Chapter 3

IoT Standardization: The Road Ahead

Arpan Pal, Hemant Kumar Rath,
Samar Shailendra and Abhijan Bhattacharyya

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.75137

Abstract

The Internet of Things (IoT) is an emerging area of the modern technology which impacts use cases across governance, education, business, manufacturing, entertainment, transportation, infrastructures, health care, and so on. Creating a generalized framework for the IoT with heterogeneous devices and technology support requires interoperability across products, applications, and services that preclude vendor lock-in. Global standardization of the IoT is the only solution to this. Though standardization efforts in the IoT are not new with many national and international standard bodies working today, there are many open areas to debate and standardize—like reconciling country-specific efforts, empowering local solutions, etc. This chapter brings a holistic view of the existing IoT standards, discusses their interlinking, and enumerates the pain points with possible solutions. It also explains the need for country-specific standardization with the example of an Indian Standard Development Organization (SDO), vis-à-vis global initiatives, as a driver for societal uplifting and economic growth.

Keywords: IoT, standardization, TSDSI, ITU, ETSI, IEEE

1. Introduction

The **Internet of Things** (**IoT**) is the network of "things" or smart devices embedded with sensing, actuation, software, and network connectivity to sense and exchange data among the things, between the things, and with the outside world. The term IoT was coined in 1999 by British technology pioneer Kevin Ashton to describe a system in which objects in the physical world could be connected to the Internet by sensors without requiring human intervention. Though the things were initially thought as machines, today, things are synonymous with any living entity including the human beings, animals, and any other device or element on earth. The "things" should not only be addressable but also reconfigurable, reusable, locatable, uniquely identifiable, and remotely controllable.

Today, the IoT is becoming a growing topic of interest and is becoming a part of our day-to-day life. IoT applications such as remote health monitoring, disease detection and monitoring, crop monitoring, accident prediction and detection, traffic monitoring, robotic rescue operation, environment pollution monitoring, unmanned aerial vehicle (*UAV*)-based rescue operation, and so on, are some of the common applications we witness today [1, 2]. With growing number of applications and devices, the IoT is going to be the dominant technology, where any device can connect with any other device in the world. The IoT integrates ambient sensing, ubiquitous communications, intelligent analytics, and pervasive computing.

The exponential growth of the IoT is mainly attributed to (i) the massive growth of low-cost devices, (ii) advancement of wireless networks, and (iii) creation of new applications. According to a recent survey [3], 50 billion smart devices are estimated to operate by 2020 which can generate avalanche of traffic which is in the order of multiple thousand times of the current Internet traffic. In addition to this, the application requirements are also going to be stringent in terms of latency (~1–100 ms) and reliability (~99.99–99.9999%).

Most of the existing Internet standards did not have the vision to include the IoT which is relatively a newer concept. Therefore, their scope is not sufficient to support the IoT technically and economically. Moreover, IoT architecture, use cases, devices, etc., are still evolving. Today, many IoT devices have been deployed with proprietary protocols. This makes the communication between multiple IoT devices difficult. However, in the era of digital revolution, with many vendors playing in the field, with researchers and entrepreneurs working hard to develop solutions and with government agencies trying hard to reach their citizens, the world has to agree to a common standard. Not only the hardware components related to the IoT, but also the software aspects of the IoT should also be standardized, creating standardized application programming interfaces (APIs) and software services such that future applications can be deployed in a level and uniform environment, thereby enabling easy migration across systems.

Standardization is necessary to ensure (i) interoperability across products, applications, and services that preclude vendor lock-in; (ii) economy of scale, where the three sections of the society—developer (researcher), government (regulator), and the user—get benefited in a reasonable time frame; (iii) security and privacy of the data and the users; (iv) space for the researchers to take our society to another height; and (v) interoperation across physical communication systems, protocol syntax, data semantics, and domain information [2]. Though there is no single body which is responsible for making IoT standards, there are considerable efforts at national and international level, at government level, and at different organizational levels for IoT standardization. Alliances have been formed by many domestic and multinational companies to agree on common standards and technology for the IoT. However, no universal body has been formed yet. While organizations such as IEEE, Internet Engineering Task Force (IETF), ITU-T, OneM2M, 3GPP, etc., are active at international level, Telecommunication Standards Development Society, India (TSDSI), Global ICT Standardization Forum for India (GISFI), Bureau of Indian Standards (BIS), Korean Agency for Technology and Standards (KATS), and so on, are active at national level and European Telecommunications Standards Institute (ETSI) in the regional level for standardization.

This chapter brings a holistic view of the existing IoT standards and their interlinking and enumerates the pain points with possible solutions. It also explains the need for country-specific standardization with the example of an Indian Standard Development Organization (SDO), vis-à-vis global initiatives, as a driver for societal uplifting and economic growth. Section 2 details about the deployment issues of the IoT, whereas Section 3 brings out the standardization effort visible today in both national and international levels. Section 4 discusses the role of local SDOs in IoT standardization. While we discuss the economics of IoT standardization in India in Section 5, we explain the open areas of IoT standardization in Section 6. Finally, we conclude this chapter in Section 7.

2. The IoT framework: Deployment Issues

Though the IoT as a term is relatively new, it is quite old as a concept. The main idea of the IoT is to control and monitor "things" through the computing devices connected over a packet switched network. Today, the IoT has become a new paradigm for the Internet through the confluence of technological advancements and easy availability of devices leading to hitherto unexplored applications. The major technology drives for the IoT are [4]:

- Improvement in connectivity in terms of data rate, availability, and cost
- Wide adoption of Internet Protocol (IP) as the basic addressing mechanism for "things"
- Miniaturization of computing and communication devices along with lowered cost
- Advancement in data analytics
- Rise of cloud computing along with cost reduction in storage systems

Depending on the settings of the exact applications, there can be several patterns of interaction among the heterogeneous entities in an IoT system [1, 5]. In this section, we intend to discuss about communication models used for typical IoT systems and perform a comparative analysis. We then plan to discuss the challenges we face while we use the state-of-the-art solutions for practical deployments.

2.1. Communication models used in the IoT

The IoT is the network of devices which sense, generate, and transmit data to an application server that can be located either in a cloud or in a sophisticated machine. To understand the collected data and to take appropriate action, data analytics are to be used on the application server. For the IoT to become a success, communication between the devices and the application server is the core, and the models used in practice are as follows [6]:

- **Direct communication between devices (D-D):** Under this model, two end devices can directly communicate without using any intermediary as illustrated in **Figure 1(a)**. The devices can connect over a Local/Personal/Wide Area Network (LAN/PAN/WAN).
- **Communication between device and an application server in cloud (D-C):** In this model, the device communicates with an application server in the cloud. If the device is a consumer (that needs some control information to execute some functions), then it receives

the required information from the concerned application in the cloud server. The model is shown in **Figure 1(b)**. A typical example of such communication model is the offering around TCS Connected Universe Platform (TCUP) [7, 8].

- **Communication through the Edge Gateway (D-E-C):** Under this model, the end devices use a local gateway as a conduit to connect to the application server in the cloud as shown **Figure 1(c)**. This deployment has a greater scope of heterogeneity at the users' end and is highly scalable. It is useful when the devices do not use generic protocols to provide the local services but need to communicate with an application server at the cloud with generic protocols (Hypertext Transfer Protocol (HTTP), Constrained Application Protocol (CoAP), etc.) [9]. Cloud service around Microsoft Azure IoT Edge [10] is a very popular example for this kind of exchange model.

2.1.1. Considerations in choosing a communication model

All the models mentioned above accomplish the fundamental objective of exchanging information among "things." With the advent of lightweight protocols like Message Queue Telemetry Transport (MQTT), CoAP [9], etc., which enable web service like transactions in constrained devices, the "things" have become more like the web citizens of the conventional Internet. While the direct communication model helps in quick control and actuation, it suffers from non-scalability, interoperability, and heterogeneity. IoT functionalities are also restricted as no additional service analytics is possible. In the DC model, a typical publish-subscribe or "observe" [9] relationship can achieve one-to-many communication. This provides a possibility of application services based on the analytics/intelligence incorporated in the cloud application. However, in this case, the end devices have to be IP enabled and should use generic standard protocols to remain interoperable.

The communication model through the Edge Gateway provides design flexibilities in terms of scalability, heterogeneity, and interoperability. The edge may itself be equipped with several local intelligence/analytics which may lead to reduction in the amount of network traffic exchanged with the cloud. It enables design decisions like data aggregation at the gateway and traffic optimization while communicating with the cloud with an extra cost due to additional infrastructure at the user premise along with the cloud service. **Figure 2** summarizes the above discussion on several deployment-specific attributes.

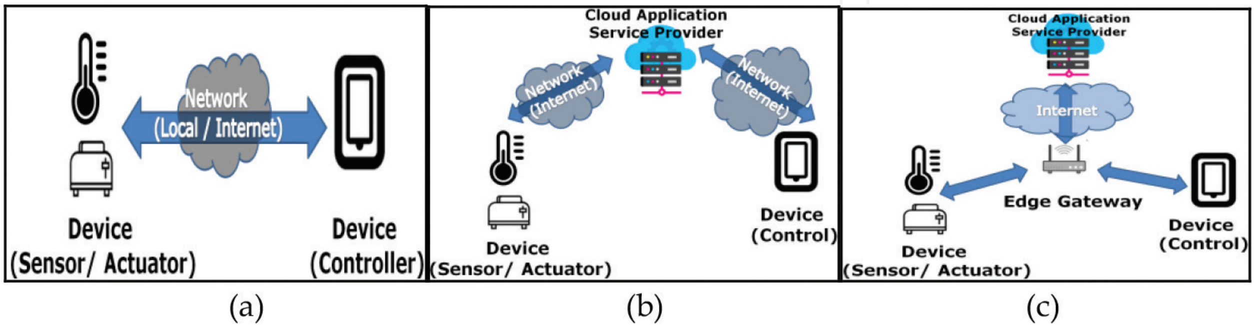
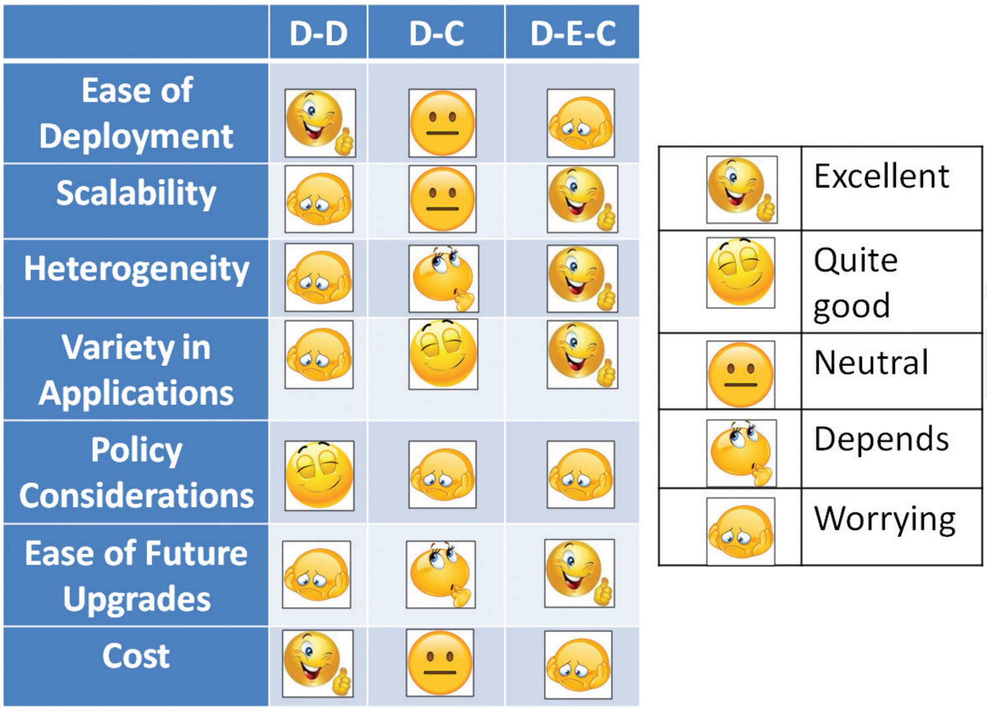


Figure 1. Communication model in the IoT: (a) D-D, (b) D-C, and (c) D-E-C.



	D-D	D-C	D-E-C
Ease of Deployment	😉👍	😐	😟
Scalability	😟	😐	😉👍
Heterogeneity	😟	🤔	😉👍
Variety in Applications	😟	😌	😉👍
Policy Considerations	😌	😟	😟
Ease of Future Upgrades	😟	🤔	😉👍
Cost	😉👍	😐	😟

😉👍	Excellent
😌	Quite good
😐	Neutral
🤔	Depends
😟	Worrying

Figure 2. Attribute-specific considerations for different IoT communication models.

2.2. Challenges: technical, deployment, business, and societal

Taking a thread from our earlier discussion, we now discuss the challenges we face for IoT deployment [5]. We categorize the challenges as follows:

- **Connectivity:** Connecting billions of devices or things is a major challenge. Connectivity impacts the scale of business, profit margin, and societal impact of the operation. Though cloud-based deployments rule the IoT world, edge-based deployments are picking up due to (i) low latency, (ii) ease of deployment, (iii) better security and privacy, and (iv) high data aggregation.
- **Interoperability:** The IoT is growing in various directions, and different technologies are playing different roles. Today, Wireless Fidelity (WiFi), Zigbee, Long-Term Evolution (LTE), LTE Advanced (LTE-A), Low-Power Wide Area Network (LPWAN), Bluetooth, etc., are some of the major communication technologies rule the IoT world. Seamless connectivity with different devices operating in different technologies is a major challenge. Interoperation at higher layers of the network protocol stack involving semantics, and domain-specific operations is another challenge.
- **IoT analytics:** The basic nature of the IoT is to obtain and to act on information. Therefore, IoT analytics play a major role. For practical deployment, placing the analytics platform in the IoT architecture is the major issue. Since information is generated or gathered at the devices and is communicated to the cloud with/without the support of edge, decision has to be taken such that parts of the analytics platform have to be deployed in appropriate places of the framework, i.e. whether at edge/fog or at the cloud. Factors such as delay, regulatory issues, cost, scale and ease of operation, etc., play significant roles on this.

- **Security and privacy:** It has been observed that IoT deployments are prone to security and privacy issues at device, edge, and cloud platform level. Therefore, security and privacy of the data, device, application, and the server are to be considered while deciding appropriate deployment architecture. Instead of considering security and privacy as afterthoughts of deployment, today, these are the prime concerns for any kind of deployment.
- **Business or return on investment (RoI):** Deployment decision can impact the vertical, horizontal, and consumer markets of IoT industry while struggling with the regulatory and legal aspects of the society. Based on the deployment usage and client base, IoT can be divided into (i) consumer IoT, which impacts the mass (like wellness, education, etc.) and the governance in the society; (ii) industrial IoT, which governs the communication framework of Industry 3.0 or Industry 4.0 scenarios; and (iii) commercial IoT, which includes retail and warehouse inventory controls, device tracking, health services, and so on.
- **Societal**: Societal challenges also play a major role in IoT deployment as IoT has to satisfy the customer, developer, and regulator needs of the society. This includes the mode of usage, the energy consumption, environmental impact, societal impact, etc.

Today various industries and academia have proprietary solutions (CISCO, TCS, Microsoft, IBM, etc.) to address some of the above challenges. However, the standard bodies across the world are attempting to collaborate to bring out a unified solution for seamless IoT deployment. The security and privacy which were the afterthoughts for earlier deployments are becoming the front seat candidates.

While the above challenges rule the deployment decision, standardization effort can play a significant role for the above issues. Taking it forward, we now discuss the standardization efforts we see for the IoT in the following sections.

3. Standardization efforts for the IoT

To maintain seamless operation of the IoT, it is essential that the “things” or devices follow a common standard with well-defined protocols and interoperable interfaces. There are several ongoing efforts in different Standard Development Organizations (SDOs) across the world to build standard platforms, protocols, and technologies to ensure seamless operation of these devices. From the perspective of technological offering, different SDOs can be broadly categorized into two classes: (i) generic and (ii) application specific.

In the first category, SDOs such as ITU, IEEE, IETF, 3GPP, and oneM2M, have traditionally performed a pivotal role in defining technology standards to cover the overall problem space. They have specified either policies or generic reference architectures or have offered a standard protocol to carry out the communication. These SDOs also specify technology domain. We shall discuss this later while discussing IETF’s efforts specific to Low-Power Wide Area Network (LPWAN). These SDOs are generally open in a sense that anyone can go through the specifications from these SDOs without being a member of the same. However, to contribute one needs to be a member. IETF is an exception to this. It is indeed open in true sense. In theory, any individual can contribute to IETF standardization, and the contribution is valued in a meritocratic manner.

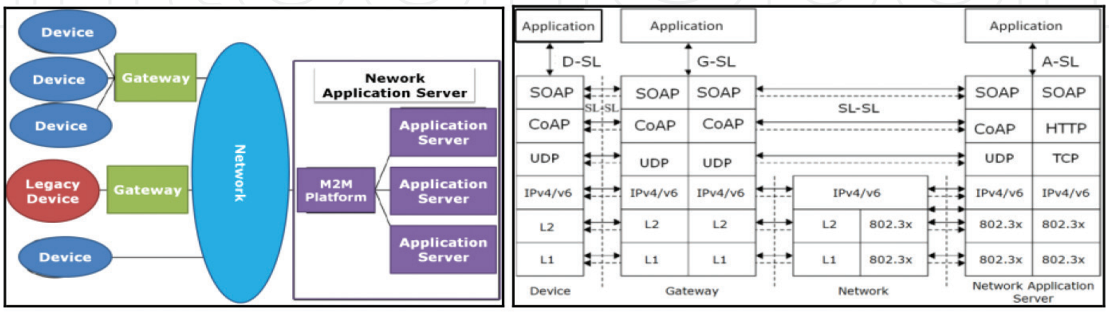
On the other hand, there are SDOs or alliances created in the interest of standardizing technologies for some specific domain of applications. These SDOs fundamentally use the existing architectures and protocol offerings with generic approach to create the communication model. They create specific standards for specific exchange models to fill up typical gaps in the available standard offerings. Fairhair Alliance [11], powered by the THREAD group [12], is one such example. These SDOs are generally closed within its member organizations. We further discuss how IETF plays a pivotal role in becoming the nodal entity for all the SDOs.

3.1. Standardization efforts for overall IoT network stack

3.1.1. IoT standardization with International Telecommunication Union (ITU)

Study Group 20 (SG20) in ITU has been in charge of "IoT and its applications, including smart cities and communities." Some of the topics of the ongoing studies include semantics aspects; big data aspects; detailed requirements of networks supporting IoT applications; accounting and charging aspects; identification, security, and privacy; openness; etc.

ITU has also defined the reference architectures for different applications including smart manufacturing and Industrial IoT, e-health and e-agriculture, wearable device and services, cooperative applications and transportation safety services, monitoring and study of global processes of the earth for disaster preparedness, and so on. **Figure 3(a)** illustrates how ITU defines the component-based reference model for IoT/M2M communication. Devices are networked with or without the help of the gateways, i.e., it is a combination of **D-C** and **D-E-C** architectures explained in Section 2. **Figure 3(b)** shows an exemplary protocol stack of the reference model. It uses the standards created by open SDOs like IETF and IEEE. **Figure 4(a)** and **(b)** show how ITU defines the application-level architectures with two specific examples of e-health protocol stack. The first one follows a local gateway centric architecture. The devices connect directly to the application server in the second example.



(a) (b)

Figure 3. (a) Component and (b) protocol stacks in M2M ref. model [13].

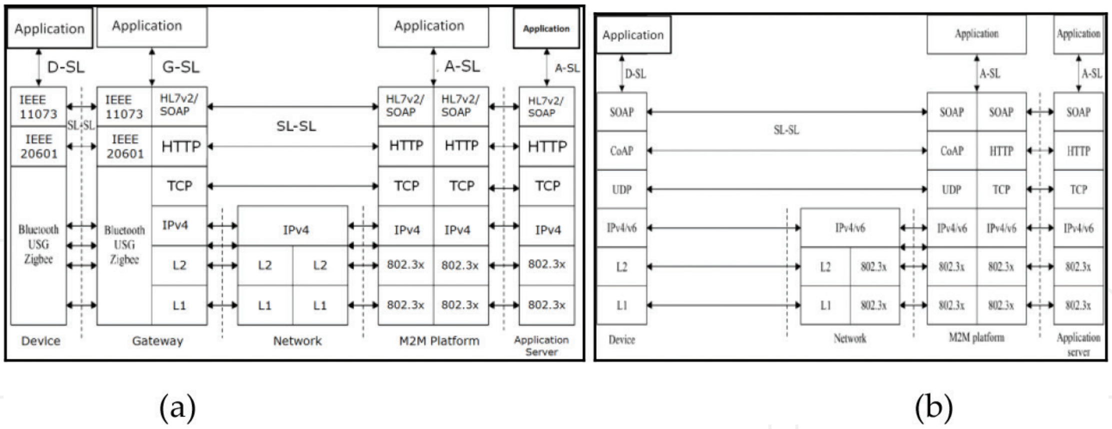


Figure 4. Protocol stacks for e-health (a) with and (b) without gateways [14].

3.1.1.1. Handling IoT deployment challenges

Though ITU has not defined any particular technology for the IoT, it has taken a key role in defining the radio spectrum. Also, as evident from the previous discussions, ITU has provided a reference architecture which can be adopted as a common platform for producing solutions for future smart city and similar IoT applications. That way ITU is taking an important role in ensuring standardization in connectivity and interoperability.

ITU	Current activities	Roadmap	Comments
Connectivity	Defines all the layers and protocols	Spectrum allocation aspects for different future technologies such as 5G	ITU is the nodal point for defining any standard
Interoperability	Ensures interoperability of all standards from all SDOs	IoT framework standardization	
Security and privacy	Based upon the corresponding SDO solutions		

3.1.2. IoT standardization with IEEE

IEEE has been producing standards for local/personal area connectivity while playing a key role in forming the physical and Medium Access Control (MAC) layer standards. It has produced new specifications keeping the typical requirements for IoT applications in mind. The IoT standardization is being undertaken by the IEEE Standards Association (SA) under the project P2413 [14, 15], which aims to come up with an architectural framework that covers the needs for different applications and to provide necessary technological solutions by leveraging the existing body of work as much as possible. IEEE P2413 considers the IoT as a simple three-tier architecture with applications, networking and data communication, and sensing, which are essential for the IoT communication.

Today wireless LAN (IEEE 802.11 family) is still a practical MAC standard for many IoT applications. However, for the low-power operation of constrained devices in IoT applications, IEEE has come up with an access mechanism for personal area network of low-power sensing devices with low rate transmissions. The technology is standardized under IEEE 802.15.4 and termed as LowPAN. It is also made IP compatible through the standardization efforts from IETF. IEEE is putting effort in defining several futuristic technology standards covering the lower layer specifications as well as application layer APIs in the specific domains of Wireless Access in Vehicular Environment (WAVE), short range communication using visible lights, and so on [16].

3.1.2.1. Handling IoT deployment challenges

IEEE is taking an important role in defining the physical and data link layers to ensure low-level interoperability among devices. With IETF collaborations, it ensures compatibility of devices across the Internet. IEEE has been instrumental in standardizing the security, authentication, and authorization mechanisms for the data-link layer.

IEEE	Current activities	Roadmap	Comments
Connectivity	Handles the MAC and physical layer aspects	To ensure interoperability with upcoming technologies for 5G and beyond along with defining technologies for low-latency/tactile Internet	IEEE's primary focus is on the user and application-related standardization
Interoperability	Works with other SDOs		
Security and privacy	Addresses security and authentication issues		
Societal	Addresses various aspects of energy consumption at devices		

3.1.3. IoT standardization with 3GPP

3GPP unites telecommunication SDOs to produce reports and specifications for cellular communication through NarrowBand IoT (NB-IoT) [17–19].

3.1.3.1. NarrowBand IoT (NB-IoT)

In June 2016, 3GPP completed its first set of specification on NarrowBand IoT (NB-IoT). It is a radio standard developed for Low-Power Wide Area Network (LPWAN) to support IoT technologies. NB-IoT is designed for indoor coverage using large number of connected devices with low cost and long battery life. NB-IoT standards are not backward compatible and support three operation modes as illustrated in **Figure 5** and are as follows: (i) In-band operations utilize a resource block within the LTE carrier, (ii) guard band operations utilize the guard band within the LTE carrier, and (iii) standalone operations utilize the bandwidth of 200 kHz traditionally used by Global System for Mobile (GSM) carriers. It targets both LTE and GSM-dominant geographies. In the case of the latter, it uses GSM carrier bands, though it can still continue to have the standard guard band between the GSM carriers. In the case of the former, it uses in-band or in the guard band of LTE carriers. Apart from the physical layer, NB-IoT uses the same protocol stack as that of LTE. NB-IoT targets massive IoT deployments.

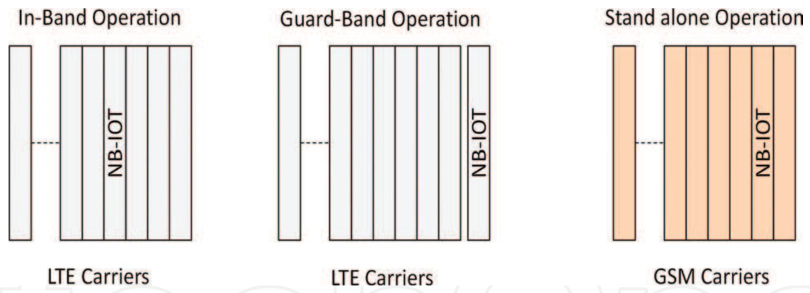


Figure 5. Operation mode of NB-IoT.

However, the nonconformity of NB-IoT standard with LTE standard may pose significant deployment challenges. Some of the salient features of NB-IoT are (i) less operational power consumption, (ii) reduced component cost, (iii) low data rate, and so on.

3.1.3.2. Handling IoT deployment challenges

3GPP's primary focus is low-power small data transfers. The issues of licensing, spectrum, interference, and so on are still need to be resolved.

NB-IoT	Current activities	Roadmap	Comments
Connectivity	MAC and physical layer	Multicasting, mobility, and service continuity enhancements	Low power small data transfer
Interoperability	Backward compatible and interoperable with other standards		
Security and privacy	Handles various aspects of security; privacy still needs to be addressed		
Societal	Low energy consumption for the IoT		

3.1.4. IoT standardization with Internet Engineering Task Force (IETF)

IETF is a leading organization in standardizing protocols for the Internet at different levels of the network stack. It has limited its scope "above the wire and below the application". IETF is a complementing organization to IEEE, 3GPP, and ITU by creating the enabling protocols that actually connect the constrained nodes in a constrained environment in an efficient manner on top of the available physical and data-link layer technologies available from other SDOs working in that area. As evident from **Figure 6**, IETF has IoT-specific protocol offerings for every layer within its purview.

Security consideration is an integral part of any IETF document. IETF uses standardized transport layer security protocols like Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) depending on whether Transport Control Protocol (TCP) or User Datagram Protocol (UDP) is used, respectively. The security mode (pre-shared key, certificate-based security, etc.) needs to be chosen depending on the device and network capability. However,

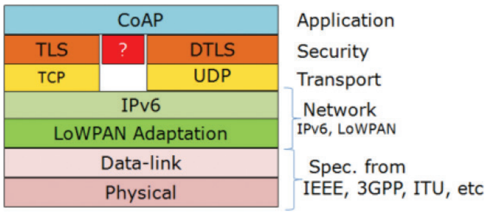


Figure 6. IoT offerings from IETF.

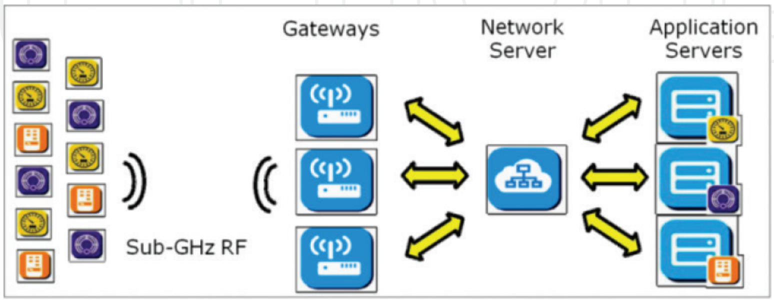


Figure 7. LoRA network topology [22].

security protocol solution optimized for constrained devices is still an open issue as TLS and DTLS are primarily not designed for constrained environments. It is an open area of research, and the question mark in **Figure 6** indicates this. In recent times, IETF has been active in creating specific standards for wide area of technologies for the IoT known as LPWAN. The IPv6 over LPWAN Working Group [20] has been formed to optimize the IETF protocol offerings for the different lower layer offerings on low-power wide area network from SigFox, LoRA [21] Alliance, 3GPP, etc., as well as to define the upper layer exchanges and signaling using the existing protocol offerings. The objective of such initiatives is to tailor the existing IETF offerings in order to cater the specific requirements to enable IP compatibility for specific access technology. LPWAN working group is yet to produce any RFCs. We need to watch out for the progress. **Figure 7** illustrates a representative network topology from LoRA alliance which is a key contributor to LPWAN-specific radio access technologies parallel to NB-IoT from 3GPP.

3.1.4.1. Handling IoT deployment challenges

It is needless to say that IETF is playing a major role in defining the core standards that enable the interoperability and connectivity of billions of devices across the Internet. IETF is the key in defining the security features for future IoT/M2M devices.

3.1.5. IoT standardization with Organization for the Advancement of Structured Information Standard (OASIS)

IBM has developed a pair of protocols called MQTT and MQTT for sensors (MQTT-S) designed to be operated over TCP/IP except some highly real-time low-power MQTT-S mode for local exchange which operates on UDP. The protocol works in publish/subscribe mode and relies on the TCP layer for ensuring reliability and security. MQTT and MQTT-S have been there in practice for quite some time. Few years back IBM brought MQTT/MQTT-S under the umbrella of OASIS open standard community. However, it cannot ignore IETF as the pivotal entity, and there are recent efforts to augment IETF standardization with MQTT considerations [23].

3.1.5.1. Handling IoT deployment challenges

MQTT provides a standardized publish-subscribe mechanism to connect devices. It allows cloud-based architectures to be developed with common protocol semantics and thus helps in interconnectivity. It adopts the available security solutions from IETF to allow a common security feature.

IETF	Current activities	Roadmap	Comments
Connectivity	Specifications for network, transport, and applications	Specify technologies for low-latency real-time Internet communication for the future. Define lightweight security solutions and privacy aware protocols	Handles Internet and core network-related standardization
Interoperability	Ensures the Interoperability with other protocols and applications and technologies		
Security and privacy	Provides security standards. Privacy is not the mainline charter		

3.1.6. IoT standardization with oneM2M

oneM2M was formed in 2012 as a global organization with an objective to consolidate global requirements and create global standards for IoT/M2M technologies. It provides specifications for architecture, APIs, security, and interoperability guidelines and certification for M2M/IoT devices and applications. oneM2M came up with the first formal release of specification in Jan 2015, which were dated by the second release of specifications in the late 2016; the work for the third release of the specification is in progress.

As part of these specifications, it has published service layer architecture for all M2M/IoT devices to interact and exchange data seamlessly. oneM2M specification considers the IoT network layered into three service layers: application, common services, and network service layer. oneM2M provides a service layer specification for M2M services so that they can interoperate

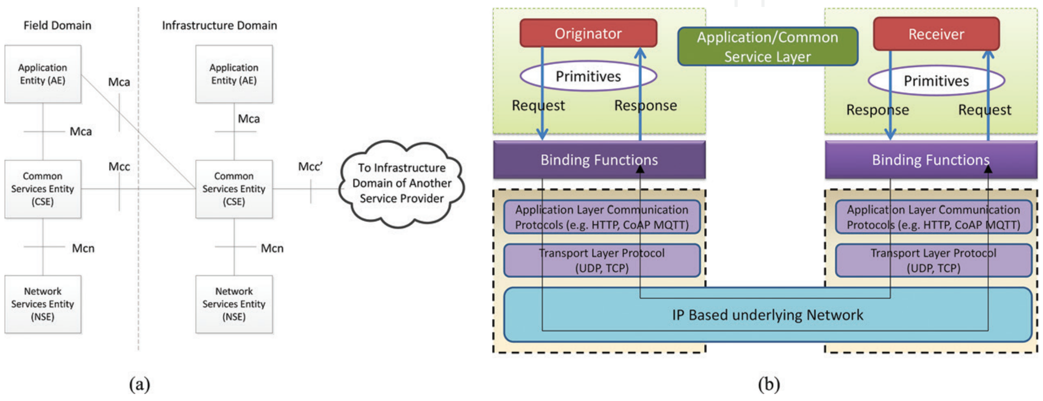

Field Domain
Infrastructure Domain
Application Entity (AE)
Mca
Application Entity (AE)
Mca
Mca
Mcc
Mcc'
Common Services Entity (CSE)
Common Services Entity (CSE)
To Infrastructure Domain of Another Service Provider
Mcn
Mcn
Network Services Entity (NSE)
Network Services Entity (NSE)
(a)
Originator
Application/Common Service Layer
Receiver
Primitives
Primitives
Request
Response
Response
Request
Binding Functions
Binding Functions
Application Layer Communication Protocols (e.g. HTTP, CoAP MQTT)
Application Layer Communication Protocols (e.g. HTTP, CoAP MQTT)
Transport Layer Protocol (UDP, TCP)
Transport Layer Protocol (UDP, TCP)
IP Based underlying Network
(b)

Figure 8. oneM2M (a) functional architecture [24] and (b) communication model [25].

and exchange messages seamlessly. It relies on the service providers' network for message communication. Any primitive of oneM2M service layer can be mapped over IP network or other networks. **Figure 8(a)** represents oneM2M functional architecture, whereas **Figure 8(b)** explains the communication model. The interactions and protocols binding with application protocols like HTTP, CoAP, and MQTT are also being defined by oneM2M specifications.

3.1.6.1. Handling IoT deployment challenges

oneM2M is providing a universal service layer architecture which can ensure the interoperability of various IoT devices. It provides a rich set of guidelines, addressing format, APIs, and bindings with most popular IoT protocols. It also provides mechanism for non-oneM2M devices to operate with oneM2M network. This makes oneM2M a unique platform that provides a unified framework for message exchange through variety of devices and networks. However, this has significant deployment challenges such as handling heterogeneity of devices, geography-specific use cases, and interaction with variety of communication protocols. oneM2M has undertaken some pilots in Korea; the learning from which needs to be incorporated in oneM2M. oneM2M also needs to standardize the security and semantics framework as well before it is widely and ubiquitously deployed. Finally, oneM2M is also discussing on providing an open implementation of its specification which can increase the deployability of oneM2M specifications.

oneM2M	Current activities	Roadmap	Comments
Connectivity	LoRA and NB-IoT at the south side. CoAP, HTTP, and MQTT at the north side	SigFox and any other physical transport. Any other application protocol at the north side	Working with ITU for IoT framework. Many SDOs including TSDSI have also adopted oneM2M as their local standard
Interoperability	Focus on device interoperability	Plan to interoperate with any other service layer specification	
Security and privacy	Provides basic security architecture	Security and privacy aspects are under further development	

3.2. Application-specific efforts

As mentioned earlier, there are alliances and SDOs with a specific task to fill up certain gaps while using the standard offerings for a specific technology. One example is the Fairhair Alliance which is dedicated towards standardizing the technologies for lighting control and building automation [23]. The core technologies and protocols are based on the generic IoT-specific offerings from IETF, IEEE, 3GPP, and so on. Fairhair tries to fill the specific technological gaps (specific security handshakes, typical supports for multicast, exclusive protocol level optimizations, etc.) related to the applications in the concerned business domain. It is being driven by the significant players in the lighting control and home/building automation business domain like Philips, Seimens, etc. Another important participant in this alliance is the "THREAD Group" which is developing standard technologies behind home automation/smart home solutions and is largely driven by Google [12]. **Figure 9(a)** shows the protocol stack for THREAD and the relationship on IETF and IEEE specifications. It uses a mesh topology contrary to the star topology of LoRA. THREAD specification defines a Border Gateway

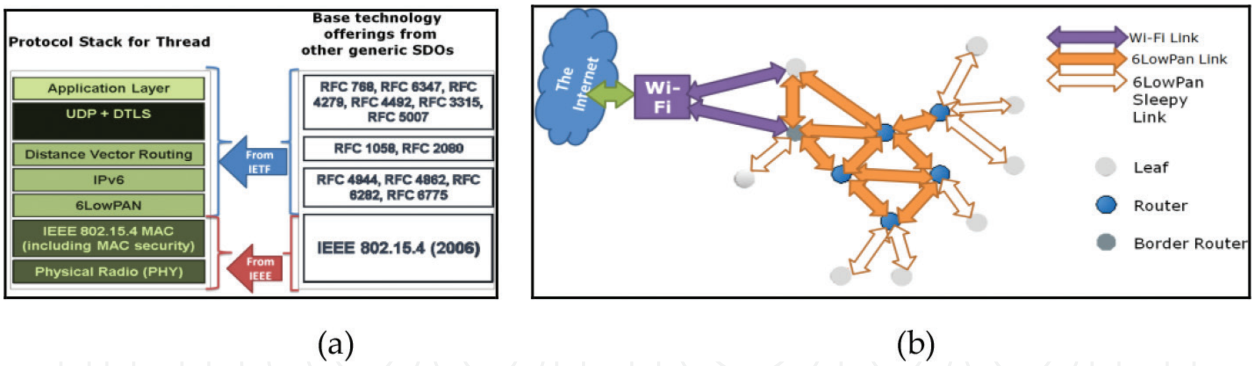


Figure 9. THREAD (a) protocol stack and (b) network topology [12].

entity to maintain connectivity between THREAD and non-THREAD networks. The topology is illustrated in **Figure 9(b)**. It defines the necessary handshakes to establish and maintain secure connection between THREAD and non-THREAD entities [12].

3.2.1. Handling IoT deployment challenges

These alliances are bridging important application-specific gaps for interoperability of edge devices in smart homes.

3.3. IETF as a nodal entity

When the Internet was migrated from a research project to a common communication mechanism to connect computers across the globe, IETF, which has been producing standards for the Internet since 1986, became a pivotal entity. Different modes of telecommunication mechanisms considered the Internet as the conduit to reach peers globally. The offerings from different SDOs started to lean toward more and more IP-centric approach. IETF impacted the activities of the other SDOs as well. The collaboration between IETF and other important SDOs, such as ITU-T and 3GPP are started in the early 1990s. There have been several RFCs describing IETF's relationship with respective SDOs. For example, RFC7241 formulates the modes of collaboration between IETF and IEEE. RFC3113 provides the set of guidelines and principles for collaboration between IETF and 3GPP. RFC6756 does the same for collaboration between IETF and ITU-T. All these guidelines are defined by the Internet Architecture Board (IAB) which acts as an advisory body to the Internet Society (ISOC). With the new paradigm of the IoT, this collaboration approach has even more strengthened. However, as evident from our earlier discussions, the wide variety of IoT applications have given rise to application-specific alliances which have created application-specific standards. While there are specific modalities of operation between IETF and other SDOs, such formal arrangement may not be specified for all the efforts sprawling for different applications. However, all of them have to depend on IETF for the core Internet protocols, and the interaction happens as voluntary efforts from people with common interest in both IETF and the respective alliance/SDO.

Sometimes, the Work Group (WG) charter is enhanced with specific requirements from such SDOs if the sought-after solution has a large enough impact to cover several application

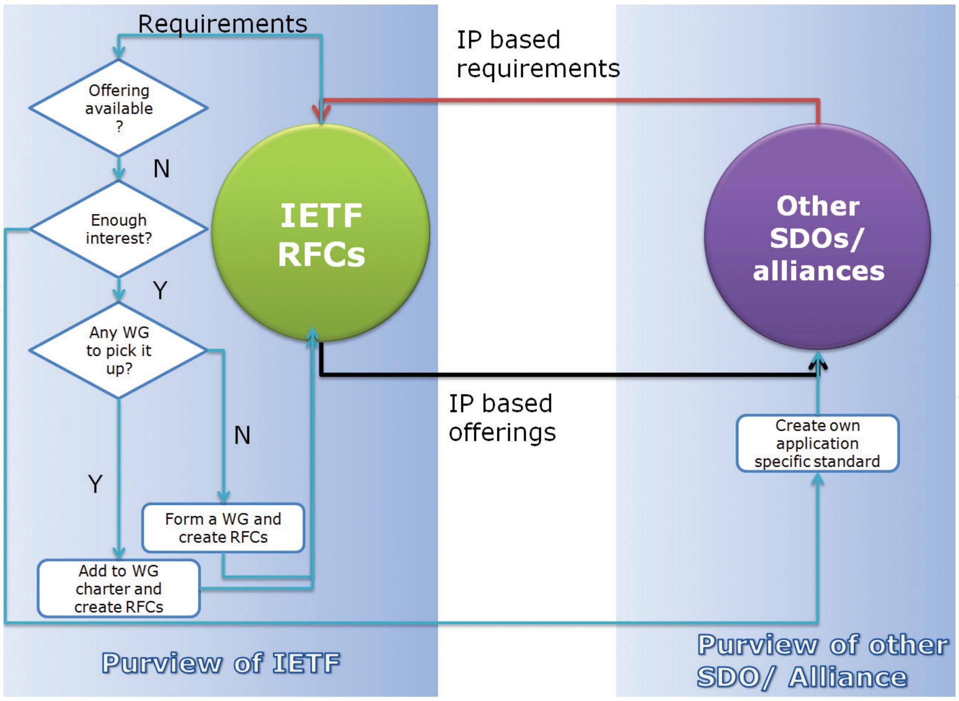


Figure 10. Interaction between IETF and other SDOs/alliances.

domains to justify it as a work item in IETF. Sometimes the interested people in the community form a new WG if the initiative gets a significant support from the communities around IETF. The LPWAN WG is such an example. Sometimes, the individual SDOs create bridging specifications to fill in the required gaps on top of the relevant IETF offerings if the sought-after solution is too application specific. THREAD group and Fairhair Alliance are typical examples for such activities. The interaction can be modeled as shown in **Figure 10**.

4. Role of local SDOs in IoT/M2M standardization

Most of the leading countries such as India, China, Korea, Japan, Europe, the USA, and so on [26–30] have their local SDOs to cater their local needs. While the global SDOs, such as ITU, IETF, and oneM2M, provide a uniform platform for the entire world, many times different geographies have conflicting requirements. Hence, these local SDOs play a major role into the success of IoT/M2M. The local SDOs are expected to adapt to the global recommendations and tailor them suitably to their requirements. Hence these local SDOs should play a dual role; (i) they should be able to provide globally interoperable ecosystem for seamless connectivity; (ii) they should also provide an equal opportunity to their local players, such as start-ups, small-scale industries, and academia, to compete in the local as well as the global IoT/M2M market.

Every country or geography in the world has very different scenarios and problems that need to be solved. Each local SDO focus is to provide requirements and standards to address the unique problems faced in the corresponding geography. However, at the same time, they should ensure that the technology used in providing solution to these use cases is not developed and deployed in isolation creating a risk of isolation of the very deployment from the rest of the IoT/M2M ecosystem.

4.1. India-specific efforts

Being one of the largest democracies in the world, India is expected to be the biggest consumer for the IoT. However, it must be noted that India is a very unique geography unlike the USA and Europe. India has more than 1.3 billion population which is approx. three times of that of the USA and equal to that of China, while the population density is among the highest of the developed countries. Moreover, there is a huge requirement to have affordable and low-cost solutions for any technology to be successful in India. Hence, the IoT use cases for India are also significantly different. This brings India-specific efforts for standardizations.

The economic condition of a developing country like India is very different from Europe or the USA. The economic ecosystem needs a lot of support from local SDOs and the government to create an impact on the IoT standardization. In the absence of that, there is a huge risk of getting obsoleted of local players in the IoT arena. The IoT requires to interoperable globally, and there is potential risk that large companies are likely to drive the entire standardization process, product development for IoT ecosystem. This puts the local manufacturers and start-ups into a great risk. Hence, the local SDOs should provide them an equal opportunity to contribute and adapt to the global standards and make a mark on the face of it.

4.1.1. IoT standardization with TSDSI

Telecommunication Standards Development Society, India (TSDSI) is an Indian SDO formed by the government of India to promote telecom standards in Indian geography. TSDSI is one of the eight organization partners of 3GPP and oneM2M for building cellular and IoT-related standards. TSDSI is an Indian counterpart of other SDOs such as ETSI [31] in Europe and ATIS in the USA. Currently TSDSI has transposed the 3GPP and onem2M specifications as TSDSI technical specifications. TSDSI also represents India in ITU-R and ITU-T for consolidating international efforts in the area of the IoT and telecommunications. TSDSI has studied various verticals important for India and consolidated all these use cases and requirements in technical reports, published in the public domain [32].

TSDSI has contributed to Low Mobility Large Cell (LMLC) standard requirements to ITU-R. LMLC is a very unique requirement of developing geographies like India with large rural populations where a vast majority of people do not even have basic networking infrastructure available. Unlike urban geography, rural areas have relative low mobility; however, they are spread over large geographic area and hence require the larger cells to cover that entire region. The members of TSDSI have provided several other key contributions to 3GPP such as TDD-based scheduling standard in future 5G networks [33].

4.1.1.1. Handling IoT deployment challenges

TSDSI has transposed 3GPP specifications including NB-IoT as TSDSI specifications. TSDSI is also considering transposing and adopting oneM2M specifications as one of the

IoT deployment recommendation. However, there are significant ongoing efforts to study the usefulness of oneM2M specifications and tailor it according to suit Indian subcontinent requirements. Indian companies like TATA Communication are also working on creating one of the largest IoT deployments. However, it is essential that the government of India provides uniform policy to avoid silos of IoT deployment and ensure the interoperability of all the deployments in India within as well as globally.

TSDSI	Current activities	Roadmap	Comments
Connectivity and interoperability	Same as oneM2M and NB-IoT	Planning to include India-specific requirements into NB-IoT and oneM2M	TSDSI is Type 1 organization partner of 3GPP and oneM2M

4.1.2. IoT standardization with GISFI

The Global ICT Standardization Forum for India (GISFI) is an Indian standardization body active in the area of Information and Communication Technology (ICT) and related application areas, such as energy, telemedicine, wireless robotics, and biotechnology. It has been actively involved in defining various use cases related to IoT and defining a generic architecture keeping India-specific requirements into consideration. It has liaison agreements with ITU, ETSI, 3GPP, and other international SDOs in the field of the IoT and 5G communications. The IoT reference architecture under GISFI is explained in [34]. It defines the following layers as a part of its generic architecture: (i) **IoT device layer** includes individual sensors, network-enabled objects, and capillary networks consisting of data sources that are near to the physical environment. (ii) **IoT gateway layer** consists of IoT gateways and connects to the IoT service platform layer through the core network; device and gateway layer functionality can coexist in a single device. (iii) **IoT service platform layer** defines different IoT service abstractions that can be used by multiple applications. (iv) **IoT core network** is envisaged to be predominantly an IP-based network. IP connectivity could be supported over multitudes of telecommunication infrastructures such as DSL, cellular networks (2G, 3G, 4G), and so on.

GISFI also identifies three reference points at the interfaces of these layers as follows: (i) I1, interface from device layer to gateway layer; (ii) I2, interface from gateway layer to service platform layer through IoT core network; and (iii) I3, interface from service platform to layer-specific vertical applications.

4.1.2.1. Handling IoT deployment challenges

GISFI’s aim is to harmonize the standardization effort within the Indian market and work closely with government or regulators, users, network providers, manufacturers, and academia and research communities. GISFI is closely working with telecom operators to decide the communication framework in addition to the frequency of operation and other communication aspects. With a generic IoT architecture proposal, it is ensuring the interoperability aspects to a certain level. IoT security and privacy framework is being framed through a separate work group, and the findings of this group are being updated with the industries and the government. With the definition of new use cases which are India specific in nature, business aspects in addition to societal aspects are also being covered to certain extent. However, the major problems we see with GISFI are as follows: (i) lack of a concrete architecture which is binding to industries and the government and (ii) difficulty in translating the India-specific requirement to standardization.

4.2. Specific challenges for the local SDOs

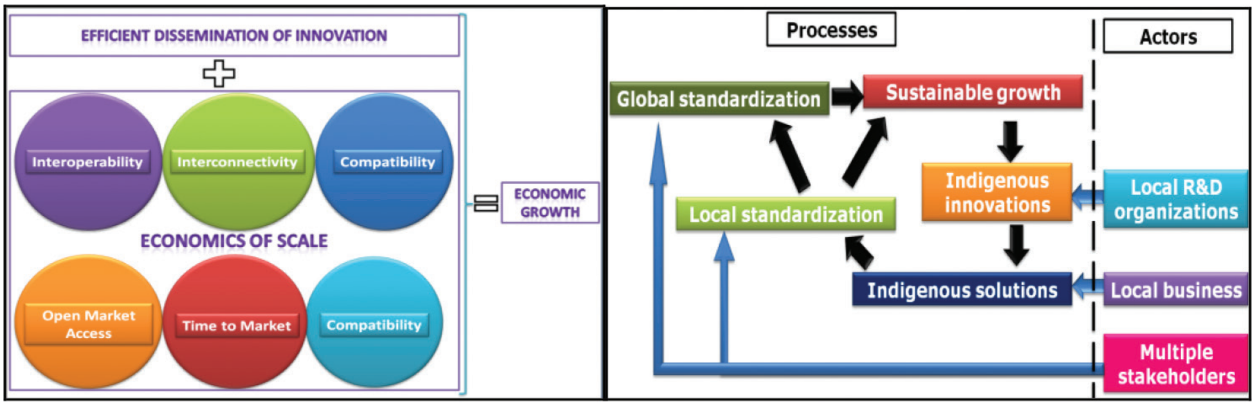
In this section, we discuss the country-specific challenges and analyze from India's perspective. India is a very unique geography in terms of population and population density. This poses unique challenges for any technology to be successful in India. People in India generally use their smart devices for longer duration of time than other parts of the world. Moreover, operators face a tough call on RoI. Therefore, for the benefit of both the parties, i.e., the user community and the operators, SDOs need to emphasize on backward compatibility while creating a new standard or adapting any existing standard. This can help in improving penetration in both rural and urban areas.

Another major concern for India is to promote the use of green and renewable energy. The pollution in India is in an alarming point. Apart from these, healthcare and education are other major areas where IoT can play a major role. The SDOs and government need to work together and build policies to ensure the maximum possible use of green energy keeping environmental issues in consideration and at the same time support various use cases. At the same time, the overall cost of the technology and devices must be kept under check. India has the advantage of the scale which makes it possible for the operators and providers to recover their RoI even with small average revenue per user (ARPU). Indian government should also keep the interest of local start-ups and manufacturers under consideration.

5. Economics of IoT standardization in India

The Internet has become the core of the connectivity among heterogeneous devices across the globe. It is important to create and adhere to global standard implementation of the outcomes of the research for advancing the telecommunication technologies. This helps in overall growth of the economy as standardization helps business through easy interoperability, ensuring interconnectivity, compatibility, quick time to market, etc. Thus, standardization helps the economy of scale which leads to overall economic growth as depicted from **Figure 11(a)**. So far, India has remained as a large consumer of technologies rather than a contributor. The stray contributions have been largely from the Indian counterparts of foreign corporates. India has been deploying the readily available global standards which are not created with India-specific requirements. However, the advent of IoT creates a renewed opportunity for Indian organizations, irrespective of public or private, to take lead in the standardization arena. It is important that at this juncture, India takes up the lead in identifying the problems to solve for a better living.

This can further enable the value chain behind a self-sustaining ecosystem of local indigenous innovations, productizing of the innovation outcomes, and standardization of the same. Though standardization can happen at the local level, it must impact the global SDOs to maintain compatibility at a global level, create a global business value, and also uphold



(a) (b)

Figure 11. (a) Standardization and economic growth and (b) conceptual ecosystem for sustainable growth in India through IoT standardization.

India's requirements in global arena. This ecosystem should get all the stakeholders with common area of interest to complement their national peers with collaborative standardization and finally add to economic growth of the country through indigenous intellectual properties. The expected chain of activities in the conceived ecosystem is depicted in **Figure 11(b)**. It is encouraging to see regional standard bodies like GISFI and TSDSI being formed. Such initiatives create a platform for Indian stakeholders to join hands.

6. Open areas for standardization in the IoT

As we discussed in previous sections, there are multiple ongoing efforts for IoT standardizations. Different standard bodies and various independent alliances are targeting different areas of the IoT ecosystem, e.g., IETF is focusing on Layer 3 to Layer 5 protocols and applications. 3GPP and ITU are focusing on the radio and MAC aspects of the ecosystem. 3GPP has proposed NB-IoT standard in its release-13 for small data transfer for IoT devices. oneM2M is focusing on the service layer aspect of IoT/M2M with a vision that all the M2M devices can interoperate seamlessly. Since IoT is a completely heterogeneous system both in terms of applications and technologies, there are several challenges which need to be addressed before we can have seamlessly deployable IoT ecosystem.

In addition to the standard bodies, Indian and western academia are involved in various state-of-the-art solutions specific to lightweight protocols for IoT data and device security, user and data privacy, green energy along energy harvesting, multimedia multicasting and broadcasting, adaptive coding for multimedia communication, SDNization of application and networks, and so on. The IT service industry is also focusing on the application API standardization for seamless access across heterogeneous device and networks.

Security and privacy: IoT systems are able to gather sensitive data about the consumers, and companies are already using lot of Machine Learning (ML) and Artificial Intelligence (AI) tools to extract information about their consumers for their marketing purposes. Elaborate systems and policies need to be formed to provide guidance about the exposure and use of private information along with the technology enhancement to ensure that such data are not compromised and mishandled by the malicious users.

Interoperability: There are several efforts that are going in parallel to capture the multibillion market of IoT. This has a risk of creating an ecosystem which is fragmented and developed in silos and is not able to interoperate with each other. We should have learning from the way the Internet has been developed, and unlike the fragmented development and patching of the Internet, we should provide elaborate policy guidance to curtail such fragmented development of IoT ecosystem.

Reliability: With the advent of IoT and 5G, society is emerging into an always connected society. The services such as healthcare, education, and connected cars are made available through the technology. This requires that underlying technology and the applications are utmost reliable, i.e., 99.9999% or better reliability is required.

Agility and scalability: The future applications and network need to be both agile and scalable to user demands and operations. Operators must be able to scale up and down dynamically without sacrificing the QoS, security, and reliability. The service providers must be able to deploy applications and services which can adjust themselves to the changing network conditions and use case requirements. Moreover, this all should be possible in a cost-effective way. Hence, it is expected that virtualization of resources and machine learning and AI-based predictions are used. SDNization of network and application can be used to predict the ever-increasing demand of massive data volumes.

IoT is same or more heterogeneous than the Internet is; hence it is not a hyperbole to call the IoT as "network of network of devices." We have witnessed in the past that the Internet has faced tremendous challenges due to unbounded, unplanned, and unregulated growth. This leads to significant inefficiency and underutilization of resources in the Internet deployment. Hence, it is imperative that all deployment of IoT should be well coordinated, supervised, and bound with the proper policy from the government and standards from the SDOs of the world. Such a coordinated effort only is able to ensure that the future deployment is efficient, interoperable, reliable, as well as seamlessly connectable to any other technology.

7. Conclusion

With exponential increase in the number and types of smart devices over the coming years, IoT poses a major challenge for the world in general and regulators in particular. One of the biggest challenges, upon which the eventual success of IoT depends, is the development of interoperable global standards. However, IoT standards today are still wide open—in device, protocol, and software level as there are no existing global validated standardization frameworks. Without enforcement of standards, the value and commercial viability of IoT will have difficulty to reach its full potential.

This chapter has highlighted various ongoing global standardization efforts along with India's contribution to these efforts besides the unique aspects of Indian geography. To make IoT and 5G, the lifeline of IoT networks, successful in India, it is important to identify the right use cases along with the right policies of deployment while keeping the cost of the technology affordable to rural Indian population along with requirement drivers for massively large-scale deployment. This is very different from the other developed geographies like the USA and Europe where only improved quality of experience may be enough for the success of the technology. This requires that India must increase its participation in global standardization process and push India-specific requirements into standard building processes so that the Indian use cases and need of Indian's are addressed. Needless to say, similar standardization efforts in other emerging market economies also need to be synergized at a global level in addition to efforts in the developed economies.

Author details

Arpan Pal, Hemant Kumar Rath*, Samar Shailendra and Abhijan Bhattacharyya

*Address all correspondence to: hemant.rath@tcs.com

Embedded Systems and Robotics, TCS Research and Innovation, India

References

[1] Bandyopadhyay S, Balamuralidhar P, Pal A. Interoperation among IoT standards. Journal of ICT Standardization. 2013;**1**(2):253-270. DOI: 10.13052/jicts2245-800X.12a9

[2] Pal A, Balamuralidhar P. IoT Technical Challenges and Solutions. Artech House; 2016. ISBN-13: 978-1630811112

[3] Ericsson. White paper "More Than 50 billion connected devices". 2011

[4] Rose K, Eldridge S, Chapin L. The Internet of Things: An Overview, Internet Society Document; October 2015

[5] Pal A. Internet-of-Things, making the hype a reality. IT Professional Magazine. IEEE Computer Society. 2015. pp. 2-4. DOI: 10.1109/MITP.2015.36

[6] Tschofenig H et al. Architectural Considerations in Smart Object Networking. Tech. no. RFC 7452. Internet Architecture Board (IAB); Mar. 2015. Available from: https://www.rfc-editor.org/rfc/rfc7452.txt. DOI: 10.17487/RFC7452

[7] Balamuralidhar P, Misra P, Pal A. Software platforms for Internet of Things. Journal of the Indian Institute of Science. 2013;**93**(3):487-498

[8] TCS Connected Universe Platform (TCUP) [Internet]. Available from: https://www.tcs.com/tcs-connected-universe-platform

[9] Hartke K. RFC 7641: Observing Resources in the Constrained Application Protocol (CoAP) [Internet]. September 2015

[10] https://azure.microsoft.com/en-in/services/iot-edge/

[11] The Fairhair Alliance [Internet]. Available from: https://www.fairhair-alliance.org/

[12] Thread Group [Internet]. Available from: https://threadgroup.org/

[13] ITU-T. Overview of application programming interfaces and protocols for the machine-to-machine service layer (Y.4411/Q.3052). February 2016

[14] IEEE Standards Association – Internet of Things [Internet]. Available from: http://standards.ieee.org/innovate/iot/

[15] IEEE-IoT. Towards a definition of the Internet of Things (IoT), revision 1. May 2015

[16] IEEE Standards Association. Internet of Things related standards

[17] LTE Evolved Universal Terrestrial Radio Access (E-UTRA). General Physical Description

[18] An Introduction to NB-IoT. https://www.link-labs.com/blog/overview-of-narrowband-iot

[19] Narrow Band IoT (NB-IoT). https://cdn.rohde-schwarz.com/pws/dl_downloads/dl_application/application_notes/1ma266/1MA266_0e_NB_IoT.pdf

[20] IPv6 over Low Power Wide-Area Networks (lpwan) [Internet]. Available from: https://datatracker.ietf.org/wg/lpwan/about/

[21] LoRa Alliance [Internet]. Available from: https://www.lora-alliance.org/

[22] LoRA Alliance: Technology [Internet]. Available from: https://www.lora-alliance.org/technology

[23] Sengul C, Kirby A, MQTT-TLS profile of ACE [Internet]. January 2017. Available from: https://tools.ietf.org/html/draft-sengul-ace-mqtt-tls-profile-00

[24] TS 0001. oneM2M Functional Architecture. http://www.onem2m.org/images/files/deliverables/Release2/TS-0001-%20Functional_Architecture-V2_10_0.pdf

[25] TS 0004. oneM2M Service Layer Core Protocol. http://www.onem2m.org/images/files/deliverables/Release2/TS-0004_Service_Layer_Core_Protocol_V2_7_1.zip

[26] Telecommunications Technology Association of Korea (South Korea). www.tta.or.kr/English/

[27] Association of Radio Industries and Businesses, Japan. https://www.arib.or.jp/english/

[28] Telecommunication Technology Committee, Japan. www.ttc.or.jp/e/

[29] Alliance for Telecommunications Industry Solutions. USA. www.atis.org/

[30] China Communications Standards Association, China. www.ccsa.org.cn/english/

[31] European Telecommunications Standards Institute. www.etsi.org

[32] Technical Reports and use case documents. http://www.tsdsi.org/main/tr/

[33] 5G India forum. https://coai.com/5g_india_forum

[34] Technical specification—IoT platform. Dec 2013. http://www.gisfi.org/wg_documents/GISFI_IoT_201312438.doc