IoT applications. SeCoMan supports semantic rules, which allows users to define location policies, thereby hiding, masking, establishing the right granularity and defining the level of closeness of their locations to others. In this manner, SeCoMan is able to manage user's privacies independent of the applications.

Access control of devices is important in order to ensure only authorized users gets access to IoT devices. Oh et al. [99], have analyzed the access control for resources in Web of Things (WoT) and proposed a decentralized access control mechanism which uses REST-compliant architecture. Giuliano et al. [100], addressed the security issues for non-IP devices and proposed security protocol based on the concept of local key renewal. The local key renewal uses local clock time for generating keys securing the transactions instead of deploying a centralized server. Hummen et al. [101], discussed the concept of adaption layer for providing security to IoT applications. The main objective of the adaption layer is to provide security offloading at the gateways for providing security to the IoT objects from Internet peers. Chi et al. [6], embedded security functionalities into IoT protocol stack. The authors have proposed a procedure to provide end-to-end security among unconstrained peers and devices. The proposed procedure is lightweight in nature because of the ability of the gateway to partially bear the computation overhead.

Zhao et al. [102], discussed data security technologies in IoT. Although IoT applications generate huge amount of data, the objective is to achieve transmission efficiency by providing security and privacy of the data. The authors have proposed a business application protocol, namely ISSAP, to support secure IoT applications with the help of cryptographic techniques. Aljawarneh et al. [103], developed an encryption method for multi-media big data in IoT. The input data is divided into blocks of different sizes and each block is further divided as plain text and key. The key is encrypted using Feistel Encryption System (FES) and used for encrypting the plain text using AES algorithm. Finally, genetic algorithm is used for integrating both cipher text and key. Liu et al. [104], discussed security aspects in IoT based on immunology. The authors have proposed an approach for simulating security in IoT applications based on immune system. A dynamic security strategy is deployed which consists of circular links to defend against security threats.

9.2 Scalability

Scalability is another major research challenges that has to be addressed because a large number of devices are going to be connected to IoT network, it is said 20 million devices will be connected to IoT network by 2020.Data generated by these devices are very large, so the scalability issue must be considered while storing data, transmitting data and existing protocols for IoT must work even when size of the network keeps on increasing. Below some implementations considering the scalability issues are listed.

Nodes of IoT should be fault tolerant, i.e., the data stored with the node should not be lost due to crash/disasters at that location. For ensuring fault tolerance replication mechanisms are used, but they can't be directly applied in IoT context since devices are resource constrained. Gonizzi et al. [105], developed a data dissemination scheme for replication of

data in distributed manner by considering scalability. Here a node before trying to replicate its data, checks the memory available with the nodes in routing table, if sufficient memory is available, then only it forwards the data to that node.

To address the issue of scalability, most of the existing research on IoT adopts cloud infrastructure. However, Zhang et al. [106], mentioned that, directly connecting smart objects with cloud is not a feasible solution because of the inherent limitations of cloud and web services. The authors have observed that there is a need for higher layer of abstraction, called as Global Data Plane (GDP), based data-centric approach for IoT applications. The main features of GDP include, single writer append only blog, location independent routing, overlay multicast, etc. The single-writer append only blog, supports multiple simultaneous readers, either through push-based or pull-based communication paradigm. The applications are built up on top of the GDP layer, which operates above network layer by inter-connecting log streams, instead of addressing objects via IP. The GDP layer also offers common access API's to applications and employs location-based routing with 256-bit address space. Jiang et al. [107], have proposed a secure and scalable IoT storage system for aggregating data in IoT applications. To ensuring security, secret sharing method is used and for scalability, Multi-coefficient polynomial and internal padding are incorporated into secret sharing scheme in which data blocks are treated separately. Authors have also provided an infrastructure of distributed IoT storage system supporting data warehousing concepts.

Venkatesh et al. [108], have provided a scalable application design for IoT applications, which uses simpler and smaller functional units called, context engines, are used to perform statistical learning. The use of context engine helps to minimize the overhead and improves scaling compared to the existing monolithic approaches. Jermyn et al. [109], addressed the scalability of M2M applications over next generation LTE (Long Term Evolution) mobile networks. Authors have studied the communication overhead created by large number of objects over mobile networks and performed experimental analysis using LTE simulation test bed for such a study. Based on such analysis, authors have observed that signaling and data traffic load scales linearly with number of connected devices. Souza et al. [110], addressed the scalability issue in IoT applications by providing a service-oriented architecture based on Path Computation Element (PCE), called as Service-oriented PCE (SPCE). In PCE, unlike in source-routing, the source node sends a Path Computation Request (PCReq), containing source and destination to the PCE. Then, PCE computes the best path towards destination using parameters in PCReq and network state information. The authors have extended PCE concepts to support IoT constraints in the proposed SPCE to address the scalability issues.

Ray et al. [111], considered the issue of scalability and security in IoT systems and proposed a RFID security framework for IoT. Although RFID is widely used in many of the IOT applications, scalability and privacy issues are grossly overlooked. So, the authors have provided an identification technique for addressing the issue related to scalability and security check handoff technique to provide adequate security features. An et al. [112], provided a Content-based Filtering Discovery Protocol (CFDP) in which, publisher/subscriber protocols is used for the service discovery mechanism. One example to publish/subscribe protocol is Simple Discovery protocol (SDP). It is a standardized protocol for service discovery, i.e., for discovering the devices containing the requested data of subscribers. The problem with SDP is, it sends the discovery messages to each and every node in the domain, though many nodes may not be related to our request (for example, if all the nodes are subscribers, then sending discovery messages to subscribers for getting the data, which is of no use). It wastes certain amount of storage space, network and computing resources.

Therefore, CFDP ensures scalability by doing some filtering operations for sending discovery messages. Kang et al. [113], considered the possibility of combining the features of clod computing and IoT and proposed a storage management system. The proposed system consists of different layers and provides stronger applicability and expansion functions as part of it.

9.3 Energy Efficiency

Since, devices have constraints in memory, processing power and battery life, etc. Therefore, IoT implementations must consider the constraints and use the battery power of devices efficiently. It can be done using smart processing of data, i.e., instead of sending data to every other device in the network, some processing must be done and then to send to the required devices, and we can use the computing power of firewalls instead of totally using devices computing power. Below are some implementations for ensuring the usage of energy in an efficient way.

Nar et al. [114], provided PCSMAC, which ensures power controlled transmission of frames by adjusting the transmission power of sensor nodes. The energy efficiency is achieved by reducing the transmission power and avoiding collisions. Mota et al. [115]., proposed an RFID mechanism for ensuring QoS requirements of IoT applications. The total number of RFID responses in IoT system is reduced by limiting the message exchanges between readers and tags.

Adame et al. [116], proposed HARE protocol stack, which adopts uplink multi-hop communications for achieving better energy efficiency compared to the existing single-hop concept used LPWANs. The basic concept of HARE is that the end devices are controlled by gateway using beacons, so that the stations can sleep for most of the time until listening to the next beacon. Also, multi-hop paths are chosen for transmitting the data to the gateway by means of low transmission power levels. An energy-aware routing protocol is also developed as part of HARE. Experiments on real testbed show that HARE achieves about 15% energy efficiency. Liu et al. [117], addressed the energy harvesting in IoT networks. The power consumption in the network is optimized using different techniques. A hill climbing MPPT mechanism is used for reducing the power consumption of the analog circuits and hysteresis regulation is used to provide constant voltage. Capacitor value modulation (CVM) is deployed to avoid quiescent power consumption.

Shu et al. [118], proposed a method for achieving energy efficiency of radio nodes in IoT applications based on game theory. The proposed method uses two level Stackelberg model, consists of leaders (primary users) and follower (secondary user). Initially, the primary users set up the spectrum price and allocate the power to the secondary users based on the spectrum cost information. Based on this, the primary users maximize their profit for a specific cost based on the power information from the secondary users. Finally, the power allocation game achieves Nash equilibrium. Wei et al. [119], proposed a framework for building energy monitoring and analysis based on IoT. The framework consists of three layers such as, (1) Perception layer: used for acquisition of the intelligent building information, (2) Network layer: used for integrating multiple connectivity options and (3): Application layer: providing interface for building management and energy consumption and monitoring through cloud platform. Liu et al. [120] proposed an energy management framework for controlling the MAC level consumption of the nodes. To be specifically, the control decisions are optimized based on the long-term task usage statistics with constraints on service delay of the task.

Yao et al. [121], outlined energy harvesting in WSN based IoT system and provided a framework for gathering multimedia information by optimizing power control and relay selection strategy. Duan et al. [122] proposed an energy-aware trust derivation scheme for WSNs based on game theoretic approach. The proposed scheme minimizes the energy utilization by providing adequate security assurance.

9.4 Social Networking with IoT

The social networking concept is widespread and attracted many users in traditional internet. Social networking with IoT is like devices communicating to each other automatically with other social communities in IoT. This can be useful for information dissemination across networks. Below are some implementations for social networking in IoT.

Guo et al. [123], described the concept of *Opportunistic IoT*, in which the devices are able to form infrastructure-less networks with the help of short-term communication techniques and use the movement and opportunistic contacts among people. The opportunistic IoT, allows the smart objects to communicate in the scenario of disruption in connectivity, and disseminate the sensed information opportunistically. The authors have proposed a reference architecture for the benefit for future researchers to develop such opportunistic IoT based applications.

Atzori et al. [124], provided the concept of *Social IoT* (SIoT) paradigm for supporting futuristic applications and network services for IoT. The main features of SIoT are (1) effective discovery of objects and services, (2) establishing trust worthiness among things (3) Ability to re-use the models used in social networks for addressing IoT related issues. In SIoT, the notion of social relationship is identified between objects and a reference architectural model is developed for the inter-object relationships. The relationships among objects are established without human intervention. Kokoris-Kogias et al. [125], scalable trust management model for IoT, namely, TRM-SIoT, based on the social approach. Each object finds the trust index of other objects based on its experience and information gathered from its friends. In TRM-SIoT, the trust and reputation are calculated similar to the way humans and their social relationships. Nitti et al. [126], studied the trustworthiness in social IoT and proposed two models, (1) subjective and (2) objective models for P2P and social networks. In the subjective model, similar to social networks, each node calculates the trustworthiness on the basis of the social relationship with other nodes and service provider. The objective model is similar to P2P networks, where the information about the nodes are stored in distributed hash table and used for calculating the trustworthiness.

In [127], authors have studied the relationships between IoT and Online social Networks (OSN) and described *Socio-Physical Interaction Network* (SPIN), which is a network formed by people and smart physical objects. The proposed SPIN framework allows objects to connect and perform social interactions with each other. Such web of physical objects allows the users to collect information of the physical objects and navigates to other objects using conceptual links as in OSNs. The experimental results show that the social interactions between SPIN entities resemble standard social network properties. Ning et al. [128], proposed a cyber-physical-social based security architecture, namely, *IPM*, for future IoT applications. The IPM architecture concerns with the information, physical and management aspects and supports *unit IoT* and *ubiquitous IoT* (U2IoT) models. The information security model is used for mapping relationships

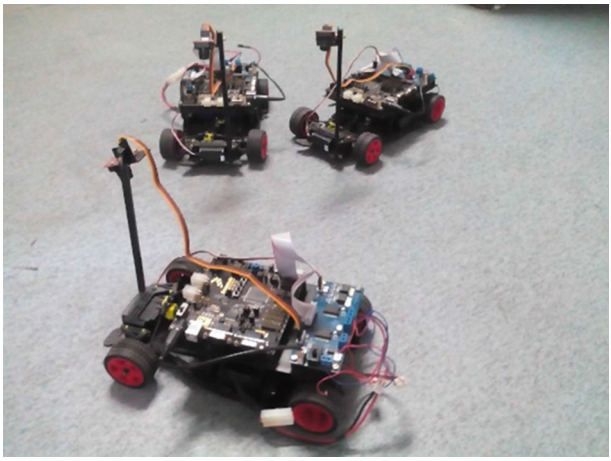

Fig. 19 Example of real testbed developed [70]

among U2IoT. Artificial immune algorithms are used for establishing physical security and social strategies are provided for achieving management security. C2PS [129], is a twin reference architecture model proposed for cyber-physical systems in which a physical thing is accompanied by a cyber thing as part of the cloud and both things can establish P2P communication through either directly or indirectly through cloud-based communication.

Ortiz et al. [130], discussed the concept of clustering between IoT and social networks, thereby providing an opportunity for the people to connect to the ubiquitous objects. The proposed Social IoT (SIoT), inherits both social networking features and ubiquitous computing paradigm and provides a uniform framework among users and objects which improve the connectivity and the availability. The integration among users and objects provide an opportunity to define new relationships, emerging services and applications as part of IoT.

10 Performance Evaluation Comparisons

In this section, we will describe the performance evaluation comparisons of some of the existing IoT-based applications developed in transportation and agriculture.

10.1 Smart Vehicular Environment

There are so many applications of IoT in vehicular environment. One of such application is *Smart Traffic Management* (STM). In STM, the sensor nodes attached with vehicles, such as cars and trucks help to sense the data in the surrounding environment and exchanges the sensed data to the other vehicles so that they can take some intelligent decisions. An example of such an application scenario is that, the sensors can identify the traffic density, or any other accidents happened and inform the other vehicles, so that they can take another route. With the introduction of driverless or self-driving cars, intelligent communication is inevitable part of the transportation system.

There are some technical challenges associated with STM. Due to high node mobility rate, STM suffers from frequent disconnections and which may affect the performance.

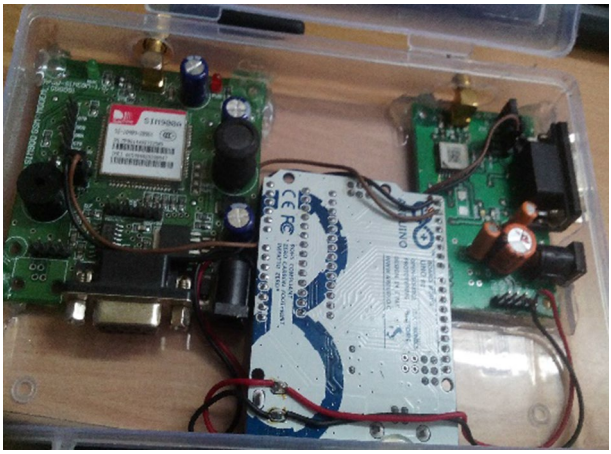

Fig. 20 Vehicle Tracking System [70]

Also, the sensors used in STM are having limited energy and buffer space which is also an issue to be addressed. In [70], Sobin et al., have proposed an energy efficient routing protocol have been developed for opportunistic communication in STM.

In the real testbed developed (Fig. 19), the sensors are deployed over TRK-MPC5604B free-scale motor cars. XBee protocol is used for communication among cars. The AT89S52 microcontroller is also used as part of the testbed for interfacing the hardware peripherals. The GPS module used with the testbed sense the location of the current environment and send to other vehicles. In case of disruptions in connectivity, opportunistic encounters are preferred.

Vehicle tracking is another important area in smart/intelligent communication. A vehicle tracking system [70] consists of AT89S52 microcontroller, GPS module and GSM module (Fig. 20). The AT89S52 microcontroller is used for serial interface to GSM modem and GPS receiver. The purpose of GPS module is to sense the latitude and longitude information of the vehicle and GSM module is used to transmit and receive data.

There are so many interesting application scenarios of IoT in vehicular communication. For example, the vehicle tracking system developed (Fig. 20) can be used for theft prevention, which is a big issue in many of the countries. In such scenarios, the device developed must very small in size and not to be powered from the vehicle itself. This will help the device to be unobtrusive and when the car theft happens, the device will send the messages to the owner so that the car can be tracked. One of the challenging issues in such a scenario is to develop long lasting batteries for the device to get power, as it is not from the vehicle. Using of solar energy is also restricted.

Misbahuddin et al. [131] have developed an IoT based traffic management system for smart cities. The proposed traffic light control system uses mobile phones to interact with the traffic police officer and adjusts the traffic light pattern accordingly. The authors have chosen holy city of Makkah Saudi Arabia as a case study for implementing their system. Miz et al. [132] have also proposed a smart traffic light system using IoT. The proposed system generates signals controlling the lights from the sensors deployed in cars as well as roads. Pham et al. [133] have proposed a cloud-based smart parking system based on IoT technologies. In the proposed system, each of the car park is formed an IoT network and the information related to GPS location, distance and free slots are sent to the server in the cloud and takes appropriate decisions accordingly.

10.2 Smart Agriculture

Another important aspect is providing smart solutions to the agriculture. Although, there are some of IoT based agricultural applications developed, satisfying the needs of local people in remote villages is a challenging task. Some of such applications are discussed here.

Kodali et al. [134] have addressed the issue of manually operating water pumps for the cultivation by farmers by developing an automated water pump controller using moisture sensor. The authors have used Message Queue Telemetry Transport (MQTT) protocol transmitting and receiving the information from the sensors deployed. The sensed information is available to the end users through web as well as mobile application. Kamienski et al. [135] have developed a smart water management system, SWAMP, for precision irrigation in agriculture. The SWAMP architecture consists of three phases, namely, (1) reserve, (2) distribution and (3) consumption of water. Real time responses are used for adapting irrigation process based on changes in crop conditions.

Suma et al. [136], have developed a smart agricultural application using temperature, moisture and PIR sensor. The information sensed from the sensors are transferred to the microcontroller 16F877A using RS 232. Rawal et al. [137], also have developed a similar application using IoT using another Microcontroller ATMEGA328P with the help of Arduino Uno board. Shekhar et al. [138] have also developed an automated irrigation system using IoT. In the proposed system, the temperature and moisture sensors collect information and sends to the Arduino and the later transmitted to Raspberry Pi3. A comparison of applications listed above is described in Table 1.

11 Open Problems

In the previous sections, we have described a comprehensive study on IoT, covering different aspects such as, applications, technologies, architecture, protocols, security, scalability, energy efficiency, social aspects, etc. Based on this, we have identified some of the research challenges and open issues, which have to be addressed by the future researchers. We summarized them below.

- *Developing Privacy Preserving Security Protocols*: Although in literature, there are many anonymization techniques, which have been proposed for providing privacy and security, most of them consumes resources, such as energy, memory, etc., considerably. So existing IP-based security solutions cannot be directly deployed in IoT applications. Most of the existing techniques as for security solutions uses either public-key (TLS, RSA, ECC, SHA, etc.) or secret –key (AES, DES, etc.) cryptographic techniques. For ensuring authentication, confidentiality, data security, non-repudiation against all types of well-known security attacks, key size defines the upper bound on the security of the technique used. Since, most of the nodes (sensors, etc.) used in IoT applications are having constraints on memory, energy, etc., deploying highly secure technique is a challenging problem to be well addressed by the future researchers.
- *Self-immunity*: Providing self-immunity to the nodes in IoT applications is an important aspect to be considered. Since, the futuristic IoT applications are moving towards providing greater autonomy for the objects (things), they should also be able to perceive

Table 1 Comparison of IoT based applications

Algorithm	Application type	Sensors/boards Used	Protocols used	Performance metric	Remarks
Kodali et al. [134]	Automated water pumps	Soil moisture sensor Esp8266 NodeMCU-12E	MQTT	Moisture value	
Suma et al. [136]	Smart Agriculture	Temerature, Moisture, PIR Sensors, 16F877A microcontroller			
Rawal et al. [137]	Smart irrigation	ATMEGA328P Microcontroller, Arduino uno			
Kamienski et al. [135]	Water management	LoRA	MQTT	Elapsed time metric	
Shekhar et al. [138]	Smart irrigation	Raspberry Pi, Arduino		Moisture sensor data Temperature	K-NN Algorithm
Sobin et al. [70]	Smart transportation	AT89S52 microcontroller Arduino	XBee	Delivery ratio	
Misbahuddin et al. [131]	Smart traffic light control	Raspberry Pi	HTTP		WebIOPI REST API
Miz et al. [132]	Smart traffic light control	M2M communication using sensors			
Pham et al. [133]	Smart parking system	Arduino, RFID		Average waiting time	Cloud computing

and able to react towards the security attacks. Also, an object should be able to protect from physical intrusion or tampering. Consider the example scenario where, sensor nodes deployed in distant or hostile areas, such as battlefields or border areas. In such situations, the sensors are unprotected and may not be able to provide security or other communication support to them because of the other constraints such as unavailability of the resources, difficulty in accessing the locations, etc. In such scenarios, the nodes should have self-immunity to defend from security attacks. So, developing defensive mechanisms to provide self-immunity to the objects in IoT is another challenging task. Examples of some of such defense systems include Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS). Although some of the researchers [20] have initiated efforts for such mechanisms, the area is still open for research.

- *Optimal Energy Utilization*: proper management of energy in IoT devices is another open problem to be addressed. Low-power communications is an important research area since battery replacement process is costly, especially for large scale deployments such as IoT. Though there are much energy efficient solutions at various layers of ISO model, there will be a need to replace batteries from time to time, which is a huge barrier for adoption IoT technology.
- *Efficient Memory Utilization*: Similar to the energy constraints, he nodes used in many of the IoT applications are storage-constrained, efficient utilization of the available storage space (memory) is a challenging task to be addressed. Although there are few buffer management schemes implemented for ad-hoc networks [139, 140], there are so many issues to be addressed.
- *Adopting Emerging Naming and Addressing in IoT*: The naming and addressing aspects used in IoT applications can adopt some of the next generation network architectures, like Named Data Networking (NDN). Instead of using IPv4 or IPv6 addresses in IoT, named data object can be directly used. Some of the researchers [141, 142] have already mentioned incorporating NDN in IoT architecture. Since, Internet is moving towards content-centric architecture further research can be focused this area.
- *Scalability*: As the number of objects being interconnected in IoT is huge in number, a scalability issue arises. Address space should be large enough to accommodate all the devices. The data generated by the vast number of sensors is enormous. Proper information extraction mechanisms must be used in order to extract useful information from the data, and to store data. Service discovery in IoT is difficult since we need to find out the node that provides required service among billions of devices.
- *Behavioral Analysis of Objects in IoT*: Since, in most of the IoT applications, objects are having high degree of autonomy; the analysis of behavior of objects is an important aspect to be considered. As an example, for a WSN based IoT application, the sensor nodes collects the data and forwards to the gateways or any other information management systems. Although most of the nodes participate equally and honestly and cooperates in data forwarding, some may deny cooperating or misbehave to other nodes, or become malicious node, by damaging other nodes. So, proper trust management mechanisms have to be developed as part of any IOT applications to detect the abnormal behavior of objects. Although some of the researchers [143, 144] have worked in this domain, there are still chances for improvements.
- *Finding New Applications of IoT in DTN and CCN*: Since, IoT connects physical devices by giving them sensing, computing and communicating ability. Incorporating delay tolerance to it can add to the communication part of traditional IoT, so that objects can communicate in the scenario of disruption in connectivity. The initial efforts to develop the delay tolerant version of IoT, called as, opportunistic IoT is proposed by

Guo et al. [145], while connecting devices to form infrastructure less networks by using short-term communication techniques such as Bluetooth or WiFi. In such an opportunistic IoT, data dissemination and sharing among devices is formed based on movement and opportunistic contact among humans. Domingo et al. [146], also outlined about applying IoT in underwater networks, *Internet of Underwater Things* (IoUT), which is a network formed by smart underwater objects. Al-Turjman et al. [147], have discussed a delay tolerant approach for integrated RFID sensor networks. Although very few researchers looked in this perspective, designing delay tolerant IoT applications is a promising area of research. Similarly, since, Internet applications are moving towards P2P Content Centric Network (CCN) approaches, investigation of how IoT could fit into such scenario is another challenge for the research community. Performance implications of IoT over ICN are discussed in [148].

- *Unified Architecture*: Although many researchers are still working for developing a unified architecture for IoT, providing a unifying architecture is needed to be compatible with all the current architectures that have been developed till now and to overcome challenges, such as, interoperability, abstracting heterogeneity, etc. In IoT, data must be transmitted to other devices through efficient routing protocols. However, due to the IoT or WSN characteristics of constrained resources and lossy wireless links designing efficient communication protocols is a challenging task.
- *Preventing DoS Attacks*: Securing IoT system from DoS attack is another open issue since in DOS attack system gets slow down because, adversary continuously sends many handshake packets in short duration of time. Current DOS mechanisms are not sufficient to defend against such attacks. Therefore, developing protocols that provide security against DOS attacks is needed.
- *Ability to Handle Massive Amount of Data*: Since, the number of connected devices to Internet are increasing enormously, IoT applications are expected to generate large volumes of data from diverse locations and devices. Also, there are many real-time applications which require analysis on such massive amount of data. So, developing *Big Data* analytic for futuristic IoT applications is a challenging task to be handled by the future researchers [149]. Sensing of big data in IoT and the challenges in big data management are discussed in [150].
- *Quality of Service (QoS)*: Providing QoS metrics for analyzing the network traffic in IoT applications is another research problem to be addressed by the future researchers. Although QoS requirements vary across applications, providing an acceptable service quality to the end users is a challenging task. Also, due to the constraints on bandwidth, and other connectivity issues, ensuring QoS guarantees in IoT applications is an open problem to be addressed.

12 Conclusion

Internet of Things (IoT) paradigm integrates all everyday objects and services into the common network platform. In IoT each object is provided with unique identification and is accessible from the network. It is the process of making physical objects intelligent. A wide range of IoT systems will get benefit from embedded intelligence in things, which helps in optimizing efficiency of environments and in improving quality of human life. In these types of situation there is a need for unifying architecture, protocols, security and privacy. This paper is a comprehensive survey of covering most of the concepts in IoT,

such as, architecture, protocols, security and privacy, scalability and energy efficiency, etc. We have also discussed briefly the most recent research works associated with the concepts mentioned and open issues for the benefit of future researchers.

References

1. http://www.iot-a.eu/public, November 2016.
2. http://www.fp7-aspire.eu/, November 2016.
3. Zhu, Q., Wang, R., Chen, Q., Liu, Y., & Qin, W. (2010). IoT gateway: Bridging wireless sensor networks into internet of things. In *IEEE/IFIP 8th international conference on embedded and ubiquitous computing (EUC)*, 2010 (pp. 347–352).
4. Fan, C., Wen, Z., Wang, F., & Wu, Y. (2011). A Middleware of Internet of things based on Zigbee and RFID. In *IET international conference on Communication Technology and Application (ICCTA)*, 2011 (pp. 732–736).
5. Castellani, A.P., Loreto, S., Bui, N., & Zorzi, M. (2011). Quickly interoperable Internet of Things using simple transparent gateways. In *Position paper in interconnecting smart objects with the internet workshop,* 2011.
6. Chi, Q., Yan, H., Zhang, C., Pang, Z., & Xu, L. D. (2014). A reconfigurable smart sensor interface for industrial WSN in IoT environment. *IEEE Transactions on Industrial Informatics, 2014,* 1417–1425.
7. Valdivieso Caraguay, A. L., Peral, A. B., Barona Lopez, L. I., & Garcia Villalba, L. J. (2014). SDN—Evolution and opportunities in development of IoT application. *International Journal of Distributed Sensor Networks, 10,* 735142.
8. ETSI, V. (2011). Machine-to-machine communications (M2M): Functional architecture. *Int. Telecommun. Union, Geneva, Switzerland, Tech. Rep. TS*, *102*, 690.
9. Atzori, L., Iera, A., & Morabitoc, G. (2010). The internet of things: A survey. *Computer Networks, 54,* 2787–2805.
10. Miorandi, D., Sicari, S., Pellegrini, F. D., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks, 10,* 1497–1516.
11. Xu, L., He, W., & Li, S. (2014). Internet of things in industries: A survey. *IEEE Transactions on Industrial Informatics, 10,* 2233–2243.
12. Singh, D., Tripathi, G., & Jara, A. J. (2014, March). A survey of Internet-of-Things: Future vision, architecture, challenges and services. In *2014 IEEE world forum on Internet of things (WF-IoT)* (pp. 287–292). IEEE.
13. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials, 17*(4), 2347–2376.
14. Dlodlo, N., Foko, T., Mvelase, P., & Mathaba, S. (2012). *The state of affairs in internet of things research*. London: Academic Conferences International Ltd.
15. Stankovic, J. A. (2014). Research directions for the internet of things. *IEEE Internet of Things Journal, 1*(1), 3–9.
16. Chen, X. Y., & Jin, Z. G. (2012). Research on key technology and applications for internet of things. *International Conference on Medical Physics and Biomedical Engineering (ICMPBE), 33,* 561–566.
17. Palattella, M. R., Accettura, N., Vilajosana, X., Watteyne, T., Grieco, L. A., Boggia, G., et al. (2013). Standardized protocol stack for the internet of (important) things. *IEEE Communications Surveys & Tutorials, 15*(3), 1389–1406.
18. Sheng, Z., Yang, S., Yu, Y., Vasilakos, A. V., McCann, J. A., & Leung, K. K. (2013). A survey on the ietf protocol suite for the internet of things: Standards, challenges, and opportunities. *IEEE Wireless Communications, 20*(6), 91–98.
19. Keoh, S., Kumar, S., & Tschofenig, H. (2014). Securing the internet of things: A standardization perspective. *IEEE Internet of Things Journal, 1*(3), 265–275.
20. Riahi, A., Natalizio, E., Challal, Y., Mitton, N., & Iera, A. (2014). A systemic and cognitive approach for IoT security. In *IEEE international conference on computing, networking and communications (ICNC)*, 2014, pp. 183-188.
21. Yan, Z., Zhang, P., & Vasilakos, A. V. (2014). A survey on trust management for Internet of Things. *Journal of Network and Computer Applications, 42,* 120–134.

22. Yang, D. L., Liu, F., & Liang, Y. D. (2010). A Survey of the Internet of Things. In *Proceedings of the 1st international conference on e-business intelligence (ICEBI)*, 2010.
23. Mattern, F., & Floerkemeier, C. (2010). From the internet of computers to the internet of things. In *From active data management to event-based systems and more* (pp. 242–259).
24. Gluhak, A., Krco, S., Nati, M., Pfisterer, D., Mitton, N., & Razafindralambo, T. (2011). A survey on facilities for experimental internet of things research. *IEEE Communications Magazine, 49*(11), 58–67.
25. Whitmore, A., Agarwal, A., & Da Xu, L. (2015). The Internet of Things—A survey of topics and trends. *Information Systems Frontiers, 17*(2), 261–274.
26. Gubbi, J., Buyya, R., Marusic, S., & Palaniswamia, M. (2013). Internet of things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29,* 1645–1660.
27. Bandyopadhyay, S., Sengupta, M., Maiti, S., & Dutta, S. (2011). A survey of middleware for internet of things. *Recent Trends in Wireless and Mobile Networks, 162,* 288–296.
28. Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2014). Context aware computing for the internet of things: A survey. *IEEE Communications Surveys & Tutorials, 16*(1), 414–454.
29. Mainetti, L., Patrono, L., & Vilei, A. (2011, September). Evolution of wireless sensor networks towards the internet of things: A survey. In *2011 19th international conference on software, telecommunications and computer networks (SoftCOM)* (pp. 1–6). IEEE.
30. Aggarwal, C. C., Ashish, N., & Sheth, A. (2013). The internet of things: A survey from the data-centric perspective. In *Managing and mining sensor data* (pp. 383–428). Springer US.
31. Schmid, S., A.Broring, Kramer, D., Kabisch, S., Zappa, A., Lorenz, M., et al. (2016). An architecture for interoperable IoT ecosystems.
32. Ramparany, F., Marquez, F. G., Soriano, J., & Elsaleh, T. (2014 October). Handling smart environment devices, data and services at the semantic level with the FI-WARE core platform. In *Proceedings of IEEE international conference on big data (Big Data)* (pp. 14–20).
33. Soldatos, J., Kefalakis, N., Hauswirth, M., Serrano, M., Calbimonte, J. P., Riahi, M., et al. (2015). Openiot: Open source internet-of-things in the cloud. In *Proceedings of conference on interoperability and open-source solutions for the internet of things* (pp. 13–25). Springer.
34. Yu, J., Lee, N., Pyo, C. S., & Lee, Y. S. (2016). WISE: Web of object architecture on IoT environment for smart home and building energy management. *Journal of Supercomputing, 2016,* 1–16.
35. Datta, S. K., Bonnet, C., & Nikaein, N. (2014 March). An IoT gateway centric architecture to provide novel M2M services. In *Proceedings of IEEE world forum on internet of things (WF-IoT)* (pp. 514–519).
36. Meloni, A., Pegoraro, P. A., Atzori, L., & Sulis, S. (2016, April). An IoT architecture for wide area measurement systems: A virtualized PMU based approach. In *Proceedings of IEEE international energy conference (ENERGYCON)* (pp. 1–6).
37. Ungurean, I., Gaitan, N. C., & Gaitan, V. G. (2014 May). An IoT architecture for things from industrial environment. In *Proceedings of 10th international conference on communications (COMM)* (pp. 1–4).
38. Yashiro, T., Kobayashi, S., Koshizuka, N., & Sakamura, K. (2013, August). An internet of things (IoT) architecture for embedded appliances. In *Proceedings of IEEE Region 10 humanitarian technology conference (R10-HTC)* (pp. 314–319).
39. Pisching, M. A., Junqueira, F., dos Santos Filho, D. J., & Miyagi, P. E. (2016, September). An architecture based on IoT and CPS to organize and locate services. In *Proceedings of IEEE 21st international conference on emerging technologies and factory automation (ETFA)* (pp. 1–4).
40. Datta, S. K., & Coughlin, T. (2016, September). An IoT architecture enabling digital senses. In *Proceedings of IEEE 6th international conference on consumer electronics-Berlin (ICCE-Berlin)* (pp. 67–68).
41. Fremantle, P. (2014). A reference architecture for the internet of things. WSO2 White Paper.
42. Hada, H., & Mitsugi, J. (2011). Epc based internet of things architecture. In *IEEE international conference on RFID technologies and applications (RFID-TA), 2011* (pp. 527–532).
43. http://www.collaberatact.com/overview-architecture-iot-works/, November 2016.
44. Qanbari, S., Behinaein, N., Rahimzadeh, R., & Dustdar, S. (2015, August). Gatica: Linked sensed data enrichment and analytics middleware for IoT gateways. In *Proceedings of 3rd international conference on future internet of things and cloud (FiCloud)* (pp. 38–43).
45. Li-Hong, W., Hai-Kun, T., & Hua, Y. G. (2014, June). Sensors access scheme design based on internet of things gateways. In *Proceedings of fifth international conference on intelligent systems design and engineering applications (ISDEA)* (pp. 901–904).
46. Nastic, S., Truong, H. L., & Dustdar, S. (2015). Sdg-pro: A programming framework for software-defined iot cloud gateways. *Journal of Internet Services and Applications, 6*(1), 21.

47. http://link.springer.com/chapter/10.1007%2F978-3-642-38082-2_14, November 2016.
48. Ning, H., & Wang, Z. (2011). Future Internet of things architecture: Like mankind neural system or social organization framework? *IEEE Communications Letters, 15*(4), 461–463.
49. Kumar, K., Bose, J., & Tripathi, S. (2016, December). A unified web interface for the internet of things. In *Proceedings of IEEE INDICON*.
50. Prehofer, C. (2015, December). Models at REST or modelling RESTful interfaces for the Internet of Things. In *Proceedings of IEEE 2nd world forum on internet of things (WF-IoT)* (pp. 251–255).
51. Abidin, S. A. H. Z., & Ibrahim, S. N. (2015, November). Web-based monitoring of an automated fertigation system: An IoT application. In *Proceedings of IEEE 12th Malaysia international conference on communications (MICC)* (pp. 1–5).
52. Serrano, M., Quoc, H. N. M., Hauswirth, M., Wang, W., Barnaghi, P., & Cousin, P. (2013). Open services for IoT cloud applications in the future internet. *IEEE international symposium on world of wireless, mobile and multimedia networks (WoWMoM), 2013,* 1–6.
53. http://postscapes.com/internet-of-things-protocols, November 2016.
54. https://en.wikipedia.org/wiki/IEEE_802.15.4, November 2016.
55. Ma, X., & Luo, W. (2008, December). The analysis of 6LoWPAN technology. In *Proceedings of IEEE Pacific-Asia workshop on computational intelligence and industrial application, PACIIA'08* (Vol. 1, pp. 963–966).
56. https://openwsn.atlassian.net/wiki/display/OW/IEEE802.15.4e, November 2016.
57. https://en.wikipedia.org/wiki/6LoWPAN, November 2016.
58. http://searchmicroservices.techtarget.com/definition/UDP-User-Datagram-Protocol, November 2016.
59. Dunkels, A. (2002). uIP-A free small TCP/IP stack. Technical report.
60. Ko, J., Terzis, A., Dawson-Haggerty, S., Culler, D. E., Hui, J. W., & Levis, P. (2011). Connecting low-power and lossy networks to the internet. *IEEE Communications Magazine, 49*(4), 96–101.
61. http://coap.technology/, November 2016.
62. https://eclipse.org/community/eclipse_newsletter/2014/february/article2.php, November 2016.
63. http://opendds.org/, November 2016.
64. http://www.deepdarc.com/2013/01/29/introducing-smcp/, November 2016.
65. Perkins, C. E., & Royer, E. M. (1999). Ad hoc on-demand distance vector routing. In *Proceedings of the second IEEE workshop on mobile computing systems and applications (WMCSA)*, 1999 (pp. 90–100).
66. Marina, M. K., & Das, S. R. (2002). Ad hoc on-demand multipath distance vector routing. *ACM SIGMOBILE Mobile Computing and Communications Review, 6*(3), 92–93.
67. Zhu, D., Cui, G., Huang, J., & Zhang, Z. (2013). The research of a new adaptive on-demand routing protocol in WSN. In *Fifth international conference on machine vision (ICMV 12)*, 2013 (pp. 87842B–87842B).
68. Zhou, J., Xu, H., Qin, Z., Peng, Y., & Lei, C. (2013). Ad hoc on-demand multipath distance vector routing protocol based on node state. *Communications and Network, 5,* 408.
69. Machado, K., Rosario, D., Cerqueira, E., Loureiro, A. A., Neto, A., & de Souza, J. N. (2013). A routing protocol based on energy and link quality for internet of things applications. *Sensors, 13*(2), 1942–1964.
70. Sobin, C. C., Raychoudhury, V., & Saha, S. (2017, January). An energy-efficient and buffer-aware routing protocol for opportunistic smart traffic management. In *Proceedings of the 18th ACM international conference on distributed computing and networking* (p. 25).
71. Raheem, A., Lasebae, A., Aiash, M., & Loo, J. (2013). Supporting Communications in the IoTs using the Location/ID Split Protocol. In *IEEE second international conference on future generation communication technology*, 2013 (pp. 143–147).
72. Xia, D. F., & Li, Q. (2013). A routing protocol for congestion control in RFID wireless sensor networks based on stackelberg game with sleep mechanism. In *IEEE 12th international symposium on distributed computing and applications to business, engineering & science (DCABES)*, 2013 (pp. 207–211).
73. Chze, P. L. R., & Leong, K. S. (2014). A secure multi-hop routing for IoT communication. In *IEEE world forum on internet of things (WF-IoT)*, 2014, (pp. 428–432).
74. Xin, H. M., & Yang, K. (2013). A routing protocol for internet of things with high-speed mobile nodes. *International Journal of Advancements in Computing Technology, 5,* 197–205.
75. Tseng, C. H. (2016). Multipath load balancing routing for internet of things. *Journal of Sensors, 2016,* 1–8.

76. Jabbar, W. A., Ismail, M., & Nordin, R. (2013, November). *Evaluation of energy consumption in multipath OLSR routing in Smart City applications*. In *Proceedings ofIEEE Malaysia international conference on communications (MICC)* (pp. 401–406).
77. http://tools.ietf.org/html/rfc6347, November 2016.
78. http://tools.ietf.org/html/draft-moskowitz-hip-dex-01, November 2016.
79. http://tools.ietf.org/html/draft-kivinen-ipsecme-ikev2-minimal-00, November 2016.
80. Choi, J., & Ha, J. (2016, June). Secret key transmission based on channel reciprocity for secure IoT. In *Proceedings of European conference on networks and communications (EuCNC)* (pp. 388–392).
81. Liu, J., Xiao, Y., & Chen, C. P. (2012, June). Authentication and access control in the internet of things. In *Proceedings of 32nd international conference on distributed computing systems workshops (ICDCSW)* (pp. 588–592).
82. Lin, X., Lu, R., Shen, X., Nemoto, Y., & Kato, N. (2009). SAGE: A strong privacy-preserving scheme against global eavesdropping for ehealth systems. *IEEE Journal on Selected Areas in Communications, 27*(4), 365–378.
83. Isa, M. A. M., Mohamed, N. N., Hashim, H., Adnan, S. F. S., Manan, J. A., & Mahmod, R. (2012). A lightweight and secure TFTP protocol for smart environment. In *IEEE symposium on computer applications and industrial electronics (ISCAIE)*, 2012, (pp. 302–306).
84. Kasinathan, P., Pastrone, C., Spirito, M. A., & Vinkovits, M. (2013, October). Denial-of-Service detection in 6LoWPAN based Internet of Things. In *Proceedings of IEEE 9th international conference on wireless and mobile computing, networking and communications (WiMob)* (pp. 600–607).
85. Oliveira, L. M., Rodrigues, J. J., Sousa, A. F., & Lloret, J. (2013). Denial of service mitigation approach for IPv6-enabled smart object networks. *Concurrency and Computation: Practice and Experience, 25*(1), 129–142.
86. Bonetto, R., Bui, N., Lakkundi, V., Olivereau, A., Serbanati, A., & Rossi, M. (2012). Secure communication for smart IoT objects. *IEEE international symposium on world of wireless, mobile and multimedia networks (WoWMoM), 2012,* 1–7.
87. Li, Z., Yin, X., Geng, Z., Zhang, H., Li, P., Sun, Y., et al. (2013). Research on PKI-like protocol for the internet of things. In *IEEE fifth international conference on measuring technology and mechatronics automation (ICMTMA)*, 2013 (pp. 915–918).
88. Pateriya, R. K., & Sharma, S. (2011). An ultralightweight mutual authentication protocol for low Cost RFID tags. *International Journal of Computer Applications, 2011,* 28–35.
89. http://link.springer.com/chapter/10.1007%2F11605805_8#page-1, November 2016.
90. Batina, L., Guajardo, J., Kerins, T., Mentens, N., Tuyls, P., & Verbauwhede, I. (2007). Public-key cryptography for RFID-tags. In *Fifth annual IEEE international conference on pervasive computing and communications workshops*, 2007 (pp. 217–222).
91. Zhang, X., Li, J., Wu, Y., & Zhang, Q. (2011). An ECDLP-based randomized key RFID authentication protocol. In *IEEE international conference on network computing and information security (NCIS)*, 2011 (pp. 146–149).
92. Liao, Y. P., & Hsiao, C. M. (2014). A secure ECC-based RFID authentication scheme integrated with ID verifier transfer protocol. *Ad Hoc Networks, 18,* 133–146.
93. Porambage, P., Schmitt, C., Kumar, P., Gurtov, A., & Ylianttila, M. (2014). Two-phase authentication protocol for wireless sensor networks in distributed IoT applications. In *Proceedings of IEEE 14th international conference on wireless communications and networking (WCNC)*, 2014, (pp. 2770–2775).
94. Palomar, E., Alcaide, A., Molina, E., & Zhang, Y. (2013). Anonymous authentication for privacy-preserving IoT target-driven applications. *Computers & Security, 37,* 111–123.
95. Alcaide, A., Palomar, E., Montero-Castillo, J., & Ribagorda, A. (2013). Anonymous authentication for privacy-preserving IoT target-driven applications. *Computers & Security, 37,* 111–123.
96. Lin, X. J., Sun, L., & Qu, H. (2015). Insecurity of an anonymous authentication for privacy-preserving IoT target-driven applications. *Computers & Security, 48,* 142–149.
97. Bernabe, J. B., Hernández, J. L., Moreno, M. V., & Gomez, A. F. S. (2014, December). Privacy-preserving security framework for a social-aware internet of things. In *Proceedings of international conference on ubiquitous computing and ambient intelligence* (pp. 408–415). Springer.
98. Celdrán, A. H., Clemente, F. J. G., Pérez, M. G., & Pérez, G. M. (2016). SeCoMan: A semantic-aware policy framework for developing privacy-preserving and context-aware smart applications. *IEEE Systems Journal, 10*(3), 1111–1124.
99. Oh, S. W., & Kim, H. S. (2014). Decentralized access permission control using resource oriented architecture for the web of things. In *Proceedings of IEEE 16th international conference on advanced communication technology (ICACT)*, 2014 (pp. 749–753).

100. Giuliano, R., Mazzenga, F., Neri, A., & A.Vegni, M. (2014). Security access protocols in IoT networks with heterogeneous non-IP terminals. In *IEEE international conference on distributed computing in sensor systems (DCOSS)*, 2014, (pp. 257–262).
101. Hummen, R., Heer, T., & Wehrle, K. (2011). A security protocol adaptation layer for the IP-based internet of things. In *Position paper in interconnecting smart objects with the internet workshop, 2011*.
102. Zhao, Y. L. (2013). Research on data security technology in IoT. *Applied Mechanics and Materials, 2013,* 1752–1755.
103. Aljawarneh, S., & Yassein, M. B. (2017). A resource-efficient encryption algorithm for multimedia big data. *Multimedia Tools and Applications, 2017,* 1–22.
104. Liu, C., Zhang, Y., & Zhang, H. (2013). A novel approach to IoT security based on immunology. In *IEEE 9th international conference on computational intelligence and security (CIS), 2013* (pp. 771–775).
105. Gonizzi, P., Ferrari, G., Gay, V., & Leguay, J. (2013). Data dissemination scheme for distributed storage for IoT observation systems at large scale. *Information Fusion, 22,* 16–25.
106. Zhang, B., Mor, N., Kolb, J., Chan, D. S., Lutz, K., Allman, E., et al. (2015, July). The cloud is not enough: Saving IoT from the cloud. In *HotCloud*.
107. Jiang, H., Shen, F., Chen, S., Li, K. C., & Jeong, Y. S. (2015). A secure and scalable storage system for aggregate data in IoT. *Future Generation Computer Systems, 49,* 133–141.
108. Venkatesh, J., Aksanli, B., Chan, C. S., Akyürek, A. S., & Rosing, T. S. (2017). Scalable-application design for the IoT. *IEEE Software, 34*(1), 62–70.
109. Jermyn, J., Jover, R. P., Murynets, I., Istomin, M., & Stolfo, S. (2015, June). Scalability of machine to machine systems and the Internet of Things on LTE mobile networks. In *Proceedings of IEEE 16th international symposium on world of wireless, mobile and multimedia networks (WoWMoM)* (pp. 1–9).
110. Souza, V. B. C., Masip-Bruin, X., Marin-Tordera, E., Ramírez, W., & Sánchez-López, S. (2015, June). Towards the scalability of a service-oriented PCE architecture for IoT scenarios. In *Proceedings of 20th European conference on networks and optical communications-(NOC)* (pp. 1–6).
111. Ray, B. R., Abawajy, J., & Chowdhury, M. (2014). Scalable RFID security framework and protocol supporting Internet of Things. *Computer Networks, 67,* 89–103.
112. An, K., Gokhale, A., Schmidt, D., Tambe, S., Pazandak, P., & Pardo-Castellote, G. (2014). Content-based filtering discovery protocol (CFDP): Scalable and Efficient OMG DDS discovery protocol. In *Proceedings of 8th ACM international conference on distributed event-based systems*, 2014 (pp. 130–141).
113. Kang, J., S. Yin and Meng, W. (2014). An intelligent storage management system based on cloud computing and IoT. In *Proceedings of international conference on computer science and information technology*, 2014, pp. 499-505.
114. Nar, P. C., & Cayirci, E. (2005). PCSMAC: A power controlled sensor-MAC protocol for wireless sensor networks. In *Proceedings of IEEE second European workshop on wireless sensor networks*, 2005 (pp. 81–92).
115. Mota, R. P. B., & Batista, D. M. (2013). A RFID QoS mechanism for IoT tracking applications. In *IEEE international symposium on wireless and pervasive computing (ISWPC)*, 2013 (pp. 1–4).
116. Adame, T., Barrachina, S., Bellalta, B., & Bel, A. (2017). HARE: Supporting efficient uplink multi-hop communications in self-organizing LPWANs. arXiv preprint arXiv: 1701.04673.
117. Liu, X., & Sánchez-Sinencio, E. (2015). An 86% efficiency 12 μw self-sustaining PV energy harvesting system with hysteresis regulation and time-domain MPPT for iot smart nodes. *IEEE Journal of Solid-State Circuits, 50*(6), 1424–1437.
118. Shu, Z., Qian, Y., Yang, Y. L., & Sharif, H. (2016). A game theoretic approach for energy-efficient communications in multi-hop cognitive radio networks. *Wireless Communications and Mobile Computing, 16*(14), 2131–2143.
119. Wei, C., & Li, Y. (2011, September). Design of energy consumption monitoring and energy-saving management system of intelligent building based on the Internet of things. In *Proceedings of international conference on electronics, communications and control (ICECC)* (pp. 3650–3652).
120. Liu, C. H., Fan, J., Branch, J. W., & Leung, K. K. (2014). Toward qoi and energy-efficiency in internet-of-things sensory environments. *IEEE Transactions on Emerging Topics in Computing, 2*(4), 473–487.
121. Yao, R., Wang, W., Baroughi, M. F., Wang, H., & Qian, Y. (2013). Quality-driven energy-neutralized power and relay selection for smart grid wireless multimodal sensor based IoTs. *IEEE Sensors Journal, 13,* 3637–3644.

122. Duan, J., Gao, D., Yang, D., Foh, C. H., & Chen, H. H. (2014). An energy-aware trust derivation scheme with game theoretic approach. *IEEE Internet of Things Journal, 1,* 58–69.
123. Guo, B., Zhang, D., Wang, Z., Yu, Z., & Zhou, X. (2013). Opportunistic IoT: Exploring the harmonious interaction between human and the internet of things. *Journal of Network and Computer Applications, 36,* 1531–1539.
124. 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. *Computer Networks, 56*(16), 3594–3608.
125. Kokoris-Kogias, E., Voutyras, O., & Varvarigou, T. (2016, September). TRM-SIoT: A scalable hybrid trust & reputation model for the social Internet of Things. In *21st International conference on emerging technologies and factory automation (ETFA)* (pp. 1–9).
126. Nitti, M., Girau, R., & Atzori, L. (2014). Trustworthiness management in the social internet of things. *IEEE Transactions on Knowledge and Data Engineering, 26*(5), 1253–1266.
127. Sobin, C. C., Sharma, A., Deepak, S., & Raychoudhary, V. (2015). Socio-physical interaction network (SPIN). In *Proceedings of IEEE international conference on advances in computing, communications and informatics (ICACCI)*, 2015 (pp. 2324–2330).
128. Ning, H., & Liu, H. (2012). Cyber-physical-social based security architecture for future internet of things. *Advances in Internet of Things, 2*(01), 1.
129. Alam, K. M., & El Saddik, A. (2017). C2PS: A digital twin architecture reference model for the cloud-based cyber-physical systems. *IEEE Access*.
130. Ortiz, A. M., Ali, D. H., Park, S., Han, S. N., & Crespi, N. (2014). The cluster between internet of things and social networks: Review and research challenges. *IEEE Internet of Things Journal, 1,* 206–215.
131. Misbahuddin, S., Zubairi, J. A., Saggaf, A., Basuni, J., Sulaiman, A., & Al-Sofi, A. (2015). IoT based dynamic road traffic management for smart cities. In *12th international conference on high-capacity optical networks and enabling/emerging technologies (HONET)* (pp. 1–5).
132. Miz, V., & Hahanov, V. (2016). Smart traffic light in terms of the cognitive road traffic management system (CTMS) based on the Internet of Things. In *Proceedings of IEEE east-west design & test symposium (EWDTS 2014)* (pp. 1–5).
133. Pham, T. N., Tsai, M. F., Nguyen, D. B., Dow, C. R., & Deng, D. J. (2015). A cloud-based smart-parking system based on Internet-of-Things technologies. *IEEE Access, 3,* 1581–1591.
134. Kodali, R. K., & Sarjerao, B. S. (2017). A low cost smart irrigation system using MQTT protocol. In *IEEE region 10 symposium (TENSYMP)* (pp. 1–5).
135. Kamienski, C., Soininen, J. P., Taumberger, M., Dantas, R., Toscano, A., Salmon Cinotti, T., et al. (2019). Smart water management platform: Iot-based precision irrigation for agriculture. *Sensors, 19*(2), 276.
136. Suma, N., Samson, S. R., Saranya, S., Shanmugapriya, G., & Subhashri, R. (2017). IOT based smart agriculture monitoring system. *International Journal on Recent and Innovation Trends in Computing and Communication, 5*(2), 177–181.
137. Rawal, S. (2017). IOT based smart irrigation system. *International Journal of Computer Applications, 159*(8), 7–11.
138. Shekhar, Y., Dagur, E., Mishra, S., & Sankaranarayanan, S. (2017). Intelligent IoT based automated irrigation system. *International Journal of Applied Engineering Research, 12*(18), 7306–7320.
139. Al-Mahdi, H., & Kalil, M. A. (2016). A dynamic hop-aware buffer management scheme for multi-hop ad hoc networks. *IEEE Wireless Communications Letters, 6,* 22–25.
140. Sobin, C. C. (2016). An efficient buffer management policy for DTN. *Procedia Computer Science, 93,* 309–314.
141. Datta, S. K., & Bonnet, C. (2016, May). Integrating named data networking in internet of things architecture. In *Proceedings of IEEE international conference on consumer electronics-Taiwan (ICCE-TW)* (pp. 1–2).
142. Baccelli, E., Mehlis, C., Hahm, O., Schmidt, T C., & Wahlisch, M. (2014, September). Information centric networking in the IoT: Experiments with NDN in the wild. In *Proceedings of the 1st international conference on Information-centric networking* (pp. 77–86).
143. Chen, D., Chang, G., Sun, D., Li, J., Jia, J., & Wang, X. (2011). TRM-IoT: A trust management model based on fuzzy reputation for internet of things. *Computer Science and Information Systems, 8*(4), 1207–1228.
144. Varghese, R., Chithralekha, T., & Kharkongor, C. (2016, March). Self-organized cluster based energy efficient meta trust model for internet of things. In *Proceedings of IEEE international conference on engineering and technology (ICETECH)* (pp. 382–389).

145. Guo, B., Zhang, D., Wang, Z., Yu, Z., & Zhou, X. (2013). Opportunistic IoT: Exploring the harmonious interaction between human and the internet of things. *Journal of Network and Computer Applications, 36*(6), 1531–1539.
146. Domingo, M. C. (2012). An overview of the internet of underwater things. *Journal of Network and Computer Applications, 35*(6), 1879–1890.
147. Al-Turjman, F. M., Al-Fagih, A. E., Alsalih, W. M., & Hassanein, H. S. (2013). A delay-tolerant framework for integrated RSNs in IoT. *Computer Communications, 36*(9), 998–1010.
148. Rao, A., Schelén, O., & Lindgren, A. (2016, October). Performance implications for IoT over information centric networks. In *Proceedings of the eleventh ACM workshop on challenged networks* (pp. 57–62).
149. Mukherjee, A., Paul, H. S., & Dey, S. (2014). ANGELS for distributed analytics in IoT. In *IEEE world forum on internet of things (WF-IoT)*, 2014, (pp. 565–570).
150. Zaslavsky, A., Perera, C., & Georgakopoulos, D. (2013). Sensing as a service and big data. arXiv preprint arXiv: 1301.0159.

C. C. Sobin is currently working as Assistant Professor, Department of CSE, SRM University, Amaravati, Andhra Pradesh, India. He completed Ph.D. in Computer Science and Engineering from Indian Institute of Technology (IIT) Roorkee, India under the guidance of Dr.Vaskar Raychoudhury and completed M.Tech from Department of CSE, Institute of Technology (IIT) Madras under the guidance of Prof. C Pandu Rangan. His research interests are Delay Tolerant Networks (DTNs), Wireless Sensor Networks (WSNs), and Internet of Things (IoT), in which he is currently working on developing efficient routing protocols for DTNs. He is also particularly interested in incorporating delay tolerance in IoT applications.